



Documentation du logiciel SnapCenter

SnapCenter software

NetApp
August 29, 2025

Sommaire

Documentation du logiciel SnapCenter	1
Notes de mise à jour	2
Notes de mise à jour	2
Chemins de mise à niveau pris en charge pour SnapCenter	2
Commencez	3
En savoir plus sur les logiciels SnapCenter	3
Présentation de SnapCenter	3
Fonctions de sécurité de SnapCenter	7
Contrôle d'accès basé sur des rôles dans SnapCenter	9
Reprise après incident dans SnapCenter	14
Licences requises par SnapCenter	15
Synchronisation active SnapMirror dans SnapCenter	18
Concepts clés de la protection des données	19
Systèmes de stockage et applications pris en charge par SnapCenter	21
Méthodes d'authentification pour les informations d'identification SnapCenter	22
Opérations SnapCenter prises en charge pour les systèmes ASA r2	23
Démarrage rapide du logiciel SnapCenter	24
Installer et configurer SnapCenter Server	26
Préparez-vous à installer le serveur SnapCenter	26
Configuration requise pour installer le serveur SnapCenter	26
Inscrivez-vous pour accéder au logiciel SnapCenter	33
Authentification multifacteur (MFA)	34
Installez le serveur SnapCenter	44
Installez le serveur SnapCenter sur l'hôte Windows	44
Installez le serveur SnapCenter sur l'hôte Linux	49
Enregistrer SnapCenter	53
Connectez-vous à SnapCenter à l'aide de l'autorisation RBAC	53
Configurer le serveur SnapCenter	57
Ajouter et provisionner le système de stockage	57
Ajout de licences SnapCenter standard basées sur le contrôleur	78
Configuration de la haute disponibilité	83
Configuration du contrôle d'accès basé sur des rôles (RBAC)	88
Configurer les paramètres du journal d'audit	117
Configurez les connexions MySQL sécurisées avec le serveur SnapCenter	118
Configurer l'authentification basée sur un certificat	124
Activer l'authentification basée sur un certificat	125
Exporter des certificats d'autorité de certification (CA) depuis le serveur SnapCenter	125
Importez le certificat de l'autorité de certification sur les hôtes du plug-in Windows	126
Importez le certificat CA sur les hôtes du plug-in UNIX	126
Exporter les certificats SnapCenter	128
Configurer le certificat CA pour l'hôte Windows	129
Générer le fichier CSR de certificat CA	129
Importer des certificats CA	129

Obtenez le certificat CA imprimé	130
Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows	130
Configuration du certificat d'autorité de certification avec le site SnapCenter	131
Activez les certificats CA pour SnapCenter	132
Configurer le certificat CA pour l'hôte Linux	133
Configurer le certificat nginx	133
Configurer le certificat du journal d'audit	133
Configurer le certificat des services SnapCenter	133
Configurez et activez la communication SSL bidirectionnelle sur l'hôte Windows	134
Configurer la communication SSL bidirectionnelle sur l'hôte Windows	134
Activez la communication SSL bidirectionnelle sur l'hôte Windows	137
Configurez et activez la communication SSL bidirectionnelle sur l'hôte Linux	138
Configurez la communication SSL bidirectionnelle sur l'hôte Linux	138
Activez la communication SSL sur l'hôte Linux	139
Configuration d'Active Directory, LDAP et LDAPS	140
Enregistrer des domaines Active Directory non fiables	140
Configurez les pools d'applications IIS pour activer les autorisations de lecture d'Active Directory	142
Configurer le certificat client CA pour LDAPS	142
Protection des bases de données Microsoft SQL Server	144
Plug-in SnapCenter pour Microsoft SQL Server	144
Présentation du plug-in SnapCenter pour Microsoft SQL Server	144
Quelles sont les possibilités du plug-in SnapCenter pour Microsoft SQL Server	144
Fonctionnalités du plug-in SnapCenter pour Microsoft SQL Server	145
Prise en charge du mappage des LUN asymétriques dans les clusters Windows	146
Types de stockage pris en charge par le plug-in SnapCenter pour Microsoft SQL Server	147
Recommandations relatives à l'organisation du stockage pour le plug-in SnapCenter pour Microsoft SQL Server	150
Privilèges ONTAP minimum requis pour le plug-in SQL	152
Préparation des systèmes de stockage pour la réplication SnapMirror et SnapVault pour le plug-in pour SQL Server	154
Stratégie de sauvegarde des ressources SQL Server	155
Stratégie de restauration pour SQL Server	160
Définissez une stratégie de clonage pour SQL Server	163
Préparez-vous à installer le plug-in SnapCenter pour Microsoft SQL Server	164
Workflow d'installation pour le plug-in SnapCenter pour Microsoft SQL Server	164
Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour Microsoft SQL Server	164
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows	165
Configurer les informations d'identification pour le progiciel de plug-ins SnapCenter pour Windows	166
Configurer les informations d'identification d'une ressource SQL Server individuelle	168
Configurez GMSA sur Windows Server 2016 ou version ultérieure	171
Installez le plug-in SnapCenter pour Microsoft SQL Server	172
Configurer le certificat CA	178
Configurer la reprise après incident	182
Installation du plug-in SnapCenter pour VMware vSphere	184

Déployer le certificat d'autorité de certification	184
Configurez le fichier CRL	184
Préparation à la protection des données	184
Conditions préalables à l'utilisation du plug-in SnapCenter pour Microsoft SQL Server	184
Utilisation des ressources, des groupes de ressources et des stratégies pour la protection de SQL Server	185
Sauvegardez la base de données SQL Server, l'instance ou le groupe de disponibilité	186
Workflow de sauvegarde	186
Déterminer si des ressources sont disponibles pour les sauvegardes	188
Migration des ressources vers un système de stockage NetApp	189
Créer des stratégies de sauvegarde pour les bases de données SQL Server	192
Créez des groupes de ressources et associez des stratégies pour SQL Server	199
Créez des groupes de ressources et activez la protection secondaire des ressources Microsoft SQL Server sur les systèmes ASA r2	202
Conditions requises pour la sauvegarde des ressources SQL	205
Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell	205
Sauvegarde des ressources SQL	207
Sauvegardez les groupes de ressources SQL Server	212
Surveillez les opérations de sauvegarde des ressources SQL dans la page tâches SnapCenter	213
Annulez les opérations de sauvegarde du plug-in SnapCenter pour Microsoft SQL Server	214
Afficher les sauvegardes et clones SQL Server sur la page topologie	215
Nettoyez le nombre de sauvegardes secondaires à l'aide des applets de commande PowerShell	217
Restaurez les ressources SQL Server	218
Restaurer le flux de travail	218
Conditions requises pour restaurer une base de données	218
Restaurez les sauvegardes des bases de données SQL Server	220
Restaurer une base de données SQL Server à partir du stockage secondaire	227
Restaurer des ressources à l'aide des applets de commande PowerShell	228
Réamorçage des bases de données du groupe de disponibilité	230
Surveiller les opérations de restauration des ressources SQL	231
Annuler les opérations de restauration des ressources SQL	232
Clonage des ressources de base de données SQL Server	232
Workflow de clonage	233
Clonage à partir d'une sauvegarde de base de données SQL Server	233
Réaliser le cycle de vie des clones	241
Surveillez les opérations de clonage des bases de données SQL	244
Annuler les opérations de clonage de ressources SQL	244
Séparer un clone	245
Protection des bases de données SAP HANA	247
Plug-in SnapCenter pour bases de données SAP HANA	247
Présentation du plug-in SnapCenter pour les bases de données SAP HANA	247
Comment utiliser le plug-in SnapCenter pour base de données SAP HANA	247
Fonctionnalités du plug-in SnapCenter pour les bases de données SAP HANA	247
Types de stockage pris en charge par le plug-in SnapCenter pour la base de données SAP HANA	248

Privilèges ONTAP minimum requis pour le plug-in SAP HANA	249
Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault pour les bases de données SAP HANA	252
Stratégie de sauvegarde pour les bases de données SAP HANA	252
Stratégie de restauration et de récupération pour les bases de données SAP HANA	256
Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA	258
Workflow d'installation du plug-in SnapCenter pour la base de données SAP HANA	258
Conditions préalables pour l'ajout d'hôtes et l'installation du plug-in SnapCenter pour la base de données SAP HANA	259
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows	262
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux	263
Configurer les identifiants du plug-in SnapCenter pour la base de données SAP HANA	264
Configurez GMSA sur Windows Server 2016 ou version ultérieure	267
Installez le plug-in SnapCenter pour les bases de données SAP HANA	268
Configurer le certificat CA	274
Installation du plug-in SnapCenter pour VMware vSphere	282
Déployer le certificat d'autorité de certification	282
Configurez le fichier CRL	283
Préparation à la protection des données	283
Conditions préalables à l'utilisation du plug-in SnapCenter pour la base de données SAP HANA	283
Mode d'utilisation des ressources, des groupes de ressources et des règles pour la protection des bases de données SAP HANA	283
Sauvegarde des ressources SAP HANA	284
Sauvegarde des ressources SAP HANA	284
Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA ..	285
Découverte des ressources et préparation de conteneurs de bases de données mutualisés pour la protection des données	286
Ajoutez des ressources manuellement au plug-in hôte	289
Créez des règles de sauvegarde pour les bases de données SAP HANA	291
Créer des groupes de ressources et attacher des stratégies	297
Créez des groupes de ressources et activez la protection secondaire des ressources SAP HANA sur les systèmes ASA r2	301
Créer une connexion au système de stockage et une certification à l'aide des applets de commande PowerShell pour la base de données SAP HANA	304
Sauvegarde des bases de données SAP HANA	306
Sauvegarder les groupes de ressources	313
Surveillez les opérations de sauvegarde des bases de données SAP HANA	313
Annuler les opérations de sauvegarde pour SAP HANA	314
Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie	315
Restauration des bases de données SAP HANA	317
Restaurer le flux de travail	317
Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement	318
Restaurez et récupérez une sauvegarde de base de données découverte automatiquement	322
Restaurer des ressources à l'aide des applets de commande PowerShell	327
Surveillez les opérations de restauration des bases de données SAP HANA	329

Clonage des sauvegardes de ressources SAP HANA	330
Workflow de clonage	330
Cloner une sauvegarde de base de données SAP HANA	331
Surveillez les opérations de clonage de bases de données SAP HANA	335
Séparer un clone	336
Supprimez ou séparez les clones de base de données SAP HANA après la mise à niveau de SnapCenter	337
Protection des bases de données Oracle	339
Présentation du plug-in SnapCenter pour la base de données Oracle	339
Quelles sont les possibilités possibles grâce au plug-in pour Oracle Database	339
Fonctionnalités du plug-in pour Oracle Database	339
Types de stockage pris en charge par le plug-in pour Oracle Database	342
Préparation des systèmes de stockage pour la réplication SnapMirror et SnapVault pour le plug-in pour Oracle	344
Privilèges ONTAP minimum requis pour le plug-in pour Oracle	344
Installation du plug-in SnapCenter pour la base de données Oracle	347
Workflow d'installation du plug-in SnapCenter pour Oracle Database	347
Conditions préalables pour l'ajout d'hôtes et l'installation de Plug-ins Package pour Linux ou AIX	347
Ajoutez des hôtes et installez Plug-ins Package pour Linux ou AIX à l'aide de l'interface utilisateur graphique	357
Autres méthodes d'installation de Plug-ins Package pour Linux ou AIX	361
Configurer le service du chargeur enfichable SnapCenter	364
Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux	367
Activez les certificats CA pour les plug-ins	370
Importation des données depuis SnapManager for Oracle et SnapManager for SAP vers SnapCenter	371
Installation du plug-in SnapCenter pour VMware vSphere	377
Déployer le certificat d'autorité de certification	377
Configurez le fichier CRL	377
Préparez-vous à la protection des bases de données Oracle	377
Sauvegarde des bases de données Oracle	379
Présentation de la procédure de sauvegarde	379
Sauvegarder les informations de configuration	380
Conditions requises pour la sauvegarde d'une base de données Oracle	392
Découvrez les bases de données Oracle disponibles pour la sauvegarde	393
Créez des règles de sauvegarde pour les bases de données Oracle	395
Créez des groupes de ressources et associez des stratégies pour les bases de données Oracle	403
Créez des groupes de ressources et activez la protection secondaire des ressources Oracle sur les systèmes ASA r2	405
Sauvegarder les ressources Oracle	408
Sauvegarder les groupes de ressources de la base de données Oracle	411
Surveillez la sauvegarde de la base de données Oracle	412
Autres opérations de sauvegarde	413
Monter et démonter les sauvegardes de base de données	417
Montez une sauvegarde de base de données	418
Démontez une sauvegarde de base de données	419

Restaurez et récupérez les bases de données Oracle	420
Restaurer le flux de travail	420
Définissez une stratégie de restauration et de reprise pour les bases de données Oracle	420
Des variables d'environnement prédéfinies pour restaurer des scripts prescripteurs et PostScript spécifiques	425
Conditions requises pour la restauration d'une base de données Oracle	426
Restaurez et récupérez la base de données Oracle	427
Restauration et restauration d'espaces de stockage à partir d'une restauration instantanée	433
Restaurez et récupérez une base de données enfichable à l'aide d'une récupération ponctuelle	434
Restaurez et récupérez des bases de données Oracle à l'aide des commandes UNIX	437
Surveillez les opérations de restauration des bases de données Oracle	438
Annuler les opérations de restauration de la base de données Oracle	438
Cloner la base de données Oracle	439
Workflow de clonage	439
Définissez une stratégie de clonage pour les bases de données Oracle	440
Variables d'environnement prédéfinies pour le prescripteur et le post-script spécifiques au clone	441
Conditions requises pour le clonage d'une base de données Oracle	443
Cloner une sauvegarde de base de données Oracle	445
Cloner une base de données enfichable	454
Cloner les sauvegardes de bases de données Oracle à l'aide des commandes UNIX	459
Séparer un clone de base de données Oracle	459
Séparer le clone d'une base de données enfichable	460
Surveillez les opérations de clonage de bases de données Oracle	461
Actualiser un clone	462
Supprimer le clone d'une base de données enfichable	463
Gestion des volumes d'applications	463
Que sont les volumes d'applications	463
Ajout de volumes d'application	464
Sauvegarder les volumes d'applications	465
Sauvegarde des volumes des applications clonées	467
Protection des systèmes de fichiers Windows	470
Le plug-in SnapCenter pour Microsoft Windows concepts	470
Présentation du plug-in SnapCenter pour Microsoft Windows	470
Ce que vous pouvez faire avec le plug-in SnapCenter pour Microsoft Windows	470
Le plug-in SnapCenter pour Windows	471
Sauvegarde des systèmes de fichiers Windows par SnapCenter	472
Types de stockage pris en charge par le plug-in SnapCenter pour Microsoft Windows	472
Privilèges ONTAP minimum requis pour le plug-in Windows	475
Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault	477
Définir une stratégie de sauvegarde pour les systèmes de fichiers Windows	478
Sources et destinations des clones pour les systèmes de fichiers Windows	480
Installez le plug-in SnapCenter pour Microsoft Windows	480
Workflow d'installation du plug-in SnapCenter pour Microsoft Windows	480
Conditions d'installation requises pour le plug-in SnapCenter pour Microsoft Windows	481
Ajoutez des hôtes et installez le plug-in SnapCenter pour Microsoft Windows	485

Installation du plug-in SnapCenter pour Microsoft Windows sur plusieurs hôtes distants à l'aide d'applets de commande PowerShell	489
Installez le plug-in SnapCenter pour Microsoft Windows silencieusement à partir de la ligne de commande	489
Contrôler l'état d'installation du module d'extension SnapCenter	491
Configurer le certificat CA	492
Installation du plug-in SnapCenter pour VMware vSphere	495
Déployer le certificat d'autorité de certification	495
Configurez le fichier CRL	495
Sauvegarder les systèmes de fichiers Windows	495
Sauvegarder les systèmes de fichiers Windows	496
Déterminez la disponibilité des ressources pour les systèmes de fichiers Windows	497
Créez des stratégies de sauvegarde pour les systèmes de fichiers Windows	498
Créez des groupes de ressources pour les systèmes de fichiers Windows	501
Créez des groupes de ressources et activez la protection secondaire pour les systèmes de fichiers Windows sur les systèmes ASA r2	504
Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell	506
Sauvegarder une seule ressource à la demande pour les systèmes de fichiers Windows	508
Sauvegarder des groupes de ressources pour les systèmes de fichiers Windows	512
Surveiller les opérations de sauvegarde	513
Annuler les opérations de sauvegarde	514
Afficher les sauvegardes et clones associés sur la page topologie	515
Nettoyez le nombre de sauvegardes secondaires à l'aide des applets de commande PowerShell	517
Restauration des systèmes de fichiers Windows	518
Restaurez les sauvegardes du système de fichiers Windows	518
Restaurer des ressources à l'aide des applets de commande PowerShell	523
Surveiller les opérations de restauration	526
Annuler les opérations de restauration	527
Clonage des systèmes de fichiers Windows	528
Clonage à partir d'une sauvegarde du système de fichiers Windows	528
Surveillance des opérations de clonage	534
Annuler les opérations de clonage	535
Séparer un clone	536
Protection des bases de données Microsoft Exchange Server	538
Concepts du plug-in SnapCenter pour Microsoft Exchange Server	538
Présentation du plug-in SnapCenter pour Microsoft Exchange Server	538
Avantages du plug-in SnapCenter pour Microsoft Exchange Server	539
Types de stockage pris en charge par le plug-in SnapCenter pour Microsoft Windows et pour Microsoft Exchange Server	539
Privilèges ONTAP minimum requis pour le plug-in Exchange	540
Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault	543
Définir une stratégie de sauvegarde pour les ressources Exchange Server	543
Définir une stratégie de restauration pour les bases de données Exchange	546
Installez le plug-in SnapCenter pour Microsoft Exchange Server	547

Workflow d'installation du plug-in SnapCenter pour Microsoft Exchange Server	548
Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour Microsoft Exchange Server	548
Configuration des informations d'identification pour le plug-in SnapCenter pour Windows	552
Configurez GMSA sur Windows Server 2016 ou version ultérieure	553
Ajoutez des hôtes et installez le plug-in pour Exchange	555
Installez le plug-in pour Exchange à partir de l'hôte SnapCenter Server à l'aide des applets de commande PowerShell	561
Installez le plug-in SnapCenter pour l'échange silencieusement à partir de la ligne de commande	562
Contrôler l'état d'installation du module d'extension SnapCenter	563
Configurer le certificat CA	564
Configurez SnapManager 7.x pour Exchange et SnapCenter afin qu'ils coexistent	567
Installation du plug-in SnapCenter pour VMware vSphere	569
Déployer le certificat d'autorité de certification	569
Configurez le fichier CRL	569
Préparation à la protection des données	570
Conditions préalables à l'utilisation du plug-in SnapCenter pour Microsoft Exchange Server	570
Mode d'utilisation des ressources, des groupes de ressources et des stratégies pour la protection d'Exchange Server	571
Sauvegarder les ressources Exchange	572
Workflow de sauvegarde	572
Vérification des sauvegardes et des bases de données Exchange	573
Déterminez si des ressources Exchange sont disponibles pour la sauvegarde	573
Créer des stratégies de sauvegarde pour les bases de données Exchange Server	575
Créer des groupes de ressources et associez des stratégies pour les serveurs Exchange	583
Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell pour Exchange Server	586
Sauvegarde des bases de données Exchange	587
Sauvegardez les groupes de ressources Exchange	593
Surveiller les opérations de sauvegarde	594
Annuler les opérations de sauvegarde pour la base de données Exchange	595
Afficher les sauvegardes Exchange sur la page topologie	596
Restaurer les ressources Exchange	598
Restaurer le flux de travail	598
Conditions requises pour la restauration d'une base de données Exchange	598
Restaurer les bases de données Exchange	599
Restauration granulaire des e-mails et des boîtes aux lettres	604
Restaurer une base de données Exchange Server à partir du stockage secondaire	604
Réamorçage d'un réplica de nœud Exchange passif	605
Réamorçage d'une réplique à l'aide des applets de commande PowerShell pour la base de données Exchange	606
Surveiller les opérations de restauration	606
Annuler les opérations de restauration de la base de données Exchange	607
Protégez IBM DB2	609
Plug-in SnapCenter pour IBM DB2	609

Présentation du plug-in SnapCenter pour IBM DB2	609
Ce que vous pouvez faire avec le plug-in SnapCenter pour IBM DB2	609
Plug-in SnapCenter pour fonctionnalités IBM DB2	610
Types de stockage pris en charge par le plug-in SnapCenter pour IBM DB2	610
Privilèges ONTAP minimum requis pour le plug-in IBM DB2	611
Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour IBM DB2	614
Stratégie de sauvegarde pour IBM DB2	614
Stratégie de restauration et de récupération pour IBM DB2	617
Préparez l'installation du plug-in SnapCenter pour IBM DB2	618
Workflow d'installation du plug-in SnapCenter pour IBM DB2	618
Conditions préalables à l'ajout d'hôtes et à l'installation du module Plug-ins pour Windows, Linux ou AIX	618
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows	624
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux	625
Configurez les informations d'identification du plug-in SnapCenter pour IBM DB2	626
Configurez GMSA sur Windows Server 2016 ou version ultérieure	629
Installez le plug-in SnapCenter pour IBM DB2	630
Configurer le certificat CA	636
Préparation à la protection des données	645
Conditions préalables à l'utilisation du plug-in SnapCenter pour IBM DB2	645
Utilisation des ressources, des groupes de ressources et des stratégies pour protéger IBM DB2	645
Sauvegarder les ressources IBM DB2	646
Sauvegarder les ressources IBM DB2	646
Découvrir les bases de données automatiquement	648
Ajoutez des ressources manuellement au plug-in hôte	648
Créez des stratégies de sauvegarde pour IBM DB2	650
Créer des groupes de ressources et attacher des stratégies	653
Créez des groupes de ressources et activez la protection secondaire des ressources IBM DB2 sur les systèmes ASA r2	657
Créez une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour IBM DB2	660
Sauvegarde des bases de données DB2	661
Sauvegarder les groupes de ressources	668
Surveillez les opérations de sauvegarde IBM DB2	669
Annulez les opérations de sauvegarde pour IBM DB2	670
Affichez les sauvegardes et clones IBM DB2 dans la page topologie	671
Restaurer IBM DB2	673
Restaurer le flux de travail	673
Restaurer une sauvegarde de ressource ajoutée manuellement	673
Restaurer et récupérez une sauvegarde de base de données découverte automatiquement	678
Surveillez les opérations de restauration IBM DB2	680
Clonage des sauvegardes de ressources IBM DB2	680
Workflow de clonage	680
Cloner une sauvegarde IBM DB2	681
Surveillez les opérations de clonage IBM DB2	688

Séparer un clone	689
Supprimez ou divisez les clones de base de données IBM DB2 après la mise à niveau de SnapCenter690	
Protéger PostgreSQL	692
Plug-in SnapCenter pour PostgreSQL	692
Présentation du plug-in SnapCenter pour PostgreSQL	692
Ce que vous pouvez faire à l'aide du plug-in SnapCenter pour PostgreSQL	692
Plug-in SnapCenter pour les fonctionnalités PostgreSQL	692
Types de stockage pris en charge par le plug-in SnapCenter pour PostgreSQL	693
Privilèges ONTAP minimum requis pour le plug-in PostgreSQL	694
Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour PostgreSQL ...	697
Stratégie de sauvegarde pour PostgreSQL	697
Stratégie de restauration et de récupération pour PostgreSQL	700
Préparez l'installation du plug-in SnapCenter pour PostgreSQL	701
Workflow d'installation du plug-in SnapCenter pour PostgreSQL	701
Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour PostgreSQL ...	702
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows ...	705
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux	706
Configurez les informations d'identification du plug-in SnapCenter pour PostgreSQL	707
Configurez GMSA sur Windows Server 2016 ou version ultérieure	710
Installez le plug-in SnapCenter pour PostgreSQL	711
Configurer le certificat CA	717
Préparation à la protection des données	725
Conditions préalables à l'utilisation du plug-in SnapCenter pour PostgreSQL	725
Utilisation des ressources, des groupes de ressources et des règles pour protéger PostgreSQL	726
Sauvegarder les ressources PostgreSQL	726
Sauvegarder les ressources PostgreSQL	726
Découverte automatique des clusters	729
Ajoutez des ressources manuellement au plug-in hôte	729
Créez des règles de sauvegarde pour PostgreSQL	731
Créer des groupes de ressources et attacher des stratégies	735
Créez des groupes de ressources et activez la protection secondaire des ressources PostgreSQL sur les systèmes ASA r2	739
Créez une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour PostgreSQL	742
Sauvegardez PostgreSQL	744
Sauvegarder les groupes de ressources	749
Surveillez les opérations de sauvegarde PostgreSQL	750
Annulez les opérations de sauvegarde pour PostgreSQL	751
Affichez les sauvegardes et clones PostgreSQL dans la page topologie	752
Restaurer PostgreSQL	753
Restaurer le flux de travail	754
Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement	754
Restaurez et récupérez une sauvegarde de cluster découverte automatiquement	758
Restaurer des ressources à l'aide des applets de commande PowerShell	761
Surveillez les opérations de restauration PostgreSQL	763

Cloner les sauvegardes de ressources PostgreSQL	764
Workflow de clonage	764
Cloner une sauvegarde PostgreSQL	765
Surveillez les opérations de clonage PostgreSQL	768
Séparer un clone	769
Supprimez ou répartissez les clones de cluster PostgreSQL après la mise à niveau de SnapCenter ..	770
Protéger MySQL	772
Plug-in SnapCenter pour MySQL	772
Présentation du plug-in SnapCenter pour MySQL	772
Ce que vous pouvez faire en utilisant le plug-in SnapCenter pour MySQL	772
Plug-in SnapCenter pour les fonctionnalités MySQL	772
Types de stockage pris en charge par le plug-in SnapCenter pour MySQL	773
Privilèges ONTAP minimum requis pour le plug-in MySQL	774
Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour MySQL	777
Stratégie de sauvegarde pour MySQL	777
Stratégie de restauration et de récupération pour MySQL	780
Préparez-vous à installer le plug-in SnapCenter pour MySQL	781
Workflow d'installation du plug-in SnapCenter pour MySQL	781
Conditions préalables pour ajouter des hôtes et installer le plug-in SnapCenter pour MySQL	781
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows	785
Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux	786
Configurez les informations d'identification pour le plug-in SnapCenter pour MySQL	787
Installez le plug-in SnapCenter pour MySQL	790
Configurer le certificat CA	795
Préparation à la protection des données	803
Conditions préalables à l'utilisation du plug-in SnapCenter pour MySQL	803
Utilisation des ressources, des groupes de ressources et des stratégies pour protéger MySQL	804
Sauvegarder les ressources MySQL	804
Sauvegarder les ressources MySQL	804
Découvrir les bases de données automatiquement	806
Ajoutez des ressources manuellement au plug-in hôte	806
Créez des stratégies de sauvegarde pour MySQL	807
Créer des groupes de ressources et attacher des stratégies	811
Créer des groupes de ressources et activez la protection secondaire des ressources MySQL sur les systèmes ASA r2	815
Créer une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour MySQL	818
Sauvegardez MySQL	820
Sauvegarder les groupes de ressources	825
Surveillez les opérations de sauvegarde MySQL	826
Annuler les opérations de sauvegarde pour MySQL	827
Afficher les sauvegardes et clones MySQL dans la page topologie	828
Restaurer MySQL	829
Restaurer le flux de travail	830
Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement	830

Restaurez et récupérez une sauvegarde de base de données découverte automatiquement	834
Restaurer des ressources à l'aide des applets de commande PowerShell	836
Surveiller les opérations de restauration MySQL	838
Cloner les sauvegardes de ressources MySQL	839
Workflow de clonage	839
Cloner une sauvegarde MySQL	840
Surveillez les opérations de clonage MySQL	843
Séparer un clone	844
Supprimez ou divisez les clones de base de données MySQL après la mise à niveau de SnapCenter	845
Protégez les applications à l'aide des plug-ins pris en charge par NetApp	847
Plug-ins pris en charge par NetApp	847
Présentation des plug-ins pris en charge par NetApp	847
Avantages des plug-ins pris en charge par NetApp	847
Fonctionnalités des plug-ins pris en charge par NetApp	848
Types de stockage pris en charge par les plug-ins NetApp pris en charge	849
Privilèges ONTAP minimum requis pour le plug-in pris en charge par NetApp	849
Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour les plug-ins pris en charge par NetApp	852
Définir une stratégie de sauvegarde	852
Stratégie de sauvegarde pour les plug-ins pris en charge par NetApp	853
Types de stratégies de restauration prises en charge pour les ressources de plug-in prises en charge par NetApp ajoutées manuellement	854
Préparez l'installation des plug-ins pris en charge par NetApp	854
Workflow d'installation des plug-ins pris en charge par SnapCenter NetApp	854
Conditions préalables à l'ajout d'hôtes et à l'installation du module Plug-ins pour Windows, Linux ou AIX	855
Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows	859
Configuration requise pour l'hôte pour l'installation du pack de plug-ins SnapCenter pour Linux et AIX	860
Configurez les informations d'identification des plug-ins pris en charge par NetApp	861
Configurez GMSA sur Windows Server 2016 ou version ultérieure	863
Installez les plug-ins pris en charge par NetApp	865
Configurer le certificat CA	872
Préparation à la protection des données	880
Conditions préalables à l'utilisation des plug-ins pris en charge par NetApp	880
Utilisation des ressources, des groupes de ressources et des règles pour protéger les ressources des plug-ins pris en charge par NetApp	881
Sauvegarde des ressources des plug-ins pris en charge par NetApp	882
Sauvegarde des ressources des plug-ins pris en charge par NetApp	882
Ajoutez des ressources aux plug-ins NetApp pris en charge	882
Créez des règles pour les ressources des plug-ins pris en charge par NetApp	887
Créer des groupes de ressources et attacher des stratégies	891
Créez des groupes de ressources et activez la protection secondaire des ressources sur les systèmes ASA r2	895
Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell	898

Sauvegarde de ressources individuelles des plug-ins pris en charge par NetApp	899
Sauvegarder les groupes de ressources des plug-ins pris en charge par NetApp	904
Surveillez les opérations de sauvegarde des ressources prises en charge par les plug-ins NetApp	905
Annulez les opérations de sauvegarde pour les plug-ins NetApp pris en charge	906
Consultez la page topologie des plug-ins pris en charge par NetApp, ainsi que les sauvegardes et clones liés aux ressources	907
Restaurer les ressources des plug-ins pris en charge par NetApp	909
Restaurer les ressources de plug-in prises en charge par NetApp	909
Restaurer une sauvegarde de ressource	909
Monitor NetApp prend en charge les opérations de restauration des ressources du plug-in	913
Cloner les sauvegardes de ressources de plug-ins pris en charge par NetApp	914
Cloner les sauvegardes de ressources de plug-ins pris en charge par NetApp	914
Cloner à partir d'une sauvegarde	915
Monitor NetApp prend en charge les opérations de clonage de ressources du plug-in	921
Protégez les systèmes de fichiers Unix	923
Ce que vous pouvez faire avec le plug-in SnapCenter pour les systèmes de fichiers Unix	923
Configurations compatibles	923
Limites	924
Caractéristiques	924
Installez le plug-in SnapCenter pour les systèmes de fichiers Unix	924
Conditions préalables à l'ajout d'hôtes et à l'installation de Plug-ins Package pour Linux	924
Ajoutez des hôtes et installez Plug-ins Package pour Linux à l'aide de l'interface graphique	926
Configurer le service du chargeur enfichable SnapCenter	929
Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux	932
Activez les certificats CA pour les plug-ins	935
Installation du plug-in SnapCenter pour VMware vSphere	936
Déployer le certificat d'autorité de certification	936
Configurez le fichier CRL	936
Préparez-vous à protéger les systèmes de fichiers Unix	936
Sauvegardez les systèmes de fichiers Unix	937
Découvrez les systèmes de fichiers UNIX disponibles pour la sauvegarde	937
Créez des règles de sauvegarde pour les systèmes de fichiers Unix	937
Créez des groupes de ressources et associez des stratégies pour les systèmes de fichiers Unix	941
Créez des groupes de ressources et activez la protection secondaire pour les systèmes de fichiers Unix sur les systèmes ASA r2	943
Sauvegardez les systèmes de fichiers Unix	946
Sauvegardez les groupes de ressources des systèmes de fichiers Unix	947
Surveiller la sauvegarde des systèmes de fichiers Unix	948
Afficher les systèmes de fichiers Unix protégés dans la page topologie	949
Restaurez et restaurez les systèmes de fichiers Unix	952
Restaurer les systèmes de fichiers Unix	952
Surveiller les opérations de restauration des systèmes de fichiers Unix	953
Cloner des systèmes de fichiers Unix	954
Cloner la sauvegarde du système de fichiers Unix	954
Séparer un clone	955

Surveillez les opérations de clonage des systèmes de fichiers Unix	956
Protégez les applications exécutées sur Azure NetApp Files	958
Protégez les applications exécutées sur Azure NetApp Files	958
Limites	958
Installez SnapCenter et créez des informations d'identification	958
Installez SnapCenter sur la machine virtuelle Azure	958
Créez les informations d'identification Azure dans SnapCenter	960
Configuration du compte de stockage Azure	961
Créez les informations d'identification pour ajouter l'hôte du plug-in	961
Protection des bases de données SAP HANA	962
Ajoutez des hôtes et installez le plug-in SnapCenter pour la base de données SAP HANA	962
Ajoutez la base de données SAP HANA	963
Créez des règles de sauvegarde pour les bases de données SAP HANA	964
Créez des groupes de ressources et associez des politiques de sauvegarde SAP HANA	964
Sauvegardez les bases de données SAP HANA s'exécutant sur Azure NetApp Files	965
Sauvegardez les groupes de ressources SAP HANA	966
Restaurez et restaurez les bases de données SAP HANA	967
Clonez la sauvegarde de la base de données SAP HANA	968
Protection des bases de données Microsoft SQL Server	969
Ajoutez des hôtes et installez le plug-in SnapCenter pour la base de données SQL Server	969
Créer des stratégies de sauvegarde pour les bases de données SQL Server	970
Créez des groupes de ressources et associez des stratégies de sauvegarde SQL	971
Sauvegardez les bases de données SQL Server exécutées sur Azure NetApp Files	972
Sauvegardez les groupes de ressources SQL Server	973
Restaurer et restaurer des bases de données SQL Server	974
Cloner la sauvegarde de la base de données SQL Server	975
Protection des bases de données Oracle	977
Ajoutez des hôtes et installez le plug-in SnapCenter pour la base de données Oracle	977
Créez des règles de sauvegarde pour les bases de données Oracle	977
Créez des groupes de ressources et associez des stratégies de sauvegarde Oracle	978
Sauvegarde des bases de données Oracle exécutées sur Azure NetApp Files	979
Sauvegarder les groupes de ressources Oracle	980
Restaurez et récupérez les bases de données Oracle	980
Cloner la sauvegarde de la base de données Oracle	983
Gestion de SnapCenter Server et des plug-ins	987
Voir le tableau de bord	987
Présentation du tableau de bord	987
Comment afficher les informations sur le tableau de bord	991
Rapports d'état des requêtes des travaux à partir du tableau de bord	991
Demander des rapports d'état de protection à partir du tableau de bord	992
Gérer le RBAC	992
Modifier un rôle	992
Modifier les utilisateurs et les groupes	993
Gérer les hôtes	993
Actualiser les informations de la machine virtuelle	995

Modifier les hôtes du plug-in	996
Démarrerez ou redémarrez les services du plug-in	997
Suspendre les planifications pour la maintenance de l'hôte	997
Opérations prises en charge à partir de la page Ressources	998
Gestion des règles	999
Modifier des règles	999
Détacher les polices	1000
Supprimer des règles	1000
Gérer les groupes de ressources	1001
Arrêter et reprendre les opérations sur les groupes de ressources	1001
Supprimer des groupes de ressources	1002
Gérer les sauvegardes	1002
Renommer les sauvegardes	1002
Supprimer les sauvegardes	1003
Déposer la protection	1004
Supprimer les clones	1004
Surveillez les tâches, les plannings, les événements et les journaux	1005
Surveiller les tâches	1005
Surveiller les plannings	1006
Contrôle des événements	1006
Surveiller les journaux	1007
Supprimer les travaux et les journaux de SnapCenter	1008
Présentation des fonctionnalités de reporting SnapCenter	1008
Accédez aux rapports	1010
Filtrez votre rapport	1010
Exporter ou imprimer des rapports	1011
Configurez le serveur SMTP pour les notifications par e-mail	1011
Configurez l'option pour envoyer des rapports par e-mail	1011
Gérer le référentiel du serveur SnapCenter	1012
Conditions préalables à la protection du référentiel SnapCenter	1012
Sauvegarder le référentiel SnapCenter	1012
Afficher les sauvegardes du référentiel SnapCenter	1013
Restaurez le référentiel de base de données SnapCenter	1013
Migrer le référentiel SnapCenter	1014
Réinitialisez le mot de passe du référentiel SnapCenter	1015
Gérer les ressources des domaines non fiables	1015
Modifier les domaines non fiables	1016
Annuler l'inscription des domaines Active Directory non fiables	1016
Gestion du système de stockage	1017
Modifier la configuration du système de stockage	1017
Supprimez le système de stockage	1019
Prise en charge de REST API	1020
Gérer la collecte de données EMS	1020
Arrêter la collecte de données EMS	1021
Démarrer la collecte de données EMS	1021

Modifier la planification de la collecte de données EMS et le SVM cible	1021
Surveiller l'état de la collecte de données EMS	1021
Mise à niveau de SnapCenter Server et des plug-ins	1023
Configurer SnapCenter pour vérifier les mises à jour disponibles	1023
Mise à niveau du workflow	1023
Chemins de mise à niveau pris en charge	1023
Mettez à niveau le serveur SnapCenter sur l'hôte Windows	1024
Mettez à niveau le serveur SnapCenter sur un hôte Linux	1026
Mettez à niveau vos modules d'extension	1027
Mise à jour technologique	1030
Mise à jour technologique de l'hôte du serveur SnapCenter	1030
Mise à jour technologique d'un nœud dans un cluster F5	1031
Mise hors service de l'ancien hôte du serveur SnapCenter	1031
Restauration vers l'ancien hôte du serveur SnapCenter	1031
Reprise après incident	1031
Mise à jour technologique des hôtes du plug-in SnapCenter	1033
Mise à jour technologique du système de stockage	1036
Mettre à jour les sauvegardes du stockage primaire	1036
Mettre à jour les sauvegardes du stockage secondaire	1038
Désinstaller SnapCenter Server et les plug-ins	1040
Désinstallez les modules du plug-in SnapCenter	1040
Conditions préalables à la suppression d'un hôte	1040
Supprimer un hôte	1041
Désinstallez les plug-ins à l'aide de l'interface graphique de SnapCenter	1042
Désinstallez les plug-ins Windows à l'aide de l'applet de commande PowerShell	1043
Désinstallez les plug-ins localement sur un hôte	1043
Désinstallez le package de plug-ins pour Linux ou AIX à l'aide de l'interface de ligne de commande	1044
Désinstallez le serveur SnapCenter sur l'hôte Windows	1044
Désinstallez le serveur SnapCenter sur l'hôte Linux	1045
Automatisez à l'aide d'API REST	1046
Automatisation SnapCenter via les API REST	1046
Comment accéder de manière native à l'API REST de SnapCenter	1046
Base de services Web REST	1046
Ressources et représentation d'état	1046
Terminaux URI	1047
Messages HTTP	1047
Formatage JSON	1047
Caractéristiques opérationnelles de base	1047
Transaction d'API de demande et de réponse	1047
Prise en charge des opérations CRUD	1047
Identifiants d'objets	1048
Instances et collections d'objets	1048
Opérations synchrones et asynchrones	1048
Sécurité	1048
Variables d'entrée contrôlant une requête API	1049

Méthodes HTTP	1049
En-têtes de demande	1049
Corps de la demande	1050
Filtrage d'objets	1050
Demande de champs d'objet spécifiques	1050
Tri des objets dans le jeu de sortie	1051
Pagination lors de la récupération d'objets dans une collection	1051
Propriétés de taille	1052
Interprétation d'une réponse API	1052
Code d'état HTTP	1052
En-têtes de réponse	1053
Corps de réponse	1053
Erreurs	1054
API REST prises en charge pour SnapCenter Server et les plug-ins	1055
Auth	1055
Domaines	1055
Emplois	1055
Paramètres	1055
Hôtes	1056
Ressources	1056
Sauvegardes	1058
Clones	1058
Répartition des clones	1058
Groupes de ressources	1058
Stratégies	1059
Stockage	1059
Partagez	1059
Plug-ins	1060
Rapports	1061
Alertes	1061
RBAC	1061
Configuration	1061
CertificateSettings	1062
Référentiel	1062
Version	1062
Comment accéder aux API REST à l'aide de la page Web de l'API swagger	1062
Commencez avec l'API REST	1063
Bonjour tout le monde	1063
Mentions légales	1064
Droits d'auteur	1064
Marques déposées	1064
Brevets	1064
Politique de confidentialité	1064
Source ouverte	1064

Documentation du logiciel SnapCenter

Notes de mise à jour

Notes de mise à jour

Découvrez les nouvelles fonctionnalités et les améliorations disponibles dans SnapCenter 6.1.

Pour obtenir la liste complète des nouvelles fonctionnalités et améliorations, reportez-vous à "[Nouveautés de SnapCenter 6.1](#)" la section .

Pour plus d'informations sur les problèmes connus, les limitations, les problèmes résolus et les commandes nouvelles et modifiées, reportez-vous au "[Notes de version du logiciel SnapCenter 6.1](#)". Vous devez vous connecter avec votre compte NetApp ou créer un compte pour accéder aux notes de version.

Chemins de mise à niveau pris en charge pour SnapCenter

Le chemin de mise à niveau vous permet de savoir à partir de quelles versions antérieures de SnapCenter vous pouvez mettre à niveau vers les dernières versions de SnapCenter et quelles versions des plug-ins sont prises en charge.

Si vous utilisez la version du serveur SnapCenter...	Vous pouvez directement mettre à niveau SnapCenter Server vers...	Versions de plug-in prises en charge
5.0	6,0	<ul style="list-style-type: none">• 5,0• 6,0
	6.0.1	<ul style="list-style-type: none">• 6.0.1
	6,1	<ul style="list-style-type: none">• 6,1
6,0	6.0.1	<ul style="list-style-type: none">• 6,0• 6.0.1
	6,1	<ul style="list-style-type: none">• 6,1
6.0.1	6,1	<ul style="list-style-type: none">• 6.0.1• 6,1

Pour plus d'informations sur la mise à niveau du plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Mettez à niveau le plug-in SnapCenter pour VMware vSphere](#)".

Commencez

En savoir plus sur les logiciels SnapCenter

Présentation de SnapCenter

Le SnapCenter software est une plate-forme simple, centralisée et évolutive pour une protection des données cohérente avec les applications. Il protège les applications, les bases de données, les systèmes de fichiers hôtes et les machines virtuelles sur les systèmes ONTAP dans le cloud hybride.

SnapCenter utilise les technologies NetApp Snapshot, SnapRestore, FlexClone, SnapMirror et SnapVault pour fournir :

- Des sauvegardes sur disque rapides, compactes et cohérentes au niveau des applications
- Restauration rapide et détaillée et récupération cohérente avec les applications
- Un clonage rapide et compact

SnapCenter inclut SnapCenter Server et des plug-ins légers. Vous pouvez automatiser le déploiement de plug-ins sur des hôtes d'applications distants, planifier des opérations de sauvegarde, de vérification et de clonage, et surveiller les opérations de protection des données.

Vous pouvez installer SnapCenter sur site ou sur un cloud public pour protéger les données.

- Sur site pour protéger les éléments suivants :
 - Les données qui résident dans les systèmes primaires ONTAP FAS, AFF ou ASA et qui sont répliquées vers les systèmes secondaires ONTAP FAS, AFF ou ASA
 - Les données qui résident dans les systèmes primaires ONTAP Select
 - Les données qui se trouvent sur les systèmes primaires et secondaires ONTAP FAS, AFF ou ASA et qui sont protégées pour le stockage objet local StorageGRID
 - Les données qui se trouvent sur les systèmes principaux et secondaires ONTAP ASA r2
- Sur site dans un cloud hybride pour protéger les éléments suivants :
 - Les données qui résident dans les systèmes primaires ONTAP FAS, AFF ou ASA et qui sont répliquées vers Cloud Volumes ONTAP
 - Les données qui se trouvent sur les systèmes primaires et secondaires ONTAP FAS, AFF ou ASA et qui sont protégées pour le stockage objet et d'archivage dans le cloud (via l'intégration de la sauvegarde et de la restauration BlueXP)
- Dans un cloud public, pour protéger :
 - Les données qui résident dans les systèmes primaires Cloud Volumes ONTAP (anciennement ONTAP Cloud)
 - Données qui se trouvent sur Amazon FSX pour ONTAP
 - Les données qui se trouvent sur un système Azure NetApp Files primaire (Oracle, Microsoft SQL et SAP HANA)

Fonctionnalités clés

SnapCenter offre les principales fonctionnalités suivantes :

- Protection des données centralisée et cohérente au niveau des applications de différentes applications

La protection des données est prise en charge pour les bases de données Microsoft Exchange Server, Microsoft SQL Server, Oracle sous Linux ou AIX, SAP HANA Database, IBM DB2, PostgreSQL, MySQL et Windows Host Filesystem exécutées sur des systèmes ONTAP. SnapCenter prend également en charge la protection d'applications telles que MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Sauvegardes basées sur des règles

Les sauvegardes basées sur des politiques exploitent la technologie NetApp Snapshot pour créer des sauvegardes sur disque rapides, économes en espace et cohérentes avec les applications. Vous pouvez également configurer la protection automatique de ces sauvegardes sur un stockage secondaire en mettant à jour les relations de protection existantes.

- Sauvegardes pour plusieurs ressources

Vous pouvez sauvegarder plusieurs ressources (applications, bases de données ou systèmes de fichiers hôtes) du même type à la fois à l'aide des groupes de ressources SnapCenter .

- Restauration et reprise

SnapCenter offre des restaurations rapides et granulaires de sauvegardes et de restaurations basées sur le temps et cohérentes avec les applications. Vous pouvez restaurer les données depuis n'importe quelle destination dans le cloud hybride.

- Clonage

SnapCenter permet un clonage rapide, peu encombrant et cohérent avec les applications. Vous pouvez cloner sur n'importe quelle destination dans le Cloud hybride.

- Interface utilisateur graphique de gestion mono-utilisateur

SnapCenter fournit une interface unique pour gérer les sauvegardes et les clones dans n'importe quelle destination de cloud hybride.

- API REST, applets de commande Windows, commandes UNIX

SnapCenter fournit des API REST pour la plupart des fonctionnalités pour l'intégration avec n'importe quel logiciel d'orchestration et l'utilisation des cmdlets Windows PowerShell et de l'interface de ligne de commandes.

- Tableau de bord et reporting centralisés pour la protection des données

- Contrôle d'accès basé sur des rôles (RBAC) pour la sécurité et la délégation

- Une base de données de référentiel intégrée haute disponibilité pour stocker toutes les métadonnées de sauvegarde

- Installation automatisée des plug-ins

- Haute disponibilité

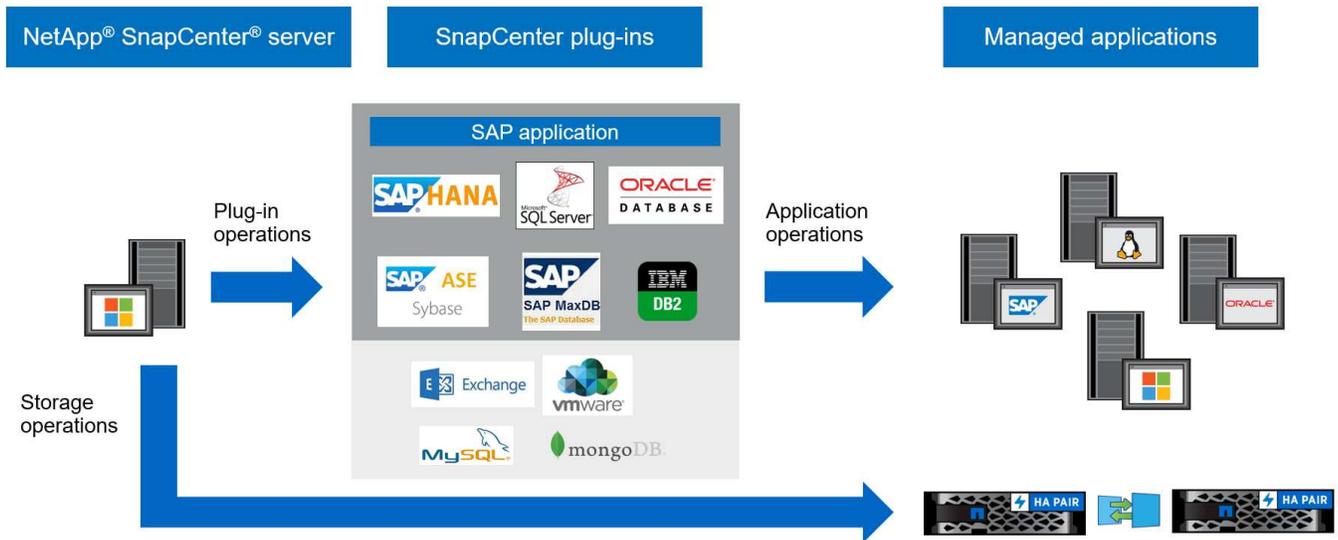
- Reprise après incident

- SnapLock "[En savoir plus](#)"

- Synchronisation active SnapMirror (initialement lancée sous la forme SnapMirror Business Continuity [SM-BC])
- La mise en miroir synchrone "En savoir plus"

Architecture et composants de SnapCenter

SnapCenter utilise une conception en couches avec un serveur de gestion central et des hôtes de plug-in. Le serveur et les hôtes du plug-in peuvent se trouver à des emplacements différents.



SnapCenter inclut le serveur SnapCenter, le package de plug-in SnapCenter pour Windows et le package de plug-in SnapCenter pour Linux. Chaque package contient des plug-ins pour divers composants d'infrastructure et d'applications.

Serveur SnapCenter

Le serveur SnapCenter prend en charge les systèmes d'exploitation Microsoft Windows et Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Le serveur SnapCenter comprend un serveur Web, une interface utilisateur HTML5 centralisée, des applets de commande PowerShell, des API REST et le référentiel SnapCenter.

SnapCenter stocke les informations sur ses opérations dans le référentiel SnapCenter .

Plug-ins SnapCenter

Chaque plug-in SnapCenter prend en charge des environnements, des bases de données et des applications spécifiques.

Nom du plug-in	Inclus dans le package d'installation	Requiert d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour Microsoft SQL Server	Package de plug-ins pour Windows	Plug-in pour Windows	Hôte SQL Server	Répertoires de base
Plug-in SnapCenter pour Windows	Package de plug-ins pour Windows		Hôte Windows	Répertoires de base

Nom du plug-in	Inclus dans le package d'installation	Requiert d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour Microsoft Exchange Server	Package de plug-ins pour Windows	Plug-in pour Windows	Hôte Exchange Server	Répertoires de base
Plug-in SnapCenter pour Oracle Database	Package de plug-ins pour Linux et package de plug-ins pour AIX	Plug-in pour UNIX	Hôte Oracle	Linux ou AIX
Plug-in SnapCenter pour base de données SAP HANA	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte client HDBSQL	Linux ou Windows
Plug-in SnapCenter pour IBM DB2	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte DB2	Linux, AIX ou Windows
Plug-in SnapCenter pour PostgreSQL	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte PostgreSQL	Linux ou Windows
Plug-in SnapCenter pour MySQL	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte MySQL	Linux ou Windows
Plug-in SnapCenter pour MongoDB	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte MongoDB	Linux ou Windows
Plug-in SnapCenter pour ORASCPM (applications Oracle)	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte Oracle	Linux ou Windows
Plug-in SnapCenter pour SAP ASE	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte SAP	Linux ou Windows

Nom du plug-in	Inclus dans le package d'installation	Requiert d'autres plug-ins	Installé sur l'hôte	Plateforme prise en charge
Plug-in SnapCenter pour SAP MaxDB	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte SAP MaxDB	Linux ou Windows
Plug-in SnapCenter pour le plug-in de stockage	Package de plug-ins pour Linux et package de plug-ins pour Windows	Plug-in pour UNIX ou plug-in pour Windows	Hôte de stockage	Linux ou Windows

Le SnapCenter Plug-in for VMware vSphere prend en charge les opérations de sauvegarde et de restauration cohérentes en cas de panne et cohérentes avec les machines virtuelles (VM), les banques de données et les disques de machines virtuelles (VMDK). Il prend également en charge les opérations de sauvegarde et de restauration cohérentes avec les applications pour les bases de données et les systèmes de fichiers virtualisés.

Pour protéger les bases de données, les systèmes de fichiers, les machines virtuelles ou les banques de données sur les machines virtuelles, déployez le SnapCenter Plug-in for VMware vSphere . Pour plus d'informations, reportez-vous à "[Documentation du plug-in SnapCenter pour VMware vSphere](#)" .

Référentiel SnapCenter

Le référentiel SnapCenter, parfois appelé base de données NSM, stocke des informations et des métadonnées pour chaque opération SnapCenter.

L'installation de SnapCenter Server installe la base de données du référentiel MySQL Server par défaut. Si vous avez déjà installé MySQL Server et que vous souhaitez effectuer une nouvelle installation de SnapCenter Server, vous devez désinstaller MySQL Server.

SnapCenter prend en charge MySQL Server 8.0.37 ou version ultérieure comme base de données de référentiel SnapCenter . Si vous utilisez une version antérieure de MySQL Server avec une version antérieure de SnapCenter, le processus de mise à niveau de SnapCenter met à niveau MySQL Server vers la version 8.0.37 ou ultérieure.

Le référentiel SnapCenter stocke les informations et métadonnées suivantes :

- Sauvegarde, clonage, restauration et vérification des métadonnées
- Informations sur les rapports, les tâches et les événements
- Informations sur l'hôte et les plug-ins
- Informations sur le rôle, l'utilisateur et les autorisations
- Informations de connexion du système de stockage

Fonctions de sécurité de SnapCenter

SnapCenter utilise des fonctionnalités de sécurité et d'authentification strictes pour sécuriser vos données.

SnapCenter comprend les fonctions de sécurité suivantes :

- Toutes les communications avec SnapCenter utilisent HTTP over SSL (HTTPS).
- Toutes les identifiants de SnapCenter sont protégés à l'aide d'un chiffrement AES (Advanced Encryption Standard).
- Prend en charge les algorithmes de sécurité conformes à la norme FIPS (Federal Information Processing Standard).
- Prend en charge l'utilisation des certificats CA autorisés fournis par le client.
- Prend en charge TLS 1.3 (transport Layer Security) pour la communication avec ONTAP. Vous pouvez également utiliser TLS 1.2 pour la communication entre les clients et les serveurs.
- Prend en charge un certain ensemble de suites de chiffrement SSL pour assurer la sécurité des communications réseau. ["En savoir plus >>"](#).
- SnapCenter est installé à l'intérieur du pare-feu de votre entreprise pour permettre l'accès au serveur SnapCenter et permettre la communication entre le serveur SnapCenter et les plug-ins.
- L'accès en opération et l'API SnapCenter utilise des jetons chiffrés avec un chiffrement AES, qui expire au bout de 24 heures.
- SnapCenter s'intègre à Windows Active Directory pour la connexion et le contrôle d'accès basé sur des rôles (RBAC) qui régissent les autorisations d'accès.
- IPsec est pris en charge avec SnapCenter sur ONTAP pour les machines hôtes Windows et Linux. ["En savoir plus >>"](#).
- Les applets de commande SnapCenter PowerShell sont sécurisés pour la session.
- Après une période d'inactivité par défaut de 15 minutes, SnapCenter vous avertit que vous serez déconnecté dans 5 minutes.

Au bout de 20 minutes d'inactivité, SnapCenter vous déconnecte et vous devez vous reconnecter. Vous pouvez modifier la période de déconnexion.

- La connexion est temporairement désactivée après 5 tentatives de connexion incorrectes.
- Prend en charge l'authentification de certificat d'autorité de certification entre le serveur SnapCenter et ONTAP. ["En savoir plus >>"](#).
- Le vérificateur d'intégrité est ajouté au serveur SnapCenter et aux plug-ins et il valide tous les binaires expédiés pendant les nouvelles opérations d'installation et de mise à niveau.

Présentation du certificat CA

Le programme d'installation du serveur SnapCenter active la prise en charge centralisée du certificat SSL pendant l'installation. Pour améliorer la communication sécurisée entre le serveur et le plug-in, SnapCenter prend en charge l'utilisation des certificats d'autorité de certification autorisés fournis par le client.

Vous devez déployer des certificats d'autorité de certification après avoir installé le serveur SnapCenter et les plug-ins correspondants. Pour plus d'informations, voir ["Générer le fichier CSR de certificat CA"](#).

Vous pouvez également déployer le certificat d'autorité de certification pour le plug-in SnapCenter pour VMware vSphere. Pour plus d'informations, voir ["Créer et importer des certificats"](#).

Communication SSL bidirectionnelle

La communication SSL bidirectionnelle sécurise la communication mutuelle entre le serveur SnapCenter et les plug-ins.

Présentation de l'authentification basée sur certificat

L'authentification basée sur certificat vérifie l'authenticité des utilisateurs qui tentent d'accéder à l'hôte du plug-in SnapCenter. L'utilisateur doit exporter le certificat du serveur SnapCenter sans clé privée et l'importer dans le magasin de confiance hôte du plug-in. L'authentification basée sur certificat fonctionne uniquement si la fonction SSL bidirectionnelle est activée.

Authentification multifacteur (MFA)

L'authentification multifacteur fait appel à un fournisseur d'identité tiers via le langage SAML pour gérer les sessions utilisateur. Cette fonctionnalité améliore la sécurité de l'authentification en ayant la possibilité d'utiliser plusieurs facteurs tels que le TOTP, la biométrie, les notifications push, etc., ainsi que le nom d'utilisateur et le mot de passe existants. De plus, il permet au client d'utiliser ses propres fournisseurs d'identité d'utilisateur pour obtenir un identifiant d'utilisateur unifié (SSO) dans son portefeuille.

L'authentification multifacteur s'applique uniquement à la connexion à l'interface utilisateur du serveur SnapCenter. Les identifiants de connexion sont authentifiés via le IDP Active Directory Federation Services (AD FS). Vous pouvez configurer différents facteurs d'authentification sur AD FS. SnapCenter est le fournisseur de services. Vous devez configurer SnapCenter en tant que fournisseur de stockage basé dans AD FS. Pour activer MFA dans SnapCenter, vous aurez besoin des métadonnées AD FS.

Pour plus d'informations sur l'activation de MFA, reportez-vous à la section ["Activer l'authentification multifacteur"](#).

Contrôle d'accès basé sur des rôles dans SnapCenter

Le contrôle d'accès basé sur des rôles (RBAC) SnapCenter et les autorisations ONTAP permettent aux administrateurs SnapCenter de déléguer le contrôle des ressources SnapCenter à différents utilisateurs ou groupes d'utilisateurs. Cet accès géré de manière centralisée permet aux administrateurs d'applications de travailler en toute sécurité dans les environnements délégués.

Vous pouvez créer et modifier des rôles et ajouter des accès aux ressources aux utilisateurs à tout moment. Cependant, lorsque vous configurez SnapCenter pour la première fois, vous devez au moins ajouter des utilisateurs ou des groupes Active Directory aux rôles, puis ajouter un accès aux ressources à ces utilisateurs ou groupes.



Vous ne pouvez pas utiliser SnapCenter pour créer des comptes d'utilisateur ou de groupe. Vous devez créer des comptes d'utilisateur ou de groupe dans Active Directory du système d'exploitation ou de la base de données.

Types de RBAC dans SnapCenter

SnapCenter utilise les types suivants de contrôle d'accès basé sur les rôles :

- RBAC SnapCenter
- RBAC au niveau des applications
- Plug-in SnapCenter pour VMware vSphere RBAC
- Autorisations ONTAP

RBAC SnapCenter

SnapCenter possède des rôles prédéfinis et vous pouvez affecter des utilisateurs ou des groupes d'utilisateurs à ces rôles. Les rôles prédéfinis sont :

- Rôle d'administrateur SnapCenter
- Rôle d'administrateur de clones et de sauvegarde des applications
- Rôle Backup and Clone Viewer
- Rôle d'administrateur de l'infrastructure

Lorsque vous attribuez un rôle à un utilisateur, seuls les travaux pertinents pour cet utilisateur sont visibles dans la page travaux, sauf si vous avez attribué le rôle SnapCenterAdmin.

Vous pouvez également créer de nouveaux rôles et gérer les autorisations et les utilisateurs. Vous pouvez attribuer des autorisations aux utilisateurs ou aux groupes pour accéder aux objets SnapCenter tels que les hôtes, les connexions de stockage et les groupes de ressources.

Vous pouvez attribuer des autorisations RBAC aux utilisateurs et groupes au sein de la même forêt et aux utilisateurs appartenant à différentes forêts. Vous ne pouvez pas attribuer d'autorisations RBAC aux utilisateurs appartenant à des groupes imbriqués dans les forêts.



Si vous créez un rôle personnalisé, il doit contenir toutes les autorisations du rôle SnapCenterAdmin. Si vous copiez uniquement certaines autorisations, par exemple, l'ajout ou le retrait d'hôte, vous ne pouvez pas effectuer ces opérations.

Les utilisateurs doivent fournir une authentification lors de la connexion, via l'interface utilisateur graphique ou via les applets de commande PowerShell. Si les utilisateurs sont membres de plusieurs rôles, après avoir saisi des informations d'identification, ils sont invités à spécifier le rôle qu'ils souhaitent utiliser. Les utilisateurs doivent également fournir une authentification pour l'exécution des API.

RBAC au niveau des applications

SnapCenter utilise les identifiants pour vérifier que les utilisateurs SnapCenter autorisés disposent également des autorisations au niveau de l'application.

Par exemple, si vous souhaitez effectuer des opérations de protection des données dans un environnement SQL Server, vous devez définir des informations d'identification avec les informations d'identification Windows ou SQL appropriées. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une ou l'autre méthode. Si vous souhaitez effectuer des opérations de protection des données dans un environnement de système de fichiers Windows sur un système de stockage ONTAP, le rôle admin SnapCenter doit avoir admin Privileges sur l'hôte Windows.

De même, si vous souhaitez effectuer des opérations de protection des données sur une base de données Oracle et si l'authentification du système d'exploitation est désactivée dans l'hôte de la base de données, vous devez définir les informations d'identification avec la base de données Oracle ou les informations d'identification Oracle ASM. Le serveur SnapCenter authentifie les informations d'identification définies à l'aide de l'une de ces méthodes, en fonction de l'opération.

Plug-in SnapCenter pour VMware vSphere RBAC

Si vous utilisez le plug-in SnapCenter pour la protection de données cohérente avec les machines virtuelles, vCenter Server offre un niveau supplémentaire de contrôle d'accès basé sur des rôles (RBAC). Le plug-in SnapCenter VMware prend en charge le RBAC vCenter Server et ONTAP RBAC. ["En savoir plus"](#)

Meilleure pratique : NetApp vous recommande de créer un rôle ONTAP pour les opérations du plug-in SnapCenter pour VMware vSphere et de lui attribuer tous les privilèges requis.

Autorisations ONTAP

Vous devez créer un compte vsadmin avec les autorisations requises pour accéder au système de stockage.
["En savoir plus"](#)

Autorisations attribuées aux rôles SnapCenter prédéfinis

Lorsque vous ajoutez un utilisateur à un rôle, vous devez attribuer l'autorisation StorageConnection pour activer la communication SVM (Storage Virtual machine) ou affecter un SVM à l'utilisateur pour permettre l'utilisation de la SVM. L'autorisation Storage Connection permet aux utilisateurs de créer des connexions SVM.

Par exemple, un utilisateur avec le rôle administrateur SnapCenter peut créer des connexions SVM et les affecter à un utilisateur avec le rôle Administrateur App Backup and Clone, qui par défaut n'a pas la permission de créer ou de modifier des connexions SVM. Sans connexion SVM, les utilisateurs ne peuvent pas mener à bien les opérations de sauvegarde, de clonage ou de restauration.

Rôle d'administrateur SnapCenter

Toutes les autorisations sont activées pour le rôle d'administrateur SnapCenter. Vous ne pouvez pas modifier les autorisations pour ce rôle. Vous pouvez ajouter des utilisateurs et des groupes au rôle ou les supprimer.

Rôle d'administrateur de clones et de sauvegarde des applications

Le rôle d'administrateur d'applications et de clones dispose des autorisations nécessaires pour effectuer des actions administratives pour les sauvegardes d'applications et les tâches liées au clonage. Ce rôle ne dispose pas des autorisations nécessaires pour la gestion des hôtes, le provisionnement, la gestion des connexions de stockage ou l'installation à distance.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Oui.	Oui.	Oui.	Oui.
Politique	Sans objet	Oui.	Oui.	Oui.	Oui.
Sauvegarde	Sans objet	Oui.	Oui.	Oui.	Oui.
Hôte	Sans objet	Oui.	Oui.	Oui.	Oui.
Connexion de stockage	Sans objet	Non	Oui.	Non	Non
Clonage	Sans objet	Oui.	Oui.	Oui.	Oui.
Provisionnement	Sans objet	Non	Oui.	Non	Non

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Installation/désinstallation du plug-in	Non	Sans objet		Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Oui.	Oui.	Sans objet	Sans objet	Sans objet
Démonter	Oui.	Oui.	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Non	Sans objet	Sans objet	Sans objet
Protection secondaire	Non	Non	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Rôle Backup and Clone Viewer

Le rôle de la visionneuse de sauvegarde et de clonage dispose d'une vue en lecture seule de toutes les autorisations. Ce rôle est également doté d'autorisations pour la découverte, le reporting et l'accès au Tableau de bord.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Non	Oui.	Non	Non
Politique	Sans objet	Non	Oui.	Non	Non
Sauvegarde	Sans objet	Non	Oui.	Non	Non
Hôte	Sans objet	Non	Oui.	Non	Non

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Connexion de stockage	Sans objet	Non	Oui.	Non	Non
Clonage	Sans objet	Non	Oui.	Non	Non
Provisionnement	Sans objet	Non	Oui.	Non	Non
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Non	Non	Sans objet	Sans objet	Sans objet
Ressource	Non	Non	Oui.	Oui.	Non
Installation/désinstallation du plug-in	Non	Sans objet	Sans objet	Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Démonter	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Sans objet	Sans objet	Sans objet	Sans objet
Protection secondaire	Non	Sans objet	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Rôle d'administrateur de l'infrastructure

Le rôle d'administrateur de l'infrastructure possède des autorisations pour la gestion des hôtes, la gestion du stockage, le provisionnement, les groupes de ressources, les rapports d'installation à distance, Et l'accès au Tableau de bord.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Groupe de ressources	Sans objet	Oui.	Oui.	Oui.	Oui.

Autorisations	Activé	Création	Lecture	Mise à jour	Supprimer
Politique	Sans objet	Non	Oui.	Oui.	Oui.
Sauvegarde	Sans objet	Oui.	Oui.	Oui.	Oui.
Hôte	Sans objet	Oui.	Oui.	Oui.	Oui.
Connexion de stockage	Sans objet	Oui.	Oui.	Oui.	Oui.
Clonage	Sans objet	Non	Oui.	Non	Non
Provisionnement	Sans objet	Oui.	Oui.	Oui.	Oui.
Tableau de bord	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Rapports	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Restaurer	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Installation/désinstallation du plug-in	Oui.	Sans objet	Sans objet	Sans objet	Sans objet
Migration	Non	Sans objet	Sans objet	Sans objet	Sans objet
Montage	Non	Sans objet	Sans objet	Sans objet	Sans objet
Démonter	Non	Sans objet	Sans objet	Sans objet	Sans objet
Restauration complète du volume	Non	Non	Sans objet	Sans objet	Sans objet
Protection secondaire	Non	Non	Sans objet	Sans objet	Sans objet
Moniteur de tâche	Oui.	Sans objet	Sans objet	Sans objet	Sans objet

Reprise après incident dans SnapCenter

La fonctionnalité de reprise après incident de SnapCenter vous permet de vous remettre

en cas d'incidents tels que la corruption de ressources ou les pannes de serveur. Il permet de restaurer le référentiel SnapCenter, les planifications des serveurs, les composants de configuration, ainsi que le plug-in SnapCenter pour SQL Server et son stockage.

Cette section décrit les deux types de reprise sur incident dans SnapCenter :

Reprise après incident du serveur SnapCenter

- Les données du serveur SnapCenter sont sauvegardées et peuvent être restaurées sans ajout ou gestion de plug-in au serveur SnapCenter.
- Le serveur SnapCenter secondaire doit être installé sur le même répertoire d'installation et sur le même port que le serveur SnapCenter principal.
- Pour l'authentification multifacteur (MFA), pendant la reprise sur incident du serveur SnapCenter, fermez tous les onglets du navigateur et rouvrez un navigateur pour vous reconnecter. Ceci effacera les cookies de session existants ou actifs et mettra à jour les données de configuration correctes.
- La fonctionnalité de reprise après incident de SnapCenter sauvegarde le serveur SnapCenter à l'aide d'API REST. Voir "[Workflows d'API REST pour la reprise après incident d'un serveur SnapCenter](#)".
- Le fichier de configuration relatif aux paramètres d'audit n'est pas sauvegardé dans la sauvegarde de reprise sur incident ni sur le serveur DR après l'opération de restauration. Vous devez répéter manuellement les paramètres du journal d'audit.

Plug-in SnapCenter et reprise après incident du stockage

La reprise sur incident est disponible uniquement pour le plug-in SnapCenter pour SQL Server. Si le plug-in est en panne, passez à un autre hôte SQL et récupérez les données en suivant quelques étapes. Voir "[Reprise après incident du plug-in SnapCenter pour SQL Server](#)".

SnapCenter utilise ONTAP SnapMirror pour répliquer les données qui peuvent être utilisées pour la reprise d'activité en synchronisant les données sur un site secondaire. Pour initier le basculement, interrompre la réplication SnapMirror. Pendant le retour arrière, inversez la synchronisation pour répliquer les données à partir du site de reprise sur incident vers l'emplacement principal.

Licences requises par SnapCenter

SnapCenter nécessite plusieurs licences pour permettre la protection des données des applications, des bases de données, des systèmes de fichiers et des machines virtuelles. Le type de licence SnapCenter que vous installez dépend de votre environnement de stockage et des fonctionnalités que vous souhaitez utiliser.

Licence	Si nécessaire
Contrôleur SnapCenter standard	<p>Requis pour FAS, AFF, ASA</p> <p>La licence standard SnapCenter est basée sur le contrôleur et est incluse dans NetApp ONTAP One. Si vous disposez de la licence SnapManager Suite, vous bénéficiez également des droits de licence SnapCenter Standard. Si vous souhaitez installer SnapCenter en version d'essai avec un système de stockage FAS, AFF ou ASA, vous pouvez obtenir une licence d'évaluation NetApp ONTAP One en contactant l'ingénieur commercial.</p> <p>Pour plus d'informations sur les licences incluses avec NetApp ONTAP One, reportez-vous à la section "Licences incluses avec NetApp ONTAP One".</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>SnapCenter fait également partie du pack de protection des données. Si vous avez acheté A400 ou une version ultérieure, vous devez acheter le pack de protection des données.</p> </div>
SnapMirror ou SnapVault	<p>ONTAP</p> <p>Une licence SnapMirror ou SnapVault est requise si la réplication est activée dans SnapCenter.</p>
SnapRestore	<p>Indispensable pour restaurer et vérifier les sauvegardes.</p> <p>Sur les systèmes de stockage primaires</p> <ul style="list-style-type: none"> • Indispensable sur les systèmes de destination SnapVault pour effectuer une vérification à distance et une restauration à partir d'une sauvegarde. • Nécessaire sur les systèmes de destination SnapMirror pour effectuer une vérification à distance.

Licence	Si nécessaire
FlexClone	<p>Requises pour cloner les bases de données et les opérations de vérification.</p> <p>Sur les systèmes de stockage primaires et secondaires</p> <ul style="list-style-type: none"> • Requis sur les systèmes de destination SnapVault pour créer des clones à partir d'une sauvegarde secondaire à distance. • Requis sur les systèmes de destination SnapMirror pour créer des clones à partir d'une sauvegarde SnapMirror secondaire
Licences de protocoles	<ul style="list-style-type: none"> • Licence iSCSI ou FC pour LUN • Licence CIFS pour les partages SMB • Licence NFS pour VMDK de type NFS • Licence iSCSI ou FC pour les VMDK de type VMFS <p>Indispensable sur les systèmes de destination SnapMirror pour transmettre les données en cas d'indisponibilité d'un volume source.</p>
Licences SnapCenter Standard (en option)	<p>Destinations secondaires</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Il est recommandé, mais pas obligatoire, d'ajouter des licences SnapCenter Standard aux destinations secondaires. Si les licences SnapCenter Standard ne sont pas activées sur les destinations secondaires, vous ne pouvez pas utiliser SnapCenter pour sauvegarder les ressources sur la destination secondaire après avoir effectué une opération de basculement. Une licence FlexClone est toutefois requise sur les destinations secondaires pour effectuer les opérations de clonage et de vérification.</p> </div>

Licence	Si nécessaire
Licences Single Mailbox Recovery (SMBR)	<p>Si vous utilisez le plug-in SnapCenter pour Exchange pour gérer les bases de données Microsoft Exchange Server et SMBR (Single Mailbox Recovery), vous devez disposer d'une licence supplémentaire pour SMBR qui doit être achetée séparément selon la boîte aux lettres des utilisateurs.</p> <p>NetApp® Single Mailbox Recovery a pris fin le 12 mai 2023. Pour plus d'informations, reportez-vous à la section "CPC-00507". NetApp continuera d'assurer le support des clients ayant acheté une capacité de boîte aux lettres, des services de maintenance et un support via des références marketing introduites le 24 juin 2020, pendant la durée du support souscrit.</p> <p>NetApp Single Mailbox Recovery est un produit partenaire fourni par Ontrack. OnTrack PowerControls offre des fonctionnalités similaires à celles de NetApp Single Mailbox Recovery. Les clients peuvent se procurer de nouvelles licences logicielles Ontrack PowerControls et des renouvellements de maintenance et de support Ontrack PowerControls auprès d'Ontrack (jusqu'à licensingteam@ontrack.com) pour une récupération granulaire des boîtes aux lettres après la date de fin de disponibilité du 12 mai 2023.</p>



Les licences SnapCenter Advanced et SnapCenter NAS File Services sont obsolètes et ne sont plus disponibles. La licence standard et la licence basée sur la capacité ne sont plus nécessaires pour Amazon FSX for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP et Azure NetApp Files.

Vous devez installer une ou plusieurs licences SnapCenter. Pour plus d'informations sur l'ajout de licences, reportez-vous à la section "[Ajout de licences SnapCenter standard basées sur le contrôleur](#)".

Synchronisation active SnapMirror dans SnapCenter

La synchronisation active SnapMirror assure la continuité des services, même en cas de défaillance complète d'un site. Les applications peuvent ainsi basculer en toute transparence au moyen d'une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

Pour plus d'informations sur la synchronisation active SnapMirror, reportez-vous à la section "[Présentation de la synchronisation active SnapMirror](#)".

Pour la synchronisation active SnapMirror, assurez-vous que vous répondez aux différentes exigences en matière de matériel, de logiciels et de configuration du système. Pour plus d'informations, reportez-vous à "[Prérequis](#)".

Les plug-ins pris en charge pour cette fonctionnalité sont le plug-in SnapCenter pour SQL Server, le plug-in SnapCenter pour Windows, le plug-in SnapCenter pour Oracle Database, le plug-in SnapCenter pour SAP HANA, le plug-in SnapCenter pour Microsoft Exchange Server et le plug-in SnapCenter pour Unix.



Pour prendre en charge la proximité de l'initiateur hôte dans SnapCenter, la source ou la destination doit être définie dans ONTAP.

Cas d'utilisation non pris en charge par SnapCenter :

- Si vous convertissez les charges de travail de synchronisation active SnapMirror asymétriques en charges de travail symétriques en modifiant la règle sur les relations de synchronisation active SnapMirror de *automatedfailover* à *automatefailoverduplex* dans ONTAP, cette règle n'est pas prise en charge dans SnapCenter.
- En cas de sauvegardes d'un groupe de ressources (déjà protégé dans SnapCenter), puis de modification de la règle de stockage sur les relations de synchronisation active SnapMirror entre *automatedfailover* et *failetedoverduplex* dans ONTAP, cette règle n'est pas prise en charge dans SnapCenter.

Concepts clés de la protection des données

Avant d'utiliser SnapCenter, maîtriser les concepts clés de la sauvegarde, du clonage et de la restauration.

Ressources

Les ressources comprennent les bases de données, les systèmes de fichiers Windows ou les partages de fichiers sauvegardés ou clonés avec SnapCenter. Selon votre environnement, les ressources peuvent également être des instances de base de données, des groupes de disponibilité SQL Server, des bases de données Oracle, des bases de données RAC ou des groupes d'applications personnalisés.

Groupe de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte ou un cluster, potentiellement provenant de plusieurs hôtes et clusters. Les opérations effectuées sur un groupe de ressources s'appliquent à toutes ses ressources en fonction de la planification spécifiée. Vous pouvez effectuer des sauvegardes à la demande ou planifiées pour des ressources ou des groupes individuels.



Si un hôte d'un groupe de ressources partagées passe en mode maintenance, toutes les opérations planifiées pour ce groupe seront suspendues sur tous les hôtes.

Utilisez les plug-ins appropriés pour sauvegarder des ressources spécifiques : plug-ins de base de données pour bases de données, plug-ins de système de fichiers pour systèmes de fichiers et plug-in SnapCenter pour VMware vSphere pour les VM et les datastores.

Stratégies

Les règles spécifient la fréquence des sauvegardes, la conservation des copies, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Une ou plusieurs règles peuvent être sélectionnées lors de la création d'un groupe de ressources ou lors d'une sauvegarde à la demande.

Un groupe de ressources définit ce qui doit être protégé et quand il doit être protégé en termes de jour et d'heure. Une politique décrit comment la protection sera effectuée. Par exemple, si la sauvegarde de toutes les

bases de données ou de tous les systèmes de fichiers d'un hôte est nécessaire, un groupe de ressources comprenant toutes les bases de données ou tous les systèmes de fichiers de l'hôte peut être créé. Deux politiques pourraient alors être associées au groupe de ressources : une politique quotidienne et une politique horaire.

Lors de la création du groupe de ressources et de l'association des stratégies, il est possible de le configurer pour effectuer une sauvegarde complète quotidienne et une autre planification pour les sauvegardes de journaux toutes les heures.

Des prescripteurs et des scripts d'appel peuvent être utilisés dans les opérations de protection des données. Ces scripts permettent l'automatisation avant ou après le travail de protection des données. Par exemple, un script peut automatiquement signaler les échecs ou les avertissements de la tâche de protection des données. Il est essentiel de comprendre les exigences de création de ces scripts avant de configurer des prescripteurs et des scripts d'exécution.

Utilisation des prescripteurs et des postscripts

Les prescripteurs personnalisés et les postscripts peuvent automatiser vos tâches de protection des données avant ou après le travail. Par exemple, vous pouvez ajouter un script pour vous informer des échecs de travaux ou des avertissements. Avant de les configurer, assurez-vous de bien comprendre les exigences de ces scripts.

Types de script pris en charge

Les types de scripts suivants sont pris en charge pour Windows :

- Fichiers de traitement par lots
- Scripts PowerShell
- Scripts Perl

Les types de scripts suivants sont pris en charge pour UNIX :

- Scripts Perl
- Scripts Python
- Scripts de shell



Outre le shell bash par défaut, d'autres shells comme sh-shell, k-shell et c-shell sont également pris en charge.

Chemin du script

Tous les prescripteurs et scripts postscripts exécutés dans le cadre des opérations SnapCenter sur les systèmes de stockage non virtualisés et virtualisés sont exécutés sur l'hôte du plug-in.

- Les scripts Windows doivent se trouver sur l'hôte du plug-in.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN_SCRIPTS.

- Les scripts UNIX doivent se trouver sur l'hôte du plug-in.



Le chemin du script est validé au moment de l'exécution.

Où spécifier des scripts

Les scripts sont spécifiés dans les politiques de sauvegarde. Lorsqu'une tâche de sauvegarde démarre, la stratégie associe automatiquement le script aux ressources sauvegardées. Lorsque vous créez une stratégie de sauvegarde, vous pouvez spécifier les arguments prescripteurs et PostScript.



Vous ne pouvez pas spécifier plusieurs scripts.

Délais d'expiration du script

Le délai est défini sur 60 secondes, par défaut. Vous pouvez modifier la valeur de temporisation.

Sortie du script

Le répertoire par défaut des fichiers de sortie Windows prescripts et postscripts est Windows\System32.

Il n'existe pas d'emplacement par défaut pour les prescripteurs et les postscripts UNIX. Vous pouvez rediriger le fichier de sortie vers n'importe quel emplacement préféré.

Systemes de stockage et applications pris en charge par SnapCenter

Vous devez connaître les systèmes de stockage, les applications et les bases de données pris en charge par SnapCenter.

Systemes de stockage pris en charge

- NetApp ONTAP 9.12.1 et versions ultérieures
- Azure NetApp Files
- Amazon FSX pour NetApp ONTAP

Prise en charge du protocole NVMe (non-volatile Memory Express) sur TCP (transport Control Protocol).

Pour plus d'informations sur Amazon FSX pour NetApp ONTAP, consultez "[Documentation Amazon FSX pour NetApp ONTAP](#)".

- Systemes NetApp ASA r2 exécutant NetApp ONTAP 9.16.1.

Applications et bases de données prises en charge

SnapCenter prend en charge la protection de différentes applications et bases de données. Pour plus d'informations sur les applications et bases de données prises en charge, reportez-vous à la section "[Matrice d'interopérabilité NetApp](#)".

SnapCenter prend en charge la protection des charges de travail Oracle et Microsoft SQL dans le cloud VMware sur les environnements SDDC (Software-Defined Data Center) Amazon Web Services (AWS). "[En savoir plus](#)".

Méthodes d'authentification pour les informations d'identification SnapCenter

Les informations d'identification utilisent différentes méthodes d'authentification selon l'application ou l'environnement. Les informations d'identification authentifient les utilisateurs pour qu'ils puissent exécuter des opérations SnapCenter. Vous devez créer un ensemble d'informations d'identification pour l'installation des plug-ins et un autre pour les opérations de protection des données.

Authentification Windows

La méthode d'authentification Windows s'authentifie auprès d'Active Directory. Pour l'authentification Windows, Active Directory est configuré en dehors de SnapCenter. L'authentification SnapCenter s'effectue sans configuration supplémentaire. Vous avez besoin d'informations d'identification Windows pour ajouter des hôtes, installer des modules de plug-in et planifier des travaux.

Authentification de domaine non fiable

SnapCenter permet aux utilisateurs et aux groupes appartenant à des domaines non approuvés de créer des informations d'identification Windows. Pour que l'authentification réussisse, vous devez enregistrer les domaines non approuvés avec SnapCenter.

Authentification locale du groupe de travail

SnapCenter permet la création d'informations d'identification Windows avec des groupes et des utilisateurs de groupes de travail locaux. L'authentification Windows pour les groupes et les utilisateurs de groupe de travail locaux ne se produit pas lors de la création des informations d'identification Windows, mais elle est différée jusqu'à ce que l'enregistrement de l'hôte et les autres opérations de l'hôte soient effectués.

Authentification SQL Server

La méthode d'authentification SQL s'authentifie par rapport à une instance SQL Server. Cela signifie qu'une instance SQL Server doit être découverte dans SnapCenter. Par conséquent, avant d'ajouter un identifiant SQL, vous devez ajouter un hôte, installer des modules de plug-in et actualiser les ressources. Vous avez besoin de l'authentification SQL Server pour effectuer des opérations telles que la planification sur SQL Server ou la découverte de ressources.

Authentification Linux

La méthode d'authentification Linux s'authentifie par rapport à un hôte Linux. Vous avez besoin d'une authentification Linux au cours de la première étape de l'ajout de l'hôte Linux et de l'installation du module SnapCenter Plug-ins Package pour Linux à distance à partir de l'interface graphique SnapCenter.

Authentification AIX

La méthode d'authentification AIX s'authentifie auprès d'un hôte AIX. L'authentification AIX doit être effectuée lors de l'étape initiale de l'ajout de l'hôte AIX et de l'installation du module plug-ins SnapCenter pour AIX à distance à partir de l'interface utilisateur graphique SnapCenter.

Authentification de la base de données Oracle

La méthode d'authentification de la base de données Oracle s'authentifie par rapport à une base de données Oracle. Une authentification de base de données Oracle est nécessaire pour effectuer des opérations sur la base de données Oracle si l'authentification du système d'exploitation est désactivée sur l'hôte de la base de

données. Par conséquent, avant d'ajouter des informations d'identification de base de données Oracle, vous devez créer un utilisateur Oracle dans la base de données Oracle avec sysdba Privileges.

Authentification Oracle ASM

La méthode d'authentification Oracle ASM s'authentifie par rapport à une instance Oracle Automatic Storage Management (ASM). L'authentification Oracle ASM est requise si vous devez accéder à une instance Oracle ASM et si l'authentification du système d'exploitation est désactivée sur l'hôte de base de données. Avant d'ajouter des informations d'identification Oracle ASM, créez un utilisateur Oracle avec System Privileges dans l'instance ASM.

Authentification du catalogue RMAN

La méthode d'authentification du catalogue RMAN s'authentifie par rapport à la base de données du catalogue Oracle Recovery Manager (RMAN). Si vous avez configuré un mécanisme de catalogue externe et enregistré votre base de données dans la base de données de catalogue, vous devez ajouter l'authentification de catalogue RMAN.

Opérations SnapCenter prises en charge pour les systèmes ASA r2

Les systèmes de stockage ASA r2 sont pris en charge à partir de SnapCenter 6.1. "[En savoir plus sur les systèmes ASA r2](#)"

SnapCenter exploite les API REST pour effectuer toutes les opérations sur les systèmes ASA r2, qui ne prennent pas en charge les ZAPI.

Opérations prises en charge par SnapCenter pour les systèmes ASA r2

- Création de sauvegardes primaires d'applications sur VMDK
- Transfert des snapshots de groupes de cohérence vers le système de stockage secondaire
- Restauration des sauvegardes des systèmes de stockage principal et secondaire vers l'hôte d'origine ou vers l'hôte alternatif
 - Restauration sur place à partir des systèmes de stockage principaux et secondaires à l'aide de VMware vMotion
 - Connectez et copiez la restauration à partir des systèmes de stockage principal et secondaire
- Clonage des sauvegardes sur l'hôte d'origine ou sur l'hôte alternatif

SnapCenter peut découvrir ou créer des groupes de cohérence ONTAP. Il peut également provisionner et initialiser des relations SnapMirror avec le cluster de destination pour une protection secondaire.

Pour plus d'informations sur l'activation de la protection secondaire sur les systèmes ASA r2 pour votre application, reportez-vous à :

- "[Activer la protection secondaire pour les ressources Microsoft SQL Server](#)"
- "[Activer la protection secondaire pour les ressources SAP HANA](#)"
- "[Activer la protection secondaire pour les ressources Oracle](#)"
- "[Activer la protection secondaire pour les systèmes de fichiers Windows](#)"
- "[Activer la protection secondaire pour les ressources IBM Db2](#)"

- ["Activer la protection secondaire pour les ressources PostgreSQL"](#)
- ["Activer la protection secondaire pour les ressources MySQL"](#)
- ["Activer la protection secondaire pour les systèmes de fichiers Unix"](#)

Opérations non prises en charge par SnapCenter pour les systèmes ASA r2

- RDM (Raw Device Mapping)
- Volumes d'application pour Oracle
- NDV SAP HANA
- LockVault
- Des snapshots inviolables
- Volumes FlexGroup
- Groupe de cohérence hiérarchique
- Migration des systèmes de stockage ASA, AFF ou FAS vers les systèmes de stockage ASA r2
- Protection des bases de données contenant un mélange de ressources ASA, AFF ou FAS et de ressources ASA r2
- Modification du nom des snapshots
- Provisionnement secondaire du répertoire de journaux de l'hôte du plug-in SQL

Démarrage rapide du logiciel SnapCenter

Le guide de démarrage rapide décrit les étapes de base pour installer et configurer le logiciel SnapCenter.

1

Préparation de l'installation du serveur SnapCenter

Vous devez vous assurer que toutes les conditions requises pour installer le serveur SnapCenter sont remplies.

- ["De formation"](#)
- ["Inscrivez-vous pour accéder au logiciel SnapCenter"](#)
- ["Activez l'authentification multifacteur"](#)

2

Installez le serveur SnapCenter

Le serveur SnapCenter peut être installé sur des hôtes Windows ou Linux. Téléchargez le package d'installation du serveur SnapCenter à partir du ["Site de support NetApp"](#) et exécutez le programme d'installation.

- ["Installez SnapCenter Server sous Windows"](#)
- ["Installez SnapCenter Server sous Linux"](#)

3

Configurer le serveur SnapCenter

Après avoir installé le serveur SnapCenter, vous devez le configurer en fonction de votre environnement.

4

Installez le plug-in pour votre application

Assurez-vous que toutes les conditions d'installation du plug-in spécifique à l'application sont remplies en fonction de l'application utilisée, puis procédez à l'installation du plug-in correspondant.

5

Protégez votre application

Après avoir installé le serveur SnapCenter et les plug-ins nécessaires, vous pouvez lancer la création de sauvegardes d'applications. Ces sauvegardes peuvent ensuite être utilisées à des fins de restauration et de clonage lorsque cela est nécessaire.

Installer et configurer SnapCenter Server

Préparez-vous à installer le serveur SnapCenter

Configuration requise pour installer le serveur SnapCenter

Avant d'installer SnapCenter Server sur un hôte Windows ou Linux, vous devez vérifier et vous assurer que toutes les conditions requises sont remplies pour votre environnement.

Configuration requise pour les domaines et les groupes de travail pour l'hôte Windows

Le serveur SnapCenter peut être installé sur un hôte Windows qui se trouve dans un domaine ou dans un groupe de travail.

L'utilisateur ayant admin Privileges est autorisé à installer le serveur SnapCenter.

- **Domaine Active Directory** : vous devez utiliser un utilisateur de domaine avec des droits d'administrateur local. L'utilisateur de domaine doit être membre du groupe administrateur local sur l'hôte Windows.
- **Groupes de travail** : vous devez utiliser un compte local disposant de droits d'administrateur local.

Bien que les approbations de domaine, les forêts multidomaines et les approbations interdomaines soient prises en charge, les domaines interforestiers ne sont pas pris en charge. La documentation Microsoft à propos des domaines et des fiducies Active Directory contient des informations supplémentaires.



Après avoir installé le serveur SnapCenter, vous ne devez pas modifier le domaine dans lequel se trouve l'hôte SnapCenter. Si vous supprimez l'hôte SnapCenter Server du domaine dans lequel il se trouvait lors de l'installation du serveur SnapCenter, puis essayez de désinstaller le serveur SnapCenter, l'opération de désinstallation échoue.

Les besoins en termes d'espace et de dimensionnement

Vous devez connaître les exigences en matière d'espace et de dimensionnement.

Élément	Configuration requise pour les hôtes Windows	Configuration requise pour l'hôte Linux
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Seules les versions anglaise, allemande, japonaise et chinoise simplifiée des systèmes d'exploitation sont prises en charge.</p> <p>Pour obtenir les informations les plus récentes sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".</p>	<ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 8 et 9• SUSE Linux Enterprise Server (SLES) 15 <p>Pour obtenir les informations les plus récentes sur les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".</p>

Élément	Configuration requise pour les hôtes Windows	Configuration requise pour l'hôte Linux
Nombre minimal de processeurs	4 cœurs	4 cœurs
RAM minimale	8 Go  Le pool de mémoire tampon du serveur MySQL utilise 20 % de la RAM totale.	8 Go
Espace minimal sur le disque dur pour le logiciel et les journaux du serveur SnapCenter	7 GO  Si vous disposez du référentiel SnapCenter dans le lecteur où est installé le serveur SnapCenter, il est recommandé d'avoir 15 Go.	15 GO
Espace disque minimum pour le référentiel SnapCenter	8 Go  REMARQUE : si le serveur SnapCenter se trouve dans le même lecteur que le référentiel SnapCenter, il est recommandé d'avoir 15 Go.	Sans objet

Élément	Configuration requise pour les hôtes Windows	Configuration requise pour l'hôte Linux
Packs logiciels requis	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle • PowerShell 7.4.2 ou version ultérieure <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section "Échec de la mise à niveau ou de l'installation de SnapCenter pour les systèmes hérités qui ne disposent pas d'une connexion Internet".</p>	<ul style="list-style-type: none"> • .NET Framework 8.0.12 (et tous les correctifs 8.0.x suivants) • PowerShell 7.4.2 ou version ultérieure • Ce serveur Web peut être utilisé comme proxy inverse • Devel-PAM <p>PAM (Pluggable Authentication modules) est un outil de sécurité système qui permet aux administrateurs système de définir une stratégie d'authentification sans avoir à recompiler les programmes qui effectuent l'authentification.</p>



Le noyau ASP.NET nécessite IIS_IUSRS pour accéder au système de fichiers temporaires dans le serveur SnapCenter sous Windows.

Exigences relatives à l'hôte SAN

SnapCenter n'inclut pas les utilitaires hôtes ou un DSM. Si l'hôte SnapCenter fait partie d'un environnement SAN (FC/iSCSI), vous devrez peut-être installer et configurer des logiciels supplémentaires sur l'hôte du serveur SnapCenter.

- Utilitaires hôtes : les utilitaires hôtes prennent en charge FC et iSCSI et vous permettent d'utiliser MPIO sur vos serveurs Windows. ["En savoir plus"](#).
- Microsoft DSM pour Windows MPIO : ce logiciel fonctionne avec les pilotes Windows MPIO pour gérer plusieurs chemins entre les ordinateurs hôtes NetApp et Windows. Un DSM est nécessaire pour les configurations haute disponibilité.



Si vous utilisez ONTAP DSM, vous devez migrer vers Microsoft DSM. Pour plus d'informations, voir ["Comment migrer de ONTAP DSM vers Microsoft DSM"](#).

Navigateurs pris en charge

Le logiciel SnapCenter prend en charge Chrome 125 et versions ultérieures, ainsi que Microsoft Edge 110.0.1587.17 et versions ultérieures.

Configuration requise pour les ports

Le logiciel SnapCenter nécessite différents ports pour la communication entre les différents composants.

- Les applications ne peuvent pas partager de port.

- Pour les ports personnalisables, vous pouvez sélectionner un port personnalisé lors de l'installation si vous ne souhaitez pas utiliser le port par défaut.
- Pour les ports fixes, vous devez accepter le numéro de port par défaut.
- Pare-feu
 - Les pare-feu, proxys ou autres périphériques réseau ne doivent pas interférer avec les connexions.
 - Si vous spécifiez un port personnalisé lors de l'installation de SnapCenter, vous devez ajouter une règle de pare-feu sur l'hôte du plug-in pour ce port pour le chargeur Plug-in SnapCenter.

Le tableau ci-dessous répertorie les différents ports et leurs valeurs par défaut.

Nom du port	Numéros de port	Protocole	Direction	Description
Port SnapCenter	8146	HTTPS	Bidirectionnel	<p>Ce port est utilisé pour la communication entre le client SnapCenter (l'utilisateur SnapCenter) et le serveur SnapCenter et est également utilisé pour la communication entre les hôtes de plug-in et le serveur SnapCenter.</p> <p>Vous pouvez personnaliser le numéro de port.</p>
Port de communication SMCORE de SnapCenter	8145	HTTPS	Bidirectionnel	<p>Ce port est utilisé pour la communication entre le serveur SnapCenter et les hôtes sur lesquels les plug-ins SnapCenter sont installés.</p> <p>Vous pouvez personnaliser le numéro de port.</p>

Nom du port	Numéros de port	Protocole	Direction	Description
Port de service du planificateur	8154	HTTPS		<p>Ce port permet d'orchestrer de manière centralisée les flux de travail du planificateur SnapCenter pour tous les plug-ins gérés au sein de l'hôte du serveur SnapCenter.</p> <p>Vous pouvez personnaliser le numéro de port.</p>
Port RabbitMQ	5672	TCP		<p>Il s'agit du port par défaut sur lequel RabbitMQ écoute et il est utilisé pour la communication du modèle éditeur-abonné entre le service Planificateur et SnapCenter.</p>
Port MySQL	3306	HTTPS		<p>Le port est utilisé pour communiquer avec la base de données du référentiel SnapCenter. Vous pouvez créer des connexions sécurisées du serveur SnapCenter au serveur MySQL.</p> <p>"En savoir plus >>"</p>

Nom du port	Numéros de port	Protocole	Direction	Description
Hôtes du plug-in Windows	135, 445	TCP		Ce port est utilisé pour la communication entre le serveur SnapCenter et l'hôte sur lequel le plug-in est installé. La plage de ports dynamique supplémentaire spécifiée par Microsoft doit également être ouverte.
Hôtes du plug-in Linux ou AIX	22	SSH	Unidirectionnel	Ce port est utilisé pour la communication entre le serveur SnapCenter et l'hôte, lancé du serveur à l'hôte client.
Module de plug-ins SnapCenter pour Windows, Linux ou AIX	8145	HTTPS	Bidirectionnel	Ce port est utilisé pour la communication entre SMCORE et les hôtes sur lesquels le package de plug-ins est installé. Personnalisable. Vous pouvez personnaliser le numéro de port.
Plug-in SnapCenter pour bases de données Oracle	27216			Le port JDBC par défaut est utilisé par le plug-in pour Oracle pour se connecter à la base de données Oracle.
Plug-in SnapCenter pour base de données Exchange	909			Le NET par défaut. Le port TCP est utilisé par le plug-in pour Windows pour se connecter aux rappels Exchange VSS.

Nom du port	Numéros de port	Protocole	Direction	Description
Plug-ins pris en charge par NetApp pour SnapCenter	9090	HTTPS		<p>Il s'agit d'un port interne utilisé uniquement sur l'hôte du plug-in ; aucune exception de pare-feu n'est requise.</p> <p>La communication entre le serveur SnapCenter et les plug-ins est acheminée via le port 8145.</p>
Cluster ONTAP ou port de communication SVM	<ul style="list-style-type: none"> • 443 (HTTPS) • 80 (HTTP) 	<ul style="list-style-type: none"> • HTTPS • HTTP 	Bidirectionnel	<p>Le port est utilisé par le SAL (Storage abstraction Layer) pour la communication entre l'hôte exécutant le serveur SnapCenter et le SVM. Le port est actuellement utilisé par le SAL sur SnapCenter pour les hôtes du plug-in Windows pour la communication entre l'hôte du plug-in SnapCenter et le SVM.</p>
Plug-in SnapCenter pour base de données SAP HANA	<ul style="list-style-type: none"> • 3instance_number13 • 3instance_number15 	<ul style="list-style-type: none"> • HTTPS • HTTP 	Bidirectionnel	<p>Pour un seul tenant de conteneur de base de données multitenant (MDC), le numéro de port se termine par 13 ; pour non MDC, le numéro de port se termine par 15.</p> <p>Vous pouvez personnaliser le numéro de port.</p>

Nom du port	Numéros de port	Protocole	Direction	Description
Plug-in SnapCenter pour PostgreSQL	5432			<p>Ce port est le port PostgreSQL par défaut utilisé pour la communication entre le plug-in pour PostgreSQL et le cluster PostgreSQL.</p> <p>Vous pouvez personnaliser le numéro de port.</p>

Inscrivez-vous pour accéder au logiciel SnapCenter

Si vous découvrez Amazon FSX pour NetApp ONTAP ou Azure NetApp Files et ne possédez pas de compte SnapCenter, vous devez vous inscrire pour accéder au logiciel NetApp.

Avant de commencer

- Vous devez avoir accès à l'ID de messagerie de l'entreprise.
- Si vous utilisez Azure NetApp Files, vous devez disposer de l'ID d'abonnement Azure.
- Si vous utilisez Amazon FSX pour NetApp ONTAP, vous devez disposer de l'ID du système de fichiers de votre système de fichiers FSX pour ONTAP.

Description de la tâche

Votre inscription est soumise à des validations d'informations et peut prendre jusqu'à une journée pour confirmer et mettre à niveau le nouveau compte du site de support NetApp (NSS) vers un accès **complet** à partir de l'accès **guest**.

Étapes

1. Cliquez sur <https://mysupport.netapp.com/site/user/registration> pour vous inscrire.
2. Entrez votre identifiant de courriel d'entreprise, remplissez le formulaire captcha, acceptez la politique de confidentialité de NetApp et cliquez sur **soumettre**.
3. Authentifiez l'enregistrement en saisissant le mot de passe à usage unique envoyé à votre ID de courriel et cliquez sur **Continuer**.
4. Sur la page de fin de l'inscription, entrez les informations suivantes pour terminer l'inscription.
 - a. Sélectionnez **client NetApp / utilisateur final**.
 - b. Dans le champ du NUMÉRO DE SÉRIE, entrez l'ID d'abonnement Azure si vous utilisez Azure NetApp Files ou l'ID du système de fichiers si vous utilisez Amazon FSX pour NetApp ONTAP.



Vous pouvez émettre un billet à <https://mysupport.netapp.com/site/help> si vous rencontrez un problème pendant l'enregistrement ou si vous connaissez le statut.

Authentification multifacteur (MFA)

Gestion de l'authentification multifacteur (MFA)

Vous pouvez gérer la fonctionnalité d'authentification multifacteur (MFA) dans le serveur AD FS (Active Directory Federation Service) et le serveur SnapCenter.

Prise en charge de l'authentification multifacteur (MFA)

Vous pouvez activer la fonctionnalité MFA pour SnapCenter Server à l'aide des commandes PowerShell.

Description de la tâche

- SnapCenter prend en charge les connexions basées sur SSO lorsque d'autres applications sont configurées dans le même AD FS. Dans certaines configurations AD FS, SnapCenter peut exiger une authentification de l'utilisateur pour des raisons de sécurité, en fonction de la persistance de la session AD FS.
- Les informations concernant les paramètres qui peuvent être utilisés avec l'applet de commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également voir "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Avant de commencer

- Windows Active Directory Federation Service (AD FS) doit être opérationnel dans le domaine respectif.
- Vous devez disposer d'un service d'authentification multifacteur pris en charge par AD FS, tel que Azure MFA, Cisco Duo, etc.
- L'horodatage du serveur SnapCenter et AD FS doit être identique, quel que soit le fuseau horaire.
- Procurez-vous et configurez le certificat d'autorité de certification autorisé pour le serveur SnapCenter.

Le certificat CA est obligatoire pour les raisons suivantes :

- Garantit que les communications ADFS-F5 ne se rompent pas, car les certificats auto-signés sont uniques au niveau du nœud.
- Garantit que lors de la mise à niveau, de la réparation ou de la reprise après incident dans une configuration autonome ou haute disponibilité, le certificat autosigné ne sera pas recréé, ce qui évite la reconfiguration de l'authentification multifacteur.
- Garantit les résolutions IP-FQDN.

Pour plus d'informations sur le certificat CA, reportez-vous à la section "[Générer le fichier CSR de certificat CA](#)".

Étapes

1. Connectez-vous à l'hôte Active Directory Federation Services (AD FS).
2. Téléchargez le fichier de métadonnées de la fédération AD FS à partir de "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>".
3. Copiez le fichier téléchargé sur le serveur SnapCenter pour activer la fonctionnalité MFA.
4. Connectez-vous au serveur SnapCenter en tant qu'administrateur SnapCenter via PowerShell.
5. À l'aide de la session PowerShell, générez le fichier de métadonnées SnapCenter MFA à l'aide de l'applet de commande `New-SmMultifactorAuthenticationMetadata -path`.

Le paramètre `PATH` spécifie le chemin d'enregistrement du fichier de métadonnées MFA sur l'hôte du

serveur SnapCenter.

6. Copiez le fichier généré sur l'hôte AD FS pour configurer SnapCenter en tant qu'entité client.
7. Activez MFA pour SnapCenter Server à l'aide du `Set-SmMultiFactorAuthentication` applet de commande.
8. (Facultatif) Vérifiez l'état et les paramètres de configuration MFA à l'aide de `Get-SmMultiFactorAuthentication` applet de commande.
9. Accédez à la console de gestion Microsoft (MMC) et effectuez les opérations suivantes :
 - a. Cliquez sur **fichier > Ajouter/Supprimer Snapin**.
 - b. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
 - c. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
 - d. Cliquez sur **Console Root > Certificates – local Computer > Personal > Certificates**.
 - e. Cliquez avec le bouton droit de la souris sur le certificat d'autorité de certification lié à SnapCenter, puis sélectionnez **toutes les tâches > gérer les clés privées**.
 - f. Sur l'assistant d'autorisations, effectuez les opérations suivantes :
 - i. Cliquez sur **Ajouter**.
 - ii. Cliquez sur **emplacements** et sélectionnez l'hôte concerné (en haut de la hiérarchie).
 - iii. Cliquez sur **OK** dans la fenêtre contextuelle **emplacements**.
 - iv. Dans le champ Nom d'objet, entrez 'IIS_IUSRS', puis cliquez sur **vérifier les noms** et cliquez sur **OK**.

Si la vérification a réussi, cliquez sur **OK**.
10. Dans l'hôte AD FS, ouvrez l'assistant de gestion AD FS et effectuez les opérations suivantes :
 - a. Cliquez avec le bouton droit de la souris sur **fiducies de partie de confiance > Ajouter confiance de partie de confiance > début**.
 - b. Sélectionnez la deuxième option, parcourez le fichier de métadonnées MFA SnapCenter et cliquez sur **Suivant**.
 - c. Spécifiez un nom d'affichage et cliquez sur **Suivant**.
 - d. Choisissez une stratégie de contrôle d'accès, le cas échéant, et cliquez sur **Suivant**.
 - e. Sélectionnez les paramètres par défaut dans l'onglet suivant.
 - f. Cliquez sur **Terminer**.

SnapCenter se reflète désormais comme une personne de confiance avec le nom d'affichage fourni.
11. Sélectionnez le nom et effectuez les opérations suivantes :
 - a. Cliquez sur **Modifier la politique d'émission des demandes de remboursement**.
 - b. Cliquez sur **Ajouter règle** et cliquez sur **Suivant**.
 - c. Spécifiez un nom pour la règle de sinistre.
 - d. Sélectionnez **Active Directory** comme magasin d'attributs.
 - e. Sélectionnez l'attribut **User-principal-Name** et le type de réclamation sortant comme **Name-ID**.
 - f. Cliquez sur **Terminer**.

12. Exécutez les commandes PowerShell suivantes sur le serveur ADFS.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-EncryptionCertificateRevocationCheck None
```

13. Procédez comme suit pour confirmer que les métadonnées ont été importées avec succès.

- a. Cliquez avec le bouton droit de la souris sur la confiance de la partie de confiance et sélectionnez **Propriétés**.
- b. Assurez-vous que les champs points finaux, identificateurs et Signature sont renseignés.

14. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

La fonctionnalité MFA de SnapCenter peut également être activée au moyen d'API REST.

Pour obtenir des informations de dépannage, reportez-vous à la section "[Les tentatives de connexion simultanées dans plusieurs onglets indiquent une erreur MFA](#)".

Mettre à jour les métadonnées AD FS MFA

Vous devez mettre à jour les métadonnées AD FS MFA dans SnapCenter en cas de modification du serveur AD FS, telles que la mise à niveau, le renouvellement du certificat CA, la reprise sur incident, etc.

Étapes

1. Téléchargez le fichier de métadonnées de la fédération AD FS à partir de "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml> »
2. Copiez le fichier téléchargé sur le serveur SnapCenter pour mettre à jour la configuration MFA.
3. Mettez à jour les métadonnées AD FS dans SnapCenter en exécutant l'applet de commande suivante :

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

Mettre à jour les métadonnées MFA de SnapCenter

Vous devez mettre à jour les métadonnées MFA SnapCenter dans AD FS en cas de modification du serveur ADFS, comme la réparation, le renouvellement du certificat CA, la reprise sur incident, etc.

Étapes

1. Dans l'hôte AD FS, ouvrez l'assistant de gestion AD FS et effectuez les opérations suivantes :
 - a. Sélectionnez **fiducies de partie utilisatrice**.
 - b. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrice qui a été créée pour SnapCenter et sélectionnez **Supprimer**.

Le nom défini par l'utilisateur de la confiance de la partie utilisatrice s'affiche.

- c. Activez l'authentification multifacteur (MFA).

Voir "[Activer l'authentification multifacteur](#)".

2. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

Désactivation de l'authentification multifacteur (MFA)

Étapes

1. Désactivez MFA et nettoyez les fichiers de configuration créés lorsque MFA a été activé à l'aide du `Set-SmMultiFactorAuthentication` applet de commande.
2. Fermez tous les onglets du navigateur et rouvrez un navigateur pour effacer les cookies de session existants ou actifs, puis reconnectez-vous.

Gérez l'authentification multifacteur (MFA) avec l'API REST, PowerShell et SCCLI

La connexion MFA est prise en charge depuis le navigateur, l'API REST, PowerShell et SCCLI. L'authentification multifacteur est prise en charge par le biais d'un gestionnaire d'identité AD FS. Vous pouvez activer MFA, désactiver MFA et configurer MFA depuis l'interface graphique, l'API REST, PowerShell et SCCLI.

Configurer AD FS comme OAuth/OIDC

Configurer AD FS à l'aide de l'assistant GUI de Windows

1. Accédez à **Server Manager Dashboard > Tools > ADFS Management**.
2. Accédez à **ADFS > groupes d'applications**.
 - a. Cliquez avec le bouton droit de la souris sur **groupes d'applications**.
 - b. Sélectionnez **Ajouter un groupe d'applications** et entrez **Nom de l'application**.
 - c. Sélectionnez **application serveur**.
 - d. Cliquez sur **Suivant**.
3. Copier **Identifiant client**.

Il s'agit de l'ID client.

.. Ajoutez l'URL de rappel (URL du serveur SnapCenter) dans l'URL de redirection.

.. Cliquez sur **Suivant**.

4. Sélectionnez **générer un secret partagé**.

Copiez la valeur secrète. C'est le secret du client.

.. Cliquez sur **Suivant**.

5. Sur la page **Résumé**, cliquez sur **Suivant**.
 - a. Sur la page **complète**, cliquez sur **Fermer**.
6. Cliquez avec le bouton droit de la souris sur le **Groupe d'applications** nouvellement ajouté et sélectionnez **Propriétés**.
7. Sélectionnez **Ajouter une application** dans Propriétés de l'application.
8. Cliquez sur **Ajouter une application**.

Sélectionnez API Web et cliquez sur **Suivant**.

9. Sur la page configurer l'API Web, entrez l'URL du serveur SnapCenter et l'identifiant client créés à l'étape précédente dans la section Identificateur.
 - a. Cliquez sur **Ajouter**.
 - b. Cliquez sur **Suivant**.
10. Sur la page **choisir la stratégie de contrôle d'accès**, sélectionnez la stratégie de contrôle en fonction de vos besoins (par exemple, Autoriser tout le monde et demander MFA) et cliquez sur **Suivant**.
11. Sur la page **configurer l'autorisation d'application**, openid est sélectionné par défaut comme portée, cliquez sur **Suivant**.
12. Sur la page **Résumé**, cliquez sur **Suivant**.

Sur la page **complète**, cliquez sur **Fermer**.

13. Sur la page **exemple de propriétés d'application**, cliquez sur **OK**.
14. Jeton JWT émis par un serveur d'autorisation (AD FS) et destiné à être consommé par la ressource.

La déclaration « aud » ou audience de ce jeton doit correspondre à l'identifiant de la ressource ou de l'API Web.

15. Modifiez l'API Web sélectionnée et vérifiez que l'URL de rappel (URL du serveur SnapCenter) et l'identifiant du client ont été correctement ajoutés.

Configurez OpenID Connect pour fournir un nom d'utilisateur comme sinistres.

16. Ouvrez l'outil **AD FS Management** situé dans le menu **Tools** en haut à droite du Gestionnaire de serveur.
 - a. Sélectionnez le dossier **application Groups** dans la barre latérale de gauche.
 - b. Sélectionnez l'API Web et cliquez sur **EDIT**.
 - c. Accédez à l'onglet règles de conversion d'émission
17. Cliquez sur **Ajouter règle**.
 - a. Sélectionnez **Envoyer les attributs LDAP en tant que sinistres** dans la liste déroulante modèle de règle de sinistre.
 - b. Cliquez sur **Suivant**.
18. Entrez le nom **Claim Rule**.
 - a. Sélectionnez **Active Directory** dans la liste déroulante magasin d'attributs.
 - b. Sélectionnez **User-principal-Name** dans la liste déroulante **LDAP Attribute** et **UPN** dans la liste déroulante O*utening Claim Type*.
 - c. Cliquez sur **Terminer**.

Créer un groupe d'applications à l'aide des commandes PowerShell

Vous pouvez créer le groupe d'applications, l'API Web et ajouter la portée et les revendications à l'aide des commandes PowerShell. Ces commandes sont disponibles au format de script automatisé. Pour plus d'informations, voir <link to KB article>.

1. Créez le nouveau groupe d'applications dans AD FS en utilisant la commande suivante.

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier
```

```
-ApplicationGroupIdentifiant $ClientRoleIdentifiant
```

ClientRoleIdentifiant nom de votre groupe d'applications

redirectURL URL valide pour la redirection après autorisation

2. Créez l'application serveur AD FS et générez le secret client.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifiant - Server app"  
-ApplicationGroupIdentifiant $ClientRoleIdentifiant -RedirectUri $redirectURL  
-Identifiant $identifiant -GenerateClientSecret
```

3. Créez l'application ADFS Web API et configurez le nom de la stratégie qu'elle doit utiliser.

```
$identifiant = (New-Guid).Guid
```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifiant $ClientRoleIdentifiant  
-Name "App Web API"  
  
-Identifiant $identifiant -AccessControlPolicyName "Permit everyone"
```

4. Obtenez l'ID client et le secret client à partir de la sortie des commandes suivantes car, il est affiché une seule fois.

```
"client_id = $identifiant"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. Accordez à l'application AD FS les autorisations d'attributs et d'openid.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifiant $identifiant  
-ServerRoleIdentifiant $identifiant -ScopeNames @('openid')
```

```
$transformrule = @"
```

```
@RuleTemplate = "LdapClaims"
```

```
@RuleName = "AD User properties and Groups"
```

```
c:[Type ==
```

```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",  
Issuer ==
```

```
"AD AUTHORITY"]
```

```
⇒ issue(store = "Active Directory", types =  
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =  
";userPrincipalName;{0}", param = c.Value);
```

```
"@"
```

6. Notez le fichier de règles de transformation.

```
$transformrule | Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Nommez l'application API Web et définissez ses règles de conversion d'émission à l'aide d'un fichier externe.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifiant - Web API"
-TargetIdentifiant

$identifiant -Identifiant $identifiant,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Mettre à jour l'heure d'expiration du jeton d'accès

Vous pouvez mettre à jour l'heure d'expiration du jeton d'accès à l'aide de la commande PowerShell.

À propos de cette tâche

- Un jeton d'accès ne peut être utilisé que pour une combinaison spécifique d'utilisateur, de client et de ressource. Les tokens d'accès ne peuvent pas être révoqués et sont valides jusqu'à leur expiration.
- Par défaut, le délai d'expiration d'un jeton d'accès est de 60 minutes. Ce délai d'expiration minimal est suffisant et mis à l'échelle. Vous devez fournir une valeur suffisante pour éviter tout travail stratégique en cours.

Étape

Pour mettre à jour l'heure d'expiration du jeton d'accès pour un groupe d'applications WebAPI, utilisez la commande suivante dans le serveur AD FS.

```
+
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

Obtenez le jeton porteur auprès d'AD FS

Vous devez remplir les paramètres mentionnés ci-dessous dans n'importe quel client REST (tel que Postman) et vous invite à saisir les informations d'identification de l'utilisateur. En outre, vous devez entrer l'authentification second facteur (quelque chose que vous avez et quelque chose que vous êtes) pour obtenir le jeton porteur.

```
+
La validité du jeton porteur est configurable à partir du serveur AD FS par application et la période de validité par défaut est de 60 minutes.
```

Champ	Valeur
Type de subvention	Code d'autorisation
URL de rappel	Entrez l'URL de base de votre application si vous n'avez pas d'URL de rappel.

URL d'authentification	[adfs-domain-name]/adfs/oauth2/authorize
Accéder à l'URL du token	[adfs-domain-name]/adfs/oauth2/token
ID client	Entrez l'ID du client AD FS
Secret client	Entrez le secret du client AD FS
Portée	OpenID
Authentification du client	Envoyer en tant qu'en-tête AUTH de base
Ressource	Dans l'onglet Options avancées , ajoutez le champ ressource avec la même valeur que l'URL de rappel, qui se présente sous la forme d'une valeur "aud" dans le jeton JWT.

Configurez MFA dans SnapCenter Server à l'aide de PowerShell, SCCLI et de l'API REST

Vous pouvez configurer MFA dans SnapCenter Server à l'aide de PowerShell, SCCLI et de l'API REST.

Authentification SnapCenter MFA CLI

Dans PowerShell et SCCLI, l'applet de commande existante (Open-SmConnection) est étendue avec un champ supplémentaire appelé "AccessToken" pour utiliser le jeton porteur pour authentifier l'utilisateur.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

Une fois l'applet de commande ci-dessus exécutée, une session est créée pour que l'utilisateur concerné exécute d'autres applets de commande SnapCenter.

Authentification SnapCenter MFA REST API

Utilisez le jeton porteur au format *Authorization=Bearer <access token>* dans le client API REST (tel que Postman ou swagger) et mentionnez l'utilisateur RoleName dans l'en-tête pour obtenir une réponse réussie de SnapCenter.

Workflow de l'API REST MFA

Lorsque MFA est configuré avec AD FS, vous devez vous authentifier à l'aide d'un jeton d'accès (porteur) pour accéder à l'application SnapCenter par n'importe quelle API REST.

À propos de cette tâche

- Vous pouvez utiliser n'importe quel client REST comme Postman, swagger UI ou FireCamp.
- Obtenez un jeton d'accès et utilisez-le pour authentifier les demandes suivantes (API REST SnapCenter) afin d'effectuer n'importe quelle opération.

Étapes

Pour s'authentifier via AD FS MFA

1. Configurez le client REST pour appeler le point de terminaison AD FS afin d'obtenir le jeton d'accès.

Lorsque vous appuyez sur le bouton pour obtenir un jeton d'accès pour une application, vous serez redirigé vers la page AD FS SSO où vous devez fournir vos informations d'identification AD et vous authentifier auprès de MFA.

1. Dans la page AD FS SSO, saisissez votre nom d'utilisateur ou votre adresse e-mail dans la zone de texte Nom d'utilisateur.

+

Les noms d'utilisateur doivent être formatés en tant qu'utilisateur@domaine ou domaine\utilisateur.

2. Dans la zone de texte Mot de passe, saisissez votre mot de passe.
3. Cliquez sur **connexion**.
4. Dans la section **Options d'ouverture de session**, sélectionnez une option d'authentification et authentifier-vous (selon votre configuration).
 - Push : approuvez la notification Push envoyée à votre téléphone.
 - Code QR : utilisez l'application mobile AUTH point pour scanner le code QR, puis saisissez le code de vérification affiché dans l'application
 - Mot de passe à usage unique : saisissez le mot de passe à usage unique de votre jeton.
5. Une fois l'authentification réussie, une fenêtre contextuelle contenant l'accès, l'ID et le jeton d'actualisation s'ouvre.

Copiez le jeton d'accès et utilisez-le dans l'API REST SnapCenter pour effectuer l'opération.

6. Dans l'API REST, vous devez transmettre le jeton d'accès et le nom de rôle dans la section d'en-tête.
7. SnapCenter valide ce jeton d'accès à partir d'AD FS.

S'il s'agit d'un jeton valide, SnapCenter le décode et obtient le nom d'utilisateur.

8. À l'aide du nom d'utilisateur et du nom de rôle, SnapCenter authentifie l'utilisateur pour une exécution d'API.

Si l'authentification réussit, SnapCenter renvoie le résultat sinon un message d'erreur s'affiche.

Activez ou désactivez la fonctionnalité SnapCenter MFA pour l'API REST, l'interface de ligne de commande et l'interface graphique

GUI

Étapes

1. Connectez-vous au serveur SnapCenter en tant qu'administrateur SnapCenter.
2. Cliquez sur **Paramètres > Paramètres globaux > Paramètres d'authentification multifacteur (MFA)**
3. Sélectionnez l'interface (GUI/RST API/CLI) pour activer ou désactiver la connexion MFA.

Interface PowerShell

Étapes

1. Exécutez les commandes PowerShell ou CLI pour activer MFA pour l'interface graphique, l'API REST, PowerShell et SCCLI.

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

Le paramètre PATH spécifie l'emplacement du fichier xml de métadonnées AD FS MFA.

Active l'authentification multifacteur pour l'interface graphique SnapCenter, l'API REST, PowerShell et SCCLI configurée avec un chemin de fichier de métadonnées AD FS spécifié.

2. Vérifier l'état et les paramètres de configuration MFA à l'aide du `Get-SmMultiFactorAuthentication` applet de commande.

Interface SCCLI

Étapes

1. # `sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. # `sccli Get-SmMultiFactorAuthentication`

API REST

1. Exécutez l'API post suivante pour activer MFA pour l'interface graphique, l'API REST, PowerShell et SCCLI.

Paramètre	Valeur
URL demandée	/api/4.9/settings/multifactorauthentication
Méthode HTTP	Post
Corps de la demande	{ "IsGuiMFAEnabled": FALSE, "IsRestApiMFAEnabled": Vrai, "IsCliMFAEnabled": FALSE, « ADFSConfigFilePath » : « C:\ADFS_metadata\abc.xml » }

Corps de réponse	<pre>{ « MFAConfiguration » : { "IsGuiMFAEnabled": FALSE, « ADFSConfigFilePath » : « C:\ADFS_metadata\abc.xml », « SCConfigFilePath » : nul, "IsRestApiMFAEnabled": Vrai, "IsCliMFAEnabled": FALSE, "ADFSHostName": "win-adfs- sc49.winscedom2.com" } }</pre>
------------------	---

2. Vérifiez l'état et les paramètres de configuration MFA à l'aide de l'API suivante.

Paramètre	Valeur
URL demandée	/api/4.9/settings/multifactorauthentication
Méthode HTTP	Obtenez
Corps de réponse	<pre>{ « MFAConfiguration » : { "IsGuiMFAEnabled": FALSE, « ADFSConfigFilePath » : « C:\ADFS_metadata\abc.xml », « SCConfigFilePath » : nul, "IsRestApiMFAEnabled": Vrai, "IsCliMFAEnabled": FALSE, "ADFSHostName": "win-adfs- sc49.winscedom2.com" } }</pre>

Installez le serveur SnapCenter

Installez le serveur SnapCenter sur l'hôte Windows

Vous pouvez exécuter le programme d'installation du serveur SnapCenter pour installer le serveur SnapCenter.

Vous pouvez éventuellement effectuer plusieurs procédures d'installation et de configuration à l'aide d'applets de commande PowerShell. Vous devez utiliser PowerShell 7.4.2 ou une version ultérieure.



L'installation silencieuse du serveur SnapCenter à partir de la ligne de commande n'est pas prise en charge.

Avant de commencer

- L'hôte SnapCenter Server doit être à jour avec les mises à jour Windows sans redémarrage système en attente.
- Vous devez vous assurer que le serveur MySQL n'est pas installé sur l'hôte où vous prévoyez d'installer le serveur SnapCenter.
- Vous devez avoir activé le débogage du programme d'installation de Windows.

Consultez le site Web de Microsoft pour plus d'informations sur l'activation "[Consignation du programme d'installation Windows](#)".



Vous ne devez pas installer le serveur SnapCenter sur un hôte doté de serveurs Microsoft Exchange, Active Directory ou de noms de domaine.

Étapes

1. Téléchargez le package d'installation du serveur SnapCenter à partir de "[Site de support NetApp](#)".
2. Lancez l'installation du serveur SnapCenter en double-cliquant sur le fichier .exe téléchargé.

Une fois l'installation lancée, tous les contrôles préalables sont effectués et si les exigences minimales ne sont pas remplies, des messages d'erreur ou d'avertissement appropriés s'affichent.

Vous pouvez ignorer les messages d'avertissement et poursuivre l'installation ; cependant, les erreurs doivent être résolues.

3. Vérifiez les valeurs pré-remplies requises pour l'installation du serveur SnapCenter et modifiez-les si nécessaire.

Vous n'avez pas besoin de spécifier le mot de passe pour la base de données du référentiel MySQL Server. Lors de l'installation du serveur SnapCenter, le mot de passe est généré automatiquement.



Le caractère spécial "»%" is not supported in the custom path for the repository database. If you include "»%" dans le chemin, l'installation échoue.

4. Cliquez sur **installer maintenant**.

Si vous avez spécifié des valeurs non valides, des messages d'erreur appropriés s'affichent. Vous devez saisir à nouveau les valeurs, puis lancer l'installation.



Si vous cliquez sur le bouton **Annuler**, l'étape en cours d'exécution est terminée, puis démarrez l'opération de restauration. Le serveur SnapCenter sera complètement supprimé de l'hôte.

Toutefois, si vous cliquez sur **Annuler** lorsque vous exécutez des opérations "redémarrage du site du serveur SnapCenter" ou "attente du démarrage du serveur SnapCenter", l'installation se poursuit sans annuler l'opération.

Les fichiers journaux sont toujours répertoriés (les plus anciens en premier) dans le dossier %temp% de l'utilisateur admin. Si vous souhaitez rediriger les emplacements des journaux, lancez l'installation du serveur SnapCenter à partir de l'invite de commande

```
:C:\installer_location\installer_name.exe /log"C:\\"
```

Fonctionnalités activées sur l'hôte Windows lors de l'installation

Le programme d'installation de SnapCenter Server active les fonctions et les rôles Windows sur votre hôte Windows au cours de l'installation. Ceux-ci peuvent être intéressants pour le dépannage et la maintenance du système hôte.

Catégorie	Fonction
Serveur Web	<ul style="list-style-type: none"> • Services d'information Internet • World Wide Web Services • Fonctionnalités HTTP courantes <ul style="list-style-type: none"> ◦ Document par défaut ◦ Navigation dans le répertoire ◦ Erreurs HTTP ◦ Redirection HTTP ◦ Contenu statique ◦ Publication WebDAV • Santé et diagnostics <ul style="list-style-type: none"> ◦ Journalisation personnalisée ◦ Journalisation HTTP ◦ Outils de journalisation ◦ Moniteur de demandes ◦ Tracé • Fonctionnalités de performances <ul style="list-style-type: none"> ◦ Compression du contenu statique • Sécurité <ul style="list-style-type: none"> ◦ Sécurité IP ◦ Authentification de base ◦ Prise en charge centralisée des certificats SSL ◦ Authentification de mappage de certificat client ◦ Authentification de mappage de certificat de client IIS ◦ Restrictions IP et de domaine ◦ Filtrage de demandes ◦ Autorisation d'URL ◦ Authentification Windows • Fonctionnalités de développement d'applications <ul style="list-style-type: none"> ◦ Extensibilité .NET 4.5 ◦ Initialisation de l'application ◦ ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle ◦ Côté serveur inclus ◦ Protocole WebSocket <p>Outils de gestion</p> <p>Console de gestion IIS</p>

Catégorie	Fonction
Outils et scripts de gestion IIS	<ul style="list-style-type: none"> • Service de gestion IIS • Outils de gestion Web
.NET Framework 8.0.12 fonctionnalités	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle • Windows communication Foundation (WCF) HTTP Activation45 <ul style="list-style-type: none"> ◦ Activation TCP ◦ Activation HTTP <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section "Échec de la mise à niveau ou de l'installation de SnapCenter pour les systèmes hérités qui ne disposent pas d'une connexion Internet".</p>
Mise en file d'attente du message	<ul style="list-style-type: none"> • Services de mise en file d'attente des messages <div style="display: flex; align-items: center; margin-top: 10px;">  <div style="border-left: 1px solid #ccc; padding-left: 10px;"> <p>Assurez-vous qu'aucune autre application n'utilise le service MSMQ créé et géré par SnapCenter.</p> </div> </div> <ul style="list-style-type: none"> • RabbitMQ • Erlang
Service d'activation de processus Windows	<ul style="list-style-type: none"> • Modèle de processus
API de configuration	Tout

Installez le serveur SnapCenter sur l'hôte Linux

Vous pouvez exécuter le programme d'installation du serveur SnapCenter pour installer le serveur SnapCenter.

Avant de commencer

- Si vous souhaitez installer le serveur SnapCenter à l'aide d'un utilisateur non root qui ne dispose pas des privilèges suffisants pour installer SnapCenter, procurez-vous le fichier de somme de contrôle sudoers sur le site de support NetApp. Vous devez utiliser le fichier de somme de contrôle approprié basé sur la version Linux.
- Si le package sudo n'est pas disponible dans SUSE Linux, installez le package sudo pour éviter tout échec d'authentification.
- Pour SUSE Linux, configurez le nom d'hôte pour éviter l'échec de l'installation.
- Vérifiez l'état de Linux sécurisé en exécutant la commande `sestatus`. Si l'état *SELinux* est "activé" et que le *mode actuel* est "application", procédez comme suit :

- Lancer la commande : `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

La valeur par défaut de `WEBAPP_EXTERNAL_PORT` est 8146

- Si le pare-feu bloque le port, exécutez `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

La valeur par défaut de `WEBAPP_EXTERNAL_PORT` est 8146

- Exécutez les commandes suivantes à partir du répertoire dans lequel vous disposez des autorisations de lecture et d'écriture :

- `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

Si la commande renvoie « rien à faire », relancez la commande après l'installation du serveur SnapCenter.

- Si la commande crée `my-nginx.pp`, exécutez la commande pour activer le package de règles : `sudo semodule -i my-nginx.pp`

- Le chemin utilisé pour le répertoire MySQL PID est `/var/opt/mysqld`. Exécutez les commandes suivantes pour définir les autorisations pour l'installation de MySQL.

- `mkdir /var/opt/mysqld`
- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
- `sudo restorecon -Rv /var/opt/mysqld`

- Le chemin utilisé pour le répertoire de données MySQL est `/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/`. Exécutez les commandes suivantes pour définir les autorisations pour le répertoire de données MySQL.

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

Description de la tâche

- Lorsque le serveur SnapCenter est installé sur l'hôte Linux, des services tiers tels que MySQL, RabbitMQ, Erlang sont installés. Vous ne devez pas les désinstaller.
- Le serveur SnapCenter installé sur l'hôte Linux ne prend pas en charge :
 - Haute disponibilité
 - Plug-ins Windows
 - Active Directory (prend uniquement en charge les utilisateurs locaux, à la fois les utilisateurs root et non root avec creds)
 - Authentification par clé pour se connecter à SnapCenter
- Pendant l'installation de .NET runtime, si l'installation ne parvient pas à résoudre les dépendances de `libcicu` library, installez `libcicu` en exécutant la commande : `yum install -y libcicu`
- Si l'installation du serveur SnapCenter échoue en raison de la non-disponibilité de `Perl`, installez `Perl` en

exécutant la commande : `yum install -y perl`

Étapes

1. Téléchargez ce qui suit à partir de "[Site de support NetApp](#)" sur */home Directory*.
 - Package d'installation du serveur SnapCenter - **snapcenter-linux-Server-(el8/el9/sles15).bin**
 - Fichier de clé publique - **snapcenter_public_key.pub**
 - Fichier de signature respectif - **snapcenter-linux-Server-(el8/el9/sles15).bin.SIG**
2. Validez le fichier de signature.
`$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Pour une installation utilisateur non-root, ajoutez le contenu visudo spécifié dans **snapcenter_Server_checksum_(el8/el9/sles15).txt** disponible avec le programme d'installation .bin.
4. Attribuez l'autorisation d'exécution au programme d'installation .bin.
`chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Effectuez l'une des actions nécessaires pour installer le serveur SnapCenter.

Si vous souhaitez effectuer...	Procédez comme ça...
Installation interactive	<pre>./snapcenter-linux-server-(el8/el9/sles15).bin</pre> <p>Vous serez invité à entrer les informations suivantes :</p> <ul style="list-style-type: none">• Port externe de l'application Web utilisé pour accéder au serveur SnapCenter en dehors de l'hôte Linux. La valeur par défaut est 8146.• Utilisateur du serveur SnapCenter qui installera le serveur SnapCenter.• Répertoire d'installation dans lequel les packages seront installés.

Si vous souhaitez effectuer...	Procédez comme ça...
Installation non interactive	<pre>sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename></pre> <p>Exemple : <code>sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log</code></p> <p>Les journaux seront stockés à <code>/var/opt/snapcenter/logs</code>.</p> <p>Paramètres à transmettre pour l'installation du serveur SnapCenter :</p> <ul style="list-style-type: none"> • <code>DWEBAPP_EXTERNAL_PORT</code> : port externe WebApp utilisé pour accéder au serveur SnapCenter en dehors de l'hôte Linux. La valeur par défaut est 8146. • <code>DWEBAPP_INTERNAL_PORT</code> : port interne de WebApp utilisé pour accéder au serveur SnapCenter au sein de l'hôte Linux. La valeur par défaut est 8147. • <code>DSMCORE_PORT</code> : port SMCore sur lequel les services smcore sont exécutés. La valeur par défaut est 8145. • <code>DSCHEDULER_PORT</code> : port du planificateur sur lequel les services du planificateur sont exécutés. La valeur par défaut est 8154. • <code>DSNAPCENTER_SERVER_USER</code> : utilisateur du serveur SnapCenter qui installera le serveur SnapCenter. Pour <code>DSNAPCENTER_SERVER_USER</code>, l'utilisateur par défaut exécute le programme d'installation. • <code>DUSER_INSTALL_DIR</code> : répertoire d'installation dans lequel les packages seront installés. Pour <code>DUSER_INSTALL_DIR</code>, le répertoire d'installation par défaut est <code>/opt</code>. • <code>DINSTALL_LOG_NAME</code> : nom du fichier journal dans lequel les journaux d'installation seront stockés. Il s'agit d'un paramètre facultatif. S'il est spécifié, aucun journal ne s'affiche sur la console. Si vous ne spécifiez pas ce paramètre, les journaux s'affichent sur la console et sont également stockés dans le fichier journal par défaut.

Et la suite ?

- Si l'état *SELinux* est "activé" et que le *mode actuel* est "application", le service **nginx** ne démarre pas. Vous devez exécuter les commandes suivantes :
 - a. Accédez au répertoire local.
 - b. Exécutez la commande : `journalctl -x|grep nginx`.
 - c. Si le port interne de WebApp (8147) n'est pas autorisé à écouter, exécutez les commandes suivantes :
 - `ausearch -c 'nginx' --raw | audit2allow -D my-nginx`
 - `semodule -i my-nginx.pp`
 - d. Exécutez `setsebool -P httpd_can_network_connect on`.
- DISELINUX** : si le *SELinux status* est "enabled", le *CURRENT mode* est "forcing" et que vous avez exécuté les commandes mentionnées dans la section avant de commencer, vous devez spécifier ce paramètre et affecter la valeur par défaut est 0. Spécifiez ce paramètre et sa valeur comme tout entier autre que 0 pour mettre à niveau le serveur SnapCenter.

Fonctionnalités activées sur l'hôte Linux lors de l'installation

Le serveur SnapCenter installe les packages logiciels ci-dessous qui peuvent aider au dépannage et à la maintenance du système hôte.

- RabbitMQ
- Erlang

Enregistrer SnapCenter

Si vous découvrez NetApp et ne possédez pas de compte NetApp, vous devez enregistrer SnapCenter pour activer le support.

Étapes

1. Après avoir installé SnapCenter, accédez à **aide > à propos de**.
2. Dans la boîte de dialogue *a propos de SnapCenter*, notez l'instance SnapCenter, un nombre à 20 chiffres commençant par 971.
3. Cliquez sur <https://register.netapp.com>.
4. Cliquez sur **Je ne suis pas un client NetApp enregistré**.
5. Indiquez vos coordonnées pour vous inscrire.
6. Laissez le champ NetApp Reference SN vide.
7. Sélectionnez **SnapCenter** dans la liste déroulante gamme de produits.
8. Sélectionnez le fournisseur de facturation.
9. Entrez l'ID d'instance SnapCenter à 20 chiffres.
10. Cliquez sur **soumettre**.

Connectez-vous à SnapCenter à l'aide de l'autorisation RBAC

SnapCenter prend en charge le contrôle d'accès basé sur des rôles (RBAC). L'administrateur SnapCenter affecte des rôles et des ressources via le RBAC SnapCenter à un utilisateur dans un groupe de travail ou un répertoire actif, ou à des groupes dans l'annuaire actif. L'utilisateur RBAC peut désormais se connecter à SnapCenter avec les rôles attribués.

Avant de commencer

- Vous devez activer Windows Process activation Service (WAS) dans Windows Server Manager.
- Si vous souhaitez utiliser Internet Explorer comme navigateur pour vous connecter au serveur SnapCenter, vous devez vous assurer que le mode protégé dans Internet Explorer est désactivé.
- Si le serveur SnapCenter est installé sur l'hôte Linux, vous devez vous connecter à l'aide du compte utilisateur utilisé pour installer le serveur SnapCenter.

À propos de cette tâche

Au cours de l'installation, l'assistant d'installation du serveur SnapCenter crée un raccourci et le place sur le bureau et dans le menu Démarrer de l'hôte sur lequel SnapCenter est installé. En outre, à la fin de l'installation, l'assistant d'installation affiche l'URL SnapCenter en fonction des informations fournies lors de l'installation, que vous pouvez copier si vous souhaitez vous connecter à partir d'un système distant.



Si plusieurs onglets sont ouverts dans votre navigateur Web, la fermeture de l'onglet navigateur SnapCenter ne vous déconnecte pas de SnapCenter. Pour mettre fin à votre connexion avec SnapCenter, vous devez vous déconnecter de SnapCenter en cliquant sur le bouton **Déconnexion** ou en fermant tout le navigateur Web.

Meilleure pratique: pour des raisons de sécurité, il est recommandé de ne pas activer votre navigateur pour enregistrer votre mot de passe SnapCenter.

L'URL de l'interface utilisateur graphique par défaut est une connexion sécurisée au port par défaut 8146 sur le serveur sur lequel le serveur SnapCenter est installé (<https://server:8146>). Si vous avez fourni un autre port serveur lors de l'installation de SnapCenter, ce port est utilisé à la place.

Pour un déploiement haute disponibilité, vous devez accéder à SnapCenter à l'aide du cluster virtuel IP https://Virtual_Cluster_IP_or_FQDN:8146. Si vous ne voyez pas l'interface utilisateur SnapCenter lorsque vous accédez à https://Virtual_Cluster_IP_or_FQDN:8146 dans Internet Explorer (IE), vous devez ajouter l'adresse IP ou le FQDN du cluster virtuel en tant que site de confiance dans IE sur chaque hôte du plug-in ou désactiver IE Enhanced Security sur chaque hôte du plug-in. Pour plus d'informations, voir ["Impossible d'accéder à l'adresse IP du cluster depuis le réseau externe"](#).

Outre l'interface graphique SnapCenter, vous pouvez utiliser les applets de commande PowerShell pour créer des scripts pour réaliser les opérations de configuration, de sauvegarde et de restauration. Il se peut que certains cmdlets aient changé à chaque version d'SnapCenter. Le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#) présente les détails.



Si vous vous connectez à SnapCenter pour la première fois, vous devez vous connecter à l'aide des informations d'identification fournies lors du processus d'installation.

Étapes

1. Lancez SnapCenter à partir du raccourci situé sur votre bureau hôte local, ou à partir de l'URL fournie à la fin de l'installation, ou à partir de l'URL fournie par votre administrateur SnapCenter.
2. Saisissez les informations d'identification de l'utilisateur.

Pour spécifier les éléments suivants...	Utilisez l'un de ces formats...
Administrateur de domaine	<ul style="list-style-type: none"> • NetBIOS\username • Suffixe username@UPN <p>Par exemple, username@netapp.com</p> <ul style="list-style-type: none"> • Nom de domaine FQDN\nom d'utilisateur
Administrateur local	Nom d'utilisateur

3. Si plusieurs rôles vous sont attribués, dans la zone rôle, sélectionnez le rôle que vous souhaitez utiliser pour cette session de connexion.

Votre utilisateur actuel et votre rôle associé s'affichent dans l'angle supérieur droit de SnapCenter une fois connecté.

Résultat

La page Tableau de bord s'affiche.

Si la journalisation échoue avec l'erreur que le site ne peut pas être atteint, vous devez mapper le certificat SSL à SnapCenter. ["En savoir plus >>"](#)

Après la fin

Après la première connexion au serveur SnapCenter en tant qu'utilisateur RBAC, actualisez la liste des ressources.

Si vous possédez des domaines Active Directory non approuvés que vous souhaitez prendre en charge par SnapCenter, vous devez enregistrer ces domaines avec SnapCenter avant de configurer les rôles des utilisateurs sur des domaines non fiables. ["En savoir plus >>"](#).

Si vous souhaitez ajouter l'hôte de plug-in dans SnapCenter s'exécutant sur un hôte Linux, vous devez obtenir le fichier de checksum à l'emplacement suivant : `/opt/NetApp/snapcenter/SnapManagerWeb/Repository`.

À partir de la version 6.0, un raccourci pour SnapCenter PowerShell est créé sur le bureau. Vous pouvez accéder directement aux applets de commande SnapCenter PowerShell en utilisant le raccourci.

Connexion au SnapCenter à l'aide de l'authentification multifacteur (MFA)

Le serveur SnapCenter prend en charge l'authentification multifacteur pour le compte de domaine, qui fait partie de l'annuaire actif.

Avant de commencer

Vous devez avoir activé MFA. Pour plus d'informations sur l'activation de MFA, reportez-vous à la section ["Activer l'authentification multifacteur"](#)

À propos de cette tâche

- Seul le FQDN est pris en charge
- Les groupes de travail et les utilisateurs inter-domaines ne peuvent pas se connecter à l'aide de MFA

Étapes

1. Lancez SnapCenter à partir du raccourci situé sur votre bureau hôte local, ou à partir de l'URL fournie à la fin de l'installation, ou à partir de l'URL fournie par votre administrateur SnapCenter.
2. Dans la page de connexion d'AD FS, saisissez Nom d'utilisateur et Mot de passe.

Lorsque le message d'erreur nom d'utilisateur ou mot de passe incorrect s'affiche sur la page AD FS, vous devez vérifier les points suivants :

- Indique si le nom d'utilisateur ou le mot de passe est valide

Le compte utilisateur doit exister dans Active Directory (AD)

- Si vous avez dépassé le nombre maximal de tentatives autorisées défini dans AD
- Si AD et AD FS sont opérationnels

Modifiez le délai d'expiration de la session de l'interface utilisateur graphique SnapCenter par défaut

Vous pouvez modifier le délai d'expiration de la session de l'interface graphique SnapCenter pour la rendre inférieure ou supérieure au délai d'expiration par défaut de 20 minutes.

Comme fonction de sécurité, après une période par défaut de 15 minutes d'inactivité, SnapCenter vous avertit que vous serez déconnecté de la session de l'interface utilisateur dans les 5 minutes. Par défaut, SnapCenter vous déconnecte de la session de l'interface utilisateur après 20 minutes d'inactivité et vous devez vous reconnecter.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres > Paramètres globaux**.
2. Dans la page Paramètres globaux, cliquez sur **Paramètres de configuration**.
3. Dans le champ délai d'expiration de session, entrez le délai d'expiration de la nouvelle session en minutes, puis cliquez sur **Enregistrer**.

Sécurisez le serveur Web SnapCenter en désactivant SSL 3.0

Pour des raisons de sécurité, vous devez désactiver le protocole SSL (Secure Socket Layer) 3.0 dans Microsoft IIS si celui-ci est activé sur votre serveur Web SnapCenter.

Le protocole SSL 3.0 comporte des défauts qu'un attaquant peut utiliser pour provoquer des échecs de connexion, ou pour exécuter des attaques d'homme en milieu et observer le trafic de cryptage entre votre site Web et ses visiteurs.

Étapes

1. Pour lancer l'éditeur du Registre sur l'hôte du serveur Web SnapCenter, cliquez sur **Démarrer > Exécuter**, puis saisissez regedit.
2. Dans l'Éditeur du Registre, accédez à HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\
 - Si la clé de serveur existe déjà :
 - i. Sélectionnez DWORD activé, puis cliquez sur **Modifier > Modifier**.

- ii. Définissez la valeur sur 0, puis cliquez sur **OK**.
 - Si la clé du serveur n'existe pas :
 - i. Cliquez sur **Modifier** > **Nouveau** > **clé**, puis nommez le serveur de clés.
 - ii. Une fois la nouvelle clé de serveur sélectionnée, cliquez sur **Édition** > **Nouveau** > **DWORD**.
 - iii. Nommez le nouveau DWORD activé, puis entrez 0 comme valeur.
3. Fermez l'Éditeur du Registre.

Configurer le serveur SnapCenter

Ajouter et provisionner le système de stockage

Ajout de systèmes de stockage

Vous devez configurer le système de stockage qui donne à SnapCenter un accès au stockage ONTAP, aux systèmes ASA r2 ou à Amazon FSX pour NetApp ONTAP afin d'effectuer des opérations de protection et de provisionnement des données.

Vous pouvez ajouter un SVM autonome ou un cluster comprenant plusieurs SVM. Si vous utilisez Amazon FSX pour NetApp ONTAP, vous pouvez soit ajouter une LIF d'administration FSX composée de plusieurs SVM à l'aide d'un compte fsxadmin, soit ajouter un SVM FSX dans SnapCenter.

Avant de commencer

- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

À propos de cette tâche

- Lorsque vous configurez des systèmes de stockage, vous pouvez également activer les fonctionnalités EMS (Event Management System) et AutoSupport. L'outil AutoSupport collecte des données relatives à l'état de santé de votre système et les envoie automatiquement au support technique NetApp. Les données y sont ainsi envoyées pour résoudre le problème de votre système.

Si vous activez ces fonctionnalités, SnapCenter envoie des informations AutoSupport au système de stockage et des messages EMS au système de stockage lorsqu'une ressource est protégée, qu'une opération de restauration ou de clonage se termine correctement ou qu'une opération échoue.

- Si vous prévoyez de répliquer des snapshots sur une destination SnapMirror ou SnapVault, vous devez configurer les connexions du système de stockage pour le SVM ou le cluster de destination ainsi que le

SVM ou le cluster source.



Si vous modifiez le mot de passe du système de stockage, les tâches planifiées, les opérations de sauvegarde à la demande et de restauration peuvent échouer. Après avoir modifié le mot de passe du système de stockage, vous pouvez mettre à jour le mot de passe en cliquant sur **Modifier** dans l'onglet stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Systems**.
2. Dans la page systèmes de stockage, cliquez sur **Nouveau**.
3. Dans la page Add Storage System, fournissez les informations suivantes :

Pour ce champ...	Procédez comme ça...
System de stockage	<p>Entrez le nom ou l'adresse IP du système de stockage.</p> <p> Les noms de système de stockage, sans inclure le nom de domaine, doivent comporter 15 caractères ou moins et les noms doivent être résolus. Pour créer des connexions de système de stockage avec des noms comportant plus de 15 caractères, vous pouvez utiliser l'applet de commande Add-SmStorageConnectionPowerShell.</p> <p> Pour les systèmes de stockage avec configuration MetroCluster (MCC), il est recommandé d'enregistrer des clusters locaux et homologues pour garantir la continuité de l'activité.</p> <p>SnapCenter ne prend pas en charge plusieurs SVM de même nom sur différents clusters. Chaque SVM pris en charge par SnapCenter doit avoir un nom unique.</p> <p> Après avoir ajouté la connexion de stockage à SnapCenter, vous ne devez pas renommer le SVM ou le cluster en utilisant ONTAP.</p> <p> Si un SVM est ajouté avec un nom court ou un nom de domaine complet, il doit être résolu à la fois à partir du serveur SnapCenter et de l'hôte du plug-in.</p>

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur/Mot de passe	Entrez les informations d'identification de l'utilisateur de stockage disposant des privilèges requis pour accéder au système de stockage.
Système de gestion des événements (EMS) et paramètres AutoSupport	<p>Pour envoyer des messages EMS au syslog du système de stockage ou pour que des messages AutoSupport soient envoyés au système de stockage à des fins de protection appliquée, de restauration terminée ou d'échec, cochez la case appropriée.</p> <p>Lorsque vous cochez la case Envoyer la notification AutoSupport pour les opérations ayant échoué sur le système de stockage, la case Enregistrer les événements du serveur SnapCenter sur syslog est également cochée car la messagerie EMS est requise pour activer les notifications AutoSupport.</p>

4. Cliquez sur **plus d'options** si vous souhaitez modifier les valeurs par défaut attribuées à la plate-forme, au protocole, au port et au délai d'attente.

a. Dans plate-forme, sélectionnez l'une des options dans la liste déroulante.

Si le SVM est le système de stockage secondaire d'une relation de sauvegarde, cochez la case **secondaire**. Lorsque l'option **Secondary** est sélectionnée, SnapCenter n'effectue pas immédiatement de vérification de licence.

Si vous avez ajouté un SVM dans SnapCenter, l'utilisateur doit sélectionner le type de plateforme dans la liste déroulante manuellement.

a. Dans Protocol, sélectionnez le protocole configuré lors de la configuration du SVM ou du Cluster, en général HTTPS.

b. Saisissez le port accepté par le système de stockage.

Le port par défaut 443 fonctionne généralement.

c. Saisissez le temps en secondes qui doit s'écouler avant que les tentatives de communication ne soient interrompues.

La valeur par défaut est 60 secondes.

d. Si le SVM possède plusieurs interfaces de gestion, cochez la case **IP préférée**, puis saisissez l'adresse IP préférée pour les connexions SVM.

e. Cliquez sur **Enregistrer**.

5. Cliquez sur **soumettre**.

Résultat

Dans la page Storage Systems (systèmes de stockage), dans la liste déroulante **Type**, effectuez l'une des

opérations suivantes :

- Sélectionnez **ONTAP SVM** si vous souhaitez afficher tous les SVM ajoutés.

Si vous avez ajouté des SVM FSX, les SVM FSX sont répertoriés ici.

- Sélectionnez **clusters ONTAP** si vous souhaitez afficher tous les clusters ajoutés.

Si vous avez ajouté des clusters FSX à l'aide de fsxadmin, les clusters FSX sont répertoriés ici.

Lorsque vous cliquez sur le nom du cluster, tous les SVM qui font partie du cluster sont affichés dans la section Storage Virtual machines.

Si un nouveau SVM est ajouté au cluster ONTAP à l'aide de l'interface graphique de ONTAP, cliquez sur **redécouvrez** pour afficher le nouveau SVM ajouté.

Après la fin

Un administrateur de cluster doit activer AutoSupport sur chaque nœud du système de stockage pour envoyer des notifications par e-mail à partir de tous les systèmes de stockage auxquels SnapCenter a accès, en exécutant la commande suivante depuis la ligne de commande du système de stockage :

```
autosupport trigger modify -node nodename -autosupport-message client.app.info  
-to enable -noteto enable
```



L'administrateur de la SVM (Storage Virtual machine) n'a pas accès à AutoSupport.

Connexions de stockage et identifiants

Avant d'effectuer les opérations de protection des données, configurez les connexions de stockage et ajoutez les identifiants que le serveur SnapCenter et les plug-ins SnapCenter utiliseront.

Connexions de stockage

Les connexions de stockage permettent au serveur SnapCenter et aux plug-ins SnapCenter d'accéder au système de stockage ONTAP. La configuration de ces connexions implique également la configuration des fonctions AutoSupport et EMS.

Informations d'identification

- Administrateur de domaine ou tout membre du groupe d'administrateurs

Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :

- *NetBIOS\username*
- *Domain FQDN\username*
- *Username@upn*

- Administrateur local (groupes de travail uniquement)

Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte.

Le format valide du champ Nom d'utilisateur est : *username*

- Informations d'identification pour des groupes de ressources individuels

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

Provisionnement du stockage sur les hôtes Windows

Création et gestion des igroups

Vous créez des groupes initiateurs pour spécifier les hôtes pouvant accéder à une LUN donnée sur le système de stockage. SnapCenter permet de créer, renommer, modifier ou supprimer un groupe initiateur sur un hôte Windows.

Créer un groupe initiateur

Vous pouvez utiliser SnapCenter pour créer un groupe initiateur sur un hôte Windows. Le groupe initiateur sera disponible dans l'assistant de création de disque ou de connexion de disque lorsque vous mappez le groupe initiateur sur une LUN.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Dans la page groupes d'initiateurs, cliquez sur **Nouveau**.
4. Dans la boîte de dialogue Créer un iGroup, définissez le groupe initiateur :

Dans ce champ...	Procédez comme ça...
System de stockage	Sélectionnez le SVM pour la LUN que vous allez mapper sur le groupe initiateur.
Hôte	Sélectionnez l'hôte sur lequel vous souhaitez créer le groupe initiateur.
Nom d'igroup	Indiquez le nom du groupe initiateur.
Initiateurs	Sélectionnez l'initiateur.
Type	Sélectionnez le type d'initiateur, iSCSI, FCP ou mixte (FCP et iSCSI).

5. Lorsque vous êtes satisfait de vos entrées, cliquez sur **OK**.

SnapCenter crée le groupe initiateur sur le système de stockage.

Renommer un groupe initiateur

Vous pouvez utiliser SnapCenter pour renommer un groupe initiateur existant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Sur la page groupes initiateurs, cliquez dans le champ **Storage Virtual machine** pour afficher la liste des SVM disponibles, puis sélectionnez la SVM du groupe initiateur que vous souhaitez renommer.
4. Dans la liste des igroups pour la SVM, sélectionnez le groupe initiateur que vous souhaitez renommer, puis cliquez sur **Renommer**.
5. Dans la boîte de dialogue Renommer le groupe initiateur, saisissez le nouveau nom du groupe initiateur, puis cliquez sur **Renommer**.

Modifier un groupe initiateur

Vous pouvez utiliser SnapCenter pour ajouter des initiateurs à un groupe initiateur existant. Lors de la création d'un groupe initiateur, vous ne pouvez ajouter qu'un seul hôte. Si vous souhaitez créer un groupe initiateur pour un cluster, vous pouvez le modifier pour ajouter d'autres nœuds à ce groupe initiateur.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Sur la page groupes initiateurs, cliquez dans le champ **Storage Virtual machine** pour afficher la liste déroulante des SVM disponibles, puis sélectionnez le SVM du groupe initiateur que vous souhaitez modifier.
4. Dans la liste des groupes initiateurs, sélectionnez un groupe initiateur, puis cliquez sur **Ajouter un initiateur au groupe initiateur**.
5. Sélectionnez un hôte.
6. Sélectionnez les initiateurs et cliquez sur **OK**.

Supprimez un groupe initiateur

Lorsque vous n'en avez plus besoin, vous pouvez utiliser SnapCenter pour supprimer un groupe initiateur.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **igroup**.
3. Sur la page groupes initiateurs, cliquez dans le champ **Storage Virtual machine** pour afficher la liste déroulante des SVM disponibles, puis sélectionnez le SVM du groupe initiateur que vous souhaitez supprimer.
4. Dans la liste des igroups pour la SVM, sélectionnez le groupe initiateur que vous souhaitez supprimer, puis cliquez sur **Delete**.

5. Dans la boîte de dialogue Supprimer un groupe initiateur, cliquez sur **OK**.

SnapCenter supprime le groupe initiateur.

Création et gestion des disques

L'hôte Windows considère que des LUN de votre système de stockage sont des disques virtuels. Vous pouvez utiliser SnapCenter pour créer et configurer une LUN connectée via FC ou connectée via iSCSI.

- SnapCenter ne prend en charge que les disques de base. Les disques dynamiques ne sont pas pris en charge.
- Pour GPT, une seule partition de données et pour MBR, une partition primaire est autorisée, dont un volume est formaté avec NTFS ou CSVFS et possède un chemin de montage.
- Styles de partition pris en charge : GPT, MBR ; dans une machine virtuelle VMware UEFI, seuls les disques iSCSI sont pris en charge



La SnapCenter ne prend pas en charge la modification du nom d'un disque. Le changement de nom d'un disque géré par SnapCenter permet d'effectuer les opérations SnapCenter sans succès.

Afficher les disques d'un hôte

Vous pouvez afficher les disques sur chaque hôte Windows que vous gérez avec SnapCenter.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

Les disques sont répertoriés.

Afficher les disques en cluster

Vous pouvez afficher les disques en cluster sur le cluster que vous gérez à l'aide de SnapCenter. Les disques en cluster sont affichés uniquement lorsque vous sélectionnez le cluster dans la liste déroulante hôtes.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez le cluster dans la liste déroulante **Host**.

Les disques sont répertoriés.

Établir une session iSCSI

Si vous utilisez iSCSI pour vous connecter à une LUN, vous devez établir une session iSCSI avant de créer la LUN pour activer la communication.

Avant de commencer

- Vous devez avoir défini le nœud du système de stockage comme cible iSCSI.
- Vous devez avoir démarré le service iSCSI sur le système de stockage. ["En savoir plus >>"](#)

À propos de cette tâche

Vous pouvez établir une session iSCSI uniquement entre les mêmes versions IP, soit d'IPv6 vers IPv6, soit d'IPv4 vers IPv4.

Vous pouvez utiliser une adresse IPv6 lien-local pour la gestion des sessions iSCSI et pour la communication entre un hôte et une cible uniquement lorsque les deux se trouvent dans le même sous-réseau.

Si vous modifiez le nom d'un initiateur iSCSI, l'accès aux cibles iSCSI est affecté. Après avoir modifié le nom, vous devrez peut-être reconfigurer les cibles auxquelles l'initiateur a accès afin qu'il puisse reconnaître le nouveau nom. Vous devez vous assurer de redémarrer l'hôte après avoir modifié le nom d'un initiateur iSCSI.

Si votre hôte dispose de plusieurs interfaces iSCSI, une fois que vous avez établi une session iSCSI vers SnapCenter à l'aide d'une adresse IP sur la première interface, vous ne pouvez pas établir de session iSCSI à partir d'une autre interface avec une autre adresse IP.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **session iSCSI**.
3. Dans la liste déroulante **Storage Virtual machine**, sélectionnez la machine virtuelle de stockage (SVM) pour la cible iSCSI.
4. Dans la liste déroulante **Host**, sélectionnez l'hôte de la session.
5. Cliquez sur **établir session**.

L'assistant d'établissement de session s'affiche.

6. Dans l'assistant établir une session, identifiez la cible :

Dans ce champ...	Entrer...
Nom du nœud cible	Nom du nœud de la cible iSCSI S'il existe un nom de nœud cible existant, le nom est affiché en lecture seule.
Adresse du portail cible	L'adresse IP du portail réseau cible
Port du portail cible	Port TCP du portail réseau cible
Adresse du portail de l'initiateur	L'adresse IP du portail réseau de l'initiateur

7. Lorsque vous êtes satisfait de vos entrées, cliquez sur **connexion**.

SnapCenter établit la session iSCSI.

8. Répétez cette procédure pour établir une session pour chaque cible.

Créer des disques ou des LUN connectés via FC ou iSCSI

L'hôte Windows voit les LUN de votre système de stockage comme des disques virtuels. Vous pouvez utiliser SnapCenter pour créer et configurer une LUN connectée via FC ou connectée via iSCSI.

Si vous souhaitez créer et formater des disques en dehors de SnapCenter, seuls les systèmes de fichiers NTFS et CSVFS sont pris en charge.

Avant de commencer

- Vous devez avoir créé un volume pour le LUN sur votre système de stockage.

Le volume doit contenir les LUN uniquement, et seules les LUN créées avec SnapCenter.



Vous ne pouvez pas créer de LUN sur un volume clone créé par SnapCenter sauf si le clone a déjà été divisé.

- Vous devez avoir démarré le service FC ou iSCSI sur le système de stockage.
- Si vous utilisez iSCSI, vous devez avoir établi une session iSCSI avec le système de stockage.
- Le module de plug-ins SnapCenter pour Windows doit être installé uniquement sur l'hôte sur lequel vous créez le disque.

À propos de cette tâche

- Vous ne pouvez pas connecter une LUN à plusieurs hôtes, sauf si celle-ci est partagée par les hôtes d'un cluster de basculement Windows Server.
- Si un LUN est partagé par les hôtes d'un cluster de basculement Windows Server qui utilise CSV (Cluster Shared volumes), vous devez créer le disque sur l'hôte qui possède le groupe de clusters.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.
4. Cliquez sur **Nouveau**.

L'assistant de création de disque s'ouvre.

5. Dans la page Nom de la LUN, identifiez la LUN :

Dans ce champ...	Procédez comme ça...
System de stockage	Sélectionnez le SVM pour la LUN.
Chemin de LUN	Cliquez sur Parcourir pour sélectionner le chemin d'accès complet du dossier contenant la LUN.
Nom de la LUN	Indiquez le nom de la LUN.

Dans ce champ...	Procédez comme ça...
Taille du cluster	Sélectionnez la taille d'allocation des blocs de LUN pour le cluster. La taille du cluster dépend du système d'exploitation et des applications.
Étiquette de LUN	Si vous le souhaitez, entrez un texte descriptif pour la LUN.

6. Sur la page Disk Type, sélectionnez le type de disque :

Sélectionner...	Si...
Disque dédié	La LUN n'est accessible qu'à un seul hôte. Ignorez le champ Groupe de ressources .
Disque partagé	Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server. Entrez le nom du groupe de ressources du cluster dans le champ Groupe de ressources . Vous devez créer le disque sur un seul hôte du cluster de basculement.
CSV (Cluster Shared Volume)	La LUN est partagée par les hôtes d'un cluster de basculement Windows Server qui utilise CSV. Entrez le nom du groupe de ressources du cluster dans le champ Groupe de ressources . Assurez-vous que l'hôte sur lequel vous créez le disque est le propriétaire du groupe de clusters.

7. Dans la page Propriétés du lecteur, spécifiez les propriétés du lecteur :

Propriété	Description
Attribuer automatiquement un point de montage	SnapCenter attribue automatiquement un point de montage de volume en fonction du lecteur du système. Par exemple, si votre lecteur système est C:, l'affectation automatique crée un point de montage de volume sous votre lecteur C: (C:\scmnt\). L'affectation automatique n'est pas prise en charge pour les disques partagés.

Propriété	Description
Attribuer une lettre de lecteur	Montez le disque sur le lecteur sélectionné dans la liste déroulante adjacente.
Utiliser un point de montage de volume	Montez le disque sur le chemin d'accès que vous spécifiez dans le champ adjacent. La racine du point de montage du volume doit appartenir à l'hôte sur lequel vous créez le disque.
N'attribuez pas de lettre de lecteur ou de point de montage de volume	Choisissez cette option si vous préférez monter le disque manuellement sous Windows.
Taille de la LUN	Spécifiez la taille de LUN ; 150 Mo minimum. Sélectionnez Mo, Go ou TB dans la liste déroulante adjacente.
Utilisez l'allocation dynamique pour le volume hébergeant cette LUN	Provisionnement fin de la LUN. Le provisionnement fin n'alloue qu'autant d'espace de stockage que nécessaire en même temps, ce qui permet à la LUN d'évoluer efficacement jusqu'à la capacité maximale disponible. Assurez-vous que l'espace disponible sur le volume est suffisant pour prendre en charge l'ensemble du stockage de LUN dont vous pensez avoir besoin.
Choisissez le type de partition	Sélectionnez partition GPT pour une table de partitions GUID ou partition MBR pour un enregistrement de démarrage maître. Les partitions MBR peuvent causer des problèmes d'alignement dans les clusters de basculement Windows Server.  Les disques de partition UEFI ne sont pas pris en charge.

8. Sur la page carte LUN, sélectionnez l'initiateur iSCSI ou FC sur l'hôte :

Dans ce champ...	Procédez comme ça...
Hôte	<p>Double-cliquez sur le nom du groupe de clusters pour afficher la liste déroulante des hôtes appartenant au cluster, puis sélectionnez l'hôte de l'initiateur.</p> <p>Ce champ s'affiche uniquement si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server.</p>
Choisissez l'initiateur hôte	<p>Sélectionnez Fibre Channel ou iSCSI, puis sélectionnez l'initiateur sur l'hôte.</p> <p>Vous pouvez sélectionner plusieurs initiateurs FC si vous utilisez FC avec des E/S multivoies (MPIO).</p>

9. Sur la page Type de groupe, indiquez si vous souhaitez mapper un groupe initiateur existant sur la LUN ou en créer un nouveau :

Sélectionner...	Si...
Créer un nouveau groupe initiateur pour les initiateurs sélectionnés	Vous souhaitez créer un nouveau groupe initiateur pour les initiateurs sélectionnés.
Sélectionnez un groupe initiateur existant ou spécifiez un nouveau groupe initiateur pour les initiateurs sélectionnés	<p>Vous souhaitez indiquer un groupe initiateur existant pour les initiateurs sélectionnés ou créer un nouveau groupe initiateur avec le nom que vous spécifiez.</p> <p>Saisissez le nom du groupe initiateur dans le champ igroup name. Saisissez les premières lettres du nom du groupe initiateur existant pour compléter automatiquement le champ.</p>

10. Dans la page Résumé, vérifiez vos sélections, puis cliquez sur **Terminer**.

SnapCenter crée le LUN et le connecte au disque ou au chemin de disque spécifié sur l'hôte.

Redimensionner un disque

Vous pouvez augmenter ou réduire la taille d'un disque en fonction de l'évolution des besoins de votre système de stockage.

À propos de cette tâche

- Pour la LUN à provisionnement fin, la taille de la géométrie de la lun ONTAP est indiquée comme taille maximale.
- Pour les LUN thick provisionnées, la taille extensible (taille disponible dans le volume) est indiquée comme taille maximale.
- Les LUN avec partitions de style MBR ont une taille limite de 2 To.

- Les LUN avec des partitions de type GPT ont une taille de système de stockage limite de 16 To.
- Avant de redimensionner une LUN, il est recommandé de créer une copie Snapshot.
- Si vous devez restaurer une LUN à partir d'une copie Snapshot effectuée avant le redimensionnement de la LUN, SnapCenter redimensionne automatiquement la LUN en fonction de sa taille.

Après l'opération de restauration, les données ajoutées à la LUN après son redimensionnement doivent être restaurées à partir d'une copie Snapshot effectuée après son redimensionnement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante hôte.

Les disques sont répertoriés.

4. Sélectionnez le disque à redimensionner, puis cliquez sur **Redimensionner**.
5. Dans la boîte de dialogue Redimensionner le disque, utilisez le curseur pour spécifier la nouvelle taille du disque ou entrez la nouvelle taille dans le champ taille.



Si vous entrez la taille manuellement, vous devez cliquer en dehors du champ taille pour que le bouton réduire ou développer soit activé de manière appropriée. Vous devez également cliquer sur MB, GB ou TB pour spécifier l'unité de mesure.

6. Lorsque vous êtes satisfait de vos entrées, cliquez sur **réduire** ou **développer**, selon les besoins.

SnapCenter redimensionne le disque.

Connectez un disque

Vous pouvez utiliser l'assistant de connexion de disque pour connecter une LUN existante à un hôte ou pour reconnecter une LUN qui a été déconnectée.

Avant de commencer

- Vous devez avoir démarré le service FC ou iSCSI sur le système de stockage.
- Si vous utilisez iSCSI, vous devez avoir établi une session iSCSI avec le système de stockage.
- Vous ne pouvez pas connecter une LUN à plusieurs hôtes, sauf si celle-ci est partagée par les hôtes d'un cluster de basculement Windows Server.
- Si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server qui utilise CSV (Cluster Shared volumes), vous devez connecter le disque sur l'hôte qui possède le groupe de clusters.
- Le plug-in pour Windows doit être installé uniquement sur l'hôte sur lequel vous connectez le disque.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

4. Cliquez sur **connexion**.

L'assistant de connexion au disque s'ouvre.

5. Dans la page Nom de LUN, identifiez la LUN à connecter sur :

Dans ce champ...	Procédez comme ça...
System de stockage	Sélectionnez le SVM pour la LUN.
Chemin de LUN	Cliquez sur Browse pour sélectionner le chemin d'accès complet du volume contenant la LUN.
Nom de la LUN	Indiquez le nom de la LUN.
Taille du cluster	Sélectionnez la taille d'allocation des blocs de LUN pour le cluster. La taille du cluster dépend du système d'exploitation et des applications.
Étiquette de LUN	Si vous le souhaitez, entrez un texte descriptif pour la LUN.

6. Sur la page Disk Type, sélectionnez le type de disque :

Sélectionner...	Si...
Disque dédié	La LUN n'est accessible qu'à un seul hôte.
Disque partagé	Le LUN est partagé par les hôtes d'un cluster de basculement Windows Server. Vous n'avez besoin de connecter le disque qu'à un hôte du cluster de basculement.
CSV (Cluster Shared Volume)	La LUN est partagée par les hôtes d'un cluster de basculement Windows Server qui utilise CSV. Assurez-vous que l'hôte sur lequel vous vous connectez au disque est le propriétaire du groupe de clusters.

7. Dans la page Propriétés du lecteur, spécifiez les propriétés du lecteur :

Propriété	Description
Attribution automatique	Laissez SnapCenter attribuer automatiquement un point de montage de volume en fonction du lecteur du système. Par exemple, si votre lecteur système est C:, la propriété affectation automatique crée un point de montage de volume sous votre lecteur C: (C:\scmnpt\). La propriété affectation automatique n'est pas prise en charge pour les disques partagés.
Attribuer une lettre de lecteur	Montez le disque sur le lecteur sélectionné dans la liste déroulante adjacente.
Utiliser un point de montage de volume	Montez le disque sur le chemin de lecteur que vous spécifiez dans le champ adjacent. La racine du point de montage du volume doit appartenir à l'hôte sur lequel vous créez le disque.
N'attribuez pas de lettre de lecteur ou de point de montage de volume	Choisissez cette option si vous préférez monter le disque manuellement sous Windows.

8. Sur la page carte LUN, sélectionnez l'initiateur iSCSI ou FC sur l'hôte :

Dans ce champ...	Procédez comme ça...
Hôte	Double-cliquez sur le nom du groupe de clusters pour afficher la liste déroulante des hôtes appartenant au cluster, puis sélectionnez l'hôte de l'initiateur. Ce champ s'affiche uniquement si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server.
Choisissez l'initiateur hôte	Sélectionnez Fibre Channel ou iSCSI , puis sélectionnez l'initiateur sur l'hôte. Vous pouvez sélectionner plusieurs initiateurs FC si vous utilisez FC avec MPIO.

9. Sur la page Type de groupe, indiquez si vous souhaitez mapper un groupe initiateur existant sur la LUN ou en créer un nouveau :

Sélectionner...	Si...
Créez un nouveau groupe initiateur pour les initiateurs sélectionnés	Vous souhaitez créer un nouveau groupe initiateur pour les initiateurs sélectionnés.
Sélectionnez un groupe initiateur existant ou spécifiez un nouveau groupe initiateur pour les initiateurs sélectionnés	<p>Vous souhaitez indiquer un groupe initiateur existant pour les initiateurs sélectionnés ou créer un nouveau groupe initiateur avec le nom que vous spécifiez.</p> <p>Saisissez le nom du groupe initiateur dans le champ igroup name. Saisissez les premières lettres du nom du groupe initiateur existant pour compléter automatiquement le champ.</p>

10. Dans la page Résumé, vérifiez vos sélections et cliquez sur **Terminer**.

SnapCenter connecte le LUN au chemin de lecteur ou de lecteur spécifié sur l'hôte.

Déconnectez un disque

Vous pouvez déconnecter une LUN d'un hôte sans affecter le contenu de la LUN, à une exception près : si vous déconnectez un clone avant sa mise hors service, vous perdez le contenu du clone.

Avant de commencer

- Assurez-vous que la LUN n'est utilisée par aucune application.
- Vérifiez que la LUN n'est pas surveillée avec le logiciel de surveillance.
- Si la LUN est partagée, assurez-vous de supprimer les dépendances liées aux ressources du cluster de la LUN et vérifiez que tous les nœuds du cluster sont sous tension, fonctionnent correctement et disponibles pour SnapCenter.

À propos de cette tâche

Si vous déconnectez une LUN d'un volume FlexClone que SnapCenter a créé et qu'aucune autre LUN du volume n'est connectée, SnapCenter supprime le volume. Avant de déconnecter la LUN, SnapCenter affiche un message vous informant que le volume FlexClone peut être supprimé.

Pour éviter la suppression automatique du volume FlexClone, vous devez renommer le volume avant de déconnecter la dernière LUN. Lorsque vous renommez le volume, assurez-vous de changer plusieurs caractères plutôt que le dernier caractère du nom.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

Les disques sont répertoriés.

4. Sélectionnez le disque à déconnecter, puis cliquez sur **déconnecter**.

5. Dans la boîte de dialogue Disconnect Disk (déconnecter le disque), cliquez sur **OK**.

SnapCenter déconnecte le disque.

Supprimer un disque

Vous pouvez supprimer un disque lorsque vous n'en avez plus besoin. Après avoir supprimé un disque, vous ne pouvez plus le supprimer.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **disques**.
3. Sélectionnez l'hôte dans la liste déroulante **Host**.

Les disques sont répertoriés.

4. Sélectionnez le disque à supprimer, puis cliquez sur **Supprimer**.
5. Dans la boîte de dialogue Supprimer le disque, cliquez sur **OK**.

SnapCenter supprime le disque.

Création et gestion de partages SMB

Pour configurer un partage SMB3 sur un SVM, vous pouvez utiliser l'interface utilisateur SnapCenter ou les applets de commande PowerShell.

Meilleure pratique: l'utilisation des applets de commande est recommandée car elle vous permet de tirer parti des modèles fournis avec SnapCenter pour automatiser la configuration du partage.

Les modèles encapsulent les meilleures pratiques pour la configuration des volumes et des partages. Vous trouverez les modèles dans le dossier modèles du dossier d'installation du module de plug-ins SnapCenter pour Windows.



Si vous vous sentez à l'aise de le faire, vous pouvez créer vos propres modèles en suivant les modèles fournis. Avant de créer un modèle personnalisé, vérifiez les paramètres dans la documentation de l'applet de commande.

Créez un partage SMB

La page partages SnapCenter permet de créer un partage SMB3 sur un SVM.

Vous ne pouvez pas utiliser SnapCenter pour sauvegarder des bases de données sur des partages SMB. Le support SMB est limité au provisionnement uniquement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **partages**.
3. Sélectionnez la SVM dans la liste déroulante **Storage Virtual machine**.

4. Cliquez sur **Nouveau**.

La boîte de dialogue Nouveau partage s'ouvre.

5. Dans la boîte de dialogue Nouveau partage, définissez le partage :

Dans ce champ...	Procédez comme ça...
Description	Entrez un texte descriptif pour le partage.
Nom de partage	Entrez le nom du partage, par exemple test_Share. Le nom que vous saisissez pour le partage sera également utilisé comme nom de volume. Le nom du partage : <ul style="list-style-type: none">• Doit être une chaîne UTF-8.• Ne doit pas inclure les caractères suivants : les caractères de contrôle de 0x00 à 0x1F (tous les deux compris), 0x22 (guillemets doubles) et les caractères spéciaux \ / [] : (vertical bar) < > + = ; , ?
Chemin du partage	<ul style="list-style-type: none">• Cliquez dans le champ pour entrer un nouveau chemin d'accès au système de fichiers, par exemple, /.• Double-cliquez dans le champ pour sélectionner un chemin de système de fichiers existant.

6. Lorsque vous êtes satisfait de vos entrées, cliquez sur **OK**.

SnapCenter crée le partage SMB sur le SVM.

Supprime un partage SMB

Vous pouvez supprimer un partage SMB lorsque vous n'en avez plus besoin.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **partages**.
3. Sur la page partages, cliquez dans le champ **Storage Virtual machine** pour afficher une liste déroulante avec la liste des SVM disponibles, puis sélectionnez le SVM pour le partage que vous souhaitez supprimer.
4. Dans la liste des partages du SVM, sélectionnez le partage que vous souhaitez supprimer et cliquez sur **Delete**.
5. Dans la boîte de dialogue Supprimer le partage, cliquez sur **OK**.

SnapCenter supprime le partage SMB du SVM.

Récupération de l'espace sur le système de stockage

Bien que NTFS surveille l'espace disponible sur une LUN lorsque des fichiers sont supprimés ou modifiés, il ne signale pas les nouvelles informations au système de stockage. Vous pouvez exécuter l'applet de commande PowerShell de récupération d'espace sur l'hôte du plug-in pour Windows afin de vous assurer que les blocs récemment libérés sont marqués comme disponibles dans le stockage.

Si vous exécutez l'applet de commande sur un hôte de plug-in distant, vous devez avoir exécuté l'applet de commande SnapCenterOpen-SMConnection pour ouvrir une connexion au serveur SnapCenter.

Avant de commencer

- Vous devez vous assurer que le processus de récupération d'espace est terminé avant d'effectuer une opération de restauration.
- Si la LUN est partagée par les hôtes d'un cluster de basculement Windows Server, vous devez effectuer la récupération d'espace sur l'hôte qui possède le groupe de clusters.
- Pour un stockage optimal en termes de performances, nous vous conseillons d'assurer la récupération d'espace aussi souvent que possible.

Assurez-vous que l'intégralité du système de fichiers NTFS a été numérisée.

À propos de cette tâche

- La récupération de l'espace étant chronophage et consommatrice en ressources système, il est généralement préférable d'exécuter les opérations lorsque le système de stockage et l'utilisation des hôtes Windows sont faibles.
- La récupération d'espace désaligne l'espace disponible, mais pas 100 %.
- Vous ne devez pas exécuter la défragmentation du disque en même temps que vous effectuez la récupération d'espace.

Cela peut ralentir le processus de récupération.

Étape

Dans l'invite de commandes PowerShell du serveur d'applications, saisissez la commande suivante :

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

Chemin_lecteur correspond au chemin d'accès du disque mappé sur la LUN.

Provisionnement du stockage avec les applets de commande PowerShell

Si vous ne souhaitez pas utiliser l'interface graphique SnapCenter pour effectuer des tâches de provisionnement d'hôte et de récupération d'espace, vous pouvez utiliser les applets de commande PowerShell. Vous pouvez utiliser les applets de commande directement ou les ajouter aux scripts.

Si vous exécutez les applets de commande sur un hôte de plug-in distant, vous devez exécuter l'applet de commande SnapCenter Open-SMConnection pour ouvrir une connexion au serveur SnapCenter.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Si les applets de commande SnapCenter PowerShell sont cassés afin de supprimer SnapDrive pour Windows du serveur, reportez-vous à ["Les applets de commande SnapCenter sont cassés lors de la désinstallation de SnapDrive pour Windows"](#).

Provisionnement du stockage dans les environnements VMware

Vous pouvez utiliser le plug-in SnapCenter pour Microsoft Windows dans les environnements VMware pour créer et gérer des LUN et gérer des snapshots.

Plateformes de système d'exploitation invité VMware prises en charge

- Versions de Windows Server prises en charge
- Configurations en cluster Microsoft

Prise en charge jusqu'à 16 nœuds pris en charge sur VMware lors de l'utilisation de l'initiateur logiciel Microsoft iSCSI, ou jusqu'à deux nœuds utilisant FC

- LUN RDM

Prise en charge d'un maximum de 56 LUN RDM avec quatre contrôleurs SCSI LSI Logic pour RDMS normal, ou 42 LUN RDM avec trois contrôleurs SCSI LSI Logic sur un plug-in VMware VM MSCS Box-to-box pour configuration Windows

Prend en charge le contrôleur SCSI paravirtuel VMware. 256 disques peuvent être pris en charge sur des disques RDM.

Pour obtenir les informations les plus récentes sur les versions prises en charge, reportez-vous à la section ["Matrice d'interopérabilité NetApp"](#).

Limitations liées au serveur VMware ESXi

- L'installation du plug-in pour Windows sur un cluster Microsoft sur des machines virtuelles utilisant des informations d'identification ESXi n'est pas prise en charge.

Vous devez utiliser vos informations d'identification vCenter lors de l'installation du plug-in pour Windows sur des machines virtuelles en cluster.

- Tous les nœuds en cluster doivent utiliser le même ID cible (sur l'adaptateur SCSI virtuel) pour le même disque en cluster.
- Lorsque vous créez une LUN RDM en dehors du plug-in pour Windows, vous devez redémarrer le service du plug-in pour lui permettre de reconnaître le nouveau disque créé.
- Vous ne pouvez pas utiliser simultanément des initiateurs iSCSI et FC sur un système d'exploitation invité VMware.

Privilèges vCenter minimum requis pour les opérations SnapCenter RDM

Vous devez disposer des privilèges vCenter suivants sur l'hôte pour effectuer des opérations RDM dans un système d'exploitation invité :

- Datastore : supprimer le fichier
- Hôte : configuration > Configuration de la partition de stockage
- Ordinateur virtuel : configuration

Vous devez attribuer ces privilèges à un rôle au niveau du serveur Virtual Center. Le rôle auquel vous attribuez ces privilèges ne peut être attribué à aucun utilisateur sans privilèges root.

Après avoir attribué ces privilèges, vous pouvez installer le plug-in pour Windows sur le système d'exploitation invité.

Gérer les LUN FC RDM dans un cluster Microsoft

Vous pouvez utiliser le plug-in pour Windows pour gérer un cluster Microsoft à l'aide de LUN RDM FC, mais vous devez d'abord créer le quorum RDM partagé et le stockage partagé en dehors du plug-in, puis ajouter les disques aux machines virtuelles du cluster.

Depuis ESXi 5.5, vous pouvez également utiliser ESX iSCSI et le matériel FCoE pour gérer un cluster Microsoft. Le plug-in pour Windows inclut une prise en charge prête à l'emploi des clusters Microsoft.

De formation

Le plug-in pour Windows prend en charge les clusters Microsoft en utilisant des LUN RDM FC sur deux machines virtuelles différentes appartenant à deux serveurs ESX ou ESXi distincts, également appelés cluster entre les boîtes, lorsque vous répondez aux exigences de configuration spécifiques.

- Les machines virtuelles doivent exécuter la même version de Windows Server.
- Les versions des serveurs ESX ou ESXi doivent être identiques pour chaque hôte parent VMware.
- Chaque hôte parent doit disposer d'au moins deux cartes réseau.
- Au moins un datastore VMware Virtual machine File System (VMFS) doit être partagé entre les deux serveurs ESX ou ESXi.
- VMware recommande de créer le datastore partagé sur un SAN FC.

Si nécessaire, le datastore partagé peut également être créé via iSCSI.

- La LUN RDM partagée doit être en mode de compatibilité physique.
- Le LUN RDM partagé doit être créé manuellement en dehors du plug-in pour Windows.

Vous ne pouvez pas utiliser de disques virtuels pour le stockage partagé.

- Un contrôleur SCSI doit être configuré sur chaque machine virtuelle du cluster en mode de compatibilité physique :

Windows Server 2008 R2 requiert la configuration du contrôleur SCSI SAS LSI Logic sur chaque machine virtuelle. Les LUN partagées ne peuvent pas utiliser le contrôleur SAS LSI Logic existant si seul un de son type existe et est déjà connecté au lecteur C:.

Les contrôleurs SCSI de type paravirtuel ne sont pas pris en charge sur les clusters VMware Microsoft.



Lorsque vous ajoutez un contrôleur SCSI à une LUN partagée sur une machine virtuelle en mode de compatibilité physique, vous devez sélectionner l'option **mappages de périphériques bruts** (RDM) et non l'option **Créer un nouveau disque** dans VMware Infrastructure client.

- Les clusters de machines virtuelles Microsoft ne peuvent pas faire partie d'un cluster VMware.
- Vous devez utiliser les informations d'identification vCenter et non les informations d'identification ESX ou ESXi lorsque vous installez le plug-in pour Windows sur des machines virtuelles appartenant à un cluster Microsoft.
- Le plug-in pour Windows ne peut pas créer un groupe initiateur unique avec des initiateurs à partir de plusieurs hôtes.

Le groupe initiateur contenant les initiateurs de tous les hôtes ESXi doit être créé sur le contrôleur de stockage avant de créer les LUN RDM qui seront utilisés comme disques de cluster partagés.

- Veillez à créer une LUN RDM sur ESXi 5.0 à l'aide d'un initiateur FC.

Lorsque vous créez une LUN RDM, un groupe initiateur est créé avec ALUA.

Limites

Le plug-in pour Windows prend en charge les clusters Microsoft à l'aide de LUN RDM FC/iSCSI sur différentes machines virtuelles appartenant à différents serveurs ESX ou ESXi.



Cette fonctionnalité n'est pas prise en charge dans les versions antérieures à ESX 5.5i.

- Le plug-in pour Windows ne prend pas en charge les clusters sur les datastores iSCSI et NFS ESX.
- Le plug-in pour Windows ne prend pas en charge les initiateurs mixtes dans un environnement de cluster.

Les initiateurs doivent être FC ou Microsoft iSCSI, mais pas les deux.

- Les initiateurs iSCSI ESX et les HBA ne sont pas pris en charge sur les disques partagés d'un cluster Microsoft.
- Le plug-in pour Windows ne prend pas en charge la migration des machines virtuelles avec vMotion si l'ordinateur virtuel fait partie d'un cluster Microsoft.
- Le plug-in pour Windows ne prend pas en charge MPIO sur des machines virtuelles d'un cluster Microsoft.

Créer une LUN FC RDM partagée

Avant de pouvoir utiliser des LUN RDM FC pour partager le stockage entre les nœuds d'un cluster Microsoft, vous devez d'abord créer le disque quorum partagé et le disque de stockage partagé, puis les ajouter aux deux machines virtuelles du cluster.

Le disque partagé n'est pas créé à l'aide du plug-in pour Windows. Vous devez créer, puis ajouter le LUN partagé à chaque machine virtuelle du cluster. Pour plus d'informations, voir "[Machines virtuelles de clusters sur des hôtes physiques](#)".

Ajout de licences SnapCenter standard basées sur le contrôleur

Une licence standard basée sur le contrôleur SnapCenter est requise si vous utilisez des

contrôleurs de stockage FAS, AFF ou ASA.

La licence basée sur le contrôleur présente les caractéristiques suivantes :

- Droits SnapCenter Standard inclus dans l'achat des bundles Premium ou Flash (non inclus dans le pack de base)
- Utilisation illimitée du stockage
- Ajouté directement au contrôleur de stockage FAS, AFF ou ASA à l'aide d' ONTAP System Manager ou de l' ONTAP CLI.



Vous n'entrez aucune information de licence dans l'interface utilisateur de SnapCenter pour les licences basées sur le contrôleur SnapCenter .

- Verrouillé pour le numéro de série du contrôleur

Pour plus d'informations sur les licences requises, reportez-vous à la section "[Licences SnapCenter](#)".

Étape 1 : vérifiez si la licence de la suite SnapManager est installée

Vous pouvez utiliser l'interface utilisateur de SnapCenter pour vérifier si une licence SnapManager Suite est installée sur les systèmes de stockage principaux FAS, AFF ou ASA et identifier les systèmes qui ont besoin de licences. Les licences SnapManager Suite s'appliquent uniquement aux SVM ou clusters FAS, AFF et ASA sur les systèmes de stockage principaux.



Si vous disposez déjà d'une licence SnapManager Suite sur votre contrôleur, SnapCenter fournit automatiquement le droit de licence standard basé sur le contrôleur. Les noms de licence SnapManagerSuite et de licence basée sur le contrôleur SnapCenter Standard sont utilisés de manière interchangeable, mais ils font référence à la même licence.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **systèmes de stockage**.
2. Dans la page Storage Systems (systèmes de stockage), dans le menu déroulant **Type**, indiquez si vous souhaitez afficher tous les SVM ou clusters ajoutés :
 - Pour afficher tous les SVM ajoutés, sélectionnez **ONTAP SVM**.
 - Pour afficher tous les clusters ajoutés, sélectionnez **ONTAP clusters**.

Lorsque vous sélectionnez le nom du cluster, tous les SVM faisant partie du cluster s'affichent dans la section Storage Virtual machines.

3. Dans la liste connexions de stockage, recherchez la colonne Licence de contrôleur.

La colonne Controller License affiche l'état suivant :

◦



Indique qu'une licence SnapManager Suite est installée sur un système de stockage principal FAS, AFF ou ASA.

◦



Indique qu'une licence SnapManager Suite n'est pas installée sur un système de stockage principal FAS, AFF ou ASA.

- Non applicable indique qu'une licence de la suite SnapManager n'est pas applicable, car le contrôleur

de stockage se trouve sur Amazon FSX pour les plateformes de stockage NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou secondaires.

Étape 2 : identifier les licences installées sur le contrôleur

Vous pouvez utiliser la ligne de commandes de ONTAP pour afficher toutes les licences installées sur votre contrôleur. Vous devez être administrateur du cluster sur le système FAS, AFF ou ASA.



Le contrôleur affiche la licence basée sur le contrôleur SnapCenter Standard comme licence SnapManagerSuite.

Étapes

1. Connectez-vous au contrôleur NetApp à l'aide de la ligne de commande ONTAP.
2. Entrez la commande `license show`, puis affichez la sortie pour voir si la licence SnapManagerSuite est installée.

Exemple de sortie

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package          Type      Description          Expiration
-----
Base             site     Cluster Base License -

Serial Number: 1-81-000000000000000000000000xx
Owner: cluster1-01
Package          Type      Description          Expiration
-----
NFS              license  NFS License         -
CIFS             license  CIFS License        -
iSCSI           license  iSCSI License       -
FCP              license  FCP License         -
SnapRestore      license  SnapRestore License -
SnapMirror       license  SnapMirror License  -
FlexClone        license  FlexClone License   -
SnapVault        license  SnapVault License   -
SnapManagerSuite license  SnapManagerSuite License -
```

Dans l'exemple, la licence SnapManager Suite est installée. Par conséquent, aucune opération de licence SnapCenter supplémentaire n'est requise.

Étape 3 : récupérer le numéro de série du contrôleur

Obtenez le numéro de série du contrôleur à l'aide de la ligne de commande ONTAP . Vous devez être administrateur de cluster sur le système FAS, AFF ou ASA pour obtenir votre numéro de série de licence basé sur le contrôleur.

Étapes

1. Connectez-vous au contrôleur à l'aide de la ligne de commande ONTAP.
2. Entrez la commande `system show -instance`, puis vérifiez les valeurs de sortie pour localiser le numéro de série du contrôleur.

Exemple de sortie

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Notez les numéros de série.

Étape 4 : récupérez le numéro de série de la licence basée sur le contrôleur

Si vous utilisez un stockage FAS, ASA ou AFF , vous pouvez récupérer la licence basée sur le contrôleur SnapCenter à partir du site de support NetApp avant de l'installer à l'aide de la ligne de commande ONTAP .

Avant de commencer

- Vous devez disposer d'identifiants de connexion valides au site du support NetApp.

Si vous ne saisissez pas d'informations d'identification valides, le système ne renvoie aucune information pour votre recherche.

- Vous devez disposer du numéro de série du contrôleur.

Étapes

1. Connectez-vous au "[Site de support NetApp](#)".
2. Accédez à **systèmes > licences logicielles**.
3. Dans la zone critères de sélection, assurez-vous que le numéro de série (situé à l'arrière de l'unité) est sélectionné, saisissez le numéro de série du contrôleur, puis sélectionnez **Go!**.

Software Licenses

Selection Criteria

Choose a method by which to search

▶ Serial Number (located on back of unit) ▾ Enter Value: Go!

Enter the Cluster Serial Number value without dashes.

- OR -

▶ Show Me All: Serial Numbers with Licenses ▾ For Company: Go!

La liste des licences du contrôleur spécifié s'affiche.

4. Recherchez et enregistrez la licence SnapCenter Standard ou SnapManager Suite.

Étape 5 : ajoutez une licence basée sur le contrôleur

Vous pouvez utiliser la ligne de commande ONTAP pour ajouter une licence basée sur un contrôleur SnapCenter lorsque vous utilisez des systèmes FAS, AFF ou ASA et que vous disposez d'une licence SnapCenter Standard ou SnapManager Suite.

Avant de commencer

- Vous devez être administrateur du cluster sur le système FAS, AFF ou ASA.
- Vous devez disposer de la licence SnapCenter Standard ou SnapManager Suite.

Description de la tâche

Si vous souhaitez installer SnapCenter en version d'essai avec un système de stockage FAS, AFF ou ASA, vous pouvez obtenir une licence d'évaluation Premium Bundle à installer sur votre contrôleur.

Si vous souhaitez installer SnapCenter sous forme d'essai, contactez votre ingénieur commercial pour obtenir

une licence d'évaluation du pack Premium pour l'installer sur votre contrôleur.

Étapes

1. Connectez-vous au cluster NetApp à l'aide de la ligne de commande ONTAP.
2. Ajoutez la clé de licence de SnapManager Suite :

```
system license add -license-code license_key
```

Cette commande est disponible au niveau de privilège admin.

3. Vérifiez que la licence SnapManager Suite est installée :

```
license show
```

Étape 6 : supprimez la licence d'essai

Si vous utilisez une licence SnapCenter Standard basée sur un contrôleur et que vous devez supprimer la licence d'essai basée sur la capacité (numéro de série se terminant par « 50 »), vous devez utiliser les commandes MySQL pour supprimer la licence d'essai manuellement. La licence d'essai ne peut pas être supprimée à l'aide de l'interface utilisateur de SnapCenter .



La suppression manuelle d'une licence d'essai n'est nécessaire que si vous utilisez une licence basée sur le contrôleur SnapCenter Standard.

Étapes

1. Sur le serveur SnapCenter, ouvrez une fenêtre PowerShell pour réinitialiser le mot de passe MySQL.
 - a. Exécutez l'applet de commande Open-SmConnection pour établir une connexion avec le serveur SnapCenter pour un compte SnapCenterAdmin.
 - b. Exécutez le mot de passe set-SmRepositoryPassword pour réinitialiser le mot de passe MySQL.

Pour plus d'informations sur les applets de commande, voir "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)" .

2. Ouvrez l'invite de commande et exécutez `mysql -u root -p` pour vous connecter à MySQL.

MySQL vous invite à saisir le mot de passe. Saisissez les informations d'identification fournies lors de la réinitialisation du mot de passe.

3. Supprimez la licence d'évaluation de la base de données :

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

Configuration de la haute disponibilité

Configurez les serveurs SnapCenter pour la haute disponibilité

Pour prendre en charge la haute disponibilité (HA) dans SnapCenter fonctionnant sous Windows ou Linux, vous pouvez installer l'équilibreur de charge F5. F5 permet au serveur SnapCenter de prendre en charge les configurations actif-passif dans un maximum de deux hôtes au même emplacement. Pour utiliser F5 Load Balancer dans

SnapCenter, vous devez configurer les serveurs SnapCenter et l'équilibreur de charge F5.

Vous pouvez également configurer l'équilibrage de la charge réseau (NLB) pour configurer la haute disponibilité SnapCenter. Vous devez configurer manuellement NLB hors de l'installation SnapCenter pour la haute disponibilité.

Pour les environnements cloud, vous pouvez configurer la haute disponibilité à l'aide d'Amazon Web Services (AWS) Elastic Load Balancing (ELB) et d'Azure load balancer.

Configurer la haute disponibilité à l'aide de F5

Pour obtenir des instructions sur la configuration des serveurs SnapCenter pour une haute disponibilité à l'aide de l'équilibreur de charge F5, reportez-vous à ["Comment configurer les serveurs SnapCenter pour la haute disponibilité à l'aide de F5 Load Balancer"](#) .

Vous devez être membre du groupe administrateurs locaux sur les serveurs SnapCenter (en plus d'être affecté au rôle SnapCenterAdmin) pour utiliser les applets de commande suivantes pour ajouter et supprimer des clusters F5 :

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

Pour plus d'informations, reportez-vous ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#) à .

Informations supplémentaires

- Après avoir installé et configuré SnapCenter pour la haute disponibilité, modifiez le raccourci du bureau SnapCenter pour pointer vers l'adresse IP du cluster F5.
- Si un basculement se produit entre les serveurs SnapCenter et s'il existe également une session SnapCenter existante, vous devez fermer le navigateur et vous reconnecter à SnapCenter.
- Dans la configuration de l'équilibreur de charge (NLB ou F5), si vous ajoutez un hôte partiellement résolu par l'hôte NLB ou F5 et si l'hôte SnapCenter n'est pas en mesure d'atteindre cet hôte, la page hôte SnapCenter bascule fréquemment entre les hôtes en panne et en cours d'exécution. Pour résoudre ce problème, vous devez vous assurer que les deux hôtes SnapCenter sont en mesure de résoudre l'hôte dans NLB ou F5.
- Les commandes SnapCenter pour les paramètres MFA doivent être exécutées sur tous les hôtes. La configuration des parties utilisatrices doit être effectuée dans le serveur Active Directory Federation Services (AD FS) à l'aide des détails du cluster F5. L'accès à l'interface utilisateur SnapCenter au niveau de l'hôte sera bloqué après l'activation de l'authentification multifacteur.
- Pendant le basculement, les paramètres du journal d'audit ne s'y reflètent pas sur le second hôte. Par conséquent, vous devez répéter manuellement les paramètres du journal d'audit sur l'hôte passif F5 lorsqu'il devient actif.

Configuration de la haute disponibilité à l'aide de l'équilibrage de la charge réseau (NLB)

Vous pouvez configurer l'équilibrage de la charge réseau (NLB) pour configurer la haute disponibilité SnapCenter. Vous devez configurer manuellement NLB hors de l'installation SnapCenter pour la haute disponibilité.

Pour plus d'informations sur la configuration de l'équilibrage de charge réseau (NLB) avec SnapCenter, reportez-vous ["Comment configurer NLB avec SnapCenter"](#) à la section .

Configuration de la haute disponibilité à l'aide d'AWS Elastic Load Balancing (ELB)

Vous pouvez configurer un environnement SnapCenter haute disponibilité dans Amazon Web Services (AWS) en configurant deux serveurs SnapCenter dans des zones de disponibilité distinctes (AZ) et en les configurant pour un basculement automatique. L'architecture comprend des adresses IP privées virtuelles, des tables de routage et la synchronisation entre les bases de données MySQL actives et de secours.

Étapes

1. Configurez l'IP de superposition privée virtuelle dans AWS. Pour plus d'informations, reportez-vous à ["Configurer l'IP de superposition privée virtuelle"](#)la .
2. Préparez votre hôte Windows
 - a. Forcer la priorité IPv4 au-dessus d'IPv6 :
 - Emplacement : HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
 - Clé : DisabledComponents
 - Tapez : REG_DWORD
 - Valeur : 0x20
 - b. Assurez-vous que les noms de domaine complets peuvent être résolus via DNS ou via la configuration de l'hôte local vers les adresses IPv4.
 - c. Assurez-vous qu'aucun proxy système n'est configuré.
 - d. Assurez-vous que le mot de passe administrateur est le même sur le serveur Windows lorsque vous utilisez une configuration sans Active Directory et que les serveurs ne se trouvent pas dans un domaine.
 - e. Ajoutez une adresse IP virtuelle sur les deux serveurs Windows.
3. Créez le cluster SnapCenter.
 - a. Démarrez PowerShell et connectez-vous à SnapCenter.

```
Open-SmConnection
```
 - b. Création du cluster.

```
Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator
```
 - c. Ajoutez le serveur secondaire.

```
Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator
```
 - d. Découvrez tous les détails sur la haute disponibilité.

```
Get-SmServerConfig
```
4. Créez la fonction Lambda pour ajuster la table de routage en cas d'indisponibilité du point de terminaison IP privé virtuel, contrôlé par AWS CloudWatch. Pour plus d'informations, reportez-vous à ["Créer une fonction Lambda"](#)la .
5. Créez un moniteur dans CloudWatch pour contrôler la disponibilité du terminal SnapCenter. Une alarme est configurée pour déclencher une fonction Lambda si le point final est inaccessible. La fonction Lambda ajuste la table de routage pour rediriger le trafic vers le serveur SnapCenter actif. Pour plus d'informations, reportez-vous à ["Créer des Canaries synthétiques"](#)la .
6. Implémenter un flux de travail en utilisant une fonction STEP comme alternative à la surveillance CloudWatch, ce qui réduit les temps de basculement. Le flux de travail comprend une fonction de sonde Lambda pour tester l'URL SnapCenter, une table DynamoDB pour le stockage des nombres de défaillances et la fonction pas à pas elle-même.
 - a. Utilisez une fonction lambda pour sonder l'URL SnapCenter. Pour plus d'informations, reportez-vous à ["Création de la fonction Lambda"](#)la .
 - b. Créez une table DynamoDB pour stocker le nombre de pannes entre deux itérations de fonction Step. Pour plus d'informations, reportez-vous à ["Commencez avec la table DynamoDB"](#)la .
 - c. Créer la fonction pas à pas. Pour plus d'informations, reportez-vous à ["Documentation des fonctions STEP"](#)la .

- d. Testez une seule étape.
- e. Tester le fonctionnement complet.
- f. Créer un rôle IAM et ajuster les autorisations à autoriser à exécuter la fonction Lambda.
- g. Créer un programme pour déclencher la fonction pas à pas. Pour plus d'informations, reportez-vous à "[Utilisation d'Amazon EventBridge Scheduler pour démarrer des fonctions Step](#)"la .

Configurez la haute disponibilité à l'aide de l'équilibreur de charge Azure

Vous pouvez configurer un environnement SnapCenter haute disponibilité à l'aide de l'équilibreur de charge Azure.

Étapes

1. Création de machines virtuelles dans un ensemble d'échelles à l'aide du portail Azure L'ensemble d'échelle des machines virtuelles Azure vous permet de créer et de gérer un groupe de machines virtuelles à charge équilibrée. Le nombre d'instances de machines virtuelles peut augmenter ou diminuer automatiquement en réponse à la demande ou à un planning défini. Pour plus d'informations, reportez-vous à "[Création de machines virtuelles dans un ensemble d'échelles à l'aide du portail Azure](#)"la .
2. Après avoir configuré les machines virtuelles, connectez-vous à chaque machine virtuelle dans le jeu de machines virtuelles et installez le serveur SnapCenter sur les deux nœuds.
3. Créer le cluster dans l'hôte 1.

```
Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
```
4. Ajoutez le serveur secondaire.

```
Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
```
5. Consultez les détails sur la haute disponibilité.

```
Get-SmServerConfig
```
6. Si nécessaire, reconstruisez l'hôte secondaire.

```
Set-SmRepositoryConfig -RebuildSlave -Verbose
```
7. Basculement vers le second hôte.

```
Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
```

== passer de NLB à F5 pour la haute disponibilité

Vous pouvez modifier votre configuration SnapCenter HA à partir de l'équilibrage de la charge du réseau (NLB) pour utiliser F5 Load Balancer.

Étapes

1. Configurez les serveurs SnapCenter pour une haute disponibilité à l'aide de F5. "[En savoir plus >>](#)".
2. Sur l'hôte SnapCenter Server, lancez PowerShell.
3. Démarrez une session à l'aide de la cmdlet Open-SmConnection, puis saisissez vos informations d'identification.
4. Mettez à jour le serveur SnapCenter pour qu'il pointe vers l'adresse IP du cluster F5 à l'aide de l'applet de commande Update-SmServerCluster.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions

peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Haute disponibilité pour le référentiel SnapCenter MySQL

La réplication MySQL est une fonctionnalité de MySQL Server qui vous permet de répliquer des données d'un serveur de base de données MySQL (maître) vers un autre serveur de base de données MySQL (esclave). SnapCenter prend en charge la réplication MySQL pour la haute disponibilité uniquement sur deux nœuds NLB (Network Load Balancing-Enabled).

SnapCenter effectue des opérations de lecture ou d'écriture sur le référentiel maître et achemine sa connexion vers le référentiel esclave en cas de défaillance sur le référentiel maître. Le référentiel esclave devient alors le référentiel maître. SnapCenter prend également en charge la réplication inverse, qui est activée uniquement pendant le basculement.

Si vous souhaitez utiliser la fonction haute disponibilité MySQL (HA), vous devez configurer Network Load Balancer (NLB) sur le premier nœud. Le référentiel MySQL est installé sur ce nœud dans le cadre de l'installation. Lors de l'installation de SnapCenter sur le second nœud, vous devez rejoindre la F5 du premier nœud et créer une copie du référentiel MySQL sur le second nœud.

SnapCenter fournit les applets de commande *get-SmRepositoryConfig* et *set-SmRepositoryConfig* PowerShell pour gérer la réplication MySQL.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Vous devez connaître les limitations liées à la fonctionnalité MySQL HA :

- NLB et MySQL HA ne sont pas pris en charge au-delà de deux nœuds.
- Le passage d'une installation autonome SnapCenter à une installation NLB ou vice versa et le passage d'une configuration autonome MySQL à MySQL à MySQL HA ne sont pas pris en charge.
- Le basculement automatique n'est pas pris en charge si les données du référentiel esclave ne sont pas synchronisées avec les données du référentiel maître.

Vous pouvez lancer un basculement forcé à l'aide de l'applet de commande *set-SmRepositoryConfig*.

- Lorsque le basculement est lancé, les tâches en cours d'exécution peuvent échouer.

Si le basculement se produit parce que le serveur MySQL ou SnapCenter est en panne, alors les travaux en cours d'exécution risquent d'échouer. Après le basculement vers le second nœud, toutes les tâches suivantes s'exécutent correctement.

Pour plus d'informations sur la configuration de la haute disponibilité, reportez-vous à la section "[Comment configurer NLB et ARR avec SnapCenter](#)".

Configuration du contrôle d'accès basé sur des rôles (RBAC)

Créer un rôle

En plus d'utiliser les rôles SnapCenter existants, vous pouvez créer vos propres rôles et personnaliser les autorisations.

Pour créer vos propres rôles, il est nécessaire de vous connecter en tant que rôle « SnapCenterAdmin ».

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **rôles**.
3. Cliquez sur **+**.
4. Spécifiez un nom et une description pour le nouveau rôle.



Seuls les caractères spéciaux suivants peuvent être utilisés dans les noms d'utilisateur et les noms de groupe : espace (), trait d'union (-), trait de soulignement (_) et deux points (:).

5. Select **tous les membres de ce rôle peuvent voir les objets d'autres membres** pour permettre aux autres membres du rôle d'afficher les ressources telles que les volumes et les hôtes après avoir actualisé la liste des ressources.

Vous devez désélectionner cette option si vous ne souhaitez pas que les membres de ce rôle voient les objets auxquels les autres membres sont affectés.



Lorsque cette option est activée, il n'est pas nécessaire d'attribuer aux utilisateurs un accès aux objets ou aux ressources si les utilisateurs appartiennent au même rôle que l'utilisateur qui a créé les objets ou les ressources.

6. Dans la page autorisations, sélectionnez les autorisations que vous souhaitez attribuer au rôle ou cliquez sur **Sélectionner tout** pour accorder toutes les autorisations au rôle.
7. Cliquez sur **soumettre**.

Ajoutez un rôle NetApp ONTAP RBAC à l'aide de commandes de connexion de sécurité

Vous pouvez utiliser les commandes de connexion de sécurité pour ajouter un rôle NetApp ONTAP RBAC lorsque vos systèmes de stockage exécutent clustered ONTAP.

Avant de commencer

- Identifiez la tâche (ou les tâches) que vous souhaitez effectuer et les privilèges requis pour effectuer ces tâches.
- Accorder des privilèges aux répertoires de commandes et/ou de commandes.

Il existe deux niveaux d'accès pour chaque répertoire de commande/commande : All-Access et read-only.

Vous devez toujours attribuer les privilèges All-Access en premier.

- Attribuez des rôles aux utilisateurs.
- Identifiez votre configuration selon que vos plug-ins SnapCenter sont connectés à l'IP de l'administrateur de cluster pour l'ensemble du cluster ou directement connectés à une SVM au sein du cluster.

Description de la tâche

Pour simplifier la configuration de ces rôles sur les systèmes de stockage, vous pouvez utiliser l'outil RBAC User Creator pour NetApp ONTAP, publié sur le forum des communautés NetApp.

Cet outil gère automatiquement la configuration correcte des privilèges ONTAP. Par exemple, l'outil RBAC User Creator for NetApp ONTAP ajoute automatiquement le Privileges dans le bon ordre afin que le Privileges tout accès apparaisse en premier. Si vous ajoutez d'abord les privilèges en lecture seule, puis ajoutez les privilèges All-Access, ONTAP marque les privilèges All-Access en tant que doublons et les ignore.



Si vous mettez ultérieurement à niveau SnapCenter ou ONTAP, vous devez exécuter à nouveau l'outil RBAC User Creator for NetApp ONTAP pour mettre à jour les rôles utilisateur que vous avez créés précédemment. Les rôles utilisateur créés pour une version antérieure de SnapCenter ou ONTAP ne fonctionnent pas correctement avec les versions mises à niveau. Lorsque vous exécutez de nouveau l'outil, il gère automatiquement la mise à niveau. Il n'est pas nécessaire de recréer les rôles.

Plus d'informations sur la configuration des rôles RBAC ONTAP, consultez le ["Guide de l'authentification de l'administrateur ONTAP 9 et de l'alimentation RBAC"](#).

Étapes

1. Sur le système de stockage, créez un nouveau rôle en entrant la commande suivante :

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

- svm_name est le nom du SVM. Si vous ne renseignez pas ce champ, l'administrateur de cluster est défini par défaut.
- nom_rôle est le nom que vous spécifiez pour le rôle.
- La commande correspond à la fonctionnalité ONTAP.



Vous devez répéter cette commande pour chaque autorisation. N'oubliez pas que les commandes All-Access doivent être répertoriées avant les commandes read-only.

Pour plus d'informations sur la liste des autorisations, reportez-vous à la section ["Commandes CLI ONTAP pour la création de rôles et l'attribution d'autorisations"](#).

2. Créez un nom d'utilisateur en entrant la commande suivante :

```
security login create -username <user_name\> -application ontapi -authmethod  
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment  
"user_description"
```

- nom_utilisateur est le nom de l'utilisateur que vous créez.
- <password> est votre mot de passe. Si vous ne spécifiez pas de mot de passe, le système vous en demandera un.
- svm_name est le nom du SVM.

3. Attribuez ce rôle à l'utilisateur en entrant la commande suivante :

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod <password\>
```

- <nom_utilisateur> est le nom de l'utilisateur que vous avez créé à l'étape 2. Cette commande vous

permet de modifier l'utilisateur pour l'associer au rôle.

- <svm_name> est le nom du SVM.
- <nom_rôle> est le nom du rôle que vous avez créé à l'étape 1.
- <password> est votre mot de passe. Si vous ne spécifiez pas de mot de passe, le système vous en demandera un.

4. Vérifiez que l'utilisateur a été créé correctement en entrant la commande suivante :

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

Nom_utilisateur est le nom de l'utilisateur que vous avez créé à l'étape 3.

Créez des rôles de SVM avec des privilèges minimaux

Il existe plusieurs commandes CLI ONTAP que vous devez exécuter lorsque vous créez un rôle pour un nouvel utilisateur SVM dans ONTAP. Ce rôle est requis si vous configurez des SVM dans ONTAP pour qu'ils soient utilisés avec SnapCenter et que vous ne souhaitez pas utiliser le rôle vsadmin.

Étapes

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>  
-cmddirname <permission\>
```



Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez-lui le rôle.

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Déverrouiller l'utilisateur.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

Commandes CLI ONTAP pour créer des rôles SVM et attribuer des autorisations

Vous devez exécuter plusieurs commandes ONTAP CLI pour créer des rôles SVM et attribuer des autorisations.

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"job show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
"job stop" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
"lun" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun igroup add" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun igroup create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun igroup delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun igroup rename" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun igroup show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun mapping add-reporting-nodes" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
"lun mapping create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun mapping delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun mapping remove-reporting-nodes" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun mapping show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun move-in-volume" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun offline" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun online" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun resize" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"lun serial" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"volume modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume offline" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume online" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume qtree show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume restrict" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot modify" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
"volume snapshot modify-snaplock-expiry-time" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot rename" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot restore" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot restore-file" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume snapshot show-delta" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"volume unmount" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"vserver cifs share create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
"vserver cifs share delete" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

- ```
"nvme namespace create" -access all
```
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
  - `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
  - `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`

## Création de rôles SVM pour les systèmes ASA r2

Plusieurs commandes de l'interface de ligne de commande ONTAP doivent être exécutées afin de créer un rôle pour un nouvel utilisateur SVM dans les systèmes ASA r2. Ce rôle est requis si vous configurez les SVM dans les systèmes ASA r2 afin qu'ils puissent être utilisés avec SnapCenter et que vous ne souhaitez pas utiliser le rôle vsadmin.

### Étapes

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```



Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez-lui le rôle.

```
security login create -user <user_name\> -vserver <svm_name\> -application
http -authmethod password -role <SVM_Role_Name\>
```

3. Déverrouiller l'utilisateur.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

### Commandes CLI ONTAP pour créer des rôles SVM et attribuer des autorisations

Vous devez exécuter plusieurs commandes ONTAP CLI pour créer des rôles SVM et attribuer des autorisations.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`

- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "lun" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname

"lun show" -access all

- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM\_Name -role SVM\_Role\_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "version" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume modify" -access all

- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM\_name -role SVM\_Role\_Name -cmddirname

```

"vserver cifs share show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver cifs show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver export-policy create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver export-policy delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver export-policy rule create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver export-policy rule show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver export-policy show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "vserver iscsi connection show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver" -access readonly
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver export-policy" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "vserver iscsi" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "volume clone split status" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
 "volume managed-feature" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem map" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem create" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem delete" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem modify" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem host" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem controller" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme subsystem show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
 "nvme namespace create" -access all

```

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

### Créez des rôles de cluster ONTAP avec des privilèges minimaux

Vous devez créer un rôle de cluster ONTAP avec des privilèges minimaux afin de ne pas avoir à utiliser le rôle d'administrateur ONTAP pour effectuer des opérations dans SnapCenter. Vous pouvez exécuter plusieurs commandes de l'interface de ligne de commandes ONTAP pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

#### Étapes

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

```
security login role create -vserver <cluster_name>- role <role_name>
-cmddirname <permission>
```



Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez-lui le rôle.

```
security login create -user <user_name> -vserver <cluster_name> -application
ontapi http -authmethod password -role <role_name>
```

3. Déverrouiller l'utilisateur.

```
security login unlock -user <user_name> -vserver <cluster_name>
```

## Commandes CLI ONTAP permettant de créer des rôles de cluster et d'attribuer des autorisations

Vous devez exécuter plusieurs commandes CLI ONTAP pour créer des rôles de cluster et attribuer des autorisations.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"nvme subsystem modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme subsystem host" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme subsystem controller" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme subsystem show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme namespace create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme namespace delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme namespace modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "nvme namespace show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "security login" -access readonly
• security login role create -role Role_Name -cmddirname "snapmirror create"
 -vserver Cluster_name -access all
• security login role create -role Role_Name -cmddirname "snapmirror list-
 destinations" -vserver Cluster_name -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy add-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy modify-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy remove-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror show-history" -access all

```

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "version" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"volume snapshot modify-snaplock-expiry-time" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume offline" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume online" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume qtree create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume qtree delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume qtree modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume qtree show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume restrict" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot promote" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot rename" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot restore-file" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot show-delta" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume unmount" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs create" -access all

```

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "vserver show" -access all

## Créez des rôles de cluster ONTAP pour les systèmes ASA r2

Vous devez créer un rôle de cluster ONTAP avec des privilèges minimaux afin de ne pas

avoir à utiliser le rôle d'administrateur ONTAP pour effectuer des opérations dans SnapCenter. Vous pouvez exécuter plusieurs commandes de l'interface de ligne de commandes ONTAP pour créer le rôle de cluster ONTAP et attribuer des privilèges minimaux.

## Étapes

1. Sur le système de stockage, créez un rôle et attribuez toutes les autorisations au rôle.

```
security login role create -vserver <cluster_name\>- role <role_name\>
-cmddirname <permission\>
```



Vous devez répéter cette commande pour chaque autorisation.

2. Créez un utilisateur et attribuez-lui le rôle.

```
security login create -user <user_name\> -vserver <cluster_name\> -application
http -authmethod password -role <role_name\>
```

3. Déverrouiller l'utilisateur.

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

## Commandes CLI ONTAP permettant de créer des rôles de cluster et d'attribuer des autorisations

Vous devez exécuter plusieurs commandes CLI ONTAP pour créer des rôles de cluster et attribuer des autorisations.

- security login role create -vserver Cluster\_name or cluster\_name -role Role\_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster\_name or cluster\_name -role Role\_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```
"job stop" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun igroup add" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun igroup create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun igroup delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun igroup modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun igroup rename" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun igroup show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun mapping add-reporting-nodes" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun mapping create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun mapping delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun mapping remove-reporting-nodes" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun mapping show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun move-in-volume" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun persistent-reservation clear" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "lun resize" -access all
```

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "security login" -access readonly
- security login role create -role Role\_Name -cmddirname "snapmirror create" -vserver Cluster\_name -access all
- security login role create -role Role\_Name -cmddirname "snapmirror list-destinations" -vserver Cluster\_name -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"snapmirror policy add-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy modify-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy remove-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror show-history" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror update" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "snapmirror update-ls-set" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system license add" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system license clean-up" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system license delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system license show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system license status show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system node modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system node show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "system status show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "version" -access all

```

- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster\_name -role Role\_Name -cmddirname

```

"volume snapshot modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot promote" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot rename" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot restore-file" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume snapshot show-delta" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "volume unmount" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs share modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs share create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs share delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs share modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs share show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver cifs show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver export-policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
 "vserver export-policy delete" -access all

```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all`

### Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources

Pour configurer le contrôle d'accès basé sur des rôles pour les utilisateurs SnapCenter, vous pouvez ajouter des utilisateurs ou des groupes et attribuer un rôle. Le rôle détermine les options auxquelles les utilisateurs de SnapCenter peuvent accéder.

#### Avant de commencer

- Vous devez avoir ouvert une session en tant que rôle « SnapCenterAdmin ».
- Vous devez avoir créé les comptes utilisateur ou groupe dans Active Directory dans le système d'exploitation ou la base de données. Vous ne pouvez pas utiliser SnapCenter pour créer ces comptes.



Vous ne pouvez inclure que les caractères spéciaux suivants dans les noms d'utilisateur et de groupe : espace ( ), tiret (-), trait de soulignement (\_) et deux-points (:).

- SnapCenter inclut plusieurs rôles prédéfinis.

Vous pouvez soit attribuer ces rôles à l'utilisateur, soit créer de nouveaux rôles.

- Les utilisateurs AD et les groupes AD qui sont ajoutés au RBAC SnapCenter doivent disposer de l'autorisation DE LECTURE sur le conteneur d'utilisateurs et le conteneur d'ordinateurs dans Active

Directory.

- Après avoir affecté un rôle à un utilisateur ou à un groupe qui contient les autorisations appropriées, vous devez attribuer l'accès de l'utilisateur aux ressources SnapCenter, telles que les hôtes et les connexions de stockage.

Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

- Vous devez à un moment ou à un autre attribuer un rôle à l'utilisateur ou au groupe afin de tirer profit des autorisations et des fonctionnalités d'efficacité RBAC.
- Vous pouvez affecter des ressources comme hôte, groupes de ressources, stratégie, connexion au stockage, plug-in, et les informations d'identification à l'utilisateur lors de la création de l'utilisateur ou du groupe.
- Les ressources minimales que vous devez affecter à un utilisateur pour effectuer certaines opérations sont les suivantes :

| Fonctionnement                | Affectation des ressources            |
|-------------------------------|---------------------------------------|
| Protéger les ressources       | hôte, règle                           |
| Sauvegarde                    | hôte, groupe de ressources, stratégie |
| Restaurer                     | hôte, groupe de ressources            |
| Clonage                       | hôte, groupe de ressources, stratégie |
| Cycle de vie des clones       | hôte                                  |
| Créer un groupe de ressources | hôte                                  |

- Lorsqu'un nouveau nœud est ajouté à un cluster Windows ou à un actif DAG (Groupe de disponibilité de la base de données Exchange Server) et si ce nouveau nœud est affecté à un utilisateur, vous devez réassigner le bien à l'utilisateur ou au groupe pour inclure le nouveau nœud à l'utilisateur ou au groupe.

Vous devez réassigner l'utilisateur ou le groupe RBAC au cluster ou au DAG pour inclure le nouveau nœud à l'utilisateur ou au groupe RBAC. Par exemple, vous avez un cluster à deux nœuds et avez affecté un utilisateur ou un groupe RBAC au cluster. Lorsque vous ajoutez un autre nœud au cluster, vous devez réattribuer l'utilisateur ou le groupe RBAC au cluster afin d'inclure le nouveau nœud pour l'utilisateur ou le groupe RBAC.

- Si vous prévoyez de répliquer des snapshots, vous devez attribuer la connexion de stockage pour le volume source et le volume de destination à l'utilisateur qui effectue l'opération.

Vous devez ajouter des ressources avant d'attribuer l'accès aux utilisateurs.



Si vous utilisez le plug-in SnapCenter pour les fonctions VMware vSphere pour protéger les machines virtuelles, les VMDK ou les datastores, vous devez utiliser l'interface graphique de VMware vSphere pour ajouter un utilisateur vCenter à un rôle de plug-in SnapCenter pour VMware vSphere. Pour plus d'informations sur les rôles VMware vSphere, reportez-vous à la section ["Rôles prédéfinis avec le plug-in SnapCenter pour VMware vSphere"](#).

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **utilisateurs et accès** > **+**.
3. Dans la page Ajouter des utilisateurs/groupes à partir d'Active Directory ou Workgroup :

| Pour ce champ...  | Procédez comme ça...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type d'accès      | <p>Sélectionnez domaine ou groupe de travail</p> <p>Pour le type d'authentification de domaine, vous devez spécifier le nom de domaine de l'utilisateur ou du groupe auquel vous souhaitez ajouter l'utilisateur à un rôle.</p> <p>Par défaut, il est pré-rempli avec le nom de domaine connecté.</p> <p> Vous devez enregistrer le domaine non approuvé dans la page <b>Paramètres</b> &gt; <b>Paramètres globaux</b> &gt; <b>Paramètres de domaine</b>.</p>                                                                                                                                                                                   |
| Type              | <p>Sélectionnez utilisateur ou Groupe</p> <p> SnapCenter prend uniquement en charge le groupe de sécurité, et non le groupe de distribution.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Nom d'utilisateur | <p>a. Saisissez le nom d'utilisateur partiel, puis cliquez sur <b>Ajouter</b>.</p> <p> Le nom d'utilisateur est sensible à la casse.</p> <p>b. Sélectionnez le nom d'utilisateur dans la liste de recherche.</p> <p> Lorsque vous ajoutez des utilisateurs d'un domaine différent ou d'un domaine non fiable, vous devez saisir le nom d'utilisateur entièrement car il n'existe aucune liste de recherche pour les utilisateurs d'un domaine à l'autre.</p> <p>Répétez cette étape pour ajouter d'autres utilisateurs ou groupes au rôle sélectionné.</p> |

| Pour ce champ... | Procédez comme ça...                                              |
|------------------|-------------------------------------------------------------------|
| Rôles            | Sélectionnez le rôle auquel vous souhaitez ajouter l'utilisateur. |

4. Cliquez sur **attribuer**, puis sur la page affecter des ressources :
  - a. Sélectionnez le type de ressource dans la liste déroulante **Asset**.
  - b. Dans le tableau actif, sélectionnez l'actif.

Les ressources sont répertoriées uniquement si l'utilisateur a ajouté les ressources à SnapCenter.

- c. Répétez cette procédure pour tous les actifs requis.
  - d. Cliquez sur **Enregistrer**.
5. Cliquez sur **soumettre**.

Après avoir ajouté des utilisateurs ou des groupes et affecté des rôles, actualisez la liste des ressources.

## Configurer les paramètres du journal d'audit

Des journaux d'audit sont générés pour chaque activité du serveur SnapCenter. Par défaut, les journaux d'audit sont sécurisés à l'emplacement d'installation par défaut *C:\Program Files\NetApp\SnapCenter WebApp\audit\*.

Les journaux d'audit sont sécurisés par la génération d'un résumé signé numériquement pour chaque événement d'audit afin de les protéger contre les modifications non autorisées. Les données de résumé générées sont conservées dans le fichier de somme de contrôle d'audit distinct et l'intégrité est soumise à des contrôles périodiques pour assurer l'intégrité du contenu.

Vous devriez avoir ouvert une session en tant que rôle « SnapCenterAdmin ».

### Description de la tâche

- Les alertes sont envoyées dans les scénarios suivants :
  - Le programme de vérification de l'intégrité du journal d'audit ou le serveur Syslog est activé ou désactivé
  - Vérification de l'intégrité du journal d'audit, journal d'audit ou échec du journal du serveur Syslog
  - Espace disque faible
- L'e-mail est envoyé uniquement en cas d'échec du contrôle d'intégrité.
- Vous devez modifier les chemins d'accès du répertoire du journal d'audit et du répertoire du journal de la somme de contrôle d'audit ensemble. Vous ne pouvez modifier qu'une seule d'entre elles.
- Lorsque les chemins du répertoire du journal d'audit et du répertoire du journal de la somme de contrôle d'audit sont modifiés, la vérification d'intégrité ne peut pas être effectuée sur les journaux d'audit présents à l'emplacement précédent.
- Les chemins du répertoire du journal d'audit et du répertoire du journal de la somme de contrôle d'audit doivent se trouver sur le disque local du serveur SnapCenter.

Les lecteurs partagés ou montés sur le réseau ne sont pas pris en charge.

- Si le protocole UDP est utilisé dans les paramètres du serveur Syslog, les erreurs dues au port sont en panne ou ne peuvent pas être capturées comme une erreur ou une alerte dans SnapCenter.
- Vous pouvez utiliser les commandes `set-SmAuditSettings` et `Get-SmAuditSettings` pour configurer les journaux d'audit.

Les informations concernant les paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `Get-Help nom_commande`. Vous pouvez également vous référer au ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Étapes

1. Dans la page **Paramètres**, accédez à **Paramètres > Paramètres globaux > Paramètres du journal d'audit**.
2. Dans la section Journal d'audit, entrez les détails.
3. Entrez le répertoire **Audit log** et le répertoire **Audit checksum log**
  - a. Entrez la taille maximale du fichier
  - b. Entrez le nombre maximal de fichiers journaux
  - c. Entrez le pourcentage d'utilisation de l'espace disque pour envoyer une alerte
4. (Facultatif) Activer **Log UTC Time**.
5. (Facultatif) activez **Audit Log Integrity Check Schedule** et cliquez sur **Start Integrity Check** pour vérifier l'intégrité à la demande.

Vous pouvez également exécuter la commande **Start-SmAuditIntegrityCheck** pour lancer le contrôle d'intégrité à la demande.

6. (Facultatif) activez les journaux d'audit transmis au serveur syslog distant et entrez les détails du serveur Syslog.

Vous devez importer le certificat depuis le serveur Syslog vers la racine de confiance pour le protocole TLS 1.2.

- a. Entrez l'hôte du serveur Syslog
  - b. Entrez le port du serveur Syslog
  - c. Entrez le protocole du serveur Syslog
  - d. Entrez le format RFC
7. Cliquez sur **Enregistrer**.
  8. Vous pouvez voir les vérifications d'intégrité des audits et les vérifications de l'espace disque en cliquant sur **Monitor > Jobs**.

## Configurez les connexions MySQL sécurisées avec le serveur SnapCenter

Vous pouvez générer des certificats SSL (Secure Sockets Layer) et des fichiers clés si vous souhaitez sécuriser la communication entre le serveur SnapCenter et le serveur MySQL dans des configurations autonomes ou dans des configurations NLB (Network Load Balancing).

## Configurez des connexions MySQL sécurisées pour des configurations serveur SnapCenter autonomes

Vous pouvez générer des certificats SSL (Secure Sockets Layer) et des fichiers de clés, si vous souhaitez sécuriser la communication entre le serveur SnapCenter et le serveur MySQL. Vous devez configurer les certificats et les fichiers de clé dans le serveur MySQL et le serveur SnapCenter.

Les certificats suivants sont générés :

- Certificat CA
- Certificat public du serveur et fichier de clé privée
- Certificat public et fichier de clé privée du client

### Étapes

1. Configurez les certificats SSL et les fichiers de clé pour les serveurs et les clients MySQL sous Windows à l'aide de la commande openssl.

Pour plus d'informations, reportez-vous à la section ["MySQL version 5.7 : création de certificats et de clés SSL à l'aide d'openssl"](#)



La valeur de nom commune utilisée pour le certificat de serveur, le certificat client et les fichiers de clé doit être différente de la valeur de nom commune utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom communes sont les mêmes, les fichiers de certificat et de clé échouent pour les serveurs compilés à l'aide d'OpenSSL.

**Meilleure pratique:** vous devez utiliser le nom de domaine complet (FQDN) du serveur comme nom commun pour le certificat de serveur.

2. Copiez les certificats SSL et les fichiers de clés dans le dossier MySQL Data.

Le chemin par défaut du dossier de données MySQL est

C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.

3. Mettez à jour le certificat CA, le certificat public du serveur, le certificat public du client, la clé privée du serveur et les chemins de clé privée du client dans le fichier de configuration du serveur MySQL (my.ini).

Le chemin par défaut du fichier de configuration du serveur MySQL (my.ini) est

C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini.



Vous devez spécifier le certificat CA, le certificat public du serveur et les chemins de clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

Vous devez spécifier le certificat CA, le certificat public du client et les chemins de clé privée du client dans la section [client] du fichier de configuration du serveur MySQL (my.ini).

L'exemple suivant montre les certificats et les fichiers de clé copiés dans la section [mysqld] du fichier my.ini dans le dossier par défaut C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Arrêtez l'application Web du serveur SnapCenter dans Internet Information Server (IIS).
5. Redémarrez le service MySQL.
6. Mettez à jour la valeur de la clé MySQLProtocol dans le fichier SnapManager.Web.UI.dll.config.

L'exemple suivant montre la valeur de la clé MySQLProtocol mise à jour dans le fichier SnapManager.Web.UI.dll.config.

```
<add key="MySQLProtocol" value="SSL" />
```

7. Mettez à jour le fichier SnapManager.Web.UI.dll.config avec les chemins fournis dans la section [client] du fichier my.ini.

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. Démarrez l'application Web du serveur SnapCenter dans IIS.

## Configurez les connexions MySQL sécurisées pour les configurations haute disponibilité

Si vous souhaitez sécuriser la communication entre le serveur SnapCenter et les serveurs MySQL, vous pouvez générer des certificats SSL (Secure Sockets Layer) et des fichiers clés pour les nœuds HA (High Availability). Vous devez configurer les certificats et les fichiers de clé dans les serveurs MySQL et sur les nœuds HA.

Les certificats suivants sont générés :

- Certificat CA

Un certificat d'autorité de certification est généré sur l'un des nœuds HA, et ce certificat est copié sur l'autre nœud HA.

- Les fichiers de clés privées de serveur et de certificat public pour les deux nœuds HA
- Certificat public du client et fichiers de clé privée du client pour les deux nœuds HA

### Étapes

1. Pour le premier nœud HA, configurez les certificats SSL et les fichiers clés pour les serveurs et les clients MySQL sur Windows à l'aide de la commande `openssl`.

Pour plus d'informations, reportez-vous à la section ["MySQL version 5.7 : création de certificats et de clés SSL à l'aide d'openssl"](#)



La valeur de nom commune utilisée pour le certificat de serveur, le certificat client et les fichiers de clé doit être différente de la valeur de nom commune utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom communes sont les mêmes, les fichiers de certificat et de clé échouent pour les serveurs compilés à l'aide d'OpenSSL.

**Meilleure pratique:** vous devez utiliser le nom de domaine complet (FQDN) du serveur comme nom commun pour le certificat de serveur.

2. Copiez les certificats SSL et les fichiers de clés dans le dossier MySQL Data.

Le chemin par défaut du dossier MySQL Data est `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Mettez à jour le certificat CA, le certificat public du serveur, le certificat public du client, la clé privée du serveur et les chemins de clé privée du client dans le fichier de configuration du serveur MySQL (`my.ini`).

Le chemin par défaut du fichier de configuration du serveur MySQL (`my.ini`) est `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.



Vous devez spécifier le certificat CA, le certificat public du serveur et les chemins de clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

Vous devez spécifier le certificat CA, le certificat public du client et les chemins de clé privée du client dans la section [client] du fichier de configuration du serveur MySQL (my.ini).

L'exemple suivant montre les certificats et les fichiers de clé copiés dans la section [mysqld] du fichier my.ini dans le dossier par défaut C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-
key.pem"
```

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-
key.pem"
```

4. Pour le second nœud HA, copiez le certificat de l'autorité de certification et générez le certificat public du serveur, les fichiers de clé privée du serveur, le certificat public client et les fichiers de clé privée du client. effectuez les opérations suivantes :

- a. Copiez le certificat CA généré sur le premier nœud HA vers le dossier MySQL Data du second nœud NLB.

Le chemin par défaut du dossier MySQL Data est C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\.



Vous ne devez pas créer de nouveau un certificat CA. Vous ne devez créer que le certificat public du serveur, le certificat public du client, le fichier de clé privée du serveur et le fichier de clé privée du client.

- b. Pour le premier nœud HA, configurez les certificats SSL et les fichiers clés pour les serveurs et les clients MySQL sur Windows à l'aide de la commande openssl.

#### "MySQL version 5.7 : création de certificats et de clés SSL à l'aide d'openssl"



La valeur de nom commune utilisée pour le certificat de serveur, le certificat client et les fichiers de clé doit être différente de la valeur de nom commune utilisée pour le certificat de l'autorité de certification. Si les valeurs de nom communes sont les mêmes, les fichiers de certificat et de clé échouent pour les serveurs compilés à l'aide d'OpenSSL.

Il est recommandé d'utiliser le FQDN du serveur comme nom commun pour le certificat du serveur.

- c. Copiez les certificats SSL et les fichiers de clés dans le dossier MySQL Data.
- d. Mettez à jour le certificat CA, le certificat public du serveur, le certificat public du client, la clé privée du serveur et les chemins de clé privée du client dans le fichier de configuration du serveur MySQL (my.ini).



Vous devez spécifier le certificat CA, le certificat public du serveur et les chemins de clé privée du serveur dans la section [mysqld] du fichier de configuration du serveur MySQL (my.ini).

Vous devez spécifier le certificat CA, le certificat public du client et les chemins de clé privée du client dans la section [client] du fichier de configuration du serveur MySQL (my.ini).

L'exemple suivant montre les certificats et les fichiers de clé copiés dans la section [mysqld] du fichier my.ini dans le dossier par défaut C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

L'exemple suivant montre les chemins mis à jour dans la section [client] du fichier my.ini.

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

5. Arrêtez l'application Web du serveur SnapCenter dans Internet Information Server (IIS) sur les deux nœuds HA.
6. Redémarrez le service MySQL sur les deux nœuds HA.
7. Mettez à jour la valeur de la clé MySQLProtocol dans le fichier SnapManager.Web.UI.dll.config pour les deux nœuds HA.

L'exemple suivant montre la valeur de la clé MySQLProtocol mise à jour dans le fichier SnapManager.Web.UI.dll.config.

```
<add key="MySQLProtocol" value="SSL" />
```

8. Mettez à jour le fichier SnapManager.Web.UI.dll.config avec les chemins que vous avez spécifiés dans la section [client] du fichier my.ini pour les deux nœuds HA.

L'exemple suivant montre les chemins mis à jour dans la section [client] des fichiers my.ini.

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem" />
```

9. Démarrez l'application Web du serveur SnapCenter dans IIS sur les deux nœuds HA.
10. Utilisez l'applet de commande Set-SmRepositoryConfig -Rebuildslave -Force PowerShell avec l'option -Force sur l'un des nœuds HA pour établir une réplique MySQL sécurisée sur les deux nœuds HA.

Même si l'état de réplique est sain, l'option -Force vous permet de reconstruire le référentiel esclave.

## Configurer l'authentification basée sur un certificat

L'authentification basée sur certificat améliore la sécurité en vérifiant l'identité du serveur SnapCenter et des hôtes de plug-in, garantissant ainsi une communication sécurisée et chiffrée.

## Activer l'authentification basée sur un certificat

Pour activer l'authentification basée sur certificat pour le serveur SnapCenter et les hôtes de plug-in Windows, exécutez l'applet de commande PowerShell suivante. Pour les hôtes plug-in Linux, l'authentification basée sur certificat sera activée lorsque vous activez le protocole SSL bidirectionnel.

- Pour activer l'authentification basée sur un certificat client :

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- Pour désactiver l'authentification basée sur des certificats client :

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname] `
```

## Exporter des certificats d'autorité de certification (CA) depuis le serveur SnapCenter

Vous devez exporter les certificats d'autorité de certification du serveur SnapCenter vers les hôtes de plug-in à l'aide de la console MMC (Microsoft Management Console).

### Avant de commencer

Vous devez avoir configuré le protocole SSL bidirectionnel.

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats - ordinateur local > personnel > certificats**.
5. Cliquez avec le bouton droit de la souris sur le certificat CA fourni, qui est utilisé pour le serveur SnapCenter, puis sélectionnez **toutes les tâches > Exporter** pour lancer l'assistant d'exportation.
6. Effectuez les actions suivantes dans l'assistant.

Pour cette option...	Procédez comme suit...
Exporter la clé privée	Sélectionnez <b>non, ne pas exporter la clé privée</b> , puis cliquez sur <b>Suivant</b> .
Exporter le format de fichier	Cliquez sur <b>Suivant</b> .
Nom du fichier	Cliquez sur <b>Parcourir</b> et spécifiez le chemin d'accès au fichier pour enregistrer le certificat, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'exportation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'exportation.



L'authentification basée sur certificat n'est pas prise en charge pour les configurations SnapCenter HA et le plug-in SnapCenter pour VMware vSphere.

## Importez le certificat de l'autorité de certification sur les hôtes du plug-in Windows

Pour utiliser le certificat de l'autorité de certification du serveur SnapCenter exporté, vous devez importer le certificat associé sur les hôtes du plug-in Windows SnapCenter à l'aide de la console MMC (Microsoft Management Console).

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats - ordinateur local > personnel > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "personnel", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Effectuez les actions suivantes dans l'assistant.

Pour cette option...	Procédez comme suit...
Emplacement du magasin	Cliquez sur <b>Suivant</b> .
Fichier à importer	Sélectionnez le certificat du serveur SnapCenter qui se termine par l'extension <b>.cer</b> .
Magasin de certificats	Cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'exportation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.

## Importez le certificat CA sur les hôtes du plug-in UNIX

Vous devez importer le certificat de l'autorité de certification sur les hôtes du plug-in UNIX.

### À propos de cette tâche

- Vous pouvez gérer le mot de passe de la base de stockage de clés SPL et l'alias de la paire de clés signées CA utilisée.
- Le mot de passe de la base de stockage de clés SPL et de tous les mots de passe alias associés à la clé privée doit être le même.

### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés SPL dans le fichier de propriétés SPL. Il s'agit de la valeur correspondant à la clé `SPL_KEYSTORE_PASS`.
2. Modifiez le mot de passe du magasin de clés :

```
$ keytool -storepasswd -keystore keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :  

```
$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```
4. Mettez à jour la même chose pour la clé `SPL_KEYSTORE_PASS` dans `spl.properties`` fichier.
5. Redémarrez le service après avoir modifié le mot de passe.

## Configurez les certificats racine ou intermédiaire sur le magasin de confiance SPL

Vous devez configurer les certificats racine ou intermédiaire dans le magasin de confiance SPL. Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Étapes

1. Accédez au dossier contenant le magasin de clés SPL : `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier `keystore.jks`.
3. Répertoriez les certificats ajoutés dans le magasin de clés :  

```
$ keytool -list -v -keystore keystore.jks
```
4. Ajouter un certificat racine ou intermédiaire :  

```
$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks
```
5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaire sur le stockage de confiance SPL.

## Configurez la paire de clés signée CA sur le magasin de confiance SPL

Vous devez configurer la paire de clés signées par l'autorité de certification dans le magasin de confiance SPL.

### Étapes

1. Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier `keystore.jks``.
3. Répertoriez les certificats ajoutés dans le magasin de clés :  

```
$ keytool -list -v -keystore keystore.jks
```
4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.  

```
$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```
5. Répertorier les certificats ajoutés dans le magasin de clés.  

```
$ keytool -list -v -keystore keystore.jks
```
6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe par défaut de la SPL keystore est la valeur de la clé `SPL_KEYSTORE_PASS` in

spl.properties fichier.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

8. Si le nom d'alias du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("\*", ",", ";"), remplacez le nom d'alias par un nom simple :

```
$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>"
-keystore keystore.jks`
```

9. Configurez le nom d'alias à partir du magasin de clés situé dans spl.properties fichier. Mettez à jour cette valeur par rapport à la clé SPL\_CERTIFICATE\_ALIAS.
10. Redémarrez le service après avoir configuré la paire de clés signée CA dans la boutique de confiance SPL.

## Exporter les certificats SnapCenter

Vous devez exporter les certificats SnapCenter au format .pfx.

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer composant logiciel enfichable**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **mon compte utilisateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > Certificates - Current User > Trusted Root Certification autorités > Certificates**.
5. Cliquez avec le bouton droit de la souris sur le certificat dont le nom est convivial SnapCenter, puis sélectionnez **toutes les tâches > Exporter** pour lancer l'assistant d'exportation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Exporter la clé privée	Sélectionnez l'option <b>Oui, exportez la clé privée</b> , puis cliquez sur <b>Suivant</b> .
Exporter le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Fichier à exporter	Spécifiez un nom de fichier pour le certificat exporté (vous devez utiliser .pfx), puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'exportation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'exportation.

# Configurer le certificat CA pour l'hôte Windows

## Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

## Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

## Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :

- a. Double-cliquez sur le certificat.
- b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
- c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
- d. Copiez les caractères hexadécimaux de la zone.
- e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :

- a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

## Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA

sont déjà déployés.

## Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Configuration du certificat d'autorité de certification avec le site SnapCenter

Vous devez configurer le certificat d'autorité de certification avec le site SnapCenter sur l'hôte Windows.

### Étapes

1. Ouvrez le Gestionnaire IIS sur le serveur Windows sur lequel SnapCenter est installé.
2. Dans le volet de navigation de gauche, cliquez sur **connexions**.
3. Développez le nom du serveur et **sites**.
4. Sélectionnez le site Web SnapCenter sur lequel vous souhaitez installer le certificat SSL.
5. Accédez à **actions** > **Modifier le site**, cliquez sur **liaisons**.
6. Dans la page liaisons, sélectionnez **Reliure pour https**.
7. Cliquez sur **Modifier**.
8. Dans la liste déroulante certificat SSL, sélectionnez le certificat SSL récemment importé.
9. Cliquez sur **OK**.



Le site du planificateur SnapCenter (port par défaut : 8154, HTTPS) est configuré avec un certificat auto-signé. Ce port communique avec l'hôte du serveur SnapCenter et il n'est pas obligatoire de le configurer avec un certificat CA. Toutefois, si votre environnement vous oblige à utiliser un certificat CA, répétez les étapes 5 à 9 à l'aide du site Planificateur SnapCenter.



Si le certificat de l'autorité de certification récemment déployé n'apparaît pas dans le menu déroulant, vérifiez si le certificat de l'autorité de certification est associé à la clé privée.



Assurez-vous que le certificat est ajouté à l'aide du chemin suivant : **racine de la console > certificats – ordinateur local > autorités de certification racine de confiance > certificats.**

## Activez les certificats CA pour SnapCenter

Vous devez configurer les certificats d'autorité de certification et activer la validation du certificat d'autorité de certification pour le serveur SnapCenter.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour le serveur SnapCenter à l'aide de l'applet de commande `Get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

### Étapes

1. Dans la page Paramètres, accédez à **Paramètres > Paramètres globaux > Paramètres de certificat CA**.
2. Sélectionnez **Activer la validation de certificat**.
3. Cliquez sur **appliquer**.

### Après la fin

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

- \* Indique qu'aucun certificat d'autorité de certification n'est activé ou attribué à l'hôte du plug-in.
- \* \* Indique que le certificat de l'autorité de certification a été validé avec succès.
- \* \* Indique que le certificat de l'autorité de certification n'a pas pu être validé.
- \* indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

# Configurer le certificat CA pour l'hôte Linux

Après avoir installé le serveur SnapCenter sous Linux, le programme d'installation crée le certificat auto-signé. Si vous souhaitez utiliser le certificat de l'autorité de certification, vous devez configurer les certificats pour le proxy inverse nginx, la journalisation d'audit et les services SnapCenter.

## Configurer le certificat nginx

### Étapes

1. Accédez à `/etc/nginx/conf.d` : `cd /etc/nginx/conf.d`
2. Ouvrez **snapcenter.conf** à l'aide de vi ou de n'importe quel éditeur de texte.
3. Accédez à la section serveur du fichier de configuration.
4. Modifiez les chemins de `ssl_certificate` et `ssl_certificate_key` pour pointer vers le certificat de l'autorité de certification.
5. Enregistrez et fermez le fichier.
6. Recharger nginx : `$nginx -s reload`

## Configurer le certificat du journal d'audit

### Étapes

1. Ouvrez `INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config` à l'aide de vi ou de tout éditeur de texte.

La valeur par défaut de `INSTALL_DIR` est `/opt`.

2. Modifiez les clés **AUDILOG\_CERTIFICATE\_PATH** et **AUDILOG\_CERTIFICATE\_PASSWORD** pour inclure respectivement le chemin d'accès au certificat de l'autorité de certification et le mot de passe.

Seul le format `.pfx` est pris en charge pour le certificat de journal d'audit.

3. Enregistrez et fermez le fichier.
4. Redémarrez le service **snapmanagerweb** : `$ systemctl restart snapmanagerweb`

## Configurer le certificat des services SnapCenter

### Étapes

1. Ouvrez les fichiers de configuration suivants à l'aide de vi ou de n'importe quel éditeur de texte.
  - `INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`
  - `INSTALL_DIR/NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config`
  - `INSTALL_DIR/NetApp/snapcenter/Scheduler/Scheduler.API.dll.config`

La valeur par défaut de `INSTALL_DIR` est `/opt`.

2. Modifiez les clés **SERVICE\_CERTIFICATE\_PATH** et **SERVICE\_CERTIFICATE\_PASSWORD** pour inclure respectivement le chemin du certificat de l'autorité de certification et le mot de passe.

Seul le format `.pfx` est pris en charge pour le certificat de services SnapCenter.

3. Enregistrez et fermez les fichiers.
4. Redémarrez tous les services.
  - `$ systemctl restart snapmanagerweb`
  - `$ systemctl restart smcore`
  - `$ systemctl restart scheduler`

## Configurez et activez la communication SSL bidirectionnelle sur l'hôte Windows

### Configurer la communication SSL bidirectionnelle sur l'hôte Windows

Vous devez configurer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter sur l'hôte Windows et les plug-ins.

#### Avant de commencer

- Vous devez avoir généré le fichier CSR du certificat de l'autorité de certification avec la longueur minimale de clé prise en charge de 3072.
- Le certificat de l'autorité de certification doit prendre en charge l'authentification du serveur et l'authentification du client.
- Vous devez disposer d'un certificat d'autorité de certification avec une clé privée et des détails d'empreinte digitale.
- Vous devez avoir activé la configuration SSL unidirectionnelle.

Pour plus de détails, voir ["Configurer la section certificat CA."](#)

- Vous devez avoir activé la communication SSL bidirectionnelle sur tous les hôtes de plug-in et sur le serveur SnapCenter.

L'environnement avec certains hôtes ou serveur non activé pour la communication SSL bidirectionnelle n'est pas pris en charge.

#### Étapes

1. Pour lier le port, effectuez les étapes suivantes sur l'hôte du serveur SnapCenter pour le port 8146 (par défaut) du serveur Web IIS de SnapCenter et une fois de plus pour le port 8145 (par défaut) de SMCORE à l'aide des commandes PowerShell.
  - a. Supprimez la liaison de port de certificat autosignée SnapCenter existante à l'aide de la commande PowerShell suivante.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

b. Liez le nouveau certificat CA fourni au serveur SnapCenter et au port SMCore.

```
> $cert = "<CA_certificate_thumbprint>"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>
certhash=$cert appid="$guid" clientcertnegotiation=enable
verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

Par exemple :

```
> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145
```

2. Pour accéder à l'autorisation du certificat de l'autorité de certification, ajoutez l'utilisateur par défaut du serveur Web IIS de SnapCenter « **IIS AppPool\SnapCenter** » dans la liste d'autorisations de certificat en effectuant les étapes suivantes pour accéder au certificat de l'autorité de certification nouvellement acquise.
  - a. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
  - b. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
  - c. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
  - d. Cliquez sur **Console Root > Certificates – local Computer > Personal > Certificates**.
  - e. Sélectionnez le certificat SnapCenter.
  - f. Pour démarrer l'assistant d'ajout d'utilisateur/d'autorisation, cliquez avec le bouton droit de la souris sur le certificat de l'autorité de certification et sélectionnez **toutes les tâches > gérer les clés privées**.
  - g. Cliquez sur **Ajouter**, dans l'assistant Sélectionner les utilisateurs et les groupes, modifiez l'emplacement en nom d'ordinateur local (en haut de la hiérarchie)
  - h. Ajoutez l'utilisateur IIS AppPool\SnapCenter et donnez des autorisations de contrôle total.
3. Pour l'autorisation IIS \* de certificat CA, ajoutez la nouvelle entrée de clés de Registre DWORD dans le serveur SnapCenter à partir du chemin suivant :

Dans l'éditeur du Registre Windows, parcourez jusqu'au chemin mentionné ci-dessous.

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. Créez une nouvelle entrée de clé de Registre DWORD dans le contexte de la configuration du registre SCHANNEL.

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

### Configurez le plug-in Windows SnapCenter pour une communication SSL bidirectionnelle

Vous devez configurer le plug-in Windows SnapCenter pour une communication SSL bidirectionnelle à l'aide des commandes PowerShell.

#### Avant de commencer

Assurez-vous que l'empreinte du certificat CA est disponible.

#### Étapes

1. Pour lier le port, effectuez les actions suivantes sur l'hôte du plug-in Windows pour le port SMCore 8145 (par défaut).

- a. Supprimez la liaison de port de certificat autosignée SnapCenter existante à l'aide de la commande PowerShell suivante.

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. Liez le nouveau certificat d'autorité de certification fourni au port SMCore.

```
> $cert = "<CA_certificate thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert
appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

Par exemple :

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

## Activez la communication SSL bidirectionnelle sur l'hôte Windows

Vous pouvez activer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre SnapCenter Server sur l'hôte Windows et les plug-ins à l'aide des commandes PowerShell.

### Avant de commencer

Exécutez d'abord les commandes de tous les plug-ins et de l'agent SMCore, puis de serveur.

### Étapes

1. Pour activer la communication SSL bidirectionnelle, exécutez les commandes suivantes sur le serveur SnapCenter pour les plug-ins, le serveur et pour chacun des agents pour lesquels la communication SSL bidirectionnelle est requise.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Exécutez l'opération de recyclage du pool d'applications SnapCenter IIS à l'aide de la commande suivante.  

```
> Restart-WebAppPool -Name "SnapCenter"
```
3. Pour les plug-ins Windows, redémarrez le service SMCore en exécutant la commande PowerShell suivante :

```
> Restart-Service -Name SnapManagerCoreService
```

### Désactiver la communication SSL bidirectionnelle

Vous pouvez désactiver la communication SSL bidirectionnelle à l'aide des commandes PowerShell.

### À propos de cette tâche

- Exécutez d'abord les commandes de tous les plug-ins et de l'agent SMCore, puis de serveur.
- Lorsque vous désactivez la communication SSL bidirectionnelle, le certificat de l'autorité de certification et sa configuration ne sont pas supprimés.
- Pour ajouter un nouvel hôte au serveur SnapCenter, vous devez désactiver le protocole SSL bidirectionnel pour tous les hôtes de plug-in.
- NLB et F5 ne sont pas pris en charge.

### Étapes

1. Pour désactiver la communication SSL bidirectionnelle, exécutez les commandes suivantes sur le serveur SnapCenter pour tous les hôtes de plug-in et l'hôte SnapCenter.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}

2. Exécutez l'opération de recyclage du pool d'applications SnapCenter IIS à l'aide de la commande suivante.
> Restart-WebAppPool -Name "SnapCenter"

3. Pour les plug-ins Windows, redémarrez le service SMCore en exécutant la commande PowerShell
suivante :

> Restart-Service -Name SnapManagerCoreService
```

## Configurez et activez la communication SSL bidirectionnelle sur l'hôte Linux

### Configurez la communication SSL bidirectionnelle sur l'hôte Linux

Vous devez configurer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter sur l'hôte Linux et les plug-ins.

#### Avant de commencer

- Vous devez avoir configuré le certificat CA pour l'hôte Linux.
- Vous devez avoir activé la communication SSL bidirectionnelle sur tous les hôtes de plug-in et sur le serveur SnapCenter.

#### Étapes

1. Copiez **certificate.pem** dans */etc/pki/ca-trust/source/anchors/*.
2. Ajoutez les certificats dans la liste de confiance de votre hôte Linux.
  - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
  - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
  - `update-ca-trust extract`
3. Vérifiez si les certificats ont été ajoutés à la liste de confiance.

```
trust list | grep "<CN of your certificate>"
```
4. Mettez à jour **ssl\_certificate** et **ssl\_certificate\_key** dans le fichier SnapCenter **nginx** et redémarrez.
  - `vim /etc/nginx/conf.d/snapcenter.conf`
  - `systemctl restart nginx`
5. Actualisez le lien de l'interface graphique du serveur SnapCenter.
6. Mettez à jour les valeurs des clés suivantes dans **SnapManager.Web.UI.dll.config** situées à l'adresse `<installation path>/NetApp/snapcenter/SnapManagerWeb_` et **SMCoreServiceHost.dll.config** situées à l'adresse `<installation path>/NetApp/snapcenter/SMCore`.
  - `<add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />`

- `<add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>`

7. Redémarrez les services suivants.

- `systemctl restart smcore.service`
- `systemctl restart snapmanagerweb.service`

8. Vérifiez que le certificat est connecté au port Web SnapManager.

```
openssl s_client -connect localhost:8146 -brief
```

9. Vérifiez que le certificat est connecté au port smcore.

```
openssl s_client -connect localhost:8145 -brief
```

10. Gérer le mot de passe pour la base de stockage de clés SPL et l'alias.

a. Récupérer le mot de passe par défaut de la SPL KEYSTORE attribué à la clé **SPL\_KEYSTORE\_PASS** dans le fichier de propriétés de la SPL.

b. Modifiez le mot de passe de la base de stockage de clés.

```
keytool -storepasswd -keystore keystore.jks
```

c. Modifiez le mot de passe pour tous les alias des entrées de clé privée.

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

d. Mettez à jour le même mot de passe pour la clé **SPL\_KEYSTORE\_PASS** dans *spl.properties*.

e. Redémarrez le service.

11. Sur l'hôte Linux du plug-in, ajoutez les certificats racine et intermédiaire dans la base de stockage de clés du plug-in SPL.

- `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`

- `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`

i. Vérifiez les entrées dans *keystore.jks*.

```
keytool -list -v -keystore <path to keystore.jks>
```

ii. Renommez tout alias si nécessaire.

```
keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass
keypass -keystore </path/to/keystore> -storepass storepas
```

12. Mettez à jour la valeur de **SPL\_CERTIFICATE\_ALIAS** dans le fichier *spl.properties* avec l'alias de **certificate.pfx** stocké dans *keystore.jks* et redémarrez le service SPL : `systemctl restart spl`

13. Vérifiez que le certificat est connecté au port smcore.

```
openssl s_client -connect localhost:8145 -brief
```

## Activez la communication SSL sur l'hôte Linux

Vous pouvez activer la communication SSL bidirectionnelle pour sécuriser la communication mutuelle entre le serveur SnapCenter sur l'hôte Linux et les plug-ins à l'aide des commandes PowerShell.

### Étape

1. Procédez comme suit pour activer la communication SSL unidirectionnelle.
  - a. Connectez-vous à l'interface graphique de SnapCenter.
  - b. Cliquez sur **Paramètres > Paramètres globaux** et sélectionnez **Activer la validation du certificat sur le serveur SnapCenter**.
  - c. Cliquez sur **hosts > Managed Hosts** et sélectionnez l'hôte plug-in pour lequel vous souhaitez activer le protocole SSL unidirectionnel.
  - d. Cliquez sur , puis sur **Activer la validation du certificat**.
2. Activez la communication SSL bidirectionnelle à partir de l'hôte Linux du serveur SnapCenter.
  - `Open-SmConnection`
  - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
  - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
  - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

## Configuration d'Active Directory, LDAP et LDAPS

### Enregistrer des domaines Active Directory non fiables

Vous devez enregistrer Active Directory avec le serveur SnapCenter pour gérer les hôtes, les utilisateurs et les groupes de plusieurs domaines Active Directory non fiables.

#### Avant de commencer

#### Protocoles LDAP et LDAPS

- Vous pouvez enregistrer les domaines d'annuaire actifs non approuvés à l'aide du protocole LDAP ou LDAPS.
- Vous devez avoir activé la communication bidirectionnelle entre les hôtes du plug-in et le serveur SnapCenter.
- La résolution DNS doit être configurée à partir du serveur SnapCenter vers les hôtes du plug-in et vice-versa.

#### Protocole LDAP

- Le nom de domaine complet (FQDN) doit être résolu à partir du serveur SnapCenter.

Vous pouvez enregistrer un domaine non approuvé avec le FQDN. Si le FQDN ne peut pas être résolu à partir du serveur SnapCenter, vous pouvez l'enregistrer avec une adresse IP de contrôleur de domaine et ceci devrait être résolu à partir du serveur SnapCenter.

#### Protocole LDAPS

- Les certificats CA sont requis pour que LDAPS puisse fournir un cryptage de bout en bout pendant la communication Active Directory.

["Configurer le certificat client CA pour LDAPS"](#)

- Les noms d'hôte du contrôleur de domaine (DCHostName) doivent être accessibles depuis le serveur SnapCenter.

## À propos de cette tâche

- Vous pouvez utiliser l'interface utilisateur SnapCenter, les applets de commande PowerShell ou l'API REST pour enregistrer un domaine non fiable.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Paramètres globaux**.
3. Dans la page Paramètres globaux, cliquez sur **Paramètres de domaine**.
4. Cliquez sur pour enregistrer un nouveau domaine.
5. Dans la page Enregistrer un nouveau domaine, sélectionnez **LDAP** ou **LDAPS**.
  - a. Si vous sélectionnez **LDAP**, spécifiez les informations requises pour l'enregistrement du domaine non fiable pour LDAP :

Pour ce champ...	Procédez comme ça...
Nom de domaine	Spécifiez le nom NetBIOS du domaine.
FQDN du domaine	Spécifiez le FQDN et cliquez sur <b>résoudre</b> .
Adresses IP du contrôleur de domaine	Si le FQDN du domaine ne peut pas être résolu à partir du serveur SnapCenter, spécifiez une ou plusieurs adresses IP de contrôleur de domaine.  Pour plus d'informations, voir " <a href="#">Ajoutez l'IP du contrôleur de domaine pour le domaine non approuvé à partir de l'interface graphique</a> ".

- b. Si vous sélectionnez **LDAPS**, spécifiez les informations requises pour l'enregistrement du domaine non fiable pour LDAPS :

Pour ce champ...	Procédez comme ça...
Nom de domaine	Spécifiez le nom NetBIOS du domaine.
FQDN du domaine	Spécifiez le FQDN.
Noms de contrôleur de domaine	Spécifiez un ou plusieurs noms de contrôleur de domaine et cliquez sur <b>résoudre</b> .
Adresses IP du contrôleur de domaine	Si les noms de contrôleurs de domaine ne peuvent pas être résolus à partir du serveur SnapCenter, vous devez corriger les résolutions DNS.

6. Cliquez sur **OK**.

## Configurez les pools d'applications IIS pour activer les autorisations de lecture d'Active Directory

Vous pouvez configurer IIS (Internet Information Services) sur votre serveur Windows pour créer un compte de pool d'applications personnalisé lorsque vous devez activer les autorisations de lecture Active Directory pour SnapCenter.

### Étapes

1. Ouvrez le Gestionnaire IIS sur le serveur Windows sur lequel SnapCenter est installé.
2. Dans le volet de navigation de gauche, cliquez sur **pools d'applications**.
3. Sélectionnez SnapCenter dans la liste pools d'applications, puis cliquez sur **Paramètres avancés** dans le volet actions.
4. Sélectionnez identité, puis cliquez sur ... pour modifier l'identité du pool d'applications SnapCenter.
5. Dans le champ compte personnalisé, entrez un nom d'utilisateur de domaine ou de compte d'administrateur de domaine avec l'autorisation de lecture Active Directory.
6. Cliquez sur OK.

Le compte personnalisé remplace le compte ApplicationPoolIdentity intégré pour le pool d'applications SnapCenter.

## Configurer le certificat client CA pour LDAPS

Vous devez configurer le certificat client CA pour LDAPS sur le serveur SnapCenter lorsque le LDAPS Active Directory Windows est configuré avec les certificats CA.

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Dans la deuxième page de l'assistant	Cliquez sur <b>Parcourir</b> , sélectionnez le <i>certificat racine</i> et cliquez sur <b>Suivant</b> .

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.

7. Répétez les étapes 5 et 6 pour les certificats intermédiaires.

# Protection des bases de données Microsoft SQL Server

## Plug-in SnapCenter pour Microsoft SQL Server

### Présentation du plug-in SnapCenter pour Microsoft SQL Server

Le plug-in SnapCenter pour Microsoft SQL Server est un composant côté hôte du logiciel NetApp SnapCenter qui permet de gérer la protection des données des bases de données Microsoft SQL Server avec la cohérence applicative. Le plug-in pour SQL Server automatise les opérations de sauvegarde, de vérification, de restauration et de clonage des bases de données SQL Server dans votre environnement SnapCenter.

Lorsque le plug-in pour SQL Server est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume et grâce à la technologie NetApp SnapVault pour effectuer une réplication de sauvegarde disque à disque à des fins de conformité et d'archivage.

- Automatise les opérations de sauvegarde, de restauration et de clonage respectueuses des applications pour les bases de données Microsoft SQL Server dans votre environnement SnapCenter.
- Prend en charge les bases de données Microsoft SQL Server sur des LUN VMDK et RDM (Raw Device Mapping) lorsque vous déployez le plug-in SnapCenter pour VMware vSphere et enregistrez le plug-in avec SnapCenter
- Prend uniquement en charge le provisionnement des partages SMB. Elle n'est pas prise en charge pour la sauvegarde des bases de données SQL Server sur les partages SMB.
- Prise en charge de l'importation de sauvegardes depuis SnapManager pour Microsoft SQL Server vers SnapCenter.

### Quelles sont les possibilités du plug-in SnapCenter pour Microsoft SQL Server

Lorsque le plug-in SnapCenter pour Microsoft SQL Server est installé dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner les bases de données SQL Server.

Vous pouvez effectuer les tâches suivantes sur la prise en charge des opérations de sauvegarde, de restauration et de clonage des bases de données SQL Server et des ressources de base de données :

- Sauvegarde des bases de données SQL Server et des journaux de transactions associés

Vous ne pouvez pas créer de sauvegarde de journal pour les bases de données système master et msdb. Toutefois, vous pouvez créer des sauvegardes de journaux pour la base de données du système modèle.

- Restaurer les ressources de base de données
  - Vous pouvez restaurer les bases de données du système maître, les bases de données du système msdb et les bases de données du système modèle.
  - Vous ne pouvez pas restaurer plusieurs bases de données, instances et groupes de disponibilité.
  - Vous ne pouvez pas restaurer la base de données système sur un chemin alternatif.

- Créer des clones ponctuelles des bases de données de production

Vous ne pouvez pas effectuer des opérations de sauvegarde, de restauration, de clonage et de clonage de cycle de vie sur les bases de données système tempdb.

- Vérifier immédiatement les opérations de sauvegarde ou reporter la vérification jusqu'à la fin du processus

La vérification de la base de données système SQL Server n'est pas prise en charge. SnapCenter clone les bases de données pour effectuer une vérification. SnapCenter ne peut pas cloner les bases de données système SQL Server. Par conséquent, la vérification de ces bases de données n'est pas prise en charge.

- Planification des opérations de sauvegarde et des opérations de clonage
- Surveillance des opérations de sauvegarde, des opérations de restauration et des opérations de clonage



Le plug-in pour SQL Server ne prend pas en charge la sauvegarde et la restauration des bases de données SQL Server sur les partages SMB.

## Fonctionnalités du plug-in SnapCenter pour Microsoft SQL Server

Le plug-in pour SQL Server s'intègre à Microsoft SQL Server sur l'hôte Windows et à la technologie NetApp Snapshot sur le système de stockage. Pour utiliser le plug-in pour SQL Server, utilisez l'interface SnapCenter.

Le plug-in pour SQL Server inclut les principales fonctionnalités suivantes :

- **Interface graphique utilisateur unifiée optimisée par SnapCenter**

L'interface SnapCenter vous permet de standardiser et d'assurer une cohérence entre les plug-ins et les environnements. L'interface SnapCenter vous permet d'effectuer des sauvegardes et des restaurations cohérentes dans l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues du tableau de bord en un coup d'œil, de configurer le contrôle d'accès basé sur les rôles et de surveiller les tâches dans tous les plug-ins. SnapCenter propose également une planification et une gestion centralisées des règles pour prendre en charge les opérations de sauvegarde et de clonage.

- **Administration centrale automatisée**

Vous pouvez planifier des sauvegardes SQL Server de routine, configurer la conservation des sauvegardes basée sur des règles et configurer des opérations de restauration instantanées et à chaud. Vous pouvez également surveiller de manière proactive votre environnement SQL Server en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie snapshot NetApp non disruptive**

Le plug-in pour SQL Server utilise la technologie Snapshot NetApp avec le plug-in NetApp SnapCenter pour Microsoft Windows. Vous pouvez ainsi sauvegarder des bases de données en quelques secondes et les restaurer rapidement sans mettre SQL Server hors ligne. Les copies Snapshot consomment un espace de stockage minimal.

Outre ces fonctionnalités majeures, le plug-in pour SQL Server offre les avantages suivants :

- Prise en charge des sauvegardes, des restaurations, des clones et des workflows de vérification

- Sécurité prise en charge par le RBAC et délégation centralisée des rôles
- Création de copies instantanées compactes de bases de données de production à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage hébergeant le clone.

- Vérification automatisée et sans interruption des sauvegardes
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs serveurs
- Les applets de commande PowerShell pour créer des scripts pour les opérations de sauvegarde, de vérification, de restauration et de clonage
- Prise en charge des groupes AlwaysOn Availability Groups (AG) dans SQL Server pour accélérer les opérations AG de configuration, de sauvegarde et de restauration
- Base de données en mémoire et extension de pool de mémoire tampon (BPE) dans le cadre de SQL Server 2014
- Prise en charge des sauvegardes des LUN et des disques de machines virtuelles (VMDK)
- Prise en charge des infrastructures physiques et virtualisées
- Prise en charge des protocoles iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM) et VMDK sur NFS et VMFS



Les volumes NAS doivent disposer d'une export policy par défaut dans la machine virtuelle de stockage (SVM).

- Prise en charge de FileStream et de groupes de fichiers dans les bases de données autonomes SQL Server.
- Prise en charge de NVMe (non-volatile Memory Express) sur Windows Server 2022
  - Workflows de sauvegarde, de restauration, de clonage et de vérification sur une disposition VMDK créée sur NVMe over TCP/IP.
  - Prend en charge la version 1.3 du firmware NVMe à partir de la mise à jour 2 d'ESX 8.0 et requiert la version 21 du matériel virtuel.
  - Windows Server Failover Clustering (WSFC) n'est pas pris en charge pour les applications sur VMDK sur NVMe over TCP/IP.
- Prise en charge de la synchronisation active SnapMirror (initialement lancée sous la forme de SnapMirror Business Continuity [SM-BC]) qui assure la continuité des services de l'entreprise même en cas de défaillance complète du site, permettant ainsi aux applications de basculer en toute transparence au moyen d'une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

## Prise en charge du mappage des LUN asymétriques dans les clusters Windows

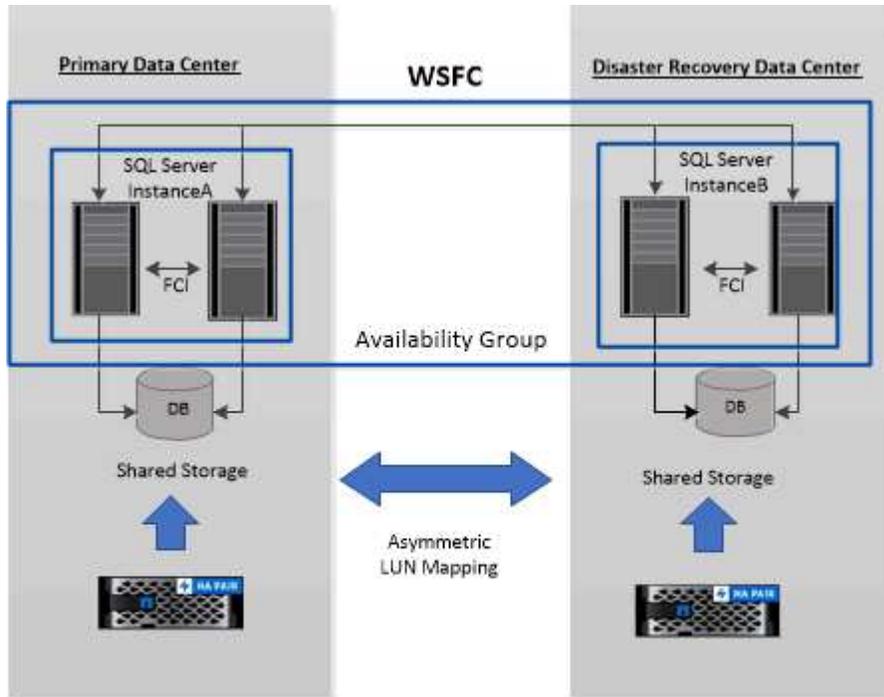
Le plug-in SnapCenter pour Microsoft SQL Server prend en charge la détection dans SQL Server 2012 et versions ultérieures, les configurations ALM (Asymmetric LUN Mapping) pour la haute disponibilité, et les groupes de disponibilité pour la reprise après incident. Lors de la découverte des ressources, SnapCenter détecte les bases de données sur les hôtes locaux et sur les hôtes distants dans les configurations ALM.

Une configuration ALM est un cluster de basculement de serveur Windows unique qui contient un ou plusieurs nœuds dans un centre de données principal et un ou plusieurs nœuds dans un centre de reprise après

incident.

Voici un exemple de configuration ALM :

- Deux instances de cluster de basculement (FCI) dans un data Center multisite
- FCI pour la haute disponibilité locale (HA) et le groupe de disponibilité (AG) pour la reprise après incident avec une instance autonome sur le site de reprise après incident



### WSFC—Windows Server Failover Cluster

Le stockage du data Center principal est partagé entre les nœuds FCI présents dans le data Center principal. Le stockage du centre de données de reprise après incident est partagé entre les nœuds FCI présents dans le centre de données de reprise après incident.

Le stockage du data Center principal n'est pas visible sur les nœuds du centre de reprise après incident, et inversement.

L'architecture ALM combine deux solutions de stockage partagé utilisées par FCI, avec une solution de stockage non partagée ou dédiée utilisée par SQL AG. La solution AG utilise des lettres de lecteur identiques pour les ressources de disque partagées sur l'ensemble des centres de données. Cet arrangement de stockage, où un disque de cluster est partagé entre un sous-ensemble de nœuds dans un WSFC, est appelé ALM.

## Types de stockage pris en charge par le plug-in SnapCenter pour Microsoft SQL Server

SnapCenter prend en charge un large éventail de types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier si la prise en charge de votre type de stockage est disponible avant d'installer le package pour votre hôte.

Le provisionnement et la protection des données SnapCenter sont pris en charge par Windows Server. Pour obtenir les dernières informations sur les versions prises en charge, consultez le ["Matrice d'interopérabilité"](#)

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur physique	LUN connectés via FC	Interface graphique SnapCenter ou applets de commande PowerShell	
Serveur physique	LUN connectées à l'iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	
Serveur physique	Partages SMB3 (CIFS) résidant sur un SVM (Storage Virtual machine)	Interface graphique SnapCenter ou applets de commande PowerShell	Prise en charge du provisionnement uniquement.
VM VMware	LUN RDM connectés par un HBA FC ou iSCSI	Applets de commande PowerShell	
VM VMware	LUN iSCSI connectés directement au système invité par l'initiateur iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	
VM VMware	Datastores VMFS (Virtual machine File Systems) ou NFS	VMware vSphere	
VM VMware	Système invité connecté à des partages SMB3 résidant sur un SVM	Interface graphique SnapCenter ou applets de commande PowerShell	Prise en charge du provisionnement uniquement.
VM VMware	Datastores vVol sur NFS et SAN	Outils ONTAP pour VMware vSphere	

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur virtuel Hyper-V.	LUN FC virtuels (VFC) connectés par un commutateur Fibre Channel virtuel	Interface graphique SnapCenter ou applets de commande PowerShell	<p data-bbox="1156 151 1489 361">Vous devez utiliser Hyper-V Manager pour provisionner les LUN FC virtuels (VFC) connectés par un commutateur Fibre Channel virtuel.</p> <div data-bbox="1188 394 1461 961" style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p data-bbox="1307 403 1455 953">Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>
Serveur virtuel Hyper-V.	LUN iSCSI connectés directement au système invité par l'initiateur iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	<div data-bbox="1188 1024 1461 1570" style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p data-bbox="1307 1024 1455 1562">Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur virtuel Hyper-V.	Système invité connecté à des partages SMB3 résidant sur un SVM	Interface graphique SnapCenter ou applets de commande PowerShell	<p>Prise en charge du provisionnement uniquement.</p> <p> Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p>

## Recommandations relatives à l'organisation du stockage pour le plug-in SnapCenter pour Microsoft SQL Server

Grâce à une disposition de stockage bien conçue, SnapCenter Server peut sauvegarder vos bases de données pour atteindre vos objectifs de restauration. Vous devez tenir compte de plusieurs facteurs lors de la définition de l'organisation du stockage, notamment la taille de la base de données, le taux de changement de la base de données et la fréquence à laquelle vous effectuez des sauvegardes.

Les sections suivantes définissent les recommandations et restrictions relatives à l'infrastructure de stockage pour les LUN et les disques des machines virtuelles (VMDK) avec le plug-in SnapCenter pour Microsoft SQL Server installé dans votre environnement.

Dans ce cas, les LUN peuvent inclure des disques VMware RDM et des LUN iSCSI à connexion directe mappés à l'invité.

### Exigences relatives aux LUN et aux VMDK

Vous pouvez choisir d'utiliser des LUN ou des VMDK dédiés pour optimiser les performances et la gestion des bases de données suivantes :

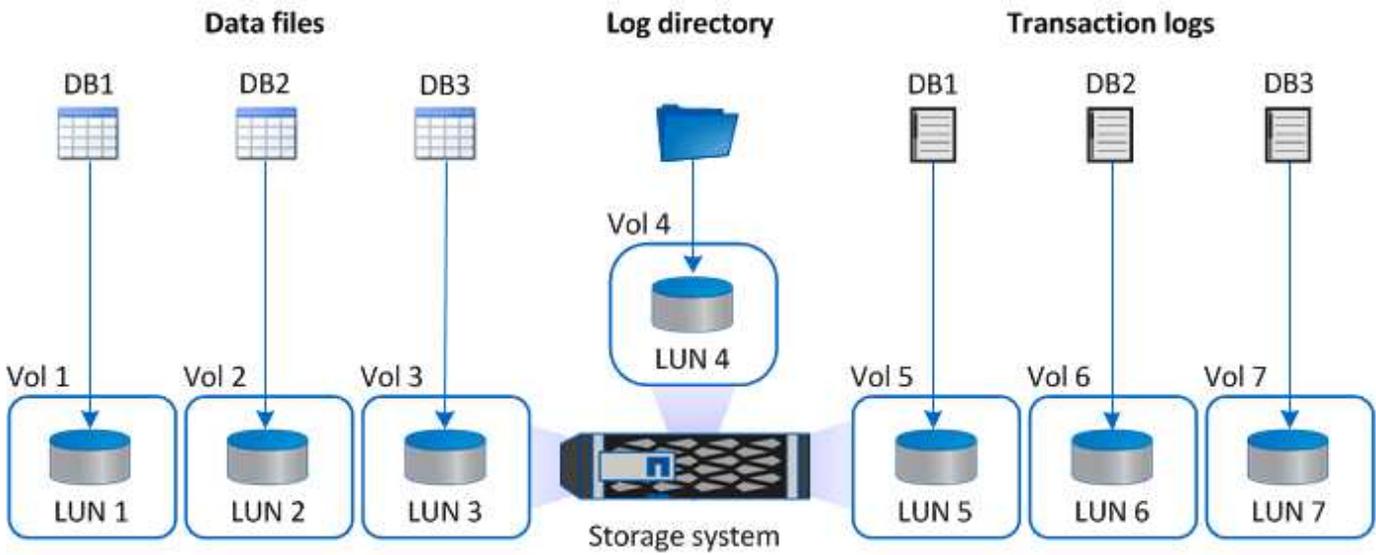
- Bases de données du système maître et modèle
- Tempdb
- Fichiers de base de données utilisateur (.mdf et .ndf)
- Fichiers du journal de transactions de la base de données utilisateur (.ldf)
- Répertoire du journal

Pour restaurer des bases de données volumineuses, il est recommandé d'utiliser des LUN ou des VMDK dédiés. Le temps nécessaire à la restauration d'une LUN ou d'un VMDK complet est inférieur au temps requis pour restaurer les fichiers individuels stockés dans le LUN ou le VMDK.

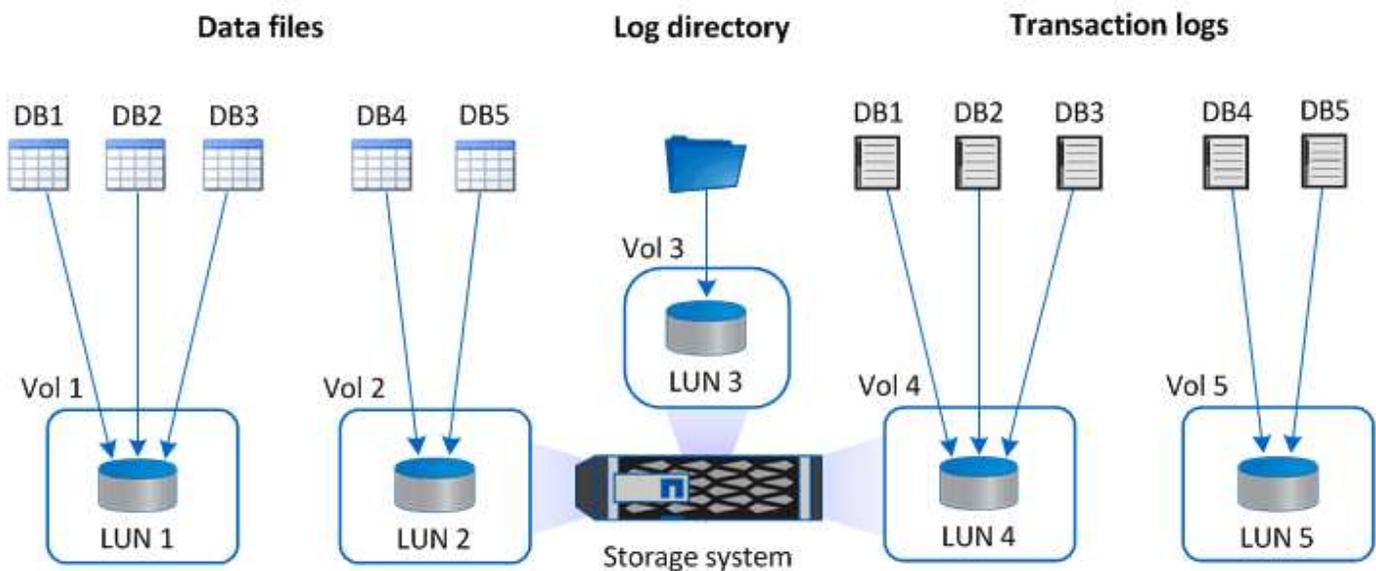
Pour le répertoire du journal, vous devez créer une LUN ou un VMDK distinct de sorte que l'espace disponible dans les disques de données ou de fichiers journaux soit suffisant.

### Exemples de dispositions des LUN et VMDK

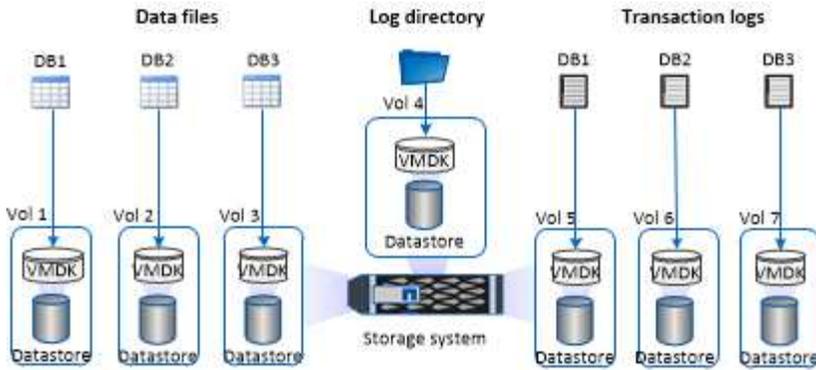
Le graphique suivant explique comment configurer l'organisation du stockage pour les bases de données volumineuses sur les LUN :



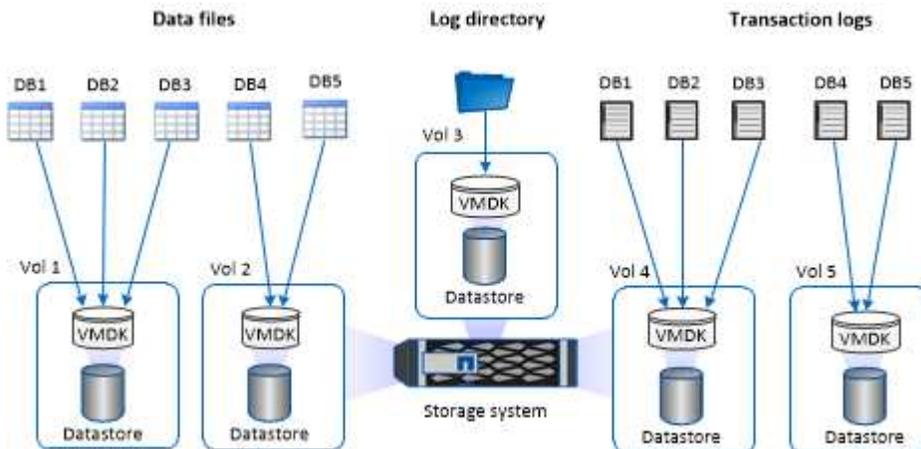
Le graphique suivant explique comment configurer l'organisation du stockage pour les bases de données de taille moyenne ou petite taille sur les LUN :



Le graphique suivant montre comment configurer l'organisation du stockage pour les grandes bases de données sur des VMDK :



Le graphique suivant montre comment configurer l'organisation du stockage pour des bases de données de taille moyenne ou petite taille sur des VMDK :



## Privilèges ONTAP minimum requis pour le plug-in SQL

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - suppression de la lun
  - lun igroup add
  - créez un groupe initiateur lun
  - suppression du groupe initiateur lun
  - renommer la lun igroup
  - affichage de la lun igroup
  - lun mapping des nœuds supplémentaires
  - création d'un mappage de lun

- suppression du mappage de lun
- mappage de lun supprimer-rapports-noeuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes
- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume

- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- interface réseau
- interface réseau affiche
- un vserver
- montrer MetroCluster

## **Préparation des systèmes de stockage pour la réplication SnapMirror et SnapVault pour le plug-in pour SQL Server**

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée.

Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire > miroir > coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Stratégie de sauvegarde des ressources SQL Server

### Définir une stratégie de sauvegarde pour les ressources SQL Server

La définition d'une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous permet de vous assurer que vous disposez des sauvegardes dont vous avez besoin pour restaurer ou cloner vos bases de données. Votre accord de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de récupération (RPO) déterminent largement votre stratégie de sauvegarde.

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés au service, notamment la disponibilité et les performances de celui-ci. Le RTO est le moment par où un processus métier doit être restauré suite à une interruption de service. Un RPO définit la stratégie selon laquelle les fichiers doivent être récupérés à partir du stockage de sauvegarde afin que des opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de sauvegarde.

### Types de sauvegardes pris en charge

Pour sauvegarder des bases de données système et utilisateur SQL Server à l'aide de SnapCenter, vous devez choisir le type de ressource, tel que les bases de données, les instances SQL Server et les groupes de disponibilité (AG). Elle permet de créer des copies en ligne en lecture seule des volumes sur lesquels résident les ressources.

Vous pouvez sélectionner l'option copie seule pour indiquer que SQL Server ne tronque pas les journaux de transactions. Vous devez utiliser cette option lorsque vous gérez également SQL Server avec d'autres applications de sauvegarde. Le fait de préserver l'intégrité des journaux de transactions permet à toute application de sauvegarde de restaurer les bases de données système. Les sauvegardes de copie uniquement sont indépendantes de la séquence des sauvegardes planifiées et n'affectent pas les procédures de sauvegarde et de restauration de la base de données.

Type de sauvegarde	Description	Option de copie uniquement avec type de sauvegarde
Sauvegarde complète et sauvegarde des journaux	<p>Sauvegarde la base de données système et tronque les journaux de transactions.</p> <p>SQL Server tronque les journaux de transactions en supprimant les entrées déjà engagées dans la base de données.</p> <p>Une fois la sauvegarde complète terminée, cette option crée un journal de transactions qui capture les informations de transaction. Généralement, vous devez choisir cette option. Toutefois, si votre temps de sauvegarde est court, vous pouvez choisir de ne pas exécuter de sauvegarde complète du journal de transactions.</p> <p>Vous ne pouvez pas créer de sauvegarde de journal pour les bases de données système master et msdb. Toutefois, vous pouvez créer des sauvegardes de journaux pour la base de données du système modèle.</p>	<p>Sauvegarde les fichiers de base de données système et les journaux de transactions sans tronquer les journaux.</p> <p>Une sauvegarde de copie uniquement ne peut pas servir de base différentielle ou de sauvegarde différentielle et n'affecte pas la base différentielle. La restauration d'une sauvegarde complète pour copie uniquement est la même que pour toute autre sauvegarde complète.</p>
Sauvegarde complète de la base de données	<p>Sauvegarde les fichiers de la base de données système.</p> <p>Vous pouvez créer une sauvegarde complète de la base de données pour les bases de données du système maître, modèle et msdb.</p>	<p>Sauvegarde les fichiers de la base de données système.</p>
Sauvegarde du journal des transactions	<p>Sauvegarde les journaux de transactions tronqués, en copiant uniquement les transactions validées depuis la sauvegarde du journal de transactions le plus récent.</p> <p>Si vous planifiez des sauvegardes fréquentes du journal des transactions parallèlement à des sauvegardes complètes de bases de données, vous pouvez choisir des points de restauration granulaires.</p>	<p>Sauvegarde les journaux de transactions sans les tronquer.</p> <p>Ce type de sauvegarde n'affecte pas le séquençement des sauvegardes de journaux standard. Les sauvegardes de journaux avec copie uniquement sont utiles pour les opérations de restauration en ligne.</p>

## Planifications de sauvegarde pour le plug-in pour SQL Server

La fréquence de sauvegarde (type de planification) est spécifiée dans les stratégies ; un planning de sauvegarde est spécifié dans la configuration du groupe de ressources. Le facteur le plus important dans la détermination d'une fréquence ou d'un planning de sauvegarde est le taux de changement pour la ressource et l'importance des données. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. Parmi les autres facteurs figurent l'importance de la ressource pour votre organisation, votre contrat de niveau de service (SLA) et votre objectif de point de récupération (RPO).

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés au service, notamment la disponibilité et les performances de celui-ci. Un RPO définit la stratégie selon laquelle les fichiers doivent être récupérés à partir du stockage de sauvegarde afin que des opérations régulières puissent reprendre après une défaillance. Les SLA et RPO contribuent à la stratégie de protection des données.

Même avec une ressource largement utilisée, il n'est pas nécessaire d'exécuter une sauvegarde complète plus d'une fois ou deux fois par jour. Par exemple, des sauvegardes régulières du journal de transactions peuvent suffire pour vous assurer que vous disposez des sauvegardes dont vous avez besoin. Plus vous sauvegardez des bases de données, plus le nombre de journaux de transaction que SnapCenter doit utiliser au moment de la restauration est élevé, ce qui accélère les opérations de restauration.

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes

La fréquence de sauvegarde (fréquence d'exécution des sauvegardes), appelée *schedule type* pour certains plug-ins, fait partie d'une configuration de stratégie. Vous pouvez sélectionner la fréquence de sauvegarde horaire, quotidienne, hebdomadaire ou mensuelle de la police. Si vous ne sélectionnez aucune de ces fréquences, la règle créée est une stratégie à la demande uniquement. Vous pouvez accéder aux stratégies en cliquant sur **Paramètres > stratégies**.

- Planifications de sauvegarde

Les planifications de sauvegarde (exactement quand les sauvegardes doivent être effectuées) font partie d'une configuration de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour sauvegarder chaque jeudi à 10 h 00. Vous pouvez accéder aux planifications de groupes de ressources en cliquant sur **Ressources > groupes de ressources**.

## Nombre de tâches de sauvegarde nécessaires pour les bases de données

Les facteurs déterminant le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la base de données, le nombre de volumes utilisés, le taux de changement de la base de données et votre contrat de niveau de service.

Pour les sauvegardes de bases de données, le nombre de tâches de sauvegarde que vous choisissez dépend généralement du nombre de volumes sur lesquels vous avez placé vos bases de données. Par exemple, si vous placez un groupe de petites bases de données sur un volume et une grande base de données sur un autre volume, vous pouvez créer une tâche de sauvegarde pour les petites bases de données et une tâche de sauvegarde pour la grande base de données.

## Conventions de nom de sauvegarde du plug-in pour SQL Server

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.
- *03-12-2015\_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, `clienttext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

## Options de conservation des sauvegardes pour le plug-in pour SQL Server

Vous pouvez choisir le nombre de jours pendant lesquels vous souhaitez conserver les copies de sauvegarde ou spécifier le nombre de copies de sauvegarde à conserver, dans un maximum de 255 copies ONTAP. Par exemple, votre entreprise peut avoir besoin de conserver 10 jours de copies de sauvegarde ou 130 copies de sauvegarde.

Lors de la création d'une stratégie, vous pouvez spécifier les options de rétention pour le type de sauvegarde et le type de planification.

Si vous configurez la réplication SnapMirror, la règle de conservation est mise en miroir sur le volume de destination.

SnapCenter supprime les sauvegardes conservées dont les étiquettes de conservation correspondent au type de planification. Si le type de planification a été modifié pour la ressource ou le groupe de ressources, les sauvegardes avec l'ancienne étiquette de type de planification peuvent rester sur le système.



Pour la conservation à long terme des copies de sauvegarde, nous vous recommandons d'utiliser la sauvegarde SnapVault.

## **Durée de conservation des sauvegardes du journal des transactions sur le système de stockage source**

Le plug-in SnapCenter pour Microsoft SQL Server requiert des sauvegardes de journal des transactions pour effectuer des opérations de restauration à chaud, qui restaurent votre base de données à un moment donné entre deux sauvegardes complètes.

Par exemple, si le plug-in pour SQL Server a pris une sauvegarde complète à 8:00 et une autre sauvegarde complète à 5:00, elle peut utiliser la dernière sauvegarde du journal de transactions pour restaurer la base de données à tout moment entre 8:00 et 5:00. Si les journaux de transactions ne sont pas disponibles, le plug-in pour SQL Server peut effectuer des opérations de restauration ponctuelles uniquement, ce qui permet de restaurer une base de données au moment où le plug-in pour SQL Server a terminé une sauvegarde complète.

En règle générale, les opérations de restauration sont réalisées en moins d'une journée ou deux. Par défaut, SnapCenter conserve un minimum de deux jours.

## **Plusieurs bases de données sur un même volume**

Vous pouvez placer toutes les bases de données sur le même volume, car la stratégie de sauvegarde a une option permettant de définir le maximum de bases de données par sauvegarde (la valeur par défaut est 100).

Par exemple, si vous avez 200 bases de données dans le même volume, deux snapshots sont créés avec 100 bases de données dans chacun des deux snapshots.

## **Vérification de la copie de sauvegarde à l'aide du volume de stockage principal ou secondaire pour le plug-in pour SQL Server**

Vous pouvez vérifier les copies de sauvegarde sur le volume de stockage primaire ou sur le volume de stockage secondaire SnapMirror ou SnapVault. La vérification à l'aide d'un volume de stockage secondaire réduit la charge sur le volume de stockage primaire.

Lorsque vous vérifiez une sauvegarde se trouvant sur le volume de stockage primaire ou secondaire, tous les snapshots primaire et secondaire sont marqués comme étant vérifiés.

Une licence SnapRestore est requise pour vérifier les copies de sauvegarde sur les volumes de stockage secondaire SnapMirror et SnapVault.

## **Quand planifier des tâches de vérification**

Bien que SnapCenter puisse vérifier les sauvegardes immédiatement après leur création, il est possible d'augmenter considérablement le temps requis pour effectuer les tâches de sauvegarde et consomme beaucoup de ressources. Par conséquent, il est presque toujours préférable de planifier la vérification dans un travail distinct pour une période ultérieure. Par exemple, si vous sauvegardez une base de données à 5:00 chaque jour, vous pouvez programmer la vérification à 6 h 00.

Pour la même raison, il n'est généralement pas nécessaire d'exécuter la vérification des sauvegardes chaque fois que vous effectuez une sauvegarde. Effectuer une vérification à intervalles réguliers mais moins fréquents est généralement suffisant pour garantir l'intégrité de la sauvegarde. Une seule tâche de vérification peut vérifier plusieurs sauvegardes simultanément.

# Stratégie de restauration pour SQL Server

## Sources et destinations pour une opération de restauration

Vous pouvez restaurer une base de données SQL Server à partir d'une copie de sauvegarde sur le stockage primaire ou secondaire. Vous pouvez également restaurer la base de données vers différentes destinations en plus de son emplacement d'origine, ce qui vous permet de choisir la destination qui répond à vos besoins.

### Sources pour une opération de restauration

Vous pouvez restaurer les bases de données à partir du stockage primaire ou secondaire.

### Destinations d'une opération de restauration

Vous pouvez restaurer des bases de données vers différentes destinations :

Destination	Description
L'emplacement d'origine	Par défaut, SnapCenter restaure la base de données au même emplacement sur la même instance SQL Server.
Un autre emplacement	Vous pouvez restaurer la base de données à un emplacement différent sur n'importe quelle instance SQL Server au sein du même hôte.
Emplacement original ou différent utilisant différents noms de base de données	Vous pouvez restaurer la base de données avec un nom différent de toute instance SQL Server sur le même hôte sur lequel la sauvegarde a été créée.



La restauration vers un autre hôte sur des serveurs ESX pour les bases de données SQL sur des VMDK (datastores NFS et VMFS) n'est pas prise en charge.

## Modèles de restauration SQL Server pris en charge par SnapCenter

Des modèles de reprise spécifiques sont attribués par défaut à chaque type de base de données. L'administrateur de base de données SQL Server peut réaffecter chaque base de données à un modèle de restauration différent.

SnapCenter prend en charge trois types de modèles de restauration SQL Server :

- Modèle de restauration simple

Lorsque vous utilisez le modèle de récupération simple, vous ne pouvez pas sauvegarder les journaux de transactions.

- Modèle de restauration complet

Lorsque vous utilisez le modèle de récupération complète, vous pouvez restaurer une base de données à son état précédent à partir du point d'échec.

- Modèle de restauration enregistré en bloc

Lorsque vous utilisez le modèle de récupération de journalisation en bloc, vous devez exécuter à nouveau manuellement l'opération de consignation en bloc. Vous devez effectuer l'opération de consignation groupée si le journal de transactions contenant l'enregistrement de validation de l'opération n'a pas été sauvegardé avant la restauration. Si l'opération de consignation groupée insère 10 millions de lignes dans une base de données et que la base de données échoue avant la sauvegarde du journal de transactions, la base de données restaurée ne contiendra pas les lignes qui ont été insérées par l'opération de consignation groupée.

## Types d'opérations de restauration

Vous pouvez utiliser SnapCenter pour effectuer différents types d'opérations de restauration sur les ressources SQL Server.

- Restaurez vos données en moins d'une minute
- Restauration à un point précédent dans le temps

Vous pouvez restaurer jusqu'à la minute ou restaurer l'ancien point dans le temps dans les situations suivantes :

- Restaurez vos données à partir de SnapMirror ou d'un système de stockage secondaire SnapVault
- Restauration vers un autre chemin (emplacement)



SnapCenter ne prend pas en charge la SnapRestore basée sur les volumes.

### Restaurez vos données en quelques minutes

Dans le cadre d'une opération de restauration en moins d'une minute (sélectionnée par défaut), les bases de données sont restaurées jusqu'au point de défaillance. Pour cela, SnapCenter effectue la séquence suivante :

1. Sauvegarde le dernier journal de transactions actif avant de restaurer la base de données.
2. Restaure les bases de données à partir de la sauvegarde de base de données complète que vous sélectionnez.
3. Applique tous les journaux de transactions qui n'ont pas été engagés dans les bases de données (y compris les journaux de transactions à partir des sauvegardes depuis la création de la sauvegarde jusqu'à la date la plus récente).

Les journaux de transactions sont déplacés vers l'avant et appliqués à toute base de données sélectionnée.

Une opération de restauration en moins d'une minute nécessite un ensemble contigu de journaux de transaction.

Étant donné que SnapCenter ne peut pas restaurer les journaux de transactions de base de données SQL Server à partir de fichiers de sauvegarde d'envoi de journaux (l'envoi de journaux vous permet d'envoyer automatiquement des sauvegardes de journal de transactions d'une base de données primaire sur une instance de serveur primaire vers une ou plusieurs bases de données secondaires sur des instances de serveur secondaire distinctes), vous ne pouvez pas effectuer une opération de restauration en moins d'une minute à partir des sauvegardes du journal de transactions. C'est pourquoi vous devez utiliser SnapCenter pour sauvegarder vos fichiers de journal de transactions de base de données SQL Server.

Si vous n'avez pas besoin de conserver une capacité de restauration à la minute pour toutes les sauvegardes, vous pouvez configurer la conservation de la sauvegarde du journal des transactions de votre système à l'aide des stratégies de sauvegarde.

### Exemple d'une opération de restauration en moins d'une minute

Supposons que vous exécutez la sauvegarde SQL Server tous les jours à midi et le mercredi à 4:00 vous devez effectuer une restauration à partir d'une sauvegarde. Pour une raison quelconque, la sauvegarde du mercredi midi a échoué à la vérification, donc vous décidez de restaurer à partir de la sauvegarde du mardi midi. Après cela, si la sauvegarde est restaurée, tous les journaux de transactions sont transférés et appliqués aux bases de données restaurées, en commençant par ceux qui n'ont pas été validés lors de la création de la sauvegarde de mardi et en passant par le dernier journal de transactions écrit le mercredi à 4:00 (si les journaux de transactions ont été sauvegardés).

### Restauration à un point précédent dans le temps

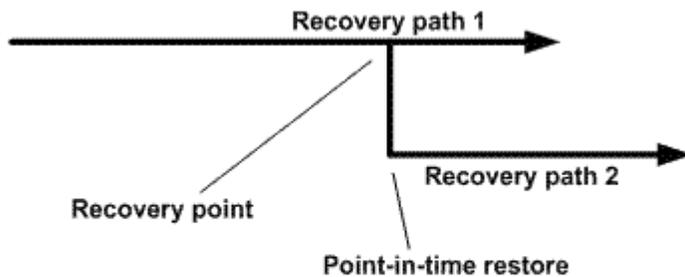
Dans le cadre d'une opération de restauration instantanée, les bases de données ne sont restaurées qu'à une heure spécifique par le passé. Une opération de restauration à un point dans le temps se produit dans les situations de restauration suivantes :

- La base de données est restaurée à une heure donnée dans un journal de transactions sauvegardé.
- La base de données est restaurée et seul un sous-ensemble des journaux de transactions sauvegardés y est appliqué.



La restauration d'une base de données à un point dans le temps génère un nouveau chemin de restauration.

L'image suivante illustre les problèmes lorsqu'une opération de restauration à un point dans le temps est effectuée :



Dans l'image, le chemin de récupération 1 consiste en une sauvegarde complète suivie de plusieurs sauvegardes du journal de transactions. Vous restaurez la base de données à un point dans le temps. De nouvelles sauvegardes du journal des transactions sont créées après l'opération de restauration instantanée, ce qui entraîne le chemin de restauration 2. Les nouvelles sauvegardes du journal de transactions sont créées sans créer de nouvelle sauvegarde complète. En raison d'une corruption des données ou d'autres problèmes, vous ne pouvez pas restaurer la base de données actuelle tant qu'une nouvelle sauvegarde complète n'est pas créée. De plus, il n'est pas possible d'appliquer les journaux de transactions créés dans le chemin de récupération 2 à la sauvegarde complète appartenant au chemin de récupération 1.

Si vous appliquez des sauvegardes du journal de transactions, vous pouvez également spécifier une date et une heure particulières à laquelle vous souhaitez arrêter l'application des transactions sauvegardées. Pour ce

faire, vous spécifiez une date et une heure dans la plage disponible et le SnapCenter supprime toutes les transactions qui n'ont pas été validées avant ce point dans le temps. Vous pouvez utiliser cette méthode pour restaurer les bases de données à un point dans le temps avant qu'une corruption ne se produise ou pour effectuer une restauration à partir d'une base de données ou d'une table supprimée accidentelle.

### Exemple d'opération de restauration instantanée

Supposons que vous effectuez des sauvegardes de base de données complètes une fois à minuit et qu'une sauvegarde du journal de transactions est effectuée toutes les heures. La base de données tombe en panne à 9:45, mais vous sauvegardez toujours les journaux de transaction de la base de données défaillante. Vous pouvez choisir l'un des scénarios de restauration instantanée suivants :

- Restaurez la sauvegarde complète de la base de données effectuée à minuit et acceptez la perte des modifications apportées par la suite à la base de données. (Option : aucune)
- Restaurez la sauvegarde complète de la base de données et appliquez toutes les sauvegardes du journal de transactions jusqu'à 9 h 45 (Option : log jusqu'à)
- Restaurez la sauvegarde complète de la base de données et appliquez les sauvegardes du journal de transactions, en indiquant l'heure à laquelle vous souhaitez restaurer les transactions à partir du dernier ensemble de sauvegardes du journal de transactions. (Option : par heure spécifique)

Dans ce cas, vous calculerez la date et l'heure auxquelles une certaine erreur a été signalée. Toutes les transactions qui n'ont pas été validées avant la date et l'heure spécifiées sont supprimées.

## Définissez une stratégie de clonage pour SQL Server

La définition d'une stratégie de clonage vous permet de cloner votre base de données avec succès.

1. Examinez les limites liées aux opérations de clonage.
2. Choisissez le type de clone dont vous avez besoin.

### Limites des opérations de clonage

Avant de cloner les bases de données, vous devez connaître les limites des opérations de clonage.

- Si vous utilisez une version d'Oracle de 11.2.0.4 à 12.1.0.1, l'opération clone sera à l'état suspendu lorsque vous exécutez la commande *renamedg*. Vous pouvez appliquer le correctif Oracle 19544733 pour résoudre ce problème.
- Le clonage de bases de données à partir d'une LUN directement connectée à un hôte (par exemple, en utilisant l'initiateur iSCSI Microsoft sur un hôte Windows) vers un VMDK ou une LUN RDM sur le même hôte Windows, ou un autre hôte Windows, ou vice versa, n'est pas pris en charge.
- Le répertoire racine du point de montage du volume ne peut pas être un répertoire partagé.
- Si vous déplacez une LUN contenant un clone vers un nouveau volume, le clone ne peut pas être supprimé.

### Types d'opérations de clonage

Vous pouvez utiliser SnapCenter pour cloner une base de données de sauvegarde SQL Server ou une base de données de production.

- Clonage à partir d'une sauvegarde de base de données

La base de données clonée peut servir de référence pour le développement de nouvelles applications et contribuer à isoler les erreurs liées aux applications qui se produisent dans l'environnement de production. La base de données clonée peut également être utilisée pour la restauration suite à des erreurs de base de données logicielle.

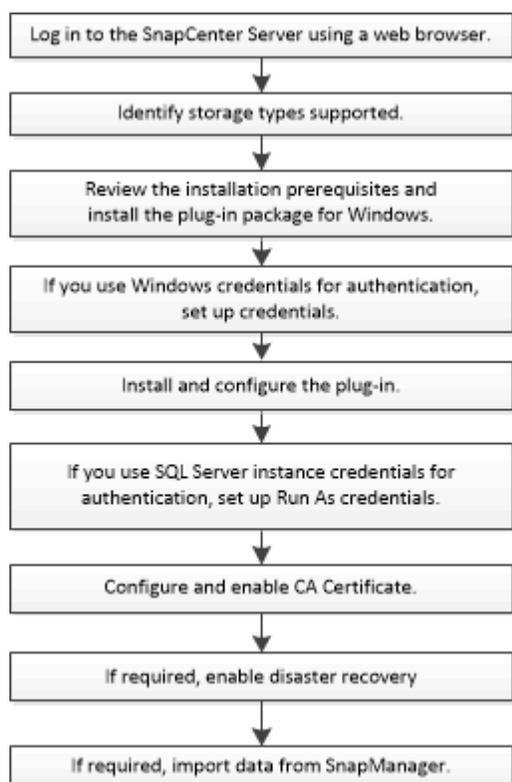
- Cycle de vie des clones

SnapCenter peut être utilisé pour planifier des tâches de clonage récurrentes qui se produiront lorsque la base de données de production n'est pas occupée.

## Préparez-vous à installer le plug-in SnapCenter pour Microsoft SQL Server

### Workflow d'installation pour le plug-in SnapCenter pour Microsoft SQL Server

Vous devez installer et configurer le plug-in SnapCenter pour Microsoft SQL Server si vous souhaitez protéger les bases de données SQL Server.



### Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour Microsoft SQL Server

Avant d'ajouter un hôte et d'installer les packages de plug-ins, vous devez respecter toutes les exigences.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous devez disposer d'un utilisateur disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.

- Si vous gérez des nœuds de cluster dans SnapCenter, vous devez disposer d'un utilisateur disposant de privilèges d'administration sur tous les nœuds du cluster.
- Vous devez disposer d'un utilisateur avec des autorisations sysadmin sur le serveur SQL.

Le plug-in SnapCenter pour Microsoft SQL Server utilise l'infrastructure VDI Microsoft, qui requiert l'accès sysadmin.

["Article 2926557 du support Microsoft : les opérations de sauvegarde et de restauration VDI SQL Server nécessitent des privilèges sysadmin"](#)

- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Si SnapManager pour Microsoft SQL Server est installé, vous devez avoir arrêté ou désactivé le service et les programmes.

Si vous envisagez d'importer des tâches de sauvegarde ou de clonage dans SnapCenter, ne désinstallez pas SnapManager pour Microsoft SQL Server.

- L'hôte doit être résolu au nom de domaine complet (FQDN) du serveur.

Si le fichier hosts est modifié pour le rendre résolu et si le nom court et le FQDN sont spécifiés dans le fichier hosts, créez une entrée dans le fichier hosts SnapCenter au format suivant : <adresse\_ip> <nom\_hôte> <nom\_hôte>

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	Microsoft Windows  Pour obtenir les dernières informations sur les versions prises en charge, consultez le " <a href="#">Matrice d'interopérabilité NetApp</a> ".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO

Élément	De formation
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <p> Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java et OpenJDK</li> </ul> <p>Java 11 Oracle Java et OpenJDK sont requis uniquement pour SAP HANA, IBM DB2, PostgreSQL, MySQL, les plug-ins pris en charge par NetApp et d'autres applications personnalisées qui peuvent être installées sur l'hôte Windows.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section "<a href="#">La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet</a>".</p>

## Configurer les informations d'identification pour le progiciel de plug-ins SnapCenter pour Windows

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

### Avant de commencer

- Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

- Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.
- Authentification SQL sur les hôtes Windows

Vous devez configurer les informations d'identification SQL après l'installation des plug-ins.

Si vous déployez le plug-in SnapCenter pour Microsoft SQL Server, vous devez configurer les informations d'identification SQL après l'installation des plug-ins. Configurez les informations d'identification d'un utilisateur avec les autorisations SQL Server sysadmin.

La méthode d'authentification SQL s'authentifie par rapport à une instance SQL Server. Cela signifie qu'une instance SQL Server doit être découverte dans SnapCenter. Par conséquent, avant d'ajouter un identifiant SQL, vous devez ajouter un hôte, installer des modules de plug-in et actualiser les ressources. Vous avez besoin de l'authentification SQL Server pour effectuer des opérations telles que la planification ou la détection des ressources.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Entrez un nom pour l'identifiant.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur/Mot de passe	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>• Administrateur de domaine <p>Spécifiez l'administrateur de domaine sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li>◦ NetBIOS\UserName</li> <li>◦ Domain FQDN\UserName</li> </ul> </li> <li>• Administrateur local (groupes de travail uniquement) <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <code>UserName</code></p> <p>N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p> </li> </ul>
Mode d'authentification	<p>Sélectionnez le mode d'authentification que vous souhaitez utiliser. Si vous sélectionnez le mode d'authentification SQL, vous devez également spécifier l'instance de serveur SQL et l'hôte où se trouve l'instance SQL.</p>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

## Configurer les informations d'identification d'une ressource SQL Server individuelle

Vous pouvez configurer les informations d'identification pour exécuter des tâches de protection des données sur des ressources SQL Server individuelles pour chaque

utilisateur. Bien que vous puissiez configurer les informations d'identification globalement, vous pouvez ne le faire que pour une ressource particulière.

### Description de la tâche

- Si vous utilisez des informations d'identification Windows pour l'authentification, vous devez configurer vos informations d'identification avant d'installer les plug-ins.

Toutefois, si vous utilisez une instance SQL Server pour l'authentification, vous devez ajouter les informations d'identification après l'installation des plug-ins.

- Si vous avez activé l'authentification SQL lors de la configuration des informations d'identification, l'instance découverte ou la base de données s'affiche avec une icône de cadenas rouge.

Si l'icône de cadenas apparaît, vous devez spécifier les informations d'identification de l'instance ou de la base de données pour pouvoir ajouter l'instance ou la base de données à un groupe de ressources.

- Vous devez attribuer ces informations d'identification à un utilisateur de contrôle d'accès basé sur des rôles (RBAC) sans accès sysadmin dans les conditions suivantes :
  - Les informations d'identification sont affectées à une instance SQL.
  - L'instance ou l'hôte SQL est affecté à un utilisateur RBAC.

L'utilisateur doit disposer à la fois des privilèges de groupe de ressources et de sauvegarde.

### Étape 1 : ajout et configuration des informations d'identification

1. Dans le volet de navigation de gauche, sélectionnez **Paramètres**.
2. Dans la page Paramètres, sélectionnez **informations d'identification**.
  - a. Pour ajouter une nouvelle information d'identification, sélectionnez **Nouveau**.
  - b. Dans la page informations d'identification, configurez les informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur	<p>Entrez le nom d'utilisateur utilisé pour l'authentification SQL Server.</p> <ul style="list-style-type: none"> <li>• L'administrateur de domaine ou tout membre du groupe d'administrateurs spécifie l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ <b>Nom d'utilisateur</b> sont les suivants : <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\username</i></li> <li>◦ <i>Domain FQDN\username</i></li> </ul> </li> <li>• Administrateur local (groupes de travail uniquement) pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide pour le champ <b>Nom d'utilisateur</b> est : <i>nom_utilisateur</i></li> </ul>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification SQL Server. Vous pouvez également choisir l'authentification Windows si l'utilisateur Windows dispose de privilèges sysadmin sur le serveur SQL.
Hôte	Sélectionnez l'hôte.
Instance SQL Server	Sélectionnez l'instance SQL Server.

c. Sélectionnez **OK** pour ajouter les informations d'identification.

## Étape 2 : configurer les instances

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**.
2. Dans la page Ressources, sélectionnez **instance** dans la liste **Affichage**.
  - a. Sélectionnez image::.../media/filter\_icon.png[filter icon], puis sélectionnez le nom d'hôte pour filtrer les instances.
  - b. Sélectionnez image::.../media/filter\_icon.png[filter icon] pour fermer le volet de filtre.
3. Dans la page protection d'instance, protégez l'instance et, si nécessaire, sélectionnez **configurer les informations d'identification**.

Si l'utilisateur connecté au serveur SnapCenter n'a pas accès au plug-in SnapCenter pour Microsoft SQL Server, alors l'utilisateur doit configurer les informations d'identification.



L'option d'informations d'identification ne s'applique pas aux bases de données et aux groupes de disponibilité.

4. Sélectionnez **Actualiser les ressources**.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

### Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

### Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediately
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

Par exemple :

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :
  - a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Installez le plug-in SnapCenter pour Microsoft SQL Server

### Ajoutez des hôtes et installez le package de plug-ins SnapCenter pour Windows

Vous devez utiliser la page SnapCenter **Ajouter hôte** pour ajouter des hôtes et installer le module de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants.

#### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré, vous devez désactiver l'UAC sur l'hôte.

- Vous devez vous assurer que le service de mise en file d'attente des messages est en cours d'exécution.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

["Configurez le compte de service géré par groupe sous Windows Server 2016 ou version ultérieure pour SQL"](#)

### Description de la tâche

Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.

Vous pouvez ajouter un hôte et installer les modules d'extension pour un hôte individuel ou pour un cluster. Si vous installez les plug-ins sur un cluster ou Windows Server Failover Clustering (WSFC), les plug-ins sont installés sur tous les nœuds du cluster.

Pour plus d'informations sur la gestion des hôtes, reportez-vous à la section ["Gérer les hôtes"](#).

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Sélectionnez **Ajouter**.
4. Dans la page hôtes, procédez comme suit :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez Windows comme type d'hôte. Le serveur SnapCenter ajoute l'hôte, puis installe le plug-in pour Windows si le plug-in n'est pas déjà installé sur l'hôte.</p> <p>Si vous sélectionnez l'option Microsoft SQL Server sur la page Plug-ins, le serveur SnapCenter installe le plug-in pour SQL Server.</p>
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. L'adresse IP n'est prise en charge pour les hôtes de domaine non approuvés que si elle résout le FQDN.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p> <p>Vous pouvez entrer les adresses IP ou FQDN de l'un des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Hôte autonome</li> <li>• WSFC si vous ajoutez un hôte à l'aide de SnapCenter et que l'hôte fait partie d'un sous-domaine, vous devez fournir le FQDN.</li> </ul>

Pour ce champ...	Procédez comme ça...
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom d'identification que vous avez spécifié.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section **Select Plug-ins to Install**, sélectionnez les plug-ins à installer.

6. Sélectionnez **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p> </div>
Chemin d'installation	<p>Le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez éventuellement personnaliser le chemin.</p>
Ajoutez tous les hôtes du cluster	<p>Cochez cette case pour ajouter tous les nœuds du cluster dans un WSFC ou un groupe de disponibilité SQL. Vous devez ajouter tous les nœuds du cluster en cochant la case de cluster appropriée dans l'interface graphique si vous souhaitez gérer et identifier plusieurs groupes de disponibilité SQL disponibles dans un cluster.</p>

Pour ce champ...	Procédez comme ça...
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	<p>Cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <p>Indiquez le nom GMSA au format suivant : domainname\accountName\$.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si l'hôte est ajouté avec GMSA et si le GMSA dispose de privilèges d'ouverture de session et d'administrateur système, le GMSA sera utilisé pour se connecter à l'instance SQL.</p> </div>

7. Sélectionnez **soumettre**.

8. Pour le plug-in SQL, sélectionnez l'hôte pour configurer le répertoire du journal.

- a. Sélectionnez **Configure log Directory** et dans la page Configure host log Directory, sélectionnez **Browse** et procédez comme suit :

Seules les LUN NetApp (disques) sont répertoriées pour être sélectionnées. SnapCenter sauvegarde et réplique le répertoire journal de l'hôte dans le cadre de l'opération de sauvegarde.

- i. Sélectionnez la lettre de lecteur ou le point de montage sur l'hôte sur lequel le journal hôte sera stocké.
- ii. Choisissez un sous-répertoire, le cas échéant.
- iii. Sélectionnez **Enregistrer**.

9. Sélectionnez **soumettre**.

Si vous n'avez pas coché la case **Skip précontrôles**, l'hôte est validé pour vérifier s'il répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse C:\Program Files\NetApp\SnapCenter\WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

10. Surveillez la progression de l'installation.

### Installez le plug-in SnapCenter pour Microsoft SQL Server sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer le plug-in SnapCenter pour Microsoft SQL Server simultanément sur plusieurs hôtes à l'aide de l'applet de commande Install-SmHostPackage PowerShell.

#### Avant de commencer

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

#### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande Open-SmConnection, puis saisissez vos informations d'identification.
3. Installez le plug-in SnapCenter pour Microsoft SQL Server sur plusieurs hôtes distants à l'aide de l'applet de commande Install-SmHostPackage et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Vous pouvez utiliser l'option `-skipreccheck` lorsque vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

4. Saisissez vos informations d'identification pour l'installation à distance.

### Installez le plug-in SnapCenter pour Microsoft SQL Server silencieusement à partir de la ligne de commande

Vous devez installer le plug-in SnapCenter pour Microsoft SQL Server à partir de l'interface utilisateur SnapCenter. Cependant, si vous ne pouvez pas pour une raison quelconque, vous pouvez exécuter le programme d'installation du plug-in pour SQL Server sans surveillance en mode silencieux à partir de la ligne de commande Windows.

#### Avant de commencer

- Vous devez supprimer la version antérieure du plug-in SnapCenter pour Microsoft SQL Server avant de procéder à l'installation.

Pour plus d'informations, voir ["Comment installer un plug-in SnapCenter manuellement et directement à partir de l'hôte du plug-in"](#).

## Étapes

1. Vérifiez si le dossier C:\temp existe sur l'hôte du plug-in et que l'utilisateur connecté dispose d'un accès complet.
2. Téléchargez le logiciel du plug-in pour SQL Server depuis C:\ProgramData\NetApp\SnapCenter\Package Repository.

Ce chemin est accessible à partir de l'hôte sur lequel le serveur SnapCenter est installé.

3. Copiez le fichier d'installation sur l'hôte sur lequel vous souhaitez installer le plug-in.
4. À partir d'une invite de commande Windows sur l'hôte local, accédez au répertoire dans lequel vous avez enregistré les fichiers d'installation du plug-in.
5. Installez le plug-in pour le logiciel SQL Server :

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
/log"Log_Path" BI_SNAPCENTER_PORT=Num
SUITE_INSTALLDIR="Install_Directory_Path"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCSQL
```

Remplacez les valeurs de paramètre fictif par vos données

- Debug\_Log\_Path est le nom et l'emplacement du fichier journal du programme d'installation de la suite.
- Log\_Path est l'emplacement des journaux d'installation des composants du plug-in (SCW, SCSQL et SMCORE).
- Num est le port sur lequel SnapCenter communique avec SMCORE
- Install\_Directory\_Path est le répertoire d'installation du module d'extension hôte.
- Domaine\Administrator est le compte de service Web SnapCenter Plug-in pour Microsoft Windows.
- Mot de passe est le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows.

```
"snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\\" BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCSQL
```



Tous les paramètres transmis lors de l'installation de Plug-in pour SQL Server sont sensibles à la casse.

6. Surveillez le planificateur de tâches Windows, le fichier journal d'installation principal C:\Installdebug.log et les fichiers d'installation supplémentaires dans C:\Temp.
7. Surveillez le répertoire %temp% pour vérifier que les programmes d'installation msiexec.exe installent le logiciel sans erreur.



L'installation du plug-in pour SQL Server enregistre le plug-in sur l'hôte et non sur le serveur SnapCenter. Vous pouvez enregistrer le plug-in sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Une fois l'hôte ajouté, le plug-in est automatiquement découvert.

## Contrôler l'état de l'installation du plug-in pour SQL Server

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

### Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

#### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

### Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

#### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :

- a. Double-cliquez sur le certificat.
- b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
- c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
- d. Copiez les caractères hexadécimaux de la zone.
- e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :

- a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

### Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

#### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCORE 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande run *set-SmCertificateSettings*.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de *get-SmCertificateSettings*.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Configurer la reprise après incident

### Reprise après incident du plug-in SnapCenter pour SQL Server

Lorsque le plug-in SnapCenter pour SQL Server est arrêté, procédez comme suit pour basculer vers un autre hôte SQL et restaurer les données.

#### Avant de commencer

- L'hôte secondaire doit avoir le même système d'exploitation, l'application et le même nom d'hôte que l'hôte principal.
- Placez le plug-in SnapCenter pour SQL Server sur un autre hôte à l'aide de la page **Ajouter hôte** ou **Modifier hôte**. Voir "[Gérer les hôtes](#)" pour en savoir plus.

#### Étapes

1. Sélectionnez l'hôte dans la page **hosts** pour modifier et installer le plug-in SnapCenter pour SQL Server.
2. (Facultatif) remplacez les fichiers de configuration du plug-in SnapCenter pour SQL Server de la sauvegarde de reprise après sinistre vers la nouvelle machine.
3. Importez les planifications Windows et SQL à partir du dossier du plug-in SnapCenter pour SQL Server à partir de la sauvegarde DR.

#### Informations associées

Voir la "[API de reprise après incident](#)" vidéo.

### Stockage de reprise après incident pour le plug-in SnapCenter pour SQL Server

Vous pouvez restaurer le plug-in SnapCenter pour stockage SQL Server en activant le mode DR pour le stockage sur la page Paramètres globaux.

#### Avant de commencer

- Assurez-vous que les plug-ins sont en mode de maintenance.
- Interrompre la relation SnapMirror/SnapVault "[Repousser les relations SnapMirror](#)"
- Reliez le LUN du système secondaire à l'ordinateur hôte avec la même lettre de lecteur.
- Assurez-vous que tous les disques sont connectés à l'aide des mêmes lettres que celles utilisées avant le DR.
- Redémarrez le service serveur MSSQL.
- Assurez-vous que les ressources SQL sont de nouveau en ligne.

#### Description de la tâche

La reprise après incident n'est pas prise en charge sur les configurations VMDK et RDM.

#### Étapes

1. Dans la page Paramètres, accédez à **Paramètres > Paramètres globaux > reprise après sinistre**.
2. Sélectionnez **Activer la récupération après sinistre**.

3. Cliquez sur **appliquer**.
4. Vérifiez si le travail DR est activé ou non en cliquant sur **Monitor > Jobs**.

### Une fois que vous avez terminé

- Si de nouvelles bases de données sont créées après le basculement, celles-ci seront en mode non-DR.

Les nouvelles bases de données continueront à fonctionner comme elles l'ont fait avant le basculement.

- Les nouvelles sauvegardes créées en mode DR seront répertoriées sous SnapMirror ou SnapVault (secondaire) sur la page topologie.

Une icône « i » s'affiche en regard des nouvelles sauvegardes pour indiquer que ces sauvegardes ont été créées en mode DR.

- Vous pouvez supprimer le plug-in SnapCenter pour les sauvegardes SQL Server créées lors du basculement à l'aide de l'interface utilisateur ou de l'applet de commande suivante : `Remove-SmBackup`
- Après le basculement, si vous souhaitez que certaines ressources soient en mode non-DR, utilisez l'applet de commande suivante : `Remove-SmResourceDRMode`

Pour plus d'informations, reportez-vous au "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

- Le serveur SnapCenter gère les ressources de stockage individuelles (bases de données SQL) en mode reprise après incident ou autre, mais pas le groupe de ressources avec les ressources de stockage en mode DR ou non.

### Rétablissement du plug-in SnapCenter pour le stockage secondaire SQL Server vers le stockage primaire

Une fois le stockage primaire du plug-in SnapCenter pour SQL Server de nouveau en ligne, il est préférable de revenir au stockage primaire.

#### Avant de commencer

- Placez le plug-in SnapCenter pour SQL Server en mode **Maintenance** à partir de la page hôtes gérés.
- Déconnectez le stockage secondaire de l'hôte et connectez-le au stockage principal.
- Pour revenir au stockage primaire, assurez-vous que la direction de la relation reste identique avant le basculement en effectuant l'opération de resynchronisation inverse.

Pour conserver les rôles de stockage primaire et secondaire après l'opération de resynchronisation inverse, effectuez à nouveau l'opération de resynchronisation inverse.

Pour plus d'informations, voir "[Resynchronisation inverse des relations du miroir](#)".

- Redémarrez le service serveur MSSQL.
- Assurez-vous que les ressources SQL sont de nouveau en ligne.



Lors du basculement ou de la restauration du plug-in, l'état global du plug-in n'est pas immédiatement actualisé. L'état global des hôtes et des plug-ins est mis à jour lors de l'opération de mise à jour suivante.

#### Étapes

1. Dans la page Paramètres, accédez à **Paramètres > Paramètres globaux > reprise après sinistre**.
2. Désélectionnez **Activer la reprise après sinistre**.
3. Cliquez sur **appliquer**.
4. Vérifiez si le travail DR est activé ou non en cliquant sur **Monitor > Jobs**.

### Une fois que vous avez terminé

Vous pouvez supprimer le plug-in SnapCenter pour les sauvegardes SQL Server créées lors du basculement à l'aide de l'interface utilisateur ou de l'applet de commande suivante : `Remove-SmDRFailoverBackups`

## Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM) ou si vous souhaitez protéger des VM et des datastores, vous devez déployer l'appliance virtuelle du plug-in SnapCenter pour VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section "[Présentation du déploiement](#)".

### Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Créez ou importez un certificat SSL](#)".

### Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est `/opt/netapp/config/crl`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

## Préparation à la protection des données

### Conditions préalables à l'utilisation du plug-in SnapCenter pour Microsoft SQL Server

Avant de commencer à utiliser le plug-in pour SQL Server, l'administrateur SnapCenter doit installer et configurer SnapCenter Server et effectuer les tâches préalables.

- Installer et configurer SnapCenter Server.
- Connectez-vous à SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant ou en attribuant des connexions du système de stockage et en créant des identifiants.



SnapCenter ne prend pas en charge plusieurs SVM de même nom sur différents clusters. Chaque SVM pris en charge par SnapCenter doit avoir un nom unique.

- Ajoutez des hôtes, installez les plug-ins, découvrez (actualisez) les ressources et configurez les plug-ins.

- Déplacez une base de données Microsoft SQL Server existante d'un disque local vers un LUN NetApp ou inversement en exécutant Invoke-SmConfigureResources.

Pour plus d'informations sur l'exécution de l'applet de commande, reportez-vous au ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#)

- Si vous utilisez SnapCenter Server pour protéger les bases de données SQL résidant sur des LUN ou des VMDK VMware RDM, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter. La documentation du plug-in SnapCenter pour VMware vSphere contient des informations supplémentaires.

["Documentation du plug-in SnapCenter pour VMware vSphere"](#)

- Provisionnez le stockage côté hôte à l'aide du plug-in SnapCenter pour Microsoft Windows.
- Configurez les relations SnapMirror et SnapVault, si vous souhaitez effectuer une réplication de sauvegarde.

Pour plus de détails, consultez les informations sur l'installation de SnapCenter.

Pour les utilisateurs de SnapCenter 4.1.1, la documentation du plug-in SnapCenter pour VMware vSphere 4.1.1 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers. Pour les utilisateurs de SnapCenter 4.2.x, NetApp Data Broker 1.0 et 1.0.1, la documentation relative à la protection des bases de données et des systèmes de fichiers virtualisés à l'aide du plug-in SnapCenter pour VMware vSphere fourni par le dispositif virtuel NetApp Data Broker basé sur Linux (format Open Virtual Appliance). Pour les utilisateurs de SnapCenter 4.3.x, la documentation du plug-in SnapCenter pour VMware vSphere 4.3 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers à l'aide du plug-in SnapCenter basé sur Linux pour l'appliance virtuelle VMware vSphere (format Open Virtual Appliance).

["Documentation du plug-in SnapCenter pour VMware vSphere"](#)

## **Utilisation des ressources, des groupes de ressources et des stratégies pour la protection de SQL Server**

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des bases de données, des instances de base de données ou des groupes de disponibilité Microsoft SQL Server que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte ou un cluster.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

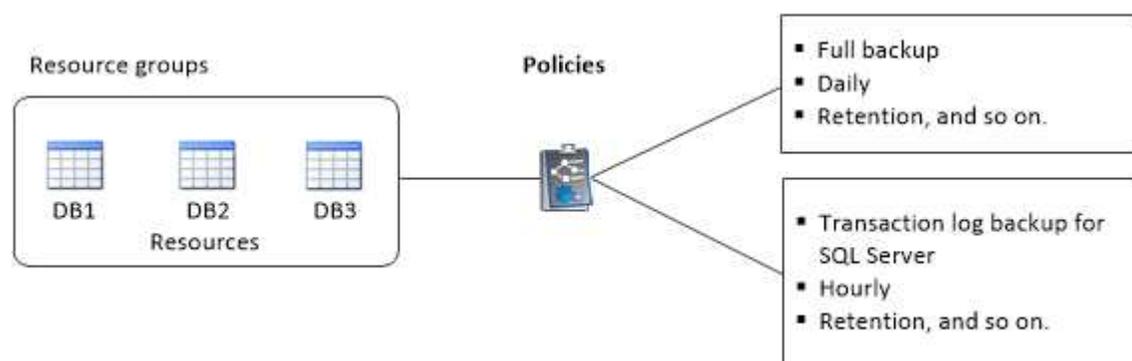
Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Ces règles précisent la fréquence des sauvegardes, la conservation des copies, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

Pensez à un groupe de ressources comme définissant *quoi* vous voulez protéger et quand vous voulez le protéger en termes de jour et de temps. Pensez à une stratégie comme définir *comment* vous voulez la protéger. Si vous sauvegardez toutes les bases de données ou que vous sauvegardez tous les systèmes de fichiers d'un hôte, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données ou tous les systèmes de fichiers de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources pour effectuer une sauvegarde complète tous les jours et un autre programme qui effectue des sauvegardes de journaux toutes les heures.

L'image suivante illustre la relation entre les ressources, les groupes de ressources et les politiques des bases de données :



## Sauvegardez la base de données SQL Server, l'instance ou le groupe de disponibilité

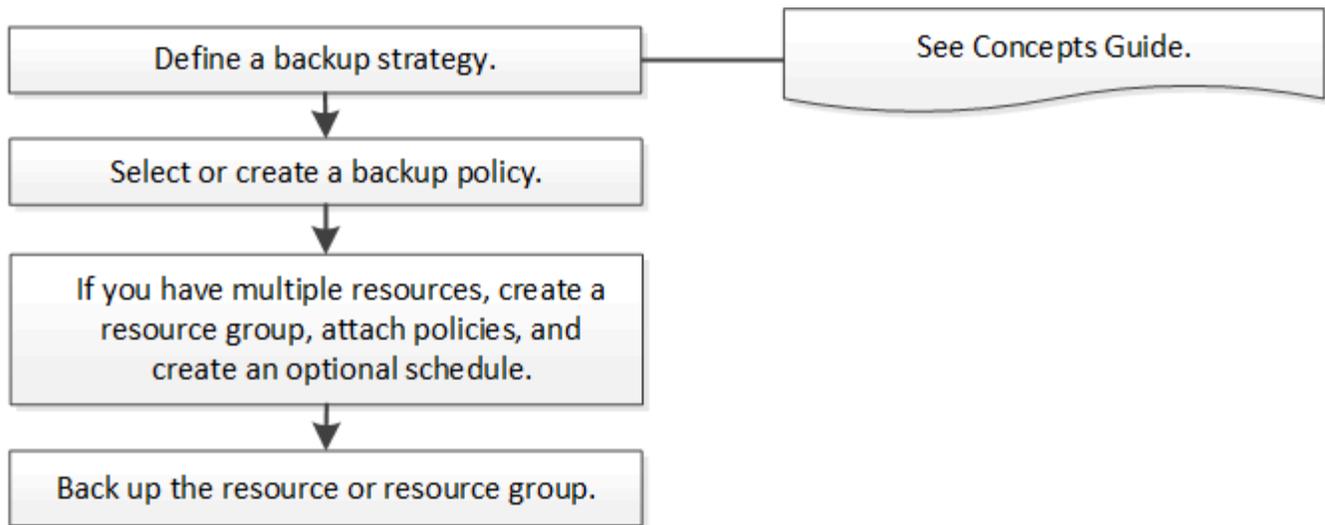
### Workflow de sauvegarde

Lorsque vous installez le plug-in SnapCenter pour Microsoft SQL Server dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder les ressources SQL Server.

Vous pouvez planifier plusieurs sauvegardes pour les exécuter simultanément sur plusieurs serveurs.

Les opérations de sauvegarde et de restauration ne peuvent pas être effectuées simultanément sur la même ressource.

Le workflow suivant montre l'ordre dans lequel vous devez effectuer les opérations de sauvegarde :



Les options sauvegarde immédiate, restauration, gestion des sauvegardes et clonage de la page Ressources sont désactivées si vous sélectionnez un LUN non NetApp, une base de données corrompue ou une base de données en cours de restauration.

Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration, de vérification et de clonage. Pour plus d'informations sur les applets de commande PowerShell, utilisez l'aide du cmdlet SnapCenter ou consultez le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#)

### Sauvegarde des bases de données par SnapCenter

SnapCenter utilise la technologie Snapshot pour sauvegarder les bases de données SQL Server qui résident sur des LUN ou des VMDK. SnapCenter crée la sauvegarde en créant des snapshots des bases de données.

Lorsque vous sélectionnez une base de données pour une sauvegarde complète de base de données dans la page Ressources, SnapCenter sélectionne automatiquement toutes les autres bases de données qui résident sur le même volume de stockage. Si le LUN ou VMDK ne stocke qu'une seule base de données, vous pouvez effacer ou resélectionner la base de données individuellement. Si le LUN ou VMDK contient plusieurs bases de données, vous devez effacer ou resélectionner les bases de données en tant que groupe.

Toutes les bases de données qui résident sur un seul volume sont sauvegardées simultanément à l'aide des snapshots. Si le nombre maximal de bases de données de sauvegarde simultanées est de 35 et si plus de 35 bases de données résident dans un volume de stockage, le nombre total de snapshots créés est égal au nombre de bases de données divisé par 35.



Vous pouvez configurer le nombre maximal de bases de données pour chaque Snapshot dans la règle de sauvegarde.

Lorsque SnapCenter crée une copie Snapshot, l'intégralité du volume du système de stockage est capturée dans la copie Snapshot. Cependant, la sauvegarde n'est valide que pour le serveur hôte SQL pour lequel la sauvegarde a été créée.

Si les données d'autres serveurs hôtes SQL résident sur le même volume, elles ne peuvent pas être restaurées à partir du Snapshot.

### Plus d'informations

## Déterminer si des ressources sont disponibles pour les sauvegardes

Les ressources sont les bases de données, les instances d'application, les groupes de disponibilité et des composants similaires gérés par les plug-ins que vous avez installés. Vous pouvez ajouter ces ressources aux groupes de ressources de sorte que vous puissiez effectuer des tâches de protection des données, mais vous devez d'abord identifier les ressources disponibles. La détermination des ressources disponibles permet également de vérifier que l'installation du plug-in s'est déroulée correctement.

### Avant de commencer

- Vous devez avoir déjà terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes, la création de connexions au système de stockage et l'ajout d'informations d'identification.
- Pour découvrir les bases de données Microsoft SQL, l'une des conditions suivantes doit être remplie.
  - L'utilisateur utilisé pour ajouter l'hôte du plug-in au serveur SnapCenter doit disposer des autorisations requises (sysadmin) sur le serveur Microsoft SQL.
  - Si la condition ci-dessus n'est pas remplie, dans le serveur SnapCenter, configurez l'utilisateur possédant les autorisations requises (sysadmin) sur le serveur Microsoft SQL. L'utilisateur doit être configuré au niveau de l'instance de Microsoft SQL Server et l'utilisateur peut être un utilisateur SQL ou Windows.
- Pour découvrir les bases de données Microsoft SQL dans un cluster Windows, vous devez débloquer le port TCP/IP de l'instance de cluster de basculement (FCI).
- Si les bases de données résident sur des LUN RDM ou des VMDK VMware, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter.

Pour plus d'informations, voir "[Déployez le plug-in SnapCenter pour VMware vSphere](#)"

- Si l'hôte est ajouté avec GMSA et si le GMSA dispose de privilèges d'ouverture de session et d'administrateur système, le GMSA sera utilisé pour se connecter à l'instance SQL.

### Description de la tâche

Vous ne pouvez pas sauvegarder les bases de données lorsque l'option **Etat général** de la page Détails est définie sur non disponible pour la sauvegarde. L'option **Etat général** est définie sur non disponible pour la sauvegarde lorsque l'un des éléments suivants est vrai :

- Les bases de données ne se trouvent pas sur un LUN NetApp.
- Les bases de données ne sont pas dans un état normal.

Les bases de données ne sont pas dans leur état normal lorsqu'elles sont hors ligne, restaurées, en attente, suspectes ou autres.

- Les bases de données disposent de privilèges insuffisants.

Par exemple, si un utilisateur dispose uniquement d'un accès en vue à la base de données, les fichiers et les propriétés de la base de données ne peuvent pas être identifiés et ne peuvent donc pas être sauvegardés.



SnapCenter ne peut sauvegarder la base de données primaire que si vous avez une configuration de groupe de disponibilité sous SQL Server Standard Edition.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database**, **instance** ou **Groupe de disponibilité** dans la liste déroulante **View**.

Cliquez sur  et sélectionnez le nom d'hôte et l'instance SQL Server pour filtrer les ressources. Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

3. Cliquez sur **Actualiser les ressources**.

Les ressources récemment ajoutées, renommées ou supprimées sont mises à jour dans l'inventaire du serveur SnapCenter.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

Les ressources s'affichent avec des informations telles que le type de ressource, le nom d'hôte ou de cluster, les groupes de ressources associés, le type de sauvegarde, les stratégies et l'état général.

- Si la base de données se trouve sur un système de stockage non-NetApp, `Not available for backup` S'affiche dans la colonne **Etat général**.

Vous ne pouvez pas effectuer d'opérations de protection des données sur une base de données se résidant sur un stockage non NetApp.

- Si la base de données se trouve sur un système de stockage NetApp et non protégée, `Not protected` S'affiche dans la colonne **Etat général**.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée, l'interface utilisateur s'affiche `Backup not run` Message dans la colonne **Etat général**.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée et si la sauvegarde est déclenchée pour la base de données, l'interface utilisateur s'affiche `Backup succeeded` Message dans la colonne **Etat général**.



Si vous avez activé une authentification SQL lors de la configuration des informations d'identification, l'instance découverte ou la base de données s'affiche avec une icône de cadenas rouge. Si l'icône de cadenas apparaît, vous devez spécifier les informations d'identification de l'instance ou de la base de données pour pouvoir ajouter l'instance ou la base de données à un groupe de ressources.

1. Une fois que l'administrateur SnapCenter a affecté les ressources à un utilisateur RBAC, l'utilisateur RBAC doit se connecter et cliquer sur **Actualiser les ressources** pour afficher le dernier **Etat général** des ressources.

## Migration des ressources vers un système de stockage NetApp

Une fois votre système de stockage NetApp provisionné à l'aide du plug-in SnapCenter

pour Microsoft Windows, vous pouvez migrer vos ressources vers le système de stockage NetApp ou d'un LUN NetApp vers un autre LUN NetApp à l'aide de l'interface graphique SnapCenter ou des applets de commande PowerShell.

#### Avant de commencer

- Vous devez avoir ajouté des systèmes de stockage à SnapCenter Server.
- Vous devez avoir actualisé (découvert) les ressources SQL Server.

La plupart des champs de ces pages de l'assistant sont explicites. Les informations suivantes décrivent certains des champs pour lesquels vous pouvez avoir besoin de conseils.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **instance** dans la liste déroulante **View**.
3. Sélectionnez la base de données ou l'instance dans la liste et cliquez sur **migrer**.
4. Dans la page Ressources, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
<b>Nom de base de données</b> (facultatif)	Si vous avez sélectionné une instance pour la migration, vous devez sélectionner les bases de données de cette instance dans la liste déroulante <b>Databases</b> .
<b>Sélectionnez destinations</b>	Sélectionnez l'emplacement cible des fichiers de données et de journaux.  Les fichiers de données et de journaux sont respectivement déplacés vers le dossier données et journaux sous le lecteur NetApp sélectionné. Si aucun dossier de la structure de dossiers n'est présent, un dossier est créé et la ressource est migrée.
<b>Afficher les détails du fichier de base de données</b> (facultatif)	Sélectionnez cette option pour migrer plusieurs fichiers d'une base de données unique.  <div style="display: flex; align-items: center;">  <p>Cette option ne s'affiche pas lorsque vous sélectionnez la ressource <b>instance</b>.</p> </div>

Pour ce champ...	Procédez comme ça...
Options	<p>Sélectionnez <b>Supprimer la copie de la base de données migrée à l'emplacement d'origine</b> pour supprimer la copie de la base de données de la source.</p> <p>Facultatif : <b>EXÉCUTEZ METTRE À JOUR LES STATISTIQUES sur les tables avant de détacher la base de données.</b></p>

5. Dans la page vérifier, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Options de vérification de cohérence de la base de données	<p>Sélectionnez <b>Exécuter avant</b> pour vérifier l'intégrité de la base de données avant la migration.</p> <p>Sélectionnez <b>Exécuter après</b> pour vérifier l'intégrité de la base de données après la migration.</p>
Options DBCC CHECKDB	<ul style="list-style-type: none"> <li>• Sélectionnez l'option <b>PHYSICAL_ONLY</b> pour limiter le contrôle d'intégrité à la structure physique de la base de données et détecter les pages déchirées, les échecs de somme de contrôle et les défaillances matérielles courantes qui ont un impact sur la base de données.</li> <li>• Sélectionnez l'option <b>NO_INFOMSGS</b> pour supprimer tous les messages d'information.</li> <li>• Sélectionnez l'option <b>ALL_ERRORMSGs</b> pour afficher toutes les erreurs signalées par objet.</li> <li>• Sélectionnez l'option <b>*ABSENCE D'index en cluster</b> si vous ne souhaitez pas vérifier les index non mis en cluster.</li> </ul> <p>La base de données SQL Server utilise le vérificateur de cohérence de base de données Microsoft SQL Server (DBCC) pour vérifier l'intégrité logique et physique des objets de la base de données.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  Vous pouvez sélectionner cette option pour réduire la durée d'exécution. </div> <ul style="list-style-type: none"> <li>• Sélectionnez l'option <b>TABLOCK</b> pour limiter les vérifications et obtenir des verrous au lieu d'utiliser un instantané de base de données interne.</li> </ul>

6. Examinez le résumé, puis cliquez sur **Terminer**.

## Créer des stratégies de sauvegarde pour les bases de données SQL Server

Vous pouvez créer une stratégie de sauvegarde pour la ressource ou le groupe de ressources avant d'utiliser SnapCenter pour sauvegarder les ressources SQL Server, ou vous pouvez créer une stratégie de sauvegarde au moment où vous créez un groupe de ressources ou sauvegardez une seule ressource.

### Avant de commencer

- Vous devez avoir défini votre stratégie de protection des données.
- Vous devez être prêt à préparer la protection des données en exécutant des tâches telles que l'installation d'SnapCenter, l'ajout d'hôtes, l'identification des ressources et la création de connexions du système de stockage.
- Vous devez avoir configuré le répertoire du journal hôte pour la sauvegarde des journaux.
- Vous devez avoir actualisé (découvert) les ressources SQL Server.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir attribué des machines virtuelles de stockage (SVM) pour les volumes source et de destination.

Pour plus d'informations sur la manière dont les administrateurs attribuent des ressources aux utilisateurs, consultez les informations d'installation de SnapCenter.

- Si vous souhaitez exécuter les scripts PowerShell dans les scripts prescripteurs et postscripts, définissez la valeur du paramètre usePowerProcessforScripts sur true dans le fichier web.config.

La valeur par défaut est FALSE.

- Vérifiez les prérequis et les limites spécifiques de la synchronisation active SnapMirror. Pour plus d'informations, reportez-vous à "[Limites d'objet pour la synchronisation active SnapMirror](#)".

### Description de la tâche

- Une stratégie de sauvegarde est un ensemble de règles qui régit la façon dont vous gérez et conservez les sauvegardes, ainsi que la fréquence de sauvegarde de la ressource ou du groupe de ressources. En outre, vous pouvez spécifier des paramètres de réplication et de script. La définition d'options dans une stratégie permet de gagner du temps lorsque vous souhaitez réutiliser la stratégie pour un autre groupe de ressources.

Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreserviceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.

La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.

Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étape 1 : création d'un nom de stratégie

1. Dans le volet de navigation de gauche, sélectionnez **Paramètres**.
2. Dans la page Paramètres, sélectionnez **stratégies**.
3. Sélectionnez **Nouveau**.
4. Sur la page **Nom**, entrez le nom et les détails de la stratégie.

### Étape 2 : configuration des options de stratégie

1. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez votre type de stockage.
  - b. Sélectionnez la portée de la règle.

### Sauvegarde complète et sauvegarde des journaux

Sauvegardez les fichiers de base de données et les journaux de transactions et tronquez les journaux de transactions.

- i. Sélectionnez **sauvegarde complète et sauvegarde du journal**.
- ii. Entrez le nombre maximal de bases de données à sauvegarder pour chaque snapshot.



Vous devez augmenter cette valeur si vous souhaitez exécuter simultanément plusieurs opérations de sauvegarde.

### Sauvegarde complète

Sauvegardez les fichiers de base de données.

- i. Sélectionnez **sauvegarde complète**.
- ii. Entrez le nombre maximal de bases de données à sauvegarder pour chaque snapshot. La valeur par défaut est 100



Vous devez augmenter cette valeur si vous souhaitez exécuter simultanément plusieurs opérations de sauvegarde.

### Sauvegarde des journaux

- i. Sauvegardez les journaux de transactions.
- ii. Sélectionnez **sauvegarde journal**.

### Copie seule sauvegarde

- i. Si vous sauvegardez vos ressources à l'aide d'une autre application de sauvegarde, sélectionnez **copie uniquement sauvegarde**.

Le fait de préserver l'intégrité des journaux de transactions permet à toute application de sauvegarde de restaurer les bases de données. En règle générale, vous ne devez pas utiliser l'option de copie uniquement dans d'autres cas.



Microsoft SQL ne prend pas en charge l'option **copie uniquement sauvegarde** avec l'option **sauvegarde complète et sauvegarde de journal** pour stockage secondaire.

## Étape 3 : configurer les paramètres du groupe de disponibilité

1. Dans la section Paramètres du groupe de disponibilité, effectuez les opérations suivantes :

- a. Sauvegarde sur le réplica de sauvegarde préféré uniquement.

Sélectionnez cette option pour sauvegarder uniquement sur la réplique de sauvegarde préférée. La réplique de sauvegarde préférée est déterminée par les préférences de sauvegarde configurées pour l'AG dans SQL Server.

- b. Sélectionnez les répliques pour la sauvegarde.

Choisissez la réplique AG principale ou la réplique AG secondaire pour la sauvegarde.

- c. Sélectionnez la priorité de sauvegarde (priorité de sauvegarde minimale et maximale)

Spécifiez un numéro de priorité de sauvegarde minimum et un numéro de priorité de sauvegarde maximum qui déterminent la réplique AG pour la sauvegarde. Par exemple, vous pouvez avoir une priorité minimale de 10 et une priorité maximale de 50. Dans ce cas, toutes les répliques AG de priorité supérieure à 10 et inférieure à 50 sont considérées comme des sauvegardes.

Par défaut, la priorité minimale est 1 et la priorité maximale est 100.



Dans les configurations en cluster, les sauvegardes sont conservées sur chaque nœud du cluster en fonction des paramètres de conservation définis dans la règle. Si le nœud propriétaire de l'AG change, les sauvegardes sont prises en fonction des paramètres de conservation et les sauvegardes du nœud propriétaire précédent seront conservées. La conservation pour le groupe AG est applicable uniquement au niveau du nœud.

#### Étape 4 : configurer les paramètres de Snapshot et de réplication

1. Dans la page instantané et réplication, effectuez les opérations suivantes :

- a. Spécifiez le type d'horaire en sélectionnant **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

Vous ne pouvez sélectionner qu'un seul type de planification pour une stratégie.



Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais vous permet d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

#### Étape 5 : configurez les paramètres de conservation à chaud

1. Dans la section Paramètres de rétention à la minute, en fonction du type de sauvegarde sélectionné dans la page Type de sauvegarde, effectuez une ou plusieurs des opérations suivantes :

### Nombre spécifique de copies

Conservez uniquement un nombre spécifique d'instantanés.

1. Sélectionnez l'option **conserver les sauvegardes de journal applicables au dernier <chiffre> jours** et indiquez le nombre de jours à conserver. Si vous vous approchez de cette limite, vous pouvez supprimer des anciennes copies.

### Nombre spécifique de jours

Conservation des copies de sauvegarde pendant un nombre spécifique de jours.

1. Sélectionnez l'option **conserver les sauvegardes de journal applicables à <nombre> jours de sauvegardes complètes** et spécifiez le nombre de jours pour conserver les copies de sauvegarde de journal.

## Étape 6 : configurer les paramètres de snapshot

1. Pour les paramètres de conservation de sauvegarde complète, effectuez les opérations suivantes :
  - a. Spécifiez le nombre total d'instantanés à conserver
    - i. Pour spécifier le nombre d'instantanés à conserver, sélectionnez **copies à conserver**.
    - ii. Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.



Par défaut, la valeur du nombre de rétention est définie sur 2. Si vous définissez le nombre de rétention sur 1, l'opération de rétention risque d'échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.



La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version NetApp ONTAP sous-jacente.

1. Durée de conservation des snapshots
  - a. Si vous souhaitez spécifier le nombre de jours pendant lesquels vous souhaitez conserver les snapshots avant de les supprimer, sélectionnez **conserver les copies pour**.
2. Si vous souhaitez spécifier la période de verrouillage de la copie d'instantané principale, sélectionnez **période de verrouillage de la copie d'instantané principale** et sélectionnez jours, mois ou années.

La période de conservation SnapLock doit être inférieure à 100 ans.
3. Si vous souhaitez spécifier la période de verrouillage de la copie d'instantané secondaire, sélectionnez **période de verrouillage de la copie d'instantané secondaire**, puis sélectionnez jours, mois ou années.

Dans cet exemple, la conservation des snapshots de journal est de 2 :

## Exemple 1. Montrer l'exemple

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup' -PluginPolicyType 'CSQL' -sqlbackuptype
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},@{BackupType='BACKUPTYPE=
';ReductionHourly='LOG';RetenCount='BackupType},
'RegroupeHourly='Hourly';RetenCount='BACKUPTYPE';RegroupeHourly=';RetenCount=';Regroupe
Hourly='
```

"SnapCenter conserve les copies Snapshot de la base de données"

### 4. Sélectionnez un libellé d'instantané

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

## Étape 7 : configurer les options de réplication secondaire

1. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

### Mettez SnapMirror à jour

Mettez à jour SnapMirror après la création d'une copie Snapshot locale.

1. Sélectionnez cette option pour créer des copies miroir des jeux de sauvegarde sur un autre volume (SnapMirror).

Cette option doit être activée pour la synchronisation active SnapMirror.

Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton **Rafraîchir** de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.

Voir "[Afficher les sauvegardes et clones SQL Server sur la page topologie](#)".

### Mettre à jour SnapVault

Mettre à jour SnapVault après avoir créé une copie Snapshot

1. Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque.

Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton **Rafraîchir** de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.

Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton **Actualiser** de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.

Pour plus d'informations sur le coffre-fort SnapLock, voir "[Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé](#)".

Voir "[Afficher les sauvegardes et clones SQL Server sur la page topologie](#)".

### Nombre de tentatives d'erreur

1. Saisissez le nombre de tentatives de réplication qui doivent se produire avant l'interruption du processus.

## Étape 8 : configurer les paramètres de script

1. Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript qui doivent être exécutés avant ou après l'opération de sauvegarde, respectivement.

Par exemple, vous pouvez exécuter un script pour mettre à jour les traps SNMP, automatiser les alertes et envoyer des logs.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP de sorte que le stockage secondaire n'atteigne pas la limite maximale des snapshots.

## Étape 9 : configurer les paramètres de vérification

Dans la page Vérification, effectuez les opérations suivantes :

1. Dans la section Exécuter la vérification pour les programmes de sauvegarde suivants, sélectionnez la fréquence de planification.
2. Dans la section Options de vérification de cohérence de la base de données, effectuez les opérations suivantes :
  - a. Limiter la structure d'intégrité à la structure physique de la base de données (PHYSIQUE\_UNIQUEMENT)
    - i. Sélectionnez **Limit the Integrity structure to Physical structure of the database (PHYSICAL\_ONLY)** (limiter la vérification de l'intégrité à la structure physique de la base de données) et pour détecter les pages déchirées, les échecs de somme de contrôle et les défaillances matérielles courantes qui affectent la base de données.
  - b. Supprimer tous les messages d'information (PAS d'INFOMSGS)
    - i. Sélectionnez **Supprimer tous les messages d'information (NO\_INFOMSGS)** pour supprimer tous les messages d'information. Sélectionné par défaut.
  - c. Afficher tous les messages d'erreur signalés par objet (ALL\_ERRORMSGs)
    - i. Sélectionnez **Afficher tous les messages d'erreur signalés par objet (ALL\_ERRORMSGs)** pour afficher toutes les erreurs signalées par objet.
  - d. Ne pas vérifier les index non mis en cluster (ABSENCE DE clusters)
    - i. Sélectionnez **ne pas cocher les index non clusterisés (REGROUPÉS EN CLUSTERS)** si vous ne souhaitez pas vérifier les index non clusterisés. La base de données SQL Server utilise le vérificateur de cohérence de base de données Microsoft SQL Server (DBCC) pour vérifier l'intégrité logique et physique des objets de la base de données.
  - e. Limiter les vérifications et obtenir les verrous au lieu d'utiliser un instantané de base de données interne (TABLOCK)
    - i. Sélectionnez **limiter les vérifications et obtenir les verrous au lieu d'utiliser une copie Snapshot de base de données interne (TABLOCK)** pour limiter les vérifications et obtenir des verrous au lieu d'utiliser un instantané de base de données interne.
3. Dans la section **Log Backup**, sélectionnez **Verify log backup upon terminés** pour vérifier la sauvegarde du journal à la fin de l'opération.
4. Dans la section **Paramètres du script de vérification**, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript qui doivent être exécutés avant ou après l'opération de vérification, respectivement.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

## Étape 10 : passez en revue le résumé

1. Passez en revue le résumé, puis sélectionnez **Terminer**.

## Créez des groupes de ressources et associez des stratégies pour SQL Server

Un groupe de ressources est un conteneur dans lequel vous ajoutez des ressources que vous souhaitez sauvegarder et protéger ensemble. Un groupe de ressources vous

permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

Vous pouvez protéger les ressources individuellement sans créer de nouveau groupe de ressources. Vous pouvez effectuer des sauvegardes sur la ressource protégée.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- L'ajout de nouvelles bases de données sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec la synchronisation active SnapMirror n'est pas pris en charge.
- L'ajout de nouvelles bases de données à un groupe de ressources existant en mode de basculement de la synchronisation active SnapMirror n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement à l'état normal ou de retour arrière.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.



Si vous avez récemment ajouté une ressource à SnapCenter, cliquez sur **Actualiser les ressources** pour afficher la nouvelle ressource ajoutée.

3. Cliquez sur **Nouveau groupe de ressources**.
4. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez le nom du groupe de ressources.   Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources. Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.
Utilisez le format de nom personnalisé pour la copie Snapshot	Facultatif : entrez un nom et un format de snapshot personnalisés. Par exemple, clienttext_resourcegroup_policy_hostname ou resourcegroup_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page Ressources, effectuez les opérations suivantes :

- a. Sélectionnez le nom d'hôte, le type de ressource et l'instance SQL Server dans les listes déroulantes pour filtrer la liste des ressources.



Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

- b. Pour déplacer des ressources de la section **Ressources disponibles** vers la section Ressources sélectionnées, effectuez l'une des opérations suivantes :

- Sélectionnez **Autosélectionner toutes les ressources sur le même volume de stockage** pour déplacer toutes les ressources du même volume vers la section Ressources sélectionnées.
- Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.

6. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Dans la section configurer les planifications pour les stratégies sélectionnées, cliquez sur \*\*  dans la colonne configurer les planifications de la stratégie pour laquelle vous souhaitez configurer le planning.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez la planification en spécifiant la date de début, la date d'expiration et la fréquence, puis cliquez sur **OK**.

Vous devez le faire pour chaque fréquence répertoriée dans la police. Les planifications configurées sont répertoriées dans la colonne programmes appliqués de la section **configurer les planifications pour les stratégies sélectionnées**.

- d. Sélectionnez le planificateur Microsoft SQL Server.

Vous devez également sélectionner une instance de planificateur à associer à la stratégie de planification.

Si vous ne sélectionnez pas le planificateur Microsoft SQL Server, le planificateur Microsoft Windows par défaut est le planificateur Microsoft Windows.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter. Vous ne devez pas modifier les plannings et renommer la tâche de sauvegarde créée dans le planificateur Windows ou l'agent SQL Server.

7. Dans la page Vérification, effectuez les opérations suivantes :

- a. Sélectionnez le serveur de vérification dans la liste déroulante **serveur de vérification**.

La liste inclut tous les serveurs SQL ajoutés dans SnapCenter. Vous pouvez sélectionner plusieurs serveurs de vérification (hôte local ou hôte distant).



La version du serveur de vérification doit correspondre à la version et à l'édition du serveur SQL qui héberge la base de données primaire.

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror et SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer votre planning de vérification, puis cliquez sur \*\*  .
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification planifiée</b> .

- d. Cliquez sur **OK**.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués. Vous pouvez

vérifier, puis modifier en cliquant sur  ou supprimer en cliquant sur  .

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface utilisateur graphique ou de la commande PowerShell set-SmtpServer.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

#### Informations associées

["Créer des stratégies de sauvegarde pour les bases de données SQL Server"](#)

## Créez des groupes de ressources et activez la protection secondaire des ressources Microsoft SQL Server sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

#### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.

- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

- a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :
  - a. Sélectionnez le type de la règle de réplication.



Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.
- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.



Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

1. Sur la page Vérification, effectuez les opérations suivantes :
  - a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
  - b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
  - c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .

Les fonctions que vous recherchez...	Procédez comme ça...
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.
- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Conditions requises pour la sauvegarde des ressources SQL

Avant de sauvegarder une ressource SQL, vous devez vous assurer que plusieurs exigences sont respectées.

- Vous devez avoir migré une ressource d'un système de stockage non NetApp vers un système de stockage NetApp.
- Vous devez avoir créé une stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror sur un stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « `napmirror All` ». Toutefois, si vous utilisez le rôle « `vsadmin` », le privilège « `napmirror all` » n'est pas requis.
- L'opération de sauvegarde initiée par un utilisateur Active Directory (AD) échoue si les informations d'identification de l'instance SQL ne sont pas affectées à l'utilisateur ou au groupe AD. Vous devez affecter les informations d'identification de l'instance SQL à l'utilisateur ou au groupe AD à partir de la page **Paramètres > accès utilisateur**.
- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si un groupe de ressources contient plusieurs bases de données provenant de différents hôtes, l'opération de sauvegarde sur certains hôtes peut être déclenchée tardivement en raison de problèmes réseau. Vous devez configurer la valeur de `FMaxRetryForUninitializedHoots` dans `web.config` à l'aide de l'applet de commande PS `set-SmConfigSettings`.

## Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell

Vous devez créer une connexion SVM (Storage Virtual machine) et une identifiant avant

d'utiliser les applets de commande PowerShell pour réaliser les opérations de protection des données.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de gestion unique.

### Étapes

1. Lancez une session de connexion PowerShell Core à l'aide de l'applet de commande `Open-SmConnection`.

Cet exemple ouvre une session PowerShell :

```
PS C:\> Open-SmConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-SmStorageConnection`.

Dans cet exemple, une nouvelle connexion au système de stockage est créée :

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol https
-Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande `Add-SmCredential`.

Cet exemple crée un nouvel identifiant nommé `FinanceAdmin` avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de](#)

## Sauvegarde des ressources SQL

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Description de la tâche

- Pour optimiser l'opération de sauvegarde, vous devez créer un enregistrement de recherche inverse des noms de cluster Windows et des adresses IP dans le serveur DNS.
- Pour l'authentification des informations d'identification Windows, vous devez configurer vos informations d'identification avant d'installer les plug-ins.
- Pour l'authentification de l'instance SQL Server, vous devez ajouter les informations d'identification après l'installation des plug-ins.
- Pour l'authentification GMSA, vous devez configurer GMSA lors de l'enregistrement de l'hôte avec SnapCenter dans la page **Ajouter hôte** ou **Modifier hôte** pour activer et utiliser le GMSA.
- Si l'hôte est ajouté avec GMSA et si GMSA dispose de privilèges d'ouverture de session et d'administration système, GMSA est autorisé à se connecter à l'instance SQL.
  - SnapCenter vérifie si l'authentification pour les instances SQL est configurée. Si l'authentification est configurée, l'instance SQL est accessible à l'aide de ces informations d'identification.
  - Si l'authentification n'est pas configurée, utilisez GMSA pour vérifier si le plug-in SQL fonctionne actuellement. Si le plug-in fonctionne, il sera utilisé pour établir une connexion à l'instance SQL.
  - L'instance SQL est accessible via l'authentification des informations d'identification Windows lorsque l'authentification des deux instances SQL n'est pas configurée et que le plug-in n'est pas opérationnel.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **base de données** ou **instance** ou **Groupe de disponibilité** dans la liste déroulante **Affichage**.

- a. Sélectionnez la base de données, l'instance ou le groupe de disponibilité à sauvegarder.

Lorsque vous effectuez une sauvegarde d'une instance, les informations relatives à l'état de la dernière sauvegarde ou à l'horodatage de cette instance ne seront pas disponibles dans la page des ressources.

Dans la vue topologique, vous ne pouvez pas différencier l'état de sauvegarde, l'horodatage ou la sauvegarde d'une instance ou d'une base de données.

3. Dans la page Ressources, cochez la case **custom name format for Snapshot copy**, puis entrez un format de nom personnalisé à utiliser pour le nom de l'instantané.

Par exemple, clienttext\_policy\_hostname ou Resource\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

4. Dans la page stratégies, effectuez les tâches suivantes :

- a. Dans la section stratégies, sélectionnez une ou plusieurs stratégies dans la liste déroulante.

Vous pouvez créer une stratégie en sélectionnant \* \* \*  pour lancer l'assistant de stratégie.

Dans la section **configurer les plannings pour les stratégies sélectionnées**, les stratégies sélectionnées sont répertoriées.

- b. Sélectionnez \* \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans **Ajouter des horaires pour la police** `policy_name` Configurez la planification, puis sélectionnez **OK**.

Ici `policy_name` est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **programmes appliqués**.

- a. Sélectionnez **utiliser le planificateur Microsoft SQL Server**, puis sélectionnez l'instance du planificateur dans la liste déroulante **instance du planificateur** associée à la stratégie de planification.

5. Dans la page Vérification, effectuez les opérations suivantes :

- a. Sélectionnez le serveur de vérification dans la liste déroulante **serveur de vérification**.

Vous pouvez sélectionner plusieurs serveurs de vérification (hôte local ou hôte distant).



La version du serveur de vérification doit être égale ou supérieure à la version de l'édition du serveur SQL qui héberge la base de données primaire.

- a. Sélectionnez **Charger les localisateurs secondaires pour vérifier les sauvegardes sur le système de stockage secondaire** afin de vérifier vos sauvegardes sur le système de stockage secondaire.
- b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer votre planning de vérification, puis sélectionnez \* \*  .
- c. Dans la boîte de dialogue Ajouter des programmes de vérification *policy\_name*, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification planifiée</b> .



Si le serveur de vérification n'a pas de connexion de stockage, l'opération de vérification échoue avec l'erreur : échec du montage du disque.

- d. Sélectionnez **OK**.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

6. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface utilisateur graphique ou de la commande PowerShell `set-SmtpServer`.

7. Passez en revue le résumé, puis sélectionnez **Terminer**.

La page topologie de la base de données s'affiche.

8. Sélectionnez **Sauvegarder maintenant**.

9. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

b. Sélectionnez **vérifier après sauvegarde** pour vérifier votre sauvegarde.

c. Sélectionnez **Backup**.



Vous ne devez pas renommer la tâche de sauvegarde créée dans le planificateur Windows ou l'agent SQL Server.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

Un groupe de ressources implicite est créé. Vous pouvez afficher ces informations en sélectionnant l'utilisateur ou le groupe concerné dans la page accès utilisateur. Le type de groupe de ressources implicite est « ressource ».

10. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

### Une fois que vous avez terminé

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer. Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, le `do_start method Command` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante : `Java -jar -Xmx8192M -Xms4096M`.

### Informations associées

["Créer des stratégies de sauvegarde pour les bases de données SQL Server"](#)

["Les opérations de sauvegarde échouent avec l'erreur de connexion MySQL en raison du délai dans TCP\\_TIMEOUT"](#)

["La sauvegarde échoue en raison d'une erreur du planificateur Windows"](#)

["Les opérations de mise en attente ou de regroupement des ressources échouent"](#)

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Créez une stratégie de sauvegarde à l'aide de l'applet de commande `Add-SmPolicy`.

Cet exemple crée une nouvelle stratégie de sauvegarde avec un type de sauvegarde SQL fullbackup

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Cet exemple crée une nouvelle stratégie de sauvegarde avec un type de sauvegarde de système de fichiers Windows de CrashConsistent :

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

### 3. Découvrez les ressources hôte à l'aide de l'applet de commande Get-SmResources.

Cet exemple recherche les ressources du plug-in Microsoft SQL sur l'hôte spécifié :

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

Cet exemple détecte les ressources des systèmes de fichiers Windows sur l'hôte spécifié :

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

### 4. Ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.

Cet exemple crée un nouveau groupe de ressources de sauvegarde de base de données SQL avec la stratégie et les ressources spécifiées :

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

Cet exemple crée un nouveau groupe de ressources de sauvegarde du système de fichiers Windows avec la stratégie et les ressources spécifiées :

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet `New-SmBackup`.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Affichez l'état de la tâche de sauvegarde à l'aide de l'applet de commande `Get-SmBackupReport`.

Cet exemple affiche un rapport récapitulatif de tous les travaux exécutés à la date spécifiée :

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegardez les groupes de ressources SQL Server

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page **Ressources**. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en  sélectionnant , puis la balise. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Dans la page **groupes de ressources**, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page **sauvegarde**, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de

conservation spécifiés pour le type de programme.

b. Après la sauvegarde, sélectionnez **Verify** pour vérifier la sauvegarde à la demande.

L'option **Verify** de la stratégie ne s'applique qu'aux tâches planifiées.

c. Sélectionnez **Backup**.

5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

#### Informations associées

["Créer des stratégies de sauvegarde pour les bases de données SQL Server"](#)

["Créez des groupes de ressources et associez des stratégies pour SQL Server"](#)

["Les opérations de sauvegarde échouent avec l'erreur de connexion MySQL en raison du délai dans TCP\\_TIMEOUT"](#)

["La sauvegarde échoue en raison d'une erreur du planificateur Windows"](#)

## Surveillez les opérations de sauvegarde des ressources SQL dans la page tâches SnapCenter

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

#### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.

4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

### Surveiller les opérations de protection des données sur les ressources SQL dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

### Annulez les opérations de sauvegarde du plug-in SnapCenter pour Microsoft SQL Server

Vous pouvez annuler les opérations de sauvegarde en cours d'exécution, en file d'attente ou non réactives. Lorsque vous annulez une opération de sauvegarde, le serveur SnapCenter arrête l'opération et supprime tous les snapshots du stockage si la sauvegarde créée n'est pas enregistrée auprès du serveur SnapCenter. Si la sauvegarde est déjà enregistrée avec le serveur SnapCenter, elle ne peut pas revenir à l'instantané déjà créé même après le déclenchement de l'annulation.

#### Avant de commencer

- Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâche pour annuler les opérations de restauration.
- Vous pouvez annuler uniquement les opérations de journalisation ou de sauvegarde complète qui sont mises en file d'attente ou en cours d'exécution.
- Vous ne pouvez pas annuler l'opération après le début de la vérification.

Si vous annulez l'opération avant vérification, l'opération est annulée et l'opération de vérification ne sera pas effectuée.

- Vous pouvez annuler une opération de sauvegarde à partir de la page moniteur ou du volet activité.
- Outre l'interface graphique SnapCenter, vous pouvez utiliser les applets de commande PowerShell pour annuler des opérations.

- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

## Étapes

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>1. Dans le volet de navigation de gauche, sélectionnez <b>Monitor &gt; Jobs</b>.</li> <li>2. Sélectionnez le travail et sélectionnez <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>1. Après avoir lancé la tâche de sauvegarde, sélectionnez  Dans le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>2. Sélectionner l'opération.</li> <li>3. Dans la page Détails du travail, sélectionnez <b>Annuler le travail</b>.</li> </ol>

## Résultat

L'opération est annulée et la ressource est rétablie à l'état précédent. Si l'opération que vous avez annulée n'est pas réactive à l'état d'annulation ou d'exécution, vous devez exécuter le `Cancel-SmJob -JobID <int> -Force cmdlet` arrête avec force l'opération de sauvegarde.

## Afficher les sauvegardes et clones SQL Server sur la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire.

### Description de la tâche

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

Vous pouvez consulter les icônes suivantes dans la vue **gérer les copies** pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies miroir ou copies coffre-fort).

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.

-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.
  - Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire.

Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Si vous utilisez une relation secondaire comme SnapMirror actif Sync (initialement commercialisé sous la forme SnapMirror Business Continuity [SM-BC]), les icônes supplémentaires suivantes s'affichent :

-  Le site de réplica est en cours.
-  Le site de réplica est en panne.
-  La relation miroir ou coffre-fort secondaire n'a pas été rétablie.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource sélectionnée est une base de données clonée, protégez la base de données clonée, la source du clone s'affiche dans la page topologie. Cliquez sur **Détails** pour afficher la sauvegarde utilisée pour le clonage.

Si la ressource est protégée, la page topologie de la ressource sélectionnée s'affiche.

4. Consultez la fiche récapitulative pour connaître le nombre de sauvegardes et de clones disponibles sur les stockages primaire et secondaire.

La section **Résumé Card** affiche le nombre total de sauvegardes et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Pour la synchronisation active SnapMirror, cliquez sur le bouton **Refresh** pour actualiser l'inventaire des sauvegardes SnapCenter en interrogeant ONTAP sur les sites principaux et de réplica. Une planification hebdomadaire effectue également cette activité pour toutes les bases de données contenant une relation de synchronisation active SnapMirror.

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations SnapMirror miroir asynchrone ou MirrorVault asynchrone vers la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir de ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.
- Après le basculement, une sauvegarde doit être créée afin que SnapCenter puisse prendre connaissance du basculement. Vous ne pouvez cliquer sur **Rafraîchir** qu'après la création d'une sauvegarde.

5. Dans la vue **gérer les copies**, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage, de renommage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

7. Sélectionnez un clone dans la table et cliquez sur **Clone Split**.

8. Si vous souhaitez supprimer un clone, sélectionnez-le dans la table, puis cliquez sur .

## Nettoyez le nombre de sauvegardes secondaires à l'aide des applets de commande PowerShell

Vous pouvez utiliser l'applet de commande `Remove-SmBackup` pour nettoyer le nombre de sauvegardes secondaires sans instantané. Vous pouvez utiliser cette applet de commande lorsque le nombre total de snapshots affichés dans la topologie gérer les copies ne correspond pas au paramètre de conservation des snapshots de stockage secondaire.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Nettoyez le nombre de sauvegardes secondaires à l'aide du paramètre `-CleanuppyBackups`.

Cet exemple nettoie le nombre de sauvegardes secondaires sans snapshots :

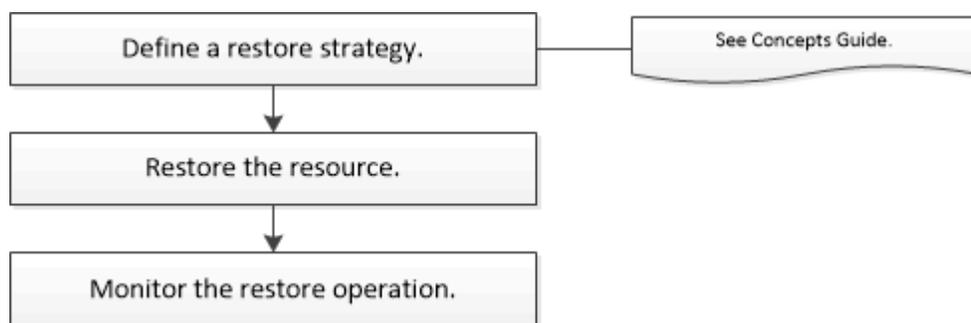
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y") :
```

## Restaurez les ressources SQL Server

### Restaurer le flux de travail

Vous pouvez utiliser SnapCenter pour restaurer les bases de données SQL Server en les restaurant depuis une ou plusieurs sauvegardes vers votre système de fichiers actif, puis en récupérant la base de données. Vous pouvez également restaurer les bases de données qui se trouvent dans les groupes de disponibilité, puis ajouter les bases de données restaurées au groupe de disponibilité. Avant de restaurer une base de données SQL Server, vous devez effectuer plusieurs tâches préparatoires.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer les opérations de restauration de la base de données :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration, de vérification et de clonage. Pour plus d'informations sur les applets de commande PowerShell, utilisez l'aide du cmdlet SnapCenter ou consultez le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#)

### Plus d'informations

["Restaurer une base de données SQL Server à partir du stockage secondaire"](#)

["Restauration et restauration des ressources via les applets de commande PowerShell"](#)

["La restauration peut échouer sur Windows 2008 R2"](#)

### Conditions requises pour restaurer une base de données

Avant de restaurer une base de données SQL Server à partir d'un plug-in SnapCenter pour sauvegarde Microsoft SQL Server, vous devez vous assurer que plusieurs

conditions sont respectées.

- L'instance SQL Server cible doit être en ligne et en cours d'exécution avant de pouvoir restaurer une base de données.

Cela s'applique aux opérations de restauration de la base de données utilisateur et aux opérations de restauration de la base de données système.

- Les opérations SnapCenter planifiées pour l'exécution des données SQL Server que vous restaurez doivent être désactivées, y compris les tâches planifiées sur les serveurs de gestion à distance ou de vérification à distance.
- Si les bases de données système ne fonctionnent pas, vous devez d'abord reconstruire les bases de données système à l'aide d'un utilitaire SQL Server.
- Si vous installez le plug-in, assurez-vous que vous accordez des autorisations pour d'autres rôles afin de restaurer les sauvegardes du groupe de disponibilité (AG).

La restauration de AG échoue lorsque l'une des conditions suivantes est remplie :

- Si le plug-in est installé par un utilisateur RBAC et qu'un administrateur tente de restaurer une sauvegarde AG
- Si le plug-in est installé par un administrateur et qu'un utilisateur RBAC tente de restaurer une sauvegarde AG
- Si vous restaurez des sauvegardes de répertoire de journaux personnalisés sur un autre hôte, le serveur SnapCenter et l'hôte du plug-in doivent avoir la même version de SnapCenter installée.
- Vous devez avoir installé le correctif Microsoft KB2887595. Le site de support Microsoft contient des informations supplémentaires sur KB2887595.

["Article 2887595 du support Microsoft : ensemble de mises à jour Windows RT 8.1, Windows 8.1 et Windows Server 2012 R2 : novembre 2013"](#)

- Vous devez avoir sauvegardé les groupes de ressources ou la base de données.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir attribué les machines virtuelles de stockage (SVM) pour les volumes source et de destination.

Pour plus d'informations sur la manière dont les administrateurs attribuent des ressources aux utilisateurs, consultez les informations d'installation de SnapCenter.

- Toutes les tâches de sauvegarde et de clonage doivent être arrêtées avant de restaurer la base de données.
- L'opération de restauration peut expirer si la taille de la base de données se trouve en téraoctets (To).

Vous devez augmenter la valeur du paramètre RESTTimeout du serveur SnapCenter à 20000000 ms en exécutant la commande suivante : `set-SmConfigSettings -Agent -configSettings @{« RESTTimeout » = « 20000000 »}`. En fonction de la taille de la base de données, la valeur de temporisation peut être modifiée et la valeur maximale que vous pouvez définir est de 86400000 ms.

Si vous souhaitez restaurer pendant que les bases de données sont en ligne, l'option de restauration en ligne doit être activée dans la page Restaurer.

## Restaurez les sauvegardes des bases de données SQL Server

Vous pouvez utiliser SnapCenter pour restaurer des bases de données SQL Server sauvegardées. La restauration de la base de données est un processus multiphase qui copie toutes les pages de données et de journaux d'une sauvegarde SQL Server spécifique vers une base de données spécifiée.

### Description de la tâche

- Vous pouvez restaurer les bases de données SQL Server sauvegardées sur une autre instance SQL Server sur le même hôte où la sauvegarde a été créée.

Vous pouvez utiliser SnapCenter pour restaurer les bases de données SQL Server sauvegardées sur un autre chemin afin de ne pas remplacer une version de production.

- SnapCenter peut restaurer les bases de données dans un cluster Windows sans mettre le groupe de clusters SQL Server hors ligne.
- En cas de défaillance d'un cluster (opération de déplacement d'un groupe de clusters) lors d'une opération de restauration (par exemple, si le nœud qui possède les ressources tombe en panne), vous devez vous reconnecter à l'instance SQL Server, puis redémarrer l'opération de restauration.
- Vous ne pouvez pas restaurer la base de données lorsque les utilisateurs ou les travaux de l'agent SQL Server accèdent à la base de données.
- Vous ne pouvez pas restaurer les bases de données système sur un chemin alternatif.
- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- La plupart des champs des pages de l'assistant de restauration sont explicites. Les informations suivantes décrivent les champs pour lesquels vous aurez peut-être besoin d'aide.
- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.
- Pour les règles activées par SnapLock, pour ONTAP 9.12.1 et versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

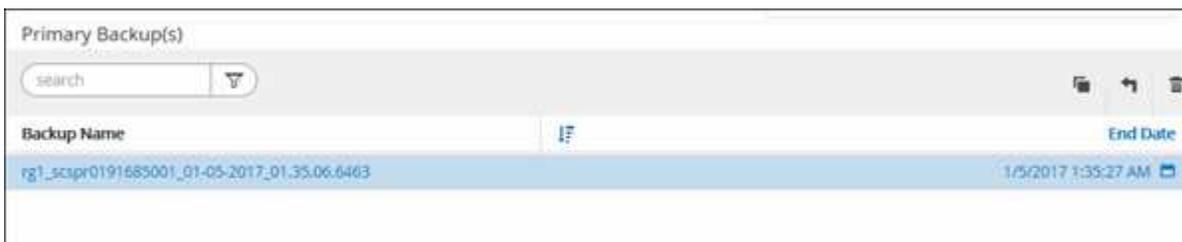
## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données ou le groupe de ressources dans la liste.

La page topologie s'affiche.

4. Dans la vue gérer les copies, sélectionnez **sauvegardes** dans le système de stockage.
5. Sélectionnez la sauvegarde dans la table, puis cliquez sur  icône.



6. Dans la page objectif de restauration, sélectionnez l'une des options suivantes :

Option	Description
Restaurez la base de données sur le même hôte où la sauvegarde a été créée	Sélectionnez cette option si vous souhaitez restaurer la base de données sur le même serveur SQL où les sauvegardes sont effectuées.
Restaurez la base de données sur un autre hôte	<p>Sélectionnez cette option si vous souhaitez que la base de données soit restaurée sur un autre serveur SQL dans le même hôte ou sur un hôte différent où des sauvegardes sont effectuées.</p> <p>Sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration.</p> <p> L'extension de fichier fournie dans le chemin alternatif doit être identique à celle du fichier de base de données d'origine.</p> <p>Si l'option <b>Restaurer la base de données sur un autre hôte</b> n'est pas affichée dans la page Restaurer l'étendue, effacez le cache du navigateur.</p>

Option	Description
Restaurez la base de données à l'aide de fichiers de base de données existants	<p>Sélectionnez cette option si vous souhaitez que la base de données soit restaurée sur un autre serveur SQL dans le même hôte ou sur un hôte différent où des sauvegardes sont effectuées.</p> <p>Les fichiers de base de données doivent déjà être présents sur les chemins de fichier existants donnés. Sélectionnez un nom d'hôte, indiquez un nom de base de données (facultatif), sélectionnez une instance et spécifiez les chemins de restauration.</p>

7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :

Option	Description
Aucune	Sélectionnez <b>aucun</b> si vous devez restaurer uniquement la sauvegarde complète sans journaux.
Toutes les sauvegardes de journaux	Sélectionnez <b>toutes les sauvegardes de journaux</b> sauvegarde à la minute pour restaurer toutes les sauvegardes de journaux disponibles après la sauvegarde complète.
En journaliser les sauvegardes jusqu'à	Sélectionnez <b>par sauvegardes de journaux</b> pour effectuer une opération de restauration ponctuelle, qui restaure la base de données en fonction des journaux de sauvegarde jusqu'à ce que le journal de sauvegarde avec la date sélectionnée.
Par date spécifique jusqu'à	<p>Sélectionnez <b>par date spécifique jusqu'à</b> pour spécifier la date et l'heure après lesquelles les journaux de transactions ne sont pas appliqués à la base de données restaurée.</p> <p>Cette opération de restauration ponctuelle interrompt la restauration des entrées du journal de transactions enregistrées après la date et l'heure spécifiées.</p>

Option	Description
Utiliser le répertoire de journaux personnalisé	<p>Si vous avez sélectionné <b>toutes les sauvegardes de journaux, par sauvegarde de journaux</b> ou <b>par date spécifique jusqu'à</b> et que les journaux se trouvent à un emplacement personnalisé, sélectionnez <b>utiliser le répertoire de journaux personnalisé</b>, puis spécifiez l'emplacement du journal.</p> <p>L'option <b>utiliser le répertoire de journaux personnalisé</b> n'est disponible que si vous avez sélectionné <b>Restaurer la base de données sur un autre hôte</b> ou <b>Restaurer la base de données à l'aide des fichiers de base de données existants</b>. Vous pouvez également utiliser le chemin partagé mais vous assurer que le chemin est accessible par l'utilisateur SQL.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le répertoire des journaux personnalisés n'est pas pris en charge pour la base de données des groupes de disponibilité.</p> </div>

8. Dans la page pré-opération, effectuez les opérations suivantes :

a. Dans la page Options de pré-restauration, sélectionnez l'une des options suivantes :

- Sélectionnez **Ecraser la base de données du même nom pendant la restauration** pour restaurer la base de données du même nom.
- Sélectionnez **conserver les paramètres de réplication de base de données SQL** pour restaurer la base de données et conserver les paramètres de réplication existants.
- Sélectionnez **Créer une sauvegarde du journal de transactions avant la restauration** pour créer un journal de transactions avant le début de l'opération de restauration.
- Sélectionnez **Quitter la restauration si la sauvegarde du journal de transactions avant la restauration échoue** pour abandonner l'opération de restauration si la sauvegarde du journal de transactions échoue.

b. Spécifiez les scripts facultatifs à exécuter avant d'effectuer une tâche de restauration.

Vous pouvez par exemple exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer les journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

9. Dans la page Post Ops, effectuez les opérations suivantes :

a. Dans la section choisir l'état de la base de données une fois la restauration terminée, sélectionnez l'une des options suivantes :

- Sélectionnez **opérationnel, mais non disponible pour la restauration de journaux de**

**transactions supplémentaires** si vous restaurez maintenant toutes les sauvegardes nécessaires.

Il s'agit du comportement par défaut, qui laisse la base de données prête à l'emploi en revenant les transactions non validées. Vous ne pouvez pas restaurer d'autres journaux de transactions tant que vous n'avez pas créé de sauvegarde.

- Sélectionnez **non opérationnel, mais disponible pour la restauration de journaux transactionnels supplémentaires** pour laisser la base de données non opérationnelle sans reprise des transactions non validées.

Des journaux de transactions supplémentaires peuvent être restaurés. Vous ne pouvez pas utiliser la base de données tant qu'elle n'a pas été restaurée.

- Sélectionnez **mode lecture seule, disponible pour la restauration de journaux transactionnels supplémentaires** pour quitter la base de données en mode lecture seule.

Cette option annule les transactions non validées, mais enregistre les actions annulées dans un fichier de secours afin que les effets de récupération puissent être restaurés.

Si l'option Annuler le répertoire est activée, davantage de journaux de transactions sont restaurés. Si l'opération de restauration du journal de transactions échoue, les modifications peuvent être annulées. La documentation de SQL Server contient des informations supplémentaires.

- b. Spécifiez les scripts facultatifs à exécuter après l'exécution d'une tâche de restauration.

Vous pouvez par exemple exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer les journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.
12. Surveillez le processus de restauration à l'aide de la page **Monitor > Jobs**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet `Restore-SmBackup`.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurer une base de données SQL Server à partir du stockage secondaire

Vous pouvez restaurer les bases de données SQL Server sauvegardées à partir des LUN physiques (RDM, iSCSI ou FCP) sur un système de stockage secondaire. La fonction Restaurer est un processus multiphase qui copie toutes les données et toutes les pages de journal à partir d'une sauvegarde SQL Server spécifiée résidant sur le système de stockage secondaire vers une base de données spécifiée.

### Avant de commencer

- Vous devez avoir répliqué les snapshots du système de stockage principal vers le système de stockage secondaire.

- Vous devez vous assurer que le serveur SnapCenter et l'hôte du plug-in peuvent se connecter au système de stockage secondaire.
- La plupart des champs des pages de l'assistant de restauration sont expliqués dans le processus de restauration de base. Les informations suivantes décrivent certains champs pour lesquels vous avez peut-être besoin d'aide.

### Description de la tâche

Pour les règles activées par SnapLock, pour ONTAP 9.12.1 et versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez **SnapCenter Plug-in for SQL Server** dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste déroulante **View**.
3. Sélectionnez la base de données ou le groupe de ressources.

La page topologie de la base de données ou du groupe de ressources s'affiche.

4. Dans la section gérer les copies, sélectionnez **sauvegardes** dans le système de stockage secondaire (miroir ou coffre-fort).
5. Sélectionnez la sauvegarde dans la liste, puis cliquez sur .
6. Dans la page emplacement, choisissez le volume de destination pour restaurer la ressource sélectionnée.
7. Terminez l'assistant Restaurer, vérifiez le résumé, puis cliquez sur **Terminer**.

Si vous avez restauré une base de données sur un chemin différent partagé par d'autres bases de données, vous devez effectuer une sauvegarde complète et vérifier la sauvegarde pour vérifier que votre base de données restaurée est exempte de corruption au niveau physique.

## Restaurer des ressources à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de ressources inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
-----		
1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet `Restore-SmBackup`.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Réamorçage des bases de données du groupe de disponibilité

Réamorçage est une option permettant de restaurer les bases de données du groupe de disponibilité (AG). Si une base de données secondaire n'est plus synchronisée avec la base de données principale d'un AG, vous pouvez réamorcer la base de données secondaire.

### Avant de commencer

- Vous devez avoir créé une sauvegarde de la base de données AG secondaire que vous souhaitez restaurer.
- La même version de SnapCenter doit être installée sur le serveur SnapCenter et l'hôte du plug-in.

### Description de la tâche

- Vous ne pouvez pas effectuer de réamorçage sur les bases de données primaires.
- Vous ne pouvez pas effectuer de réamorçage si la base de données de réplica est supprimée du groupe de disponibilité. Lorsque le réplica est supprimé, l'opération de réamorçage échoue.
- Lors de l'exécution de l'opération de réamorçage sur la base de données du groupe de disponibilité SQL, vous ne devez pas déclencher de sauvegardes de journaux sur les bases de données de réplica de cette base de données du groupe de disponibilité. Si vous déclenchez des sauvegardes de journaux pendant le réamorçage, l'opération de réamorçage échoue avec la base de données miroir, "nom\_base\_de\_données" a des données de journal de transactions insuffisantes pour préserver la chaîne de sauvegarde du journal du message d'erreur de la base de données principale.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez **SnapCenter Plug-in for SQL Server** dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.
3. Sélectionnez la base de données AG secondaire dans la liste.
4. Cliquez sur **Reseed**.
5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Surveiller les opérations de restauration des ressources SQL

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.

- d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
  5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Annuler les opérations de restauration des ressources SQL

Vous pouvez annuler les travaux de restauration mis en file d'attente.

Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâche pour annuler les opérations de restauration.

### Description de la tâche

- Vous pouvez annuler une opération de restauration en file d'attente à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de restauration en cours.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes de l'interface de ligne de commande pour annuler les opérations de restauration en attente.
- Le bouton **Annuler tâche** est désactivé pour les opérations de restauration qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de restauration en file d'attente d'autres membres tout en utilisant ce rôle.

### Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>2. Sélectionnez le travail et cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>1. Après avoir lancé l'opération de restauration, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>2. Sélectionner l'opération.</li> <li>3. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

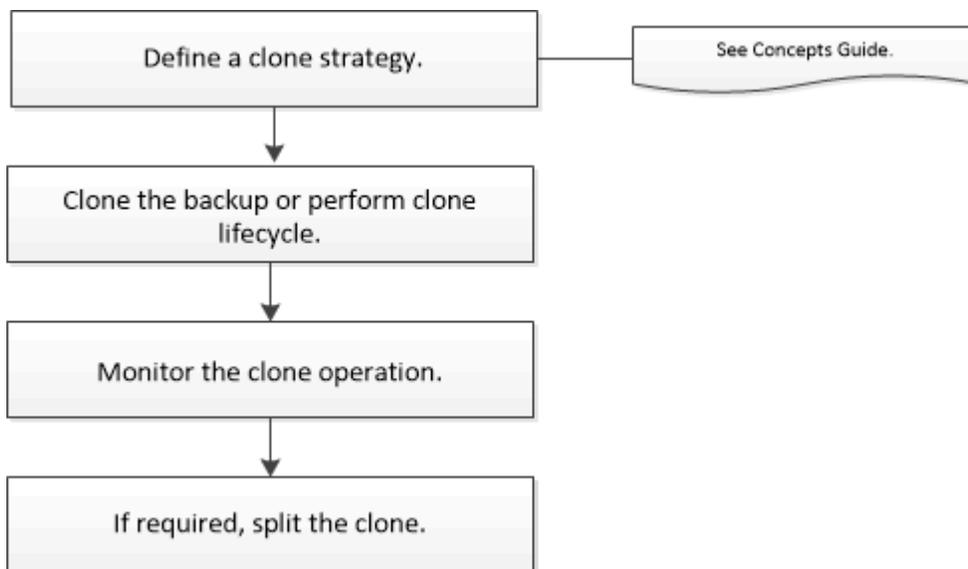
## Clonage des ressources de base de données SQL Server

## Workflow de clonage

Vous devez effectuer plusieurs tâches à l'aide du serveur SnapCenter avant de cloner les ressources de base de données à partir d'une sauvegarde. Le clonage de la base de données consiste à créer une copie instantanée d'une base de données de production ou de son jeu de sauvegarde. Vous pouvez cloner les bases de données pour tester les fonctionnalités qui doivent être implémentées en utilisant la structure et le contenu actuels de la base de données pendant les cycles de développement d'applications, pour utiliser les outils d'extraction et de manipulation des données lors du remplissage des data warehouses, ou pour récupérer les données qui ont été supprimées ou modifiées par erreur.

Une opération de clonage de base de données génère des rapports basés sur les ID de travail.

Le workflow suivant montre l'ordre dans lequel vous devez effectuer les opérations de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration, de vérification et de clonage. Pour plus d'informations sur les applets de commande PowerShell, utilisez l'aide du cmdlet SnapCenter ou consultez le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#)

### Plus d'informations

["Clonage à partir d'une sauvegarde de base de données SQL Server"](#)

["Réaliser le cycle de vie des clones"](#)

["Le clonage peut échouer ou prendre plus de temps avec la valeur TCP\\_TIMEOUT par défaut"](#)

## Clonage à partir d'une sauvegarde de base de données SQL Server

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde de base de données SQL Server. Pour accéder ou restaurer une ancienne version des données, vous pouvez cloner les sauvegardes de bases de données à la demande.

## Avant de commencer

- Vous devez préparer la protection des données en effectuant des tâches telles que l'ajout d'hôtes, l'identification des ressources et la création de connexions du système de stockage.
- Vous devez avoir sauvegardé des bases de données ou des groupes de ressources.
- Le type de protection tel que miroir, coffre-fort ou miroir-vault pour LUN de données et LUN de journaux doit être identique pour détecter les dispositifs de localisation secondaires lors du clonage sur un autre hôte à l'aide de sauvegardes de journaux.
- Si le lecteur de clone monté ne peut pas être trouvé pendant une opération de clonage SnapCenter, vous devez modifier le paramètre CloneRerryTimeout du serveur SnapCenter à 300.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).

## Description de la tâche

- Lors du clonage vers une instance de base de données autonome, assurez-vous que le chemin du point de montage existe et qu'il s'agit d'un disque dédié.
- Lors du clonage vers une instance de cluster de basculement (FCI), assurez-vous que les points de montage existent, qu'il s'agit d'un disque partagé, et que le chemin et le FCI doivent appartenir au même groupe de ressources SQL.
- Assurez-vous qu'un seul initiateur VFC ou FC est connecté à chaque hôte. En effet, SnapCenter ne prend en charge qu'un seul initiateur par hôte.
- Si la base de données source ou l'instance cible se trouve sur un volume partagé de cluster (csv), la base de données clonée se trouve dans le fichier csv.
- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : [API /4.7/configsettings](#)

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.



Pour les environnements virtuels (VMDK/RDM), assurez-vous que le point de montage est un disque dédié.

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis **SnapCenter Plug-in pour SQL Server** dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.



Le clonage d'une sauvegarde d'instance n'est pas pris en charge.

3. Sélectionnez la base de données ou le groupe de ressources.
4. Dans la page d'affichage **gérer les copies**, sélectionnez la sauvegarde à partir du système de stockage principal ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde, puis sélectionnez .
6. Dans la page **Clone Options**, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Serveur clone	Choisissez l'hôte sur lequel le clone doit être créé.
Cloner l'instance	Choisissez une instance de clone dans laquelle vous souhaitez cloner la sauvegarde de la base de données.  Cette instance SQL doit se trouver dans le serveur clone spécifié.
Suffixe du clone	Indiquez un suffixe à ajouter au nom du fichier clone pour identifier que la base de données est un clone.  Par exemple, <i>db1_clone</i> . Si vous effectuez un clonage au même emplacement que la base de données d'origine, vous devez fournir un suffixe permettant de différencier la base de données clonée de la base de données d'origine. Dans le cas contraire, l'opération échoue.

Pour ce champ...	Procédez comme ça...
Attribuer automatiquement un point de montage ou attribuer automatiquement un point de montage de volume sous le chemin	<p>Choisissez d'attribuer automatiquement un point de montage ou un point de montage de volume sous un chemin d'accès.</p> <p>Affectation automatique d'un point de montage de volume sous le chemin d'accès : le point de montage sous un chemin vous permet de fournir un répertoire spécifique. Les points de montage seront créés dans ce répertoire. Avant de choisir cette option, vous devez vous assurer que le répertoire est vide. Si une base de données se trouve dans le répertoire, la base de données sera dans un état non valide après l'opération de montage.</p>

7. Dans la page journaux, sélectionnez l'une des options suivantes :

Pour ce champ...	Procédez comme ça...
Aucune	Choisissez cette option si vous souhaitez cloner uniquement la sauvegarde complète sans journaux.
Toutes les sauvegardes de journaux	Sélectionnez cette option pour cloner toutes les sauvegardes de journaux disponibles datées après la sauvegarde complète.
En journaliser les sauvegardes jusqu'à	Choisissez cette option pour cloner la base de données en fonction des journaux de sauvegarde créés jusqu'au journal de sauvegarde à la date sélectionnée.
Par date spécifique jusqu'à	<p>Spécifiez la date et l'heure après lesquelles les journaux de transactions ne sont pas appliqués à la base de données clonée.</p> <p>Ce clone instantané interrompt le clone des entrées du journal de transactions qui ont été enregistrées après la date et l'heure spécifiées.</p>

8. Sur la page **script**, entrez le délai d'expiration du script, le chemin et les arguments du prescripteur ou du postscript qui doivent être exécutés avant ou après l'opération de clonage, respectivement.

Vous pouvez par exemple exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer les journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

Le délai par défaut du script est de 60 secondes.

9. Dans la page **notification**, dans la liste déroulante **préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

Pour EMS, reportez-vous à la section "[Gérer la collecte de données EMS](#)"

10. Passez en revue le résumé, puis sélectionnez **Terminer**.
11. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

### Une fois que vous avez terminé

Une fois le clone créé, vous ne devez jamais le renommer.

### Informations associées

"[Le clonage peut échouer ou prendre plus de temps avec la valeur TCP\\_TIMEOUT par défaut](#)"

"[Le clone de base de données de l'instance de cluster de basculement échoue](#)"

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Répertoriez les sauvegardes pouvant être clonées à l'aide de l'applet de commande `Get-SmBackup` ou `Get-SmResourceGroup`.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
C:\PS>PS C:\> Get-SmBackup

BackupId BackupName BackupTime BackupType

1 Payroll Dataset_vise-f6_08... 8/4/2015 Full Backup
 11:02:32 AM

2 Payroll Dataset_vise-f6_08... 8/4/2015
 11:23:17 AM
```

Cet exemple affiche des informations sur un groupe de ressources spécifié, ses ressources et les

stratégies associées :

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCOREContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCOREContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCOREContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
```

```
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCOREContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCOREContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
```

```
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Lancez une opération de clonage à partir d'une sauvegarde existante à l'aide de l'applet de commande New-SmClone.

Dans cet exemple, un clone est créé à partir d'une sauvegarde spécifiée avec tous les journaux :

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\squlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

Dans cet exemple, un clone est créé dans une instance Microsoft SQL Server spécifiée :

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Affichez l'état du travail clone à l'aide de l'applet de commande Get-SmCloneReport.

Cet exemple affiche un rapport de clonage pour l'ID de tâche spécifié :

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
 Sally_DRAPER}
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Réaliser le cycle de vie des clones

SnapCenter permet de créer des clones à partir d'un groupe de ressources ou d'une base de données. Vous pouvez cloner à la demande ou planifier des opérations de clonage récurrentes d'un groupe de ressources ou d'une base de données. Si vous clonez régulièrement une sauvegarde, vous pouvez utiliser le clone pour développer des applications, remplir des données ou restaurer des données.

SnapCenter vous permet de planifier plusieurs opérations de clonage afin de s'exécuter simultanément sur plusieurs serveurs.

### Avant de commencer

- Lors du clonage vers une instance de base de données autonome, assurez-vous que le chemin du point de montage existe et qu'il s'agit d'un disque dédié.
- Lors du clonage vers une instance de cluster de basculement (FCI), assurez-vous que les points de montage existent, qu'il s'agit d'un disque partagé, et que le chemin et le FCI doivent appartenir au même groupe de ressources SQL.
- Si la base de données source ou l'instance cible se trouve sur un volume partagé de cluster (csv), la base de données clonée se trouve dans le fichier csv.



Pour les environnements virtuels (VMDK/RDM), assurez-vous que le point de montage est un disque dédié.

### Description de la tâche

- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- La plupart des champs des pages de l'assistant de clonage de cycle de vie sont explicites. Les informations suivantes décrivent les champs pour lesquels vous aurez peut-être besoin d'aide.
- Pour ONTAP 9.12.1 et les versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

- Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
- Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
- Sélectionnez le groupe de ressources ou la base de données, puis cliquez sur **Cloner le cycle de vie**.
- Dans la page Options, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Cloner le nom de la tâche	Spécifiez le nom de la tâche de cycle de vie du clone qui permet de surveiller et de modifier la tâche de cycle de vie du clone.
Serveur clone	Choisissez l'hôte sur lequel placer le clone.
Cloner l'instance	Sélectionnez l'instance de clone dans laquelle vous souhaitez cloner la base de données. Cette instance SQL doit se trouver dans le serveur clone spécifié.

Pour ce champ...	Procédez comme ça...
Suffixe du clone	Indiquez un suffixe que vous allez ajouter à la base de données clone pour identifier le clone. Chaque instance SQL utilisée pour créer un groupe de ressources clones doit avoir un nom de base de données unique. Par exemple, si le groupe de ressources clone contient une base de données source "db1" à partir d'une instance SQL "inst1" et si "db1" est cloné sur "insta1", le nom de la base de données clone doit être "db1clone". "clone" est un suffixe obligatoire défini par l'utilisateur car la base de données est clonée dans la même instance. Si "db1" est cloné dans l'instance SQL "inst2", alors le nom de la base de données clone peut rester "db1" (le suffixe est facultatif) car la base de données est clonée dans une autre instance.
Attribuer automatiquement un point de montage ou attribuer automatiquement un point de montage de volume sous le chemin	Choisissez d'attribuer automatiquement un point de montage ou un point de montage de volume sous un chemin d'accès. La sélection de l'affectation automatique d'un point de montage de volume sous un chemin vous permet de fournir un répertoire spécifique. Les points de montage seront créés dans ce répertoire. Avant de choisir cette option, vous devez vous assurer que le répertoire est vide. Si une base de données se trouve dans le répertoire, la base de données sera dans un état non valide après l'opération de montage.

5. Dans la page emplacement, sélectionnez un emplacement de stockage pour créer un clone.
6. Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript qui doivent être exécutés avant ou après l'opération de clonage, respectivement.

Vous pouvez par exemple exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer les journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

Le délai par défaut du script est de 60 secondes.

7. Dans la page planification, effectuez l'une des opérations suivantes :
  - Sélectionnez **Exécuter maintenant** si vous souhaitez exécuter le travail de clonage immédiatement.
  - Sélectionnez **Configure schedule** lorsque vous souhaitez déterminer la fréquence à laquelle l'opération de clonage doit se produire, lorsque la planification de clonage doit démarrer, le jour où l'opération de clonage doit avoir lieu, quand la planification doit expirer et si les clones doivent être supprimés après la date d'expiration de la planification.
8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

Pour EMS, reportez-vous à la section "[Gérer la collecte de données EMS](#)"

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

Vous devez surveiller le processus de clonage à l'aide de la page **moniteur > travaux**.

## Surveillez les opérations de clonage des bases de données SQL

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Annuler les opérations de clonage de ressources SQL

Vous pouvez annuler les opérations de clonage mises en file d'attente.

Pour annuler les opérations de clonage, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâches.

### Description de la tâche

- Vous pouvez annuler une opération de clonage en file d'attente à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de clonage en cours d'exécution.
- Vous pouvez utiliser l'interface utilisateur graphique SnapCenter, les applets de commande PowerShell ou les commandes de l'interface de ligne de commande pour annuler les opérations de clonage mises en attente.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de clonage en file d'attente d'autres membres tout en utilisant ce rôle.

### Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>2. Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li></ol>
Volet activité	<ol style="list-style-type: none"><li>1. Après avoir lancé l'opération de clonage, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li><li>2. Sélectionner l'opération.</li><li>3. Dans la page <b>Détails du travail</b>, cliquez sur <b>Annuler le travail</b>.</li></ol>

### Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.

- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur **\*\*** .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

## Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

# Protection des bases de données SAP HANA

## Plug-in SnapCenter pour bases de données SAP HANA

### Présentation du plug-in SnapCenter pour les bases de données SAP HANA

Le plug-in SnapCenter pour base de données SAP HANA est un composant côté hôte du logiciel NetApp SnapCenter qui permet de gérer la protection des données des bases de données SAP HANA avec cohérence applicative. Le plug-in pour base de données SAP HANA automatise la sauvegarde, la restauration et le clonage des bases de données SAP HANA dans votre environnement SnapCenter.

SnapCenter prend en charge le MDC (conteneur unique et base de données mutualisée). Vous pouvez utiliser le plug-in pour base de données SAP HANA dans les environnements Windows et Linux. Le plug-in qui n'est pas installé sur l'hôte de base de données HANA est appelé le plug-in hôte centralisé. Le plug-in hôte centralisé peut gérer plusieurs bases de données HANA sur plusieurs hôtes.

Lorsque le plug-in pour la base de données SAP HANA est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Vous pouvez également utiliser le plug-in doté de la technologie SnapVault de NetApp pour effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes.

Le plug-in pour SAP HANA Database prend en charge la synchronisation active SnapMirror (initialement commercialisé sous le nom de SnapMirror Business Continuity [SM-BC]). Les services de l'entreprise peuvent ainsi continuer de fonctionner même en cas de défaillance complète du site, ce qui permet aux applications de basculer en toute transparence via une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

### Comment utiliser le plug-in SnapCenter pour base de données SAP HANA

Lorsque vous installez le plug-in pour base de données SAP HANA dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner les bases de données SAP HANA et leurs ressources. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Ajouter des bases de données.
- Création de sauvegardes.
- Effectuez des restaurations à partir des sauvegardes.
- Sauvegardes clones.
- Planifiez les opérations de sauvegarde.
- Contrôle des opérations de sauvegarde, de restauration et de clonage
- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.

### Fonctionnalités du plug-in SnapCenter pour les bases de données SAP HANA

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour travailler avec le plug-in pour base de données SAP HANA,

vous utilisez l'interface graphique de SnapCenter.

- **Interface utilisateur graphique unifiée**

L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

Vous pouvez planifier des opérations de sauvegarde, configurer la conservation des sauvegardes basée sur des règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie de copie Snapshot NetApp non disruptive**

SnapCenter utilise la technologie Snapshot de NetApp avec le plug-in pour la base de données SAP HANA pour sauvegarder les ressources.

L'utilisation du plug-in pour base de données SAP HANA offre également les avantages suivants :

- Prise en charge des workflows de sauvegarde, de restauration et de clonage
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Création de copies compactes et ponctuelles de ressources à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonctionnalité Snapshot de groupe de cohérence (CG) de ONTAP dans le cadre de la création des sauvegardes.
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

En une seule opération, les snapshots sont consolidés lorsque les ressources d'un hôte unique partagent le même volume.

- Possibilité de créer des instantanés à l'aide de commandes externes.
- Prise en charge des sauvegardes basées sur des fichiers.
- Prise en charge de Linux LVM sur le système de fichiers XFS.

## **Types de stockage pris en charge par le plug-in SnapCenter pour la base de données SAP HANA**

SnapCenter prend en charge de nombreux types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier la prise en charge de votre type de stockage avant d'installer le plug-in SnapCenter pour la base de données SAP HANA.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"> <li>• LUN connectés via FC</li> <li>• LUN connectées à l'iSCSI</li> <li>• Volumes connectés par NFS</li> </ul>
VMware ESXi	<ul style="list-style-type: none"> <li>• L'exécution des LUN RDM connectés par un HBA FC ou iSCSI ESXi peut prendre du temps car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte.</li> </ul> <p data-bbox="862 510 1487 743">Vous pouvez modifier le fichier <b>LinuxConfig.pm</b> situé à  <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> à 1 pour analyser uniquement les HBA répertoriés dans les NOMS de PILOTE HBA.</p> <ul style="list-style-type: none"> <li>• LUN iSCSI connectés directement au système invité par l'initiateur iSCSI</li> <li>• VMDK sur des datastores NFS</li> <li>• VMDK sur VMFS créés</li> <li>• Volumes NFS connectés directement au système invité</li> <li>• Datastores vVol sur NFS et SAN</li> </ul> <p data-bbox="862 1115 1468 1213">Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>

## Privilèges ONTAP minimum requis pour le plug-in SAP HANA

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - la création de lun
  - la création de lun
  - suppression de la lun

- lun igroup add
- créez un groupe initiateur lun
- suppression du groupe initiateur lun
- renommer la lun igroup
- renommer la lun igroup
- affichage de la lun igroup
- lun mapping des nœuds supplémentaires
- création d'un mappage de lun
- suppression du mappage de lun
- mappage de lun supprimer-rapports-nœuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- suppression de la réservation persistante de lun
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes

- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- volume snapshot modify-snaplock-expiration-time
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau
  - interface réseau affiche

- un vserver

## Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault pour les bases de données SAP HANA

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Stratégie de sauvegarde pour les bases de données SAP HANA

### Définissez une stratégie de sauvegarde pour les bases de données SAP HANA

Définir une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous aide à disposer des sauvegardes dont vous avez besoin pour restaurer ou cloner vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

#### Description de la tâche

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

#### Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.

2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décidez si vous souhaitez créer une règle basée sur les copies Snapshot pour sauvegarder des copies Snapshot cohérentes au niveau des applications de la base de données.
5. Décidez si vous voulez vérifier l'intégrité de la base de données.
6. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
7. Déterminez la période de conservation des snapshots sur le système de stockage source et la destination SnapMirror.
8. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescripteur ou un PostScript.

### **Découverte automatique des ressources sur l'hôte Linux**

Les ressources sont les bases de données SAP HANA et les volumes non data sur l'hôte Linux gérés par SnapCenter. Après avoir installé le plug-in SnapCenter pour la base de données SAP HANA, les bases de données SAP HANA sur cet hôte Linux sont automatiquement découvertes et affichées sur la page Ressources.

La découverte automatique est prise en charge pour les ressources SAP HANA suivantes :

- Des conteneurs uniques

Après l'installation ou la mise à niveau du plug-in, les ressources du conteneur unique situées sur un plug-in hôte centralisé continueront d'être ajoutées manuellement.

Après l'installation ou la mise à niveau du plug-in, les bases de données SAP HANA sont automatiquement découvertes uniquement sur les hôtes SAP HANA Linux, qui sont directement enregistrés dans SnapCenter.

- Conteneur de base de données mutualisée (MDC)

Après l'installation ou la mise à niveau du plug-in, les ressources MDC situées sur un plug-in d'hôte centralisé continueront d'être ajoutées manuellement.

Après la mise à niveau vers SnapCenter 4.3, vous devez continuer à ajouter manuellement les ressources MDC sur le plug-in d'hôte centralisé.

Pour les hôtes SAP HANA Linux directement enregistrés dans SnapCenter, l'installation ou la mise à niveau du plug-in déclenchera une détection automatique des ressources sur l'hôte. Après la mise à niveau du plug-in, pour chaque ressource MDC située sur l'hôte du plug-in, une autre ressource MDC sera automatiquement découverte avec un format GUID différent et enregistrée dans SnapCenter. La nouvelle ressource sera à l'état verrouillé.

Par exemple, dans SnapCenter 4.2, si la ressource MDC E90 était située sur l'hôte du plug-in et enregistrée manuellement, après la mise à niveau vers SnapCenter 4.3, une autre ressource MDC E90 avec un GUID différent sera découverte et enregistrée dans SnapCenter.

La détection automatique n'est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK



Lorsque les ressources ci-dessus sont découvertes, les opérations de protection des données ne sont pas prises en charge sur ces ressources.

- Configuration HANA avec plusieurs hôtes
- Plusieurs instances sur le même hôte
- Réplication système HANA scale-out multi-niveaux
- Environnement de réplication en cascade en mode réplication du système

### Types de sauvegardes pris en charge

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge la sauvegarde basée sur fichier et les types de sauvegarde basés sur des copies Snapshot pour les bases de données SAP HANA.

#### Sauvegarde basée sur des fichiers

Les sauvegardes basées sur des fichiers vérifient l'intégrité de la base de données. Vous pouvez planifier l'opération de sauvegarde basée sur des fichiers afin d'effectuer à des intervalles spécifiques. Seuls les locataires actifs sont sauvegardés. Vous ne pouvez ni restaurer ni cloner des sauvegardes basées sur des fichiers à partir de SnapCenter.

#### Sauvegarde basée sur des copies Snapshot

Les sauvegardes basées sur des copies Snapshot utilisent la technologie Snapshot de NetApp pour créer des copies en ligne en lecture seule des volumes sur lesquels résident les bases de données SAP HANA.

#### Comment le plug-in SnapCenter pour SAP HANA Database utilise les snapshots de groupe de cohérence

Vous pouvez utiliser le plug-in pour créer des snapshots de groupe de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes, de sorte que vous puissiez les gérer comme une entité unique. Un groupe de cohérence est constitué de copies Snapshot simultanées de plusieurs volumes, ce qui procure des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente nécessaire au contrôleur de stockage pour regrouper les snapshots de manière cohérente. Les options de temps d'attente disponibles sont **urgent**, **Moyen** et **détendu**. Vous pouvez également activer ou désactiver la synchronisation WAFL (Write Anywhere File Layout) pendant le fonctionnement d'un snapshot de groupe cohérent. Le système WAFL Sync améliore les performances d'un snapshot de groupe de cohérence.

#### SnapCenter gère l'organisation des sauvegardes de journaux et de données

SnapCenter gère l'organisation des sauvegardes des journaux et des données au niveau du système de stockage et des systèmes de fichiers, ainsi que dans le catalogue des sauvegardes SAP HANA.

Les snapshots du stockage primaire ou secondaire et les entrées correspondantes dans le catalogue SAP HANA sont supprimés en fonction des paramètres de conservation. Les entrées du catalogue SAP HANA sont également supprimées lors de la sauvegarde et de la suppression des groupes de ressources.

## Considérations relatives à la détermination des planifications de sauvegarde pour les bases de données SAP HANA

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes (fréquence des sauvegardes)

La fréquence de sauvegarde, également appelée type de planification pour certains plug-ins, fait partie d'une configuration de règles. Par exemple, vous pouvez configurer la fréquence des sauvegardes sous forme horaire, quotidienne, hebdomadaire ou mensuelle.

- Planifications de sauvegardes (exactement quand les sauvegardes doivent être effectuées)

Les planifications de sauvegarde font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour la sauvegarder tous les jeudis à 10 h 00

## Nombre de tâches de sauvegarde nécessaires pour les bases de données SAP HANA

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

## Conventions de nom de sauvegarde pour le plug-in pour bases de données SAP HANA

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.

- *mach1x88* est le nom d'hôte.
- *03-12-2015\_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, `clienttext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

## Stratégie de restauration et de récupération pour les bases de données SAP HANA

### Définissez une stratégie de restauration et de reprise pour les ressources SAP HANA

Vous devez définir une stratégie avant de restaurer et de récupérer votre base de données pour que vous puissiez effectuer correctement les opérations de restauration et de récupération.

#### Étapes

1. Déterminez les stratégies de restauration prises en charge pour les ressources SAP HANA ajoutées manuellement
2. Déterminez les stratégies de restauration prises en charge pour les bases de données SAP HANA découvertes automatiquement
3. Choisissez le type d'opérations de restauration à effectuer.

### Types de stratégies de restauration pris en charge pour les ressources SAP HANA ajoutées manuellement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les ressources SAP HANA ajoutées manuellement. Vous ne pouvez pas restaurer des ressources SAP HANA ajoutées manuellement.



Vous ne pouvez pas restaurer des ressources SAP HANA ajoutées manuellement.

#### Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

#### Restauration au niveau des fichiers

- Restaure les fichiers à partir de volumes, de qtrees ou de répertoires
- Restaure uniquement les LUN sélectionnées

## Types de stratégies de restauration pris en charge pour les bases de données SAP HANA automatiquement découvertes

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les bases de données SAP HANA automatiquement découvertes.

### Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource
  - L'option **Volume Revert** doit être sélectionnée pour restaurer l'intégralité du volume.



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

### Base de données des locataires

- Restaure la base de données des locataires

Si l'option **tenant Database** est sélectionnée, vous devez utiliser des scripts de reprise HANA Studio ou HANA externes à SnapCenter pour effectuer l'opération de reprise.

## Types d'opérations de restauration des bases de données SAP HANA découvertes automatiquement

SnapCenter prend en charge la technologie SnapRestore (VBSR) basée sur des volumes, le SnapRestore de fichiers uniques et les types de restauration de connexion et de copie pour les bases de données SAP HANA automatiquement découvertes.

La technologie SnapRestore basée sur les volumes (VBSR) est effectuée dans des environnements NFS pour les scénarios suivants :

- Lorsque la sauvegarde sélectionnée pour la restauration est prise sur des versions antérieures à SnapCenter 4.3 et uniquement si l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde sélectionnée pour la restauration est prise dans SnapCenter 4.3 et si l'option **Retour volume** est sélectionnée

Single File SnapRestore s'effectue dans des environnements NFS pour les scénarios suivants :

- Lorsque la sauvegarde sélectionnée pour la restauration est prise dans SnapCenter 4.3 et que seule l'option **ressource complète** est sélectionnée
- Pour les conteneurs de base de données multilocataires (MDC), lorsque la sauvegarde sélectionnée pour la restauration est prise sur SnapCenter 4.3 et que l'option **base de données locataire** est sélectionnée
- Lorsque la sauvegarde sélectionnée provient d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Complete Resource** est sélectionnée

Single File SnapRestore s'effectue dans des environnements SAN pour les scénarios suivants :

- Lorsque des sauvegardes sont effectuées sur des versions antérieures à SnapCenter 4.3 et uniquement si l'option **ressource complète** est sélectionnée

- Lorsque des sauvegardes sont effectuées dans SnapCenter 4.3, et seulement si l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée depuis un emplacement secondaire SnapMirror ou SnapVault et l'option **Complete Resource** est sélectionnée

La restauration par connexion ou copie s'effectue dans des environnements SAN pour le scénario suivant :

- Pour MDC, lorsque la sauvegarde sélectionnée pour la restauration est prise dans SnapCenter 4.3 et que l'option **base de données locataire** est sélectionnée



Les options **ressource complète**, **Retour de volume** et **base de données locataire** sont disponibles sur la page étendue de la restauration.

### Types d'opérations de récupération pris en charge pour les bases de données SAP HANA

SnapCenter permet d'effectuer différents types d'opérations de restauration pour les bases de données SAP HANA.

- Restaurez la base de données à l'état le plus récent
- Restaurez la base de données à un point dans le temps spécifique

Vous devez indiquer la date et l'heure de la récupération.

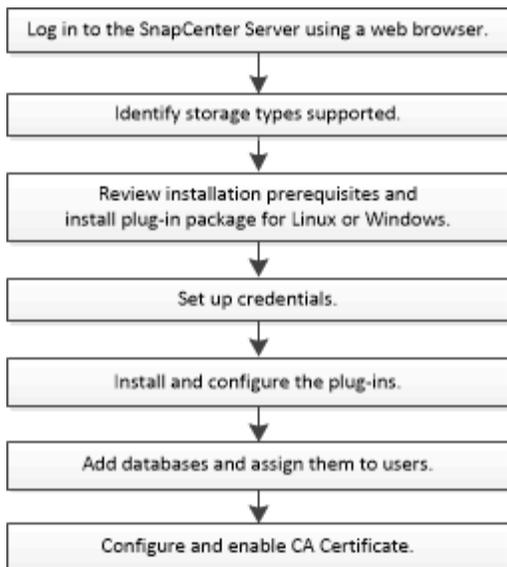
- Restaurer la base de données jusqu'à une sauvegarde de données spécifique

SnapCenter fournit également l'option pas de restauration pour les bases de données SAP HANA.

## Préparez l'installation du plug-in SnapCenter pour la base de données SAP HANA

### Workflow d'installation du plug-in SnapCenter pour la base de données SAP HANA

Vous devez installer et configurer le plug-in SnapCenter pour base de données SAP HANA si vous souhaitez protéger vos bases de données SAP HANA.



## Conditions préalables pour l'ajout d'hôtes et l'installation du plug-in SnapCenter pour la base de données SAP HANA

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour base de données SAP HANA est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 11 sur votre hôte.



IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Vous devez avoir installé le terminal interactif de la base de données SAP HANA (client HDBSQL) sur l'hôte.
- Pour Windows, Plug-in Creator Service doit être en cours d'exécution à l'aide de l'utilisateur Windows « LocalSystem », ce qui est le comportement par défaut lorsque Plug-in pour SAP HANA Database est installé en tant qu'administrateur de domaine.
- Pour Windows, les clés de la boutique utilisateur doivent être créées en tant qu'utilisateur SYSTÈME.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in SAP HANA sur les hôtes Windows.
- Pour l'hôte Linux, les clés HDB Secure User Store sont accessibles en tant qu'utilisateur HDBSQL OS.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte de base de données SAP HANA.

### Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour base de données SAP HANA sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.

- Vous devez avoir installé Java 11 sur votre hôte Windows.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Matrice d'interopérabilité NetApp"](#)

## Hôtes Linux

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Matrice d'interopérabilité NetApp"](#)

- Pour les bases de données SAP HANA qui s'exécutent sur un hôte Linux, lors de l'installation du plug-in pour base de données SAP HANA, le plug-in SnapCenter pour UNIX est installé automatiquement.
- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

## Commandes supplémentaires

Pour exécuter une commande supplémentaire sur le plug-in SnapCenter pour SAP HANA, vous devez l'inclure dans le fichier *allowed\_commands.config*.

- Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
- Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*

Pour autoriser des commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier *allowed\_commands.config* dans un éditeur. Entrez chaque commande sur une ligne distincte et les commandes ne sont pas sensibles à la casse. Assurez-vous de spécifier le chemin d'accès complet et de le joindre entre guillemets (") s'il contient des espaces.

Par exemple :

commande : mount

commande : umount

Commande : « C:\Program Files\NetApp\SnapCreator commands\sdcli.exe »

commande : myscript.bat

Si le fichier *allowed\_commands.config* n'est pas présent, les commandes ou l'exécution du script seront bloquées et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »

Si la commande ou le script n'est pas présent dans *allowed\_commands.config*, l'exécution de la commande ou du script sera bloquée et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »



Vous ne devez pas utiliser de caractère générique (\*) pour autoriser toutes les commandes.

## Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux

Les versions SnapCenter 2.0 et ultérieures permettent à un utilisateur non-root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

### À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- `/Home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/Custom_location/NetApp/snapcenter/spl/installation/plugins/désinstaller`
- `/Custom_location/NetApp/snapcenter/spl/bin/spl`

### Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.

2. Ajoutez les lignes suivantes au fichier `/etc/sudoers` à l'aide de l'utilitaire visudo Linux.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`LINUX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Linux. .



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java et OpenJDK</li> </ul> <p>Java 11 Oracle Java et OpenJDK sont requis uniquement pour SAP HANA, IBM DB2, PostgreSQL, MySQL, les plug-ins pris en charge par NetApp et d'autres applications personnalisées qui peuvent être installées sur l'hôte Windows.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

## Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux

Avant d'installer le module de plug-ins SnapCenter pour Linux, vous devez connaître

certains besoins en espace système hôte de base et en dimensionnement.

Élément	De formation
Systèmes d'exploitation	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>2 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
Packs logiciels requis	<p>Java 11 Oracle Java et OpenJDK</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>

## Configurer les identifiants du plug-in SnapCenter pour la base de données SAP HANA

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

### Description de la tâche

- Hôtes Linux

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

**Meilleure pratique:** bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.

Credential

Provide information for the Credential you want to add

Credential Name

Username  i

Password

Authentication

Use sudo privileges i

Cancel OK

4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.
Nom d'utilisateur	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>• Administrateur de domaine ou tout membre du groupe d'administrateurs</li> </ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li>◦ <i>NetBIOS\username</i></li> <li>◦ <i>Domain FQDN\username</i></li> </ul> <ul style="list-style-type: none"> <li>• Administrateur local (groupes de travail uniquement)</li> </ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p> <p>N'utilisez pas de guillemets (") ou de contre-coches (') dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.

Pour ce champ...	Procédez comme ça...
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p> <p> Applicable uniquement aux utilisateurs Linux.</p>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

### Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

### Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediely
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```

domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.

```

Par exemple :

```

New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.

```

4. Configurez le GMSA sur vos hôtes :

- a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Installez le plug-in SnapCenter pour les bases de données SAP HANA

### Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour un cluster.

#### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :

- Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
- Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

["Configurez le compte de service géré par groupe sous Windows Server 2016 ou version ultérieure pour SAP HANA"](#)

### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.
- Pour la réplication système SAP HANA afin de détecter les ressources sur les systèmes principal et secondaire, il est recommandé d'ajouter à la fois les systèmes principal et secondaire à l'aide de l'utilisateur root ou sudo.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez le type d'hôte :</p> <ul style="list-style-type: none"> <li>• Répertoires de base</li> <li>• Linux</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Le plug-in pour SAP HANA est installé sur l'hôte client HDBSQL et cet hôte peut se trouver sur un système Windows ou Linux.</p> </div>

Pour ce champ...	Procédez comme ça...
Nom d'hôte	<p>Entrez le nom d'hôte de communication. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p> <p>Vous devez configurer le client HDBSQL et HDBUserStore sur cet hôte.</p>
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez fourni.</p> <div data-bbox="873 982 927 1041" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div data-bbox="873 1629 927 1688" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p> </div>

Pour ce champ...	Procédez comme ça...
Chemin d'installation	<p>Le plug-in pour SAP HANA est installé sur l'hôte client HDBSQL et cet hôte peut se trouver sur un système Windows ou Linux.</p> <ul style="list-style-type: none"> <li>• Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin.</li> <li>• Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.</li> </ul>
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	<p>Pour l'hôte Windows, cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Indiquez le nom GMSA au format suivant : domainname\accountName\$.</p> <p> GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.</p> </div>

7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse C:\Program Files\NetApp\SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

9. Surveillez la progression de l'installation.

Les fichiers journaux spécifiques à l'installation se trouvent dans `/custom_location/snapcenter/logs`.

### Installez les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer simultanément les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage` PowerShell.

#### Avant de commencer

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

#### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande `Open-SmConnection`, puis saisissez vos informations d'identification.
3. Installez le plug-in sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Vous pouvez utiliser l'option `-skipreccheck` lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

4. Saisissez vos informations d'identification pour l'installation à distance.

### Installez le plug-in SnapCenter pour SAP HANA Database sur des hôtes Linux à l'aide de l'interface de ligne de commandes

Vous devez installer le plug-in SnapCenter pour la base de données SAP HANA à l'aide de l'interface utilisateur de SnapCenter. Si votre environnement n'autorise pas l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter, vous pouvez installer le plug-in pour base de données SAP HANA en mode console ou en mode silencieux à l'aide de l'interface de ligne de commandes.

#### Avant de commencer

- Vous devez installer le plug-in pour la base de données SAP HANA sur chacun des hôtes Linux sur lesquels réside le client HDBSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour la base de données SAP HANA doit répondre aux exigences des logiciels, bases de données et systèmes d'exploitation qui en dépendent.

La matrice d'interopérabilité (IMT) contient les dernières informations sur les configurations prises en charge.

<https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT>

- Le plug-in SnapCenter pour base de données SAP HANA fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé SnapCenter sur un hôte Windows.

## Étapes

1. Copiez le fichier d'installation du package de plug-ins SnapCenter pour Linux (snapcenter\_linux\_host\_plugin.bin) depuis C:\ProgramData\NetApp\SnapCenter\Package Repository vers l'hôte où vous souhaitez installer le plug-in pour la base de données SAP HANA.

Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in :

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server
```

  - -DPORT spécifie le port de communication SMCORE HTTPS.
  - -DSERVER\_IP spécifie l'adresse IP du serveur SnapCenter.
  - -DSERVER\_HTTPS\_PORT spécifie le port HTTPS du serveur SnapCenter.
  - -DUSER\_INSTALL\_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
  - DINSTALL\_LOG\_NAME indique le nom du fichier journal.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Modifiez le fichier /<répertoire d'installation>/NetApp/snapcenter/scc/etc/SC\_SMS\_Services.properties, puis ajoutez le paramètre PLUGINS\_ENABLED = hana:3.0.
5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Contrôler l'état de l'installation du plug-in pour SAP HANA

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour

déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

## Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

## Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
  - a. Double-cliquez sur le certificat.
  - b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
  - c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
  - d. Copiez les caractères hexadécimaux de la zone.
  - e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :
  - a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

### Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

#### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Configurez le certificat d'autorité de certification pour le service de plug-ins SnapCenter SAP HANA sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier « keystore.jks », qui se trouve dans `/opt/NetApp/snapcenter/scc/etc` à la fois comme magasin de confiance et magasin de clés.

### Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Procédez de même pour la clé KEYSTORE\_PASS dans le fichier `agent.properties`.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

## Étapes

1. Accédez au dossier contenant le keystore du plug-in : /opt/NetApp/snapcenter/scc/etc.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaires pour le plug-in trust-store.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

## Étapes

1. Accédez au dossier contenant le keystore du plug-in /opt/NetApp/snapcenter/scc/etc.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Répertorier les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé KEYSTORE\_PASS dans le fichier agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
```

. Si le nom d'alias du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("\*", ",", "), remplacez le nom d'alias par un nom simple :

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
```

. Configurez le nom d'alias à partir du certificat CA dans le fichier `agent.properties`.

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in `trust-store`.

### Configurer la liste de révocation de certificats (CRL) pour les plug-ins

#### Description de la tâche

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est « `opt/NetApp/snapcenter/scc/etc/crl` ».

#### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `agent.properties` par rapport à la clé `CRL_PATH`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

### Configurez le certificat d'autorité de certification pour le service de plug-ins SnapCenter SAP HANA sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier `keystore.jks`, qui se trouve dans `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc` à la fois comme magasin de confiance et magasin de clés.

### Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé `KEYSTORE_PASS`.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
```



Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks
```

Procédez de même pour la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

4. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
Keytool -import -truacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du

plug-in.

## Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier *keystore.jks*.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier *agent.properties*.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configurez le nom d'alias à partir du certificat CA dans le fichier *agent.properties*.

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in *trust-store*.

## Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

### Description de la tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section ["Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter"](#).
- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est *'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'*.

### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier *agent.properties* par rapport à la clé `CRL_PATH`.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM) ou si vous souhaitez protéger des VM et des datastores, vous devez déployer l'appliance virtuelle du plug-in SnapCenter pour VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section ["Présentation du déploiement"](#).

### Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section ["Créez ou importez un certificat SSL"](#).

## Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est */opt/netapp/config/crl*.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

## Préparation à la protection des données

### Conditions préalables à l'utilisation du plug-in SnapCenter pour la base de données SAP HANA

Avant d'utiliser le plug-in SnapCenter pour base de données SAP HANA, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches préalables.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.
- Installez Java 11 sur votre hôte Linux ou Windows.

Vous devez définir le chemin Java dans la variable de chemin d'environnement de la machine hôte.

- Configurer SnapMirror et SnapVault pour la réplication de sauvegarde.
- Installez le client HDBSQL sur l'hôte sur lequel vous installerez le plug-in pour la base de données SAP HANA.

Configurez les clés de magasin utilisateur pour les nœuds SAP HANA que vous allez gérer via cet hôte.

- Pour la base de données SAP HANA 2.0SPS05, si vous utilisez un compte utilisateur de base de données SAP HANA, assurez-vous que vous disposez des autorisations suivantes pour effectuer des opérations de sauvegarde, de restauration et de clonage dans SnapCenter Server :
  - Administrateur des sauvegardes
  - Lecture du catalogue
  - Administrateur de sauvegarde de base de données
  - Opérateur de récupération de base de données

### Mode d'utilisation des ressources, des groupes de ressources et des règles pour la protection des bases de données SAP HANA

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des bases de données SAP HANA que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Les règles spécifient la fréquence des sauvegardes, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

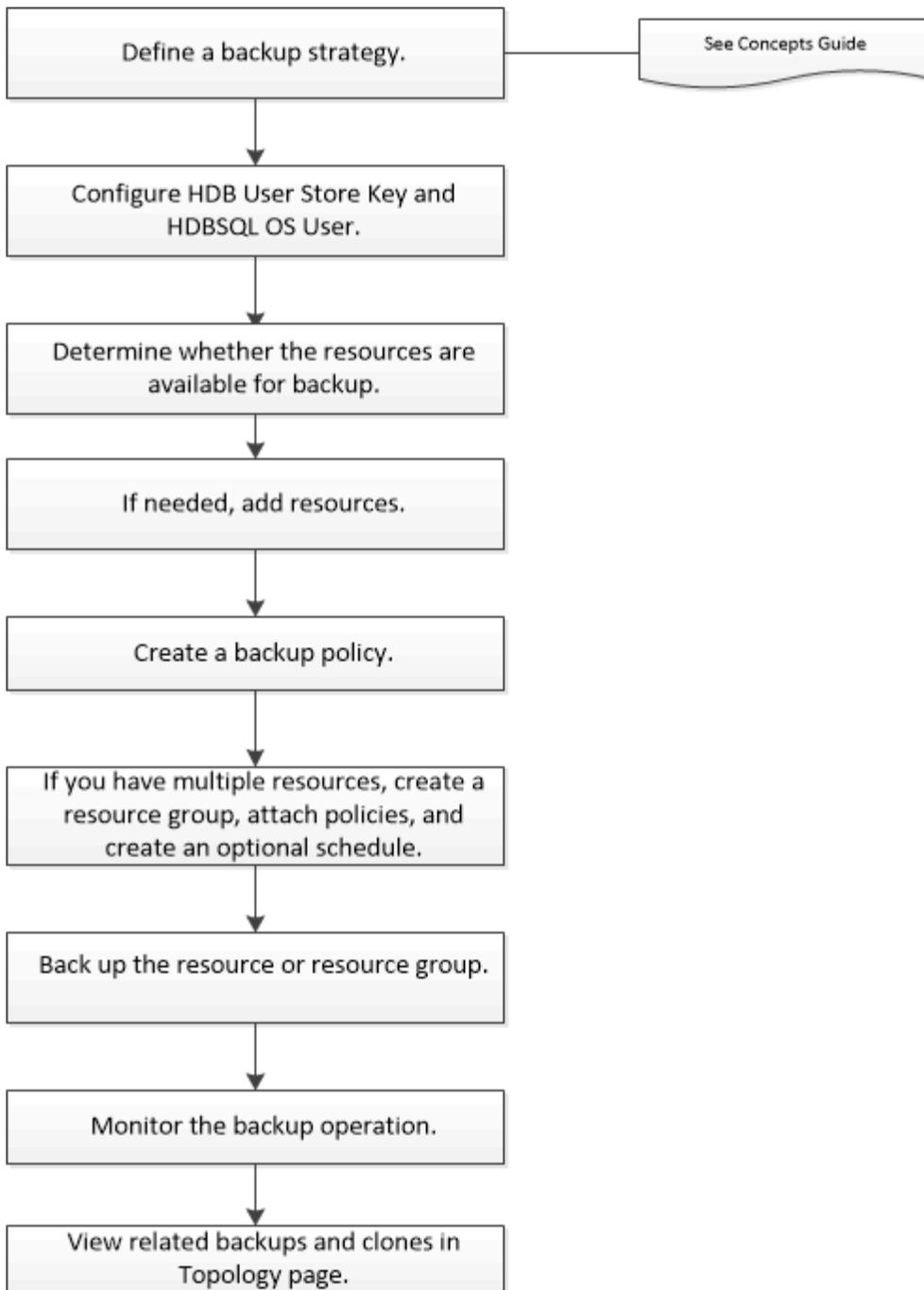
Considérez un groupe de ressources comme définissant ce que vous voulez protéger et quand vous voulez le protéger en termes de jour et d'heure. Considérez une stratégie comme une définition de la façon dont vous voulez la protéger. Si vous sauvegardez toutes les bases de données, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources de manière à effectuer une sauvegarde complète tous les jours.

## **Sauvegarde des ressources SAP HANA**

### **Sauvegarde des ressources SAP HANA**

Vous pouvez créer une sauvegarde d'une ressource (base de données) ou d'un groupe de ressources. Le workflow de sauvegarde inclut la planification, l'identification des bases de données pour la sauvegarde, la gestion des stratégies de sauvegarde, la création de groupes de ressources et la connexion de stratégies, la création de sauvegardes et le contrôle des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent plus d'informations sur les applets de commande PowerShell. ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA

Vous devez configurer la clé de stockage utilisateur HDB et l'utilisateur HDBSQL pour effectuer des opérations de protection des données sur des bases de données SAP HANA.

### Avant de commencer

- Si la clé HDB Secure User Store et l'utilisateur HDB SQL OS ne sont pas configurés dans la base de données SAP HANA, une icône de cadenas rouge s'affiche uniquement pour les ressources découvertes automatiquement. Si, au cours d'une opération de découverte ultérieure, la clé de stockage sécurisée HDB configurée a été détectée comme incorrecte ou n'a pas fourni d'accès à la base de données elle-même, l'icône rouge du cadenas réapparaîtra.
- Vous devez configurer la clé du magasin d'utilisateurs sécurisé HDB et l'utilisateur HDB SQL OS pour pouvoir protéger la base de données ou l'ajouter à un groupe de ressources pour effectuer des opérations de protection des données.
- Vous devez configurer HDB SQL OS User pour accéder à la base de données système. Si HDB SQL OS User est configuré pour accéder uniquement à la base de données de tenant, l'opération de découverte échoue.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez Plug-in SnapCenter pour base de données SAP HANA dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste **Affichage**.
3. (Facultatif) cliquez sur  et sélectionnez le nom d'hôte.

Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

4. Sélectionnez la base de données, puis cliquez sur **configurer la base de données**.
5. Dans la section configurer les paramètres de la base de données, entrez la clé de stockage sécurisée de l'utilisateur HDB.



Le nom d'hôte du plug-in s'affiche et l'utilisateur HDB SQL OS est automatiquement renseigné sur <sid>adm.

6. Cliquez sur **OK**.

Vous pouvez modifier la configuration de la base de données à partir de la page topologie.

## Découverte des ressources et préparation de conteneurs de bases de données mutualisés pour la protection des données

### Découvrir les bases de données automatiquement

Les ressources sont les bases de données SAP HANA et les volumes non data sur l'hôte Linux gérés par SnapCenter. Vous pouvez ajouter ces ressources aux groupes de ressources pour effectuer des opérations de protection des données après avoir découvert les bases de données SAP HANA disponibles.

### Avant de commencer

- Vous devez avoir déjà terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'une clé de stockage utilisateur HDB, l'ajout d'hôtes et la configuration des connexions du système de stockage.
- Vous devez avoir configuré la clé de stockage utilisateur sécurisée HDB et l'utilisateur HDB SQL OS sur l'hôte Linux.
  - Vous devez configurer la clé de stockage utilisateur HDB avec l'utilisateur adm SID. Par exemple, pour un système HANA avec A22 comme SID, la clé de stockage utilisateur HDB doit être configurée avec a22adm.

- Le plug-in SnapCenter pour base de données SAP HANA ne prend pas en charge la découverte automatique des ressources résidant dans des environnements virtuels RDM/VMDK. Vous devez fournir les informations de stockage pour les environnements virtuels tout en ajoutant les bases de données manuellement.

### Description de la tâche

Après l'installation du plug-in, toutes les ressources de cet hôte Linux sont automatiquement découvertes et affichées sur la page Ressources.

Les ressources détectées automatiquement ne peuvent pas être modifiées ou supprimées.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in pour la base de données SAP HANA dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste vue.
3. (Facultatif) cliquez sur \* , puis sélectionnez le nom d'hôte.

Vous pouvez alors cliquer sur \*  pour fermer le volet de filtre.

4. Cliquez sur **Actualiser les ressources** pour découvrir les ressources disponibles sur l'hôte.

Les ressources s'affichent avec des informations telles que le type de ressource, le nom d'hôte, les groupes de ressources associés, le type de sauvegarde, les stratégies et l'état global.

- Si la base de données se trouve sur un système de stockage NetApp et qu'elle n'est pas protégée, elle s'affiche dans la colonne État global.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée, et si aucune opération de sauvegarde n'est effectuée, alors l'option sauvegarde non exécutée s'affiche dans la colonne État global. Dans le cas contraire, l'état passe en échec de la sauvegarde ou la sauvegarde a réussi en fonction de l'état de la dernière sauvegarde.



Si une clé de stockage HDB Secure User Store n'est pas configurée dans la base de données SAP HANA, une icône de cadenas rouge apparaît à côté de la ressource. Si, au cours d'une opération de découverte ultérieure, la clé de stockage sécurisée HDB configurée a été détectée comme incorrecte ou n'a pas fourni d'accès à la base de données elle-même, l'icône rouge du cadenas réapparaîtra.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

### Une fois que vous avez terminé

Vous devez configurer la clé du magasin d'utilisateurs sécurisé HDB et l'utilisateur HDBSQL pour pouvoir protéger la base de données ou l'ajouter au groupe de ressources pour effectuer des opérations de protection des données.

["Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA"](#)

### Préparez des conteneurs de bases de données mutualisés pour protéger les données

Pour les hôtes SAP HANA directement enregistrés dans SnapCenter, l'installation ou la mise à niveau du plug-in SnapCenter pour base de données SAP HANA déclenchera

une détection automatique des ressources sur l'hôte. Après l'installation ou la mise à niveau du plug-in, pour chaque ressource MDC (conteneur de base de données multitenant) située sur l'hôte du plug-in, une autre ressource MDC sera automatiquement découverte avec un format GUID différent et enregistrée dans SnapCenter. La nouvelle ressource sera à l'état « verrouillée ».

### Description de la tâche

Par exemple, dans SnapCenter 4.2, si la ressource MDC E90 était située sur l'hôte du plug-in et enregistrée manuellement, après la mise à niveau vers SnapCenter 4.3, une autre ressource MDC E90 avec un GUID différent sera découverte et enregistrée dans SnapCenter.



Les sauvegardes associées à la ressource de SnapCenter 4.2 et versions antérieures doivent être conservées jusqu'à l'expiration de la période de conservation. Après l'expiration de la période de conservation, vous pouvez supprimer l'ancienne ressource MDC et continuer à gérer la nouvelle ressource MDC découverte automatiquement.

`Old MDC resource` Est la ressource MDC pour un hôte de plug-in qui a été ajouté manuellement dans SnapCenter 4.2 ou une version antérieure.

Pour commencer à utiliser la nouvelle ressource découverte dans SnapCenter 4.3 pour les opérations de protection des données, procédez comme suit :

### Étapes

1. Dans la page Ressources, sélectionnez l'ancienne ressource MDC avec les sauvegardes ajoutées à la version précédente de SnapCenter, puis placez-la dans "mode de maintenance" à partir de la page topologie.

Si la ressource fait partie d'un groupe de ressources, placez le groupe de ressources dans "mode de provenance".

2. Configurez la nouvelle ressource MDC découverte après la mise à niveau vers SnapCenter 4.3 en sélectionnant la nouvelle ressource dans la page Ressources.

« Nouvelle ressource MDC » est la nouvelle ressource MDC découverte une fois le serveur SnapCenter et l'hôte du plug-in mis à niveau vers 4.3. La nouvelle ressource MDC peut être identifiée comme une ressource avec le même SID que l'ancienne ressource MDC, pour un hôte donné, et avec une icône de cadenas rouge à côté de celle-ci dans la page Ressources.

3. Protégez la nouvelle ressource MDC détectée après la mise à niveau vers SnapCenter 4.3 en sélectionnant des stratégies de protection, des plannings et des paramètres de notification.
4. Supprimez les sauvegardes effectuées dans SnapCenter 4.2 ou les versions antérieures en fonction des paramètres de conservation.
5. Supprimez le groupe de ressources de la page topologie.
6. Supprimez l'ancienne ressource MDC de la page Ressources.

Par exemple, si la période de conservation des snapshots primaires est de 7 jours et que la conservation des snapshots secondaires est de 45 jours, après 45 jours et après la suppression de toutes les sauvegardes, vous devez supprimer le groupe de ressources et l'ancienne ressource MDC.

### Informations associées

["Configurez la clé HDB User Store et l'utilisateur HDBSQL OS pour la base de données SAP HANA"](#)

## Ajoutez des ressources manuellement au plug-in hôte

La détection automatique n'est pas prise en charge pour certaines instances HANA. Vous devez ajouter ces ressources manuellement.

### Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout d'une clé de stockage utilisateur HDB.
- Pour la réplication des systèmes SAP HANA, il est recommandé d'ajouter toutes les ressources de ce système HANA dans un groupe de ressources et de sauvegarder un groupe de ressources. Cela garantit une sauvegarde transparente en mode basculement/retour arrière.

"Créer des groupes de ressources et attacher des stratégies".

### Description de la tâche

La détection automatique n'est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK



Lorsque les ressources ci-dessus sont découvertes, les opérations de protection des données ne sont pas prises en charge sur ces ressources.

- Configuration HANA avec plusieurs hôtes
- Plusieurs instances sur le même hôte
- Réplication système HANA scale-out multi-niveaux
- Environnement de réplication en cascade en mode réplication du système

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez le plug-in SnapCenter pour base de données SAP HANA dans la liste déroulante, puis cliquez sur **Ressources**.
2. Dans la page Ressources, cliquez sur **Ajouter une base de données SAP HANA**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type de ressource	Entrez le type de ressource. Les types de ressources sont conteneur unique, conteneur de base de données mutualisé (MDC) et volume non data.
Nom du système HANA	Entrez le nom descriptif du système SAP HANA. Cette option n'est disponible que si vous avez sélectionné des types de ressources conteneur unique ou MDC.

Pour ce champ...	Procédez comme ça...
SID	Saisissez l'ID système (SID). Le système SAP HANA installé est identifié par un SID unique.
Hôte de plug-in	Sélectionnez l'hôte du plug-in.
Clés de stockage sécurisé HDB	Entrez la clé pour vous connecter au système SAP HANA.  La clé contient les informations de connexion à la base de données.  Pour la réplication système SAP HANA, la clé utilisateur secondaire n'est pas validée. Ceci sera utilisé pendant le basculement.
Utilisateur HDBSQL	Entrez le nom d'utilisateur pour lequel la clé de stockage sécurisée de l'utilisateur HDB est configurée. Pour Windows, il est obligatoire que l'utilisateur HDBSQL OS soit l'utilisateur SYSTÈME. Par conséquent, vous devez configurer la clé de stockage sécurisée de l'utilisateur HDB pour l'utilisateur SYSTÈME.

4. Dans la page Entitetur Storage Footprint, sélectionnez un système de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Save**.

Facultatif : vous pouvez cliquer sur l'icône \*  pour ajouter d'autres volumes, LUN et qtrees à partir d'autres systèmes de stockage.

5. Vérifiez le résumé, puis cliquez sur **Terminer**.

Les bases de données s'affichent avec des informations telles que le SID, l'hôte du plug-in, les groupes de ressources et les stratégies associés et l'état global

Si vous souhaitez donner aux utilisateurs l'accès aux ressources, vous devez affecter ces ressources aux utilisateurs. Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

["Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources"](#)

Après avoir ajouté les bases de données, vous pouvez modifier les détails de la base de données SAP HANA.

Vous ne pouvez pas modifier ce qui suit si des sauvegardes sont associées à la ressource SAP HANA :

- Conteneurs de base de données mutualisés (MDC) : SID ou hôte HDBSQL client (plug-in)
- Conteneur unique : SID ou hôte client HDBSQL (plug-in)
- Volume non-données : nom de la ressource, SID associé ou hôte du plug-in

## Créez des règles de sauvegarde pour les bases de données SAP HANA

Avant d'utiliser SnapCenter pour sauvegarder les ressources de base de données SAP HANA, vous devez créer une règle de sauvegarde pour la ressource ou le groupe de ressources à sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.

Pour en savoir plus, découvrez comment définir une stratégie de protection des données pour les bases de données SAP HANA.

- Vous devez vous préparer à la protection des données en effectuant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout de ressources.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir affecté des SVM aux volumes source et de destination.

En outre, vous pouvez spécifier des paramètres de réplication, de script et d'application dans la stratégie. Ces options vous permettent de gagner du temps lorsque vous souhaitez réutiliser la stratégie d'un autre groupe de ressources.

- Vérifiez les prérequis et les limites spécifiques de la synchronisation active SnapMirror. Pour plus d'informations, reportez-vous à "[Limites d'objet pour la synchronisation active SnapMirror](#)".

### Description de la tâche

- Réplication système SAP HANA
  - Vous pouvez protéger le système SAP HANA principal et toutes les opérations de protection des données peuvent être effectuées.
  - Vous pouvez protéger le système SAP HANA secondaire, mais les sauvegardes ne peuvent pas être créées.

Après le basculement, toutes les opérations de protection des données peuvent être effectuées lorsque le système SAP HANA secondaire devient le système SAP HANA principal.

Vous ne pouvez pas créer de sauvegarde pour le volume de données SAP HANA, mais SnapCenter continue à protéger les volumes non-data.

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.
  - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - Choisissez un type de stockage
  - Choisissez un type de sauvegarde :

Les fonctions que vous recherchez...	Procédez comme ça...
Créer une sauvegarde à l'aide de la technologie Snapshot	Sélectionnez <b>basé sur les instantanés</b> .
Effectuer un contrôle d'intégrité de la base de données	Sélectionnez <b>sauvegarde basée sur fichier</b> . Seuls les locataires actifs sont sauvegardés.

6. Dans la page instantané et réplication, effectuez les opérations suivantes :
  - Spécifiez le type d'horaire en sélectionnant **On Demand, Hourly, Daily, Weekly** ou **Monthly**.



Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais aussi d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

7. Dans la page instantané et réplication, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionnés dans la page Type de sauvegarde :



Les fonctions que vous recherchez...	Alors...
<p>Conserver un certain nombre d'instantanés</p>	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> <p> Dans le cas des sauvegardes basées sur des copies Snapshot, vous devez définir le nombre de rétention à 2 ou plus si vous prévoyez d'activer la réplication SnapVault. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> <p> Pour la réplication des systèmes SAP HANA, il est recommandé d'ajouter toutes les ressources du système SAP HANA dans un groupe de ressources unique. Cela permet de conserver le nombre adéquat de sauvegardes.</p> <p> Pour la réplication système SAP HANA, le total des snapshots pris sera égal au jeu de conservation défini pour le groupe de ressources. La suppression de l'instantané le plus ancien est basée sur le nœud sur lequel se trouve l'instantané le plus ancien.</p> <p> Par exemple, la conservation est définie sur 7 pour un groupe de ressources avec réplication système primaire SAP HANA et réplication système secondaire SAP HANA. Vous pouvez effectuer un maximum de 7 copies Snapshot à la fois, y compris la réplication système primaire SAP HANA et la réplication système secondaire SAP HANA.</p>

Les fonctions que vous recherchez...	Alors...
Conserver les instantanés pendant un certain nombre de jours	Sélectionnez <b>conserver les copies pour</b> , puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage des copies Snapshot principales	Sélectionnez la période de verrouillage des copies Snapshot, puis sélectionnez les jours, les mois ou les années.  La période de conservation SnapLock doit être inférieure à 100 ans.
Période de verrouillage des copies Snapshot secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.

8. Sélectionnez une étiquette Snapshot.

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

9. Pour les sauvegardes basées sur des copies Snapshot, dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes, ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
<p><b>Mettre à jour SnapMirror après avoir créé une copie Snapshot locale</b></p>	<p>Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).</p> <p>Cette option doit être activée pour la synchronisation active SnapMirror.</p> <p>Si la relation de protection dans ONTAP est de type miroir et coffre-fort et si vous sélectionnez uniquement cette option, le snapshot créé sur le primaire ne sera pas transféré vers la destination, mais sera répertorié dans la destination. Si cet instantané est sélectionné à partir de la destination pour effectuer une opération de restauration, le message d'erreur emplacement secondaire n'est pas disponible pour la sauvegarde voûtée/miroir sélectionnée s'affiche.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir "<a href="#">Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie</a>".</p>

Pour ce champ...	Procédez comme ça...
<b>Mettre à jour SnapVault après avoir créé une copie Snapshot locale</b>	<p>Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton <b>Actualiser</b> de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, voir <a href="#">"Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé"</a></p> <p>Voir <a href="#">"Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie"</a>.</p>
<b>Nombre de tentatives d'erreur</b>	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer des groupes de ressources et attacher des stratégies

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Description de la tâche

- Pour créer des sauvegardes de réplication du système SAP HANA, il est recommandé d'ajouter toutes les ressources du système SAP HANA dans un groupe de ressources. Cela garantit une sauvegarde transparente en mode basculement/retour arrière.

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- L'ajout de nouvelles bases de données sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec la synchronisation active SnapMirror n'est pas pris en charge.
- L'ajout de nouvelles bases de données à un groupe de ressources existant en mode de basculement de la synchronisation active SnapMirror n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement à l'état normal ou de retour arrière.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	<p>Entrez un nom pour le groupe de ressources.</p> <div style="display: flex; align-items: center;">  <p>Le nom du groupe de ressources ne doit pas dépasser 250 caractères.</p> </div>
Étiquettes	<p>Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.</p> <p>Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.</p>
Utilisez le format de nom personnalisé pour la copie Snapshot	<p>Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.</p> <p>Par exemple, clienttext_Resource group_policy_hostname ou Resource group_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.</p>

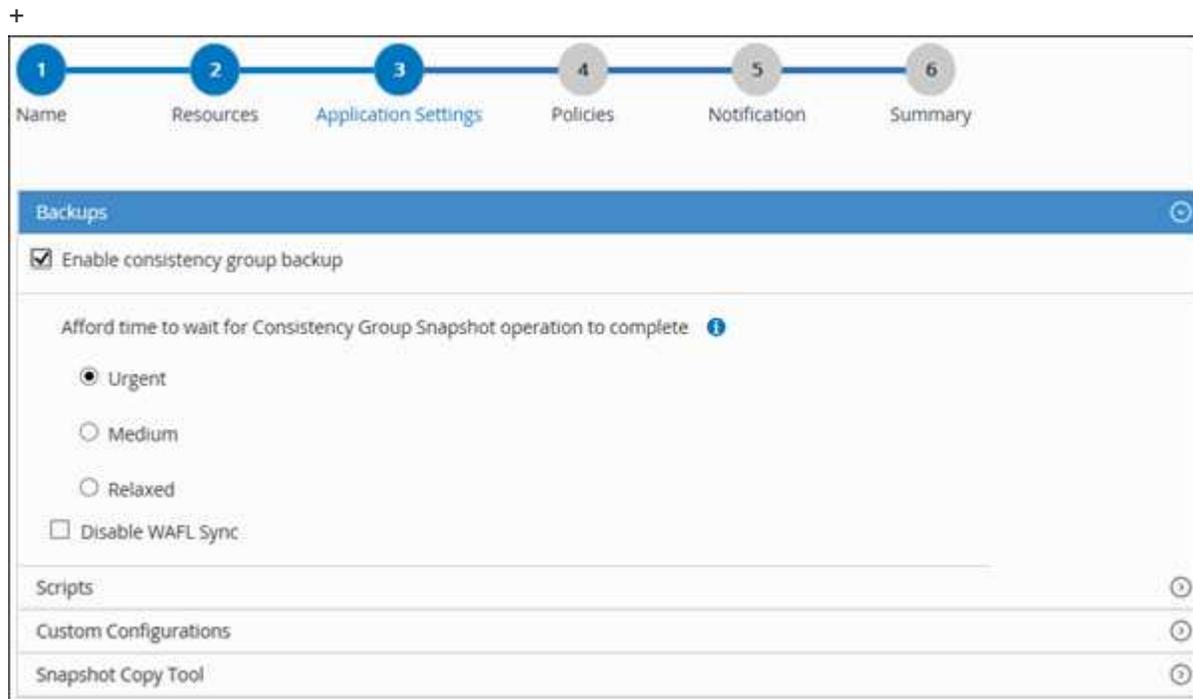
4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.

Cela aide à filtrer les informations affichées à l'écran.

5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page Paramètres de l'application, procédez comme suit :
  - a. Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde de groupe de cohérence et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Permet d'attendre la fin de l'opération Snapshot du groupe de cohérence	Sélectionnez <b>urgent</b> , <b>Moyen</b> ou <b>détendu</b> pour spécifier le temps d'attente pour l'exécution de l'opération Snapshot.  Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.



- Cliquez sur la flèche **scripts** et entrez les commandes pré et post pour les opérations quiesce, Snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- Cliquez sur la flèche **configurations personnalisées** et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.

Paramètre	Réglage	Description
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés.  Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.
ARCHIVE_LOG_EXT	extension_fichier	Spécifie la longueur d'extension du fichier journal d'archives.  Par exemple, si le journal d'archives est log_backup_0_0_0_0.1615185519429 et si la valeur file_extension est 5, l'extension du journal conserve 5 chiffres, soit 16151.
ARCHIVE_LOG_RÉCURSIVE_ARCH	(O/N)	Permet la gestion des journaux d'archivage dans les sous-répertoires.  Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.



Les paires de clé à valeur personnalisée sont prises en charge pour les systèmes du plug-in SAP HANA Linux et ne sont pas prises en charge pour la base de données SAP HANA enregistrée en tant que plug-in centralisé Windows.

c. Cliquez sur la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et placer le système de fichiers dans un état cohérent avant de créer un Snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .  Cette option ne s'applique pas au plug-in SnapCenter pour base de données SAP HANA.
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
Pour saisir la commande à exécuter sur l'hôte pour créer des copies Snapshot.	Sélectionnez <b>autre</b> , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.

7. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Les stratégies sont répertoriées dans la section Configuration des planifications pour les stratégies sélectionnées.

- b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.

Où, nom\_stratégie est le nom de la règle que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **programmes appliqués**.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Le serveur SMTP doit être configuré dans **Paramètres > Paramètres globaux**.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire des ressources SAP HANA sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la

fonction **Secondaryprotection** est activée.

- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

- 8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

- a. Sélectionnez le type de la règle de réplication.

 Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.
- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.

 Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.

 Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

- 1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de

stockage secondaire.

e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer une connexion au système de stockage et une certification à l'aide des applets de commande PowerShell pour la base de données SAP HANA

Vous devez créer une connexion SVM (Storage Virtual machine) et une identifiant d'identification avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner les bases de données SAP HANA.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

### Étapes

1. Lancez une session de connexion PowerShell à l'aide de la cmdlet `Open-SmConnection`.

```
PS C:\> Open-SmStorageConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-SmStorageConnection`.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande Add-SmCredential.

Cet exemple montre comment créer un nouvel identifiant nommé FinanceAdmin avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Ajoutez l'hôte de communication SAP HANA au serveur SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Installez le package et le plug-in SnapCenter pour base de données SAP HANA sur l'hôte.

Pour Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

Pour Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. Définissez le chemin d'accès au client HDBSQL.

Pour Windows :

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

Pour Linux :

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarde des bases de données SAP HANA

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Avant de commencer

- Vous devez avoir créé une stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « `napmirror All` ». Toutefois, si vous utilisez le rôle « `vsadmin` », le privilège « `napmirror all` » n'est pas requis.
- Pour l'opération de sauvegarde basée sur des copies Snapshot, vérifiez que toutes les bases de données des locataires sont valides et actives.
- Pour créer des sauvegardes de réplication du système SAP HANA, il est recommandé d'ajouter toutes les ressources du système SAP HANA dans un groupe de ressources. Cela garantit une sauvegarde transparente en mode basculement/retour arrière.

["Créer des groupes de ressources et attacher des stratégies"](#).

["Sauvegarder les groupes de ressources"](#)

- Si vous souhaitez créer une sauvegarde basée sur des fichiers alors qu'une ou plusieurs bases de données de tenant sont en panne, définissez le paramètre `ALLOW_FILE_BASED_BACKUP_IFINA_TENANTS_PRESIDENT` sur **YES** dans le fichier de propriétés HANA à l'aide de `Set-SmConfigSettings` applet de commande.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également vous référer au ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#)

- Pour les commandes PRE et post pour les opérations quiesce, Snapshot et unquiesce, vous devez vérifier que les commandes existent dans la liste de commandes disponible sur l'hôte plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
  - Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Sélectionnez \* , puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Sélectionnez la ressource à sauvegarder.
4. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page Paramètres de l'application, procédez comme suit :

- Sélectionnez la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde du groupe de cohérence, si nécessaire, et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Temps d'attente avant la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , ou <b>Moyen</b> , ou <b>détendu</b> pour spécifier le temps d'attente pour la fin de l'opération Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

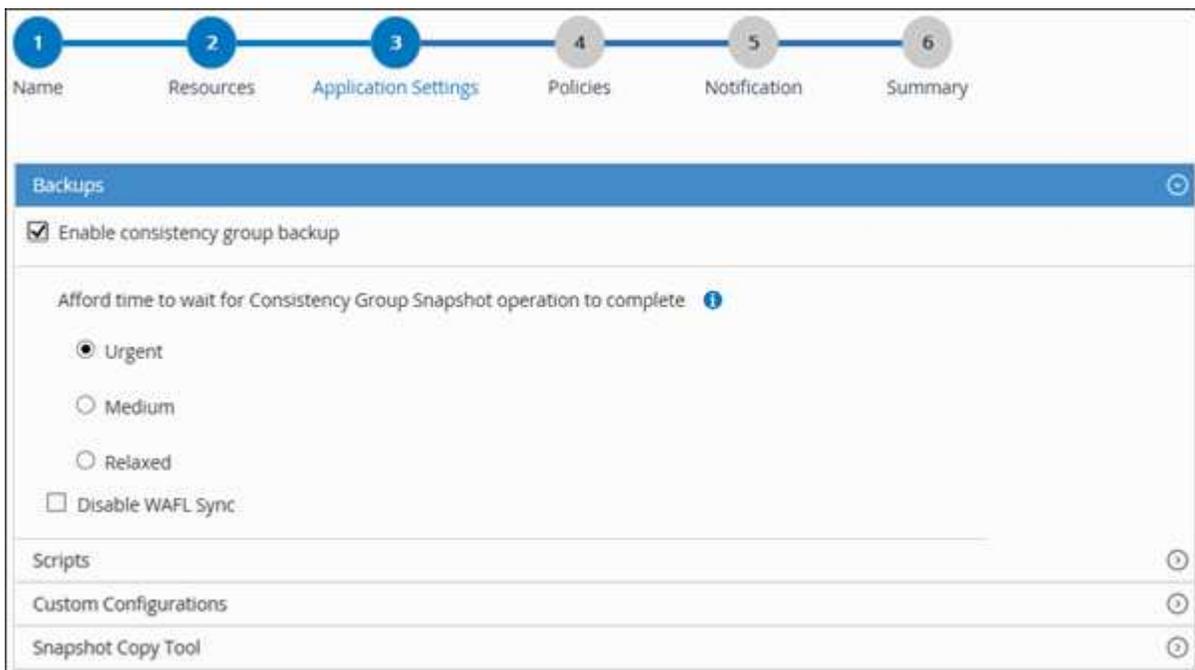
- Sélectionnez la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce.

Vous pouvez également exécuter des pré-commandes avant de quitter l'opération de sauvegarde. Des préscripts et des postscripts sont exécutés sur le serveur SnapCenter.

- Sélectionnez la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- Sélectionner la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows afin de mettre le système de fichiers dans un état cohérent, puis de créer un Snapshot	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
Pour saisir la commande permettant de créer un Snapshot	Sélectionnez <b>autre</b> , puis entrez la commande pour créer un instantané.



6. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Sélectionnez \* \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres > Paramètres globaux**.

8. Passez en revue le résumé, puis sélectionnez **Terminer**.

La page topologie des ressources s'affiche.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

Pour plus d'informations, voir : ["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer.

Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, la commande `do_start method` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante :  
`Java -jar -Xmx8192M -Xms4096M`

## Applets de commande PowerShell

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Ajoutez des ressources à l'aide de l'applet de commande `Add-SmResources`.

Cet exemple montre comment ajouter une base de données SAP HANA de type `SingleContainer` :

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary
"}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

Cet exemple montre comment ajouter une base de données SAP HANA de type MultipleContainers :

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

Cet exemple montre comment créer une ressource de volume autre que de données :

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

### 3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.

Dans cet exemple, une règle de sauvegarde est créée pour une sauvegarde basée sur des copies Snapshot :

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

Cet exemple crée une stratégie de sauvegarde pour une sauvegarde en mode fichier :

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

### 4. Protégez la ressource ou ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.

Cet exemple protège une ressource de conteneur unique :

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Cet exemple protège plusieurs conteneurs :

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

Cet exemple crée un nouveau groupe de ressources avec la stratégie et les ressources spécifiées :

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sscore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sscore.test.com";"Uid"="MDC\SID"})
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

Dans cet exemple, nous allons créer un groupe de ressources sans volume de données :

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

##### 5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet New-SmBackup.

Cet exemple montre comment sauvegarder un groupe de ressources :

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

Cet exemple sauvegarde une ressource protégée :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Surveillez l'état du travail (en cours d'exécution, terminé ou en échec) à l'aide de l'applet de commande `Get-smJobSummaryReport`.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Surveillez les détails de la tâche de sauvegarde comme ID de sauvegarde, nom de sauvegarde pour effectuer une opération de restauration ou de clonage à l'aide de l'applet de commande `Get-SmBackupReport`.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects : {DB1}
FailedObjects : {}
IsScheduled : False
HasMetadata : False
SmBackupId : 269
SmJobId : 2361
StartDateTime : 10/4/2016 11:20:45 PM
EndDateTime : 10/4/2016 11:21:32 PM
Duration : 00:00:46.2536470
CreatedDateTime : 10/4/2016 11:21:09 PM
Status : Completed
ProtectionGroupName : Verify_ASUP_Message_windows
SmProtectionGroupId : 211
PolicyName : test2
SmPolicyId : 20
BackupName : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus : NotVerified
VerificationStatuses :
SmJobError :
BackupType : SCC_BACKUP
CatalogingStatus : NotApplicable
CatalogingStatuses :
ReportDataCreatedDateTime :
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarder les groupes de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

### Description de la tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en sélectionnant , puis en  sélectionnant la balise. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.
5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Surveillez les opérations de sauvegarde des bases de données SAP HANA

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours

-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Surveillez les opérations de protection des données des bases de données SAP HANA dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

## Annuler les opérations de sauvegarde pour SAP HANA

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

## Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

## Étapes

1. Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>a. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>b. Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li></ol>
Volet activité	<ol style="list-style-type: none"><li>a. Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li><li>b. Sélectionner l'opération.</li><li>c. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li></ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Affichez les sauvegardes et les clones des bases de données SAP HANA sur la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire.

### Description de la tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).



affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.

-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.



Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

Si vous utilisez une relation secondaire comme SnapMirror actif Sync (initialement commercialisé sous la forme SnapMirror Business Continuity [SM-BC]), les icônes supplémentaires suivantes s'affichent :

-  Le site de réplica est en cours.
-  Le site de réplica est en panne.
-  La relation miroir ou coffre-fort secondaire n'a pas été rétablie.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la **carte Résumé** pour afficher un résumé du nombre de sauvegardes et de clones disponibles sur le stockage primaire et secondaire.

La section **Summary Card** affiche le nombre total de sauvegardes basées sur des fichiers, de sauvegardes basées sur des copies Snapshot et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration

SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Pour la synchronisation active SnapMirror, cliquez sur le bouton **Refresh** pour actualiser l'inventaire des sauvegardes SnapCenter en interrogeant ONTAP sur les sites principaux et de réplica. Une planification hebdomadaire effectue également cette activité pour toutes les bases de données contenant une relation de synchronisation active SnapMirror.

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations SnapMirror miroir asynchrone ou MirrorVault asynchrone vers la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir de ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.
  - Après le basculement, une sauvegarde doit être créée afin que SnapCenter puisse prendre connaissance du basculement. Vous ne pouvez cliquer sur **Rafraîchir** qu'après la création d'une sauvegarde.
5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

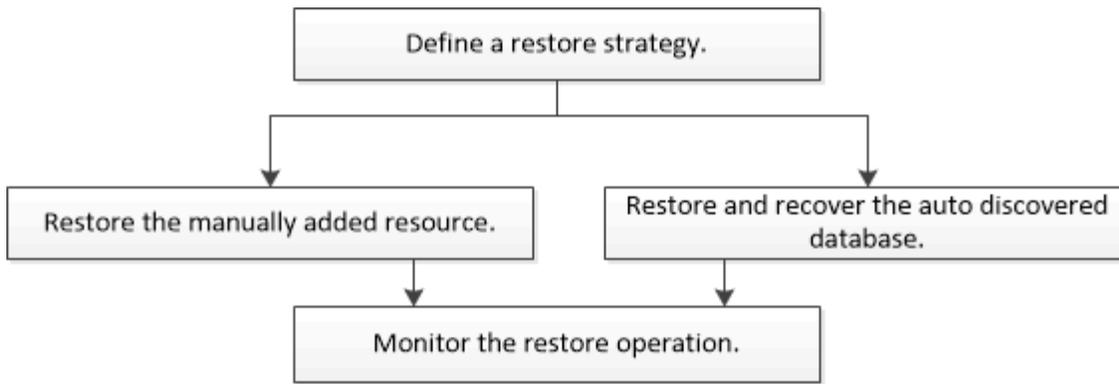
7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur .
8. Si vous souhaitez diviser un clone, sélectionnez-le dans le tableau, puis cliquez sur .

## Restauration des bases de données SAP HANA

### Restaurer le flux de travail

Le workflow de restauration et de reprise comprend la planification, la réalisation des opérations de restauration et la surveillance des opérations.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
  - Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées depuis SnapCenter.
- Après la mise à niveau vers SnapCenter 4.3, les sauvegardes effectuées dans SnapCenter 4.2 peuvent être restaurées, mais ne peuvent pas être restaurées. Vous devez utiliser des scripts de restauration HANA Studio ou HANA externes à SnapCenter pour restaurer les sauvegardes prises dans SnapCenter 4.2.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur



Backup Name	End Date
rg1_scipr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page objectif de restauration, sélectionnez **ressource complète** ou **niveau de fichier**.

- a. Si vous sélectionnez **Complete Resource**, tous les volumes de données configurés de la base de données SAP HANA sont restaurés.

Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

- b. Si vous sélectionnez **File Level**, vous pouvez sélectionner **All** ou sélectionner des volumes ou des qtrees spécifiques, puis entrer le chemin d'accès associé à ces volumes ou qtrees, séparés par des virgules
  - Vous pouvez sélectionner plusieurs volumes et qtrees.

- Si le type de ressource est LUN, l'ensemble de la LUN est restauré.

Vous pouvez sélectionner plusieurs LUN.



Si vous sélectionnez **tous**, tous les fichiers des volumes, qtrees ou LUN sont restaurés.

7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

### 3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurez et récupérez une sauvegarde de base de données découverte automatiquement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.

- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
  - Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées depuis SnapCenter.
- Après la mise à niveau vers SnapCenter 4.3, les sauvegardes effectuées dans SnapCenter 4.2 peuvent être restaurées, mais ne peuvent pas être restaurées. Vous devez utiliser des scripts de restauration HANA Studio ou HANA externes à SnapCenter pour restaurer les sauvegardes prises dans SnapCenter 4.2.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).

5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur  .

Primary Backup(s)	
search 	
Backup Name	End Date
rg1_scispr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. Sur la page étendue de la restauration, sélectionnez **ressource complète** pour restaurer les volumes de données configurés de la base de données SAP HANA.



Vous pouvez sélectionner **Complete Resource** (avec ou sans **Volume Revert**) ou **tenant Database**.

L'opération de récupération n'est pas prise en charge par le serveur SnapCenter pour plusieurs locataires lorsque l'utilisateur sélectionne l'option **base de données locataire** ou **Restauration complète**. Vous devez utiliser HANA Studio ou le script python HANA pour effectuer l'opération de restauration.

- a. Sélectionnez **Volume Revert** si vous souhaitez restaurer l'intégralité du volume.

Cette option est disponible pour les sauvegardes prises en charge dans SnapCenter 4.3 dans les environnements NFS.

Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée. Ceci est applicable lorsque l'option **Complete Resource** avec **Volume Revert** est sélectionnée pour la restauration.

- b. Sélectionnez **base de données de tenant**.

Cette option n'est disponible que pour les ressources MDC.

Assurez-vous d'arrêter la base de données des locataires avant d'effectuer l'opération de restauration.

Si vous sélectionnez l'option **tenant Database**, vous devez utiliser HANA Studio ou utiliser des scripts de reprise HANA externes à SnapCenter pour effectuer l'opération de restauration.

7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :

<b>Si...</b>	<b>Procédez comme ça...</b>
Vous souhaitez effectuer une restauration aussi proche que possible de l'heure actuelle	<p>Sélectionnez <b>recupérer à l'état le plus récent</b>.</p> <p>Pour les ressources de conteneur unique, spécifiez un ou plusieurs emplacements de sauvegarde de journaux et de catalogues.</p> <p>Pour les ressources MDC (conteneur de base de données mutualisée), spécifiez un ou plusieurs emplacements de sauvegarde du journal et l'emplacement du catalogue de sauvegarde.</p> <p>Pour les ressources MDC, le chemin doit contenir à la fois des journaux de base de données système et des bases de données de tenant.</p>

Si...	Procédez comme ça...
<p data-bbox="183 159 808 226">Vous souhaitez effectuer une restauration au point dans le temps spécifié</p>	<p data-bbox="841 159 1487 191">Sélectionnez <b>recupérer à un point dans le temps</b>.</p> <p data-bbox="854 226 1273 258">a. Sélectionnez le fuseau horaire.</p> <p data-bbox="889 294 1463 359">Le fuseau horaire du navigateur est utilisé par défaut.</p> <p data-bbox="889 394 1487 459">Le fuseau horaire sélectionné et l'heure d'entrée sont convertis en GMT absolu.</p> <p data-bbox="854 495 1455 625">b. Entrez la date et l'heure. Par exemple, l'hôte Linux HANA est situé à Sunnyvale, CA et l'utilisateur à Raleigh, NC rétablit les journaux au SnapCenter.</p> <p data-bbox="889 661 1487 863">La différence de temps entre ces deux emplacements est de 3 heures et, puisque l'utilisateur s'est connecté à Raleigh, NC, le fuseau horaire par défaut du navigateur qui sera sélectionné dans l'interface utilisateur est GMT-04:00.</p> <p data-bbox="889 898 1487 1066">Si l'utilisateur souhaite effectuer une restauration à 5 h, Sunnyvale, CA, l'utilisateur doit définir le fuseau horaire du navigateur sur le fuseau horaire de l'hôte HANA Linux, GMT-07:00 et préciser la date et l'heure à 5 h 00</p> <p data-bbox="889 1102 1422 1199">Pour les ressources de conteneur unique, spécifiez un ou plusieurs emplacements de sauvegarde de journaux et de catalogues.</p> <p data-bbox="889 1234 1422 1367">Pour les ressources MDC, spécifiez un ou plusieurs emplacements de sauvegarde du journal et l'emplacement du catalogue de sauvegarde.</p> <p data-bbox="889 1402 1471 1535">Pour les ressources MDC, le chemin doit contenir à la fois des journaux de base de données système et des bases de données de tenant.</p>
<p data-bbox="183 1602 716 1667">Veulent effectuer une restauration vers une sauvegarde de données spécifique</p>	<p data-bbox="841 1602 1398 1667">Sélectionnez <b>recupérer à la sauvegarde de données spécifiée</b>.</p>
<p data-bbox="183 1719 399 1751">Ne pas récupérer</p>	<p data-bbox="841 1719 1487 1816">Sélectionnez <b>pas de récupération</b>. Vous devez effectuer l'opération de restauration manuellement à partir du studio HANA.</p>

Vous ne pouvez restaurer que les sauvegardes effectuées après la mise à niveau vers SnapCenter 4.3, à condition que l'hôte et le plug-in soient mis à niveau vers SnapCenter 4.3, et que les sauvegardes

sélectionnées pour la restauration soient effectuées après la conversion ou la découverte automatique de la ressource.

8. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.
12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Restaurer des ressources à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de ressources inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
-----		
1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet `Restore-SmBackup`.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveillez les opérations de restauration des bases de données SAP HANA

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours

-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

# Clonage des sauvegardes de ressources SAP HANA

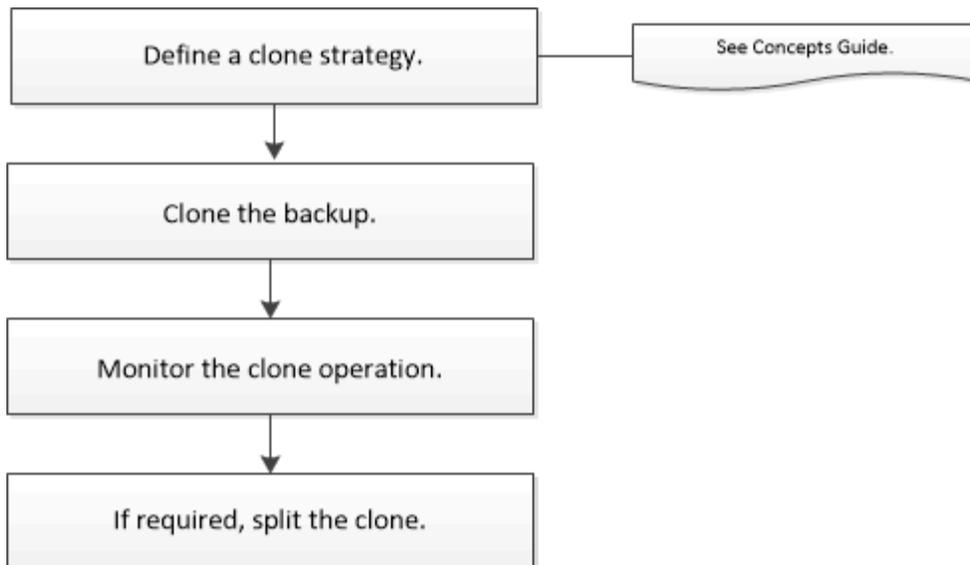
## Workflow de clonage

Le workflow de clonage inclut la réalisation de l'opération de clonage et le contrôle de l'opération.

### Description de la tâche

- Vous pouvez cloner sur le serveur SAP HANA source.
- Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :
  - Tester les fonctionnalités à implémenter à l'aide de la structure de ressources actuelle et du contenu pendant les cycles de développement d'applications
  - Pour les outils d'extraction et de manipulation de données lors du remplissage d'entrepôts de données
  - Pour récupérer les données qui ont été supprimées ou modifiées par erreur

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

## Cloner une sauvegarde de base de données SAP HANA

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde. Vous pouvez cloner à partir d'une sauvegarde principale ou secondaire.

### Avant de commencer

- Vous devriez avoir sauvegardé les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Vous ne pouvez pas cloner des sauvegardes basées sur des fichiers.
- Le serveur clone cible doit avoir le même SID d'instance SAP HANA que celui fourni dans le champ SID de clone cible.
- Pour les commandes pré-clone ou post-clone, vérifiez si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
  - Pour Windows : `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
  - Pour Linux : `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Pour plus d'informations sur les limites des opérations de fractionnement de clonage, reportez-vous à la section "[Guide de gestion du stockage logique ONTAP 9](#)".
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources s'affichent avec des informations telles que le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

3. Sélectionnez la ressource ou le groupe de ressources.

Vous devez sélectionner une ressource si vous sélectionnez un groupe de ressources.

La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Hôte de plug-in	Sélectionnez l'hôte sur lequel le clone doit être monté et le plug-in est installé.
SID de clone cible	Entrez l'ID d'instance SAP HANA à cloner à partir des sauvegardes existantes.
Adresse IP d'exportation NFS	Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.
Initiateur iSCSI	Entrez le nom de l'initiateur iSCSI de l'hôte sur lequel les LUN sont exportées. Cette option n'est disponible que si vous avez sélectionné le type de ressource LUN.
Protocole	Indiquez le protocole de LUN. Cette option n'est disponible que si vous avez sélectionné le type de ressource LUN.

Si la ressource sélectionnée est une LUN et que vous effectuez un clonage à partir d'une sauvegarde secondaire, les volumes de destination sont répertoriés. Une source unique peut avoir plusieurs volumes de destination.



Avant le clonage, vous devez vous assurer que l'initiateur iSCSI ou le FCP est présent et configuré et connecté aux hôtes secondaires.

7. Dans la page scripts, effectuez les opérations suivantes :



Les scripts sont exécutés sur l'hôte du plug-in.

- a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
  - Commande de pré-clonage : permet de supprimer les bases de données existantes portant le même nom
  - Commande post-clone : vérifiez une base de données ou démarrez une base de données.
- b. Entrez la commande mount pour monter un système de fichiers sur un hôte.

Commande mount pour un volume ou un qtree sur une machine Linux :

Exemple pour NFS : `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Récupérez les sauvegardes pour effectuer l'opération de clonage à l'aide de l'applet de commande Get-SmBackup.

Cet exemple montre que deux sauvegardes sont disponibles pour le clonage :

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. Lancez une opération de clonage à partir d'une sauvegarde existante et spécifiez les adresses IP d'exportation NFS sur lesquelles les volumes clonés sont exportés.

Cet exemple montre que la sauvegarde à cloner possède une adresse NFSExportIPS de 10.232.206.169 :

```
New-SmClone -AppPluginCode hana -BackupName
scscore1_sscore_test_com_hana_H73_scscore1_06-07-
2017_02.54.29.3817 -Resources
@{"Host"="scscore1.sscore.test.com";"Uid"="H73"} -CloneToInstance
shivsc4.sscore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data'
-preclonecreatecommands '/home/scripts/scpre_clone.sh'
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```



Si NFSExportIPS n'est pas spécifié, la valeur par défaut est exportée vers l'hôte cible du clone.

4. Vérifiez que les sauvegardes ont été correctement clonées à l'aide de l'applet de commande Get-SmCloneReport pour afficher les détails du travail clone.

Vous pouvez afficher des informations telles que l'ID de clone, la date et l'heure de début, la date et l'heure de fin.

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError :

```

## Surveillez les opérations de clonage de bases de données SAP HANA

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.

3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur \* \* .

5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

#### Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

## Supprimez ou séparez les clones de base de données SAP HANA après la mise à niveau de SnapCenter

Après la mise à niveau vers SnapCenter 4.3, vous ne verrez plus les clones. Vous pouvez supprimer le clone ou séparer les clones de la page topologie de la ressource à partir de laquelle les clones ont été créés.

#### Description de la tâche

Si vous souhaitez localiser l'empreinte de stockage des clones masqués, exécutez la commande suivante :  
`Get-SmClone -ListStorageFootprint`

#### Étapes

1. Supprimez les sauvegardes des ressources clonées à l'aide de la cmdlet `remove-smbbackup`.
2. Supprimez le groupe de ressources des ressources clonées à l'aide de la cmdlet `remove-smresregroupement`.
3. Supprimez la protection de la ressource clonée à l'aide de l'applet de commande `remove-smprotectResource`.
4. Sélectionnez la ressource parente dans la page Ressources.

La page topologie de ressources s'affiche.

5. Dans la vue Manage copies (gérer les copies), sélectionnez les clones dans les systèmes de stockage principal ou secondaire (en miroir ou répliqué).

6. Sélectionnez les clones, puis cliquez sur  pour supprimer les clones ou sur  pour les séparer.

7. Cliquez sur **OK**.

# Protection des bases de données Oracle

## Présentation du plug-in SnapCenter pour la base de données Oracle

### Quelles sont les possibilités possibles grâce au plug-in pour Oracle Database

Le plug-in SnapCenter pour base de données Oracle est un composant côté hôte du logiciel NetApp SnapCenter qui permet de gérer la protection des données des bases de données Oracle avec cohérence applicative.

Le plug-in pour Oracle Database automatise la sauvegarde, le catalogage et le décatalogage grâce à Oracle Recovery Manager (RMAN), la vérification, le montage, le démontage, la restauration, Récupération et clonage de bases de données Oracle dans votre environnement SnapCenter. Le plug-in pour base de données Oracle installe le plug-in SnapCenter pour UNIX afin d'effectuer toutes les opérations de protection des données.

Vous pouvez utiliser le plug-in pour Oracle Database afin de gérer les sauvegardes de bases de données Oracle exécutant des applications SAP. Cependant, l'intégration de SAP BR\*Tools n'est pas prise en charge.

- Sauvegardez les fichiers de données, les fichiers de contrôle et les fichiers journaux d'archivage.

La sauvegarde n'est prise en charge qu'au niveau de la base de données du conteneur (CDB).

- Restauration et récupération des bases de données, CDBS et des bases de données enfichables (PDB).

La récupération incomplète des BDD n'est pas prise en charge.

- Créer des clones de bases de données de production à un point dans le temps.

Le clonage n'est pris en charge qu'au niveau CDB.

- Vérifier immédiatement les sauvegardes.
- Monter et démonter les sauvegardes de données et de journaux pour une opération de restauration.
- Planifiez les opérations de sauvegarde et de vérification.
- Contrôle de toutes les opérations.
- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.
- Automatisation de la sauvegarde, de la restauration et de la récupération respectueuses des applications, de la vérification, du montage et Démontez et clonez des opérations de base de données Oracle dans votre environnement SnapCenter
- Prend en charge les bases de données Oracle pour SAP, mais l'intégration de SAP BR\*Tools n'est pas fournie

### Fonctionnalités du plug-in pour Oracle Database

Le plug-in pour base de données Oracle s'intègre à la base de données Oracle sur l'hôte Linux ou AIX et aux technologies NetApp sur le système de stockage.

- Interface utilisateur graphique unifiée

L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- Administration centralisée automatisée

Vous pouvez planifier des opérations de sauvegarde et de clonage, configurer la conservation des sauvegardes à l'aide de règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- La technologie Snapshot de NetApp sans interruption

SnapCenter utilise la technologie Snapshot de NetApp avec le plug-in pour Oracle Database et le plug-in pour UNIX pour sauvegarder des bases de données. Les copies Snapshot consomment un espace de stockage minimal.

Le plug-in pour base de données Oracle offre également les avantages suivants :

- Prise en charge de la sauvegarde, de la restauration, du clonage, du montage, du démontage, et de vérification des workflows
- Découverte automatique des bases de données Oracle configurées sur l'hôte
- Prise en charge du catalogage et du non-catalogage à l'aide d'Oracle Recovery Manager (RMAN)
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Prise en charge de la gestion des journaux d'archivage (ALM) pour les opérations de restauration et de clonage
- Création de copies instantanées et compactes de bases de données de production à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonction Groupe de cohérence de ONTAP dans le cadre de la création de sauvegardes dans les environnements SAN et ASM
- Vérification automatisée et sans interruption des sauvegardes
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de base de données

Dans une seule opération, les snapshots sont consolidés lorsque les bases de données d'un hôte unique partagent le même volume.

- Prise en charge des infrastructures physiques et virtualisées
- Prise en charge de NFS, iSCSI, Fibre Channel (FC), RDM, VMDK over NFS et VMFS et ASM sur NFS, SAN, RDM et VMDK
- Prise en charge de la fonctionnalité SLM (Selective LUN Map) de ONTAP

Activé par défaut, la fonction SLM détecte régulièrement les LUN qui ne disposent pas de chemins optimisés et les corrige. Vous pouvez configurer SLM en modifiant les paramètres dans le fichier `scu.properties` situé dans `/var/opt/snapcenter/scu/etc`

- Vous pouvez le désactiver en définissant la valeur DU paramètre `ENABLE_LUNPATH_MONITORING` sur `FALSE`.
- Vous pouvez spécifier la fréquence de correction automatique des chemins de LUN en attribuant la valeur (en heures) au paramètre `LUNPATH_MONITORING_INTERVAL`. Pour plus d'informations sur SLM, reportez-vous au "[Section Administration du SAN ONTAP 9](#)".

- Prise en charge de NVMe (non-volatile Memory Express) sur Linux

- Le util NVMe doit être installé sur l'hôte.

Vous devez installer NVMe util sur cloner ou monter sur un autre hôte.

- Sauvegarde, restauration, clone, montage, démontage, les opérations de catalogue, d'annulation de catalogue et de vérification sont prises en charge sur le matériel NVMe, à l'exception des environnements virtualisés tels que RDM.

Les opérations ci-dessus sont prises en charge sur les périphériques sans partitions ou avec une seule partition.



Vous pouvez configurer la solution de chemins d'accès multiples pour les périphériques NVMe en définissant l'option de chemins d'accès multiples natifs dans le noyau. Les chemins d'accès multiples de Device Mapper (DM) ne sont pas pris en charge.

- Sauvegarde, restauration, clone, montage, démontage, les workflows de catalogue, d'annulation de catalogue et de vérification sont pris en charge sur NVMe via TCP/IP.
- Sauvegarde, restauration, clone, montage, démontage, les workflows de catalogue, d'annulation de catalogue et de vérification sont pris en charge sur la disposition VMDK créée sur NVMe over TCP/IP.

- Prise en charge de la synchronisation active SnapMirror (initialement lancée sous la forme de SnapMirror Business Continuity [SM-BC]) qui assure la continuité des services de l'entreprise même en cas de défaillance complète du site, permettant ainsi aux applications de basculer en toute transparence au moyen d'une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

- Prise en charge des utilisateurs non par défaut au lieu d'oracle et de Grid.

Pour prendre en charge les utilisateurs non par défaut, vous devez définir les utilisateurs non par défaut en modifiant les valeurs des paramètres dans le fichier **`sco.properties`** situé dans *file* `/var/opt/snapcenter/sco/etc/`.

Les valeurs par défaut des paramètres sont définies comme oracle et Grid.

- `DB_USER=oracle`
- `DB_GROUP=oinstall`
- `GI_USER=grille`
- `GI_GROUP=oinstall`

## Types de stockage pris en charge par le plug-in pour Oracle Database

SnapCenter prend en charge un large éventail de types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier la prise en charge de votre type de stockage avant d'installer SnapCenter Plug-ins Package pour Linux ou SnapCenter Plug-ins Package pour AIX.

SnapCenter ne prend pas en charge le provisionnement du stockage pour Linux et AIX.

### Types de stockage pris en charge sous Linux

Le tableau suivant répertorie les types de stockage pris en charge par Linux.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"><li>• LUN connectés via FC</li><li>• LUN connectées à l'iSCSI</li><li>• Volumes connectés par NFS</li><li>• FC-NVMe</li><li>• NVMe/TCP</li></ul>

Machine	Type de stockage
VMware ESXi	<ul style="list-style-type: none"> <li>• L'exécution des LUN RDM connectés par un HBA FC ou iSCSI ESXi peut prendre du temps car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte.</li> </ul> <p>Vous pouvez modifier le fichier <b>LinuxConfig.pm</b> situé à  <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> à 1 pour analyser uniquement les HBA répertoriés dans les NOMS de PILOTE HBA.</p> <ul style="list-style-type: none"> <li>• LUN iSCSI connectés directement au système invité par l'initiateur iSCSI</li> <li>• VMDK sur des datastores NFS</li> <li>• VMDK sur VMFS créés sur NVMe/TCP</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>RAC est pris en charge sur ESX 8.0U2 qui prend en charge le VMDK partagé</p> </div> <ul style="list-style-type: none"> <li>• Volumes NFS connectés directement au système invité</li> <li>• Datastores vVol sur NFS et SAN</li> </ul> <p>Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>

### Types de stockage pris en charge sous AIX

Le tableau suivant répertorie les types de stockage pris en charge sous AIX.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"> <li>• LUN connectés via FC et iSCSI.</li> </ul> <p>Dans un environnement SAN, les systèmes de fichiers ASM, LVM et SAN sont pris en charge.</p> <div style="display: flex; align-items: center; margin: 10px 0;">  <p>NFS sous AIX et le système de fichiers n'est pas pris en charge.</p> </div> <ul style="list-style-type: none"> <li>• Système de fichiers journalisé amélioré (JFS2)</li> </ul> <p>Prend en charge la connexion en ligne sur les systèmes de fichiers SAN et la disposition LVM.</p>

Le "[Matrice d'interopérabilité NetApp](#)" contient les dernières informations sur les versions prises en charge.

## Préparation des systèmes de stockage pour la réplication SnapMirror et SnapVault pour le plug-in pour Oracle

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Privilèges ONTAP minimum requis pour le plug-in pour Oracle

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter

utilisés pour la protection des données.

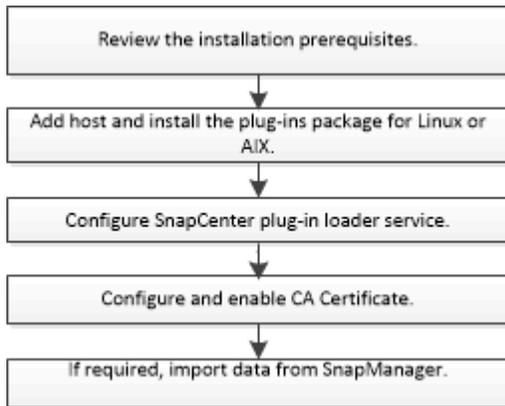
- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - l'attribut de lun affiche
  - la création de lun
  - suppression de la lun
  - géométrie de lun
  - lun igroup add
  - créez un groupe initiateur lun
  - suppression du groupe initiateur lun
  - renommer la lun igroup
  - affichage de la lun igroup
  - lun mapping des nœuds supplémentaires
  - création d'un mappage de lun
  - suppression du mappage de lun
  - mappage de lun supprimer-rapports-nœuds
  - les mappages de lun s'affichent
  - modification de lun
  - déplacement des lun dans le volume
  - lun hors ligne
  - lun en ligne
  - suppression de la réservation persistante de lun
  - redimensionner la lun
  - série de lun
  - affichage de la lun
  - ajout de règle snapmirror
  - règle de modification de snapmirror
  - règle de suppression de snapmirror
  - affichage des règles snapmirror
  - restauration snapmirror
  - montrer snapmirror
  - historique des données du mode snapmirror
  - mise à jour snapmirror
  - snapmirror update-ls-set

- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes
- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- un vserver
- cifs vserver
- vserver cifs shadowcopy show
- vserver show
- interface réseau
- interface réseau affiche
- montrer MetroCluster

# Installation du plug-in SnapCenter pour la base de données Oracle

## Workflow d'installation du plug-in SnapCenter pour Oracle Database

Vous devez installer et configurer le plug-in SnapCenter pour la base de données Oracle si vous souhaitez protéger les bases de données Oracle.



## Conditions préalables pour l'ajout d'hôtes et l'installation de Plug-ins Package pour Linux ou AIX

Avant d'ajouter un hôte et d'installer les packages de plug-ins, vous devez respecter toutes les exigences.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.

Le plug-in SnapCenter pour base de données Oracle peut être installé par un utilisateur non root. Cependant, vous devez configurer les privilèges sudo pour que l'utilisateur non-root installe et démarre le processus de plug-in. Après l'installation du plug-in, les processus s'exécutent en tant qu'utilisateur non-racine efficace.

- Si vous installez le module de plug-ins SnapCenter pour AIX sur un hôte AIX, vous devez avoir résolu manuellement les liens symboliques au niveau du répertoire.

Le module de plug-ins SnapCenter pour AIX résout automatiquement le lien symbolique au niveau du fichier, mais pas les liens symboliques au niveau du répertoire pour obtenir le chemin absolu JAVA\_HOME.

- Créez des informations d'identification avec le mode d'authentification sous Linux ou AIX pour l'utilisateur d'installation.
- Vous devez avoir installé Java 11 sur votre hôte Linux ou AIX.
  - Java d'Oracle et OpenJDK est pris en charge pour Linux
  - IBM Java pour AIX. Vous pouvez le télécharger à partir de "[Téléchargements IBM Semeru RunTimes](#)"



Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux.

- Pour les bases de données Oracle qui s'exécutent sur un hôte Linux ou AIX, installez le plug-in SnapCenter pour base de données Oracle et le plug-in SnapCenter pour UNIX.



Vous pouvez utiliser le plug-in pour Oracle Database afin de gérer également les bases de données Oracle pour SAP. Cependant, l'intégration de SAP BR\*Tools n'est pas prise en charge.

- Si vous utilisez Oracle Database 11.2.0.3 ou une version ultérieure, vous devez installer le correctif Oracle 13366202.



Le mappage UUID dans le fichier `/etc/fstab` n'est pas pris en charge par SnapCenter.

- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

### Configuration requise pour l'hôte Linux

Vous devez vous assurer que l'hôte répond à la configuration requise avant d'installer le module de plug-ins SnapCenter pour Linux.

Élément	De formation
<p>Systemes d'exploitation</p>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• Oracle Linux</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Si vous utilisez une base de données Oracle sur LVM sous Oracle Linux ou Red Hat Enterprise Linux 6.6 ou 7.0, vous devez installer la dernière version de Logical Volume Manager (LVM).</p> </div> <ul style="list-style-type: none"> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul>
<p>RAM minimale pour le plug-in SnapCenter sur l'hôte</p>	<p>2 GO</p>
<p>Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte</p>	<p>2 GO</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>

Élément	De formation
Packs logiciels requis	<p>Java 11 Oracle et OpenJDK</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  <p>Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux.</p> </div> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p>

Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp](#)".

### Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux

Les versions SnapCenter 2.0 et ultérieures permettent à un utilisateur non-root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/*LINUX\_USER*/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /Custom\_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom\_location/NetApp/snapcenter/spl/bin/spl

## Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`LINUX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

### Configuration requise pour l'hôte AIX

Vous devez vous assurer que l'hôte répond aux exigences requises avant d'installer le module de plug-ins SnapCenter pour AIX.



Le plug-in SnapCenter pour UNIX qui fait partie du package de plug-ins SnapCenter pour AIX ne prend pas en charge les groupes de volumes simultanés.

Élément	De formation
Systèmes d'exploitation	AIX 7.1 ou version ultérieure
RAM minimale pour le plug-in SnapCenter sur l'hôte	4 Go
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	2 GO  <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes. </div>
Packs logiciels requis	Java 11 IBM Java  Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans /var/opt/snapcenter/spl/etc/spl.properties est définie sur la version JAVA correcte et le chemin correct.

Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp](#)".

#### Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte AIX

SnapCenter 4.4 et version ultérieure permet à un utilisateur non-root d'installer le module de plug-ins SnapCenter pour AIX et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

#### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256

```

## À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/AIX\_USER/.sc\_netapp/snapcenter\_aix\_host\_plugin.bsx
- /Custom\_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom\_location/NetApp/snapcenter/spl/bin/spl

## Étapes

1. Connectez-vous à l'hôte AIX sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour AIX.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.

```

Cmdnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmdnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmdnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmdnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`AIX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configurez les informations d'identification

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation du module d'extension sur des hôtes Linux ou AIX.

### À propos de cette tâche

Les informations d'identification sont créées pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

Pour plus d'informations, voir : [Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux](#) ou [Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte AIX](#)

**Meilleure pratique** : bien que vous soyez autorisé à créer des informations d'identification après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, entrez les informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur/Mot de passe	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>Administrateur de domaine <p>Spécifiez l'administrateur de domaine sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li><i>NetBIOS\username</i></li> <li><i>Domain FQDN\username</i></li> </ul> </li> <li>Administrateur local (groupes de travail uniquement) <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p> </li> </ul>
Mode d'authentification	<p>Sélectionnez le mode d'authentification que vous souhaitez utiliser.</p> <p>En fonction du système d'exploitation de l'hôte du plug-in, sélectionnez Linux ou AIX.</p>
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs sur la page **utilisateur et accès**.

### Configurer les informations d'identification d'une base de données Oracle

Vous devez configurer les informations d'identification utilisées pour effectuer des opérations de protection des données sur les bases de données Oracle.

#### À propos de cette tâche

Consultez les différentes méthodes d'authentification prises en charge pour la base de données Oracle. Pour plus d'informations, voir "[Méthodes d'authentification pour vos informations d'identification](#)".

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, le nom d'utilisateur doit au moins disposer de privilèges de groupe de ressources et de sauvegarde.

Si vous avez activé l'authentification de la base de données Oracle, une icône de cadenas rouge s'affiche dans la vue Ressources. Vous devez configurer les informations d'identification de la base de données pour pouvoir protéger la base de données ou l'ajouter au groupe de ressources pour effectuer des opérations de protection des données.



Si vous spécifiez des détails incorrects lors de la création d'informations d'identification, un message d'erreur s'affiche. Vous devez cliquer sur **Annuler**, puis réessayer.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.
3. Cliquez sur , puis sélectionnez le nom d'hôte et le type de base de données pour filtrer les ressources.

Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

4. Sélectionnez la base de données, puis cliquez sur **Paramètres de base de données > configurer la base de données**.
5. Dans la section configurer les paramètres de la base de données, dans la liste déroulante **utiliser les informations d'identification existantes**, sélectionnez les informations d'identification qui doivent être utilisées pour effectuer des tâches de protection des données sur la base de données Oracle.



L'utilisateur Oracle doit disposer des privilèges sysdba.

Vous pouvez également créer des informations d'identification en cliquant sur .

6. Dans la section configurer les paramètres ASM, dans la liste déroulante **utiliser les informations d'identification existantes**, sélectionnez les informations d'identification qui doivent être utilisées pour exécuter des tâches de protection des données sur l'instance ASM.



L'utilisateur ASM doit disposer du privilège sysasm.

Vous pouvez également créer des informations d'identification en cliquant sur .

7. Dans la section configurer les paramètres du catalogue RMAN, dans la liste déroulante **utiliser les informations d'identification existantes**, sélectionnez les informations d'identification qui doivent être utilisées pour effectuer des tâches de protection des données sur la base de données du catalogue Oracle Recovery Manager (RMAN).

Vous pouvez également créer des informations d'identification en cliquant sur .

Dans le champ **TNSName**, entrez le nom du fichier TNS (transparent Network Substrand) qui sera utilisé par le serveur SnapCenter pour communiquer avec la base de données.

8. Dans le champ **Preferred RAC Nodes**, indiquez les nœuds RAC (Real application Cluster) préférés pour la sauvegarde.

Les nœuds préférés peuvent être un ou tous les nœuds de cluster où sont présentes les instances de base de données RAC. L'opération de sauvegarde est déclenchée uniquement sur ces nœuds préférés, par ordre de préférence.

Dans RAC One Node, un seul nœud est répertorié dans les nœuds préférés, et ce nœud préféré est le nœud où la base de données est actuellement hébergée.

Après le basculement ou le déplacement de la base de données RAC One Node, l'actualisation des ressources de la page Ressources SnapCenter supprimera l'hôte de la liste **Preferred RAC Nodes** où la base de données était hébergée précédemment. Le nœud RAC où la base de données est déplacée sera répertorié dans **RAC Nodes** et devra être configuré manuellement comme nœud RAC préféré.

Pour plus d'informations, voir "[Nœuds préférés dans la configuration RAC](#)".

9. Cliquez sur **OK**.

## Ajoutez des hôtes et installez Plug-ins Package pour Linux ou AIX à l'aide de l'interface utilisateur graphique

Vous pouvez utiliser la page Ajouter un hôte pour ajouter des hôtes, puis installer le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX. Les plug-ins sont automatiquement installés sur les hôtes distants.

### À propos de cette tâche

Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour un cluster. Si vous installez le plug-in sur un cluster (Oracle RAC), le plug-in est installé sur tous les nœuds du cluster. Pour Oracle RAC One Node, vous devez installer le plug-in sur les nœuds actif et passif.



Seule l'authentification par mot de passe est prise en charge lorsque vous installez le plug-in sur un RAC Oracle. L'authentification basée sur la clé SSH n'est pas prise en charge.

Vous devez être affecté à un rôle doté des autorisations d'installation et de désinstallation du plug-in, telles que le rôle d'administrateur SnapCenter.



Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez <b>Linux</b> ou <b>AIX</b> comme type d'hôte.</p> <p>Le serveur SnapCenter ajoute l'hôte, puis installe le plug-in pour Oracle Database et le plug-in pour UNIX si les plug-ins ne sont pas déjà installés sur l'hôte.</p>
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p> <p>Vous pouvez entrer les adresses IP ou FQDN de l'un des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Hôte autonome</li> <li>• N'importe quel nœud dans l'environnement Oracle Real application clusters (RAC)</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Le nœud VIP ou l'analyse IP n'est pas pris en charge</p> </div> <p>Si vous ajoutez un hôte à l'aide de SnapCenter et que l'hôte fait partie d'un sous-domaine, vous devez fournir le FQDN.</p>
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification.</p> <p>Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez spécifié.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port.</p> <p>Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</div>
Chemin d'installation	<p>Le chemin par défaut est <code>/opt/NetApp/snapcenter</code>.</p> <p>Vous pouvez éventuellement personnaliser le chemin.</p>
Ajoutez tous les hôtes dans Oracle RAC	<p>Cochez cette case pour ajouter tous les nœuds du cluster dans un RAC Oracle.</p> <p>Dans une configuration Flex ASM, tous les nœuds, qu'il s'agisse d'un nœud Hub ou Leaf, seront ajoutés.</p>
Ignorer les vérifications de préinstallation facultatives	<p>Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.</p>

7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in.



Le script de vérification préalable ne valide pas l'état du pare-feu du port du plug-in s'il est spécifié dans les règles de rejet du pare-feu.

Les messages d'erreur ou d'avertissement appropriés s'affichent si les exigences minimales ne sont pas respectées. Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier `web.config` situé à l'adresse `C:\Program Files\NetApp\SnapCenter\WebApp` pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier `web.config`, vous devez le mettre à jour sur les deux nœuds.

8. Vérifiez l’empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l’empreinte de chacun des nœuds du cluster.



SnapCenter ne prend pas en charge l’algorithme ECDSA.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l’empreinte a été confirmée.

9. Surveillez la progression de l’installation.

Les fichiers journaux spécifiques à l’installation se trouvent à l’adresse `/Custom_location/snapcenter/logs`.

## Résultat

Toutes les bases de données de l’hôte sont automatiquement découvertes et affichées dans la page Ressources. Si rien ne s’affiche, cliquez sur **Actualiser les ressources**.

## Surveiller l’état de l’installation

Vous pouvez contrôler la progression de l’installation du module d’extension SnapCenter à l’aide de la page travaux. Vous pouvez vérifier la progression de l’installation pour déterminer quand elle est terminée ou s’il y a un problème.

## Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l’état de l’opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d’avertissements
-  En file d’attente

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d’installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l’état de l’installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d’installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Autres méthodes d'installation de Plug-ins Package pour Linux ou AIX

Vous pouvez également installer manuellement le module Plug-ins pour Linux ou AIX en utilisant les applets de commande ou les interfaces de ligne de commande.

Avant d'installer le plug-in manuellement, vous devez valider la signature du package binaire à l'aide de la clé **snapcenter\_public\_key.pub** et **snapcenter\_linux\_host\_plugin.bin.bin** située à la position *C:\ProgramData\NetApp\SnapCenter\Package Repository*.



Assurez-vous que **OpenSSL 1.0.2g** est installé sur l'hôte sur lequel vous souhaitez installer le plug-in.

Valider la signature du package binaire en exécutant la commande :

- Pour hôte Linux : `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Pour l'hôte AIX : `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

### Installation sur plusieurs hôtes distants à l'aide d'applets de commande

Vous devez utiliser l'applet de commande *Install-SmHostPackage* PowerShell pour installer le module de plug-ins SnapCenter pour Linux ou le module de plug-ins SnapCenter pour AIX sur plusieurs hôtes.

#### Ce dont vous aurez besoin

Vous devez être connecté à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

#### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande *Open-SmConnection*, puis saisissez vos informations d'identification.
3. Installez le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX à l'aide de l'applet de commande *Install-SmHostPackage* et des paramètres requis.

Vous pouvez utiliser l'option *-skipprecheck* lorsque vous avez déjà installé les plug-ins manuellement et ne voulez pas vérifier si l'hôte répond aux exigences requises pour installer le plug-in.



Le script de vérification préalable ne valide pas l'état du pare-feu du port du plug-in s'il est spécifié dans les règles de rejet du pare-feu.

4. Saisissez vos informations d'identification pour l'installation à distance.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Installez-le sur l'hôte du cluster

Vous devez installer SnapCenter Plug-ins Package pour Linux ou SnapCenter Plug-ins Package pour AIX sur les deux nœuds de l'hôte cluster.

Chacun des nœuds de l'hôte de cluster a deux adresses IP. L'une des adresses IP sera l'adresse IP publique des nœuds respectifs et la seconde sera l'adresse IP du cluster partagée entre les deux nœuds.

### Étapes

1. Installez le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX sur les deux nœuds de l'hôte de cluster.
2. Vérifiez que les valeurs correctes pour les paramètres `SNAPCENTER_SERVER_HOST`, `SPL_PORT`, `SNAPCENTER_SERVER_PORT` et `SPL_ENABLED_PLUGINS` sont spécifiées dans le fichier `spl.properties` situé à `/var/opt/snapcenter/SPL/etc/`.

Si `SPL_ENABLED_PLUGINS` n'est pas spécifié dans `spl.properties`, vous pouvez l'ajouter et attribuer la valeur `SCO,SCU`.

3. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande *Open-SmConnection*, puis saisissez vos informations d'identification.
4. Dans chacun des nœuds, définissez les adresses IP préférées du nœud à l'aide de la commande *set-PreferredHostIPsInStorageExportPolicy* `sccli` et des paramètres requis.
5. Dans l'hôte SnapCenter Server, ajoutez une entrée pour l'adresse IP du cluster et le nom DNS correspondant dans `C:\Windows\System32\drivers\etc\hosts`.
6. Ajoutez le nœud au serveur SnapCenter à l'aide de l'applet de commande *Add-SmHost* en spécifiant l'adresse IP du cluster pour le nom d'hôte.

Découvrez la base de données Oracle sur le nœud 1 (en supposant que l'adresse IP du cluster est hébergée sur le nœud 1) et créez une sauvegarde de la base de données. En cas de basculement, vous pouvez utiliser la sauvegarde créée sur le nœud 1 pour restaurer la base de données sur le nœud 2. Vous pouvez également utiliser la sauvegarde créée sur le nœud 1 pour créer un clone sur le nœud 2.



En cas de basculement, des volumes, des répertoires et des fichiers seront obsolètes, lorsque d'autres opérations SnapCenter sont en cours d'exécution.

## Installez Plug-ins Package pour Linux en mode silencieux

Vous pouvez installer le module de plug-ins SnapCenter pour Linux en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

### Ce dont vous aurez besoin

- Vous devez passer en revue les conditions préalables à l'installation du package de plug-ins.
- Vous devez vous assurer que la variable d'environnement `D'affichage` n'est pas définie.

Si la variable d'environnement `D'affichage` est définie, vous devez annuler `D'affichage`, puis essayer d'installer manuellement le plug-in.

### À propos de cette tâche

Vous devez fournir les informations nécessaires à l'installation lors de l'installation en mode console, alors

qu'en mode silencieux, vous n'avez pas à fournir d'informations d'installation.

## Étapes

1. Téléchargez le module de plug-ins SnapCenter pour Linux à partir de l'emplacement d'installation du serveur SnapCenter.

Le chemin d'installation par défaut est *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Ce chemin est accessible à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez téléchargé le fichier d'installation.
3. Courez

```
./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR=/opt/custom_path
```

4. Modifiez le fichier *spl.properties* situé à l'adresse */var/opt/snapcenter/spl/etc/* pour ajouter `SPL_ENABLED_PLUGINS=SCO,SCU`, puis redémarrez le service de chargeur de plug-in SnapCenter.



L'installation du package plug-ins enregistre les plug-ins sur l'hôte et non sur le serveur SnapCenter. Vous devez enregistrer les plug-ins sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Lors de l'ajout de l'hôte, sélectionnez « aucun » comme identifiant. Une fois l'hôte ajouté, les plug-ins installés sont automatiquement découverts.

## Installez le module plug-ins pour AIX en mode silencieux

Vous pouvez installer le module de plug-ins SnapCenter pour AIX en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

### Ce dont vous aurez besoin

- Vous devez passer en revue les conditions préalables à l'installation du package de plug-ins.
- Vous devez vous assurer que la variable d'environnement `D'AFFICHAGE` n'est pas définie.

Si la variable d'environnement `D'AFFICHAGE` est définie, vous devez annuler `D'AFFICHAGE`, puis essayer d'installer manuellement le plug-in.

## Étapes

1. Téléchargez le module de plug-ins SnapCenter pour AIX à partir de l'emplacement d'installation du serveur SnapCenter.

Le chemin d'installation par défaut est *C:\ProgramData\NetApp\SnapCenter\PackageRepository*. Ce chemin est accessible à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez téléchargé le fichier d'installation.
3. Courez

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-
```

```
DSEVER_IP=SnapCenter_Server_FQDN-DSEVER_HTTPS_PORT=SnapCenter_Server_Port-
DUSER_INSTALL_DIR==/opt/custom_path-
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. Modifiez le fichier `spl.properties` situé à l'adresse `/var/opt/snapcenter/spl/etc/` pour ajouter `SPL_ENABLED_PLUGINS=SCO,SCU`, puis redémarrez le service de chargeur de plug-in SnapCenter.



L'installation du package plug-ins enregistre les plug-ins sur l'hôte et non sur le serveur SnapCenter. Vous devez enregistrer les plug-ins sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Lors de l'ajout de l'hôte, sélectionnez « aucun » comme identifiant. Une fois l'hôte ajouté, les plug-ins installés sont automatiquement découverts.

## Configurer le service du chargeur enfichable SnapCenter

Le service de chargeur de plug-in SnapCenter charge le package de plug-in pour Linux ou AIX afin d'interagir avec le serveur SnapCenter. Le service de chargeur de plug-in SnapCenter est installé lorsque vous installez le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX.

### À propos de cette tâche

Après avoir installé le progiciel de plug-ins SnapCenter pour Linux ou le progiciel de plug-ins SnapCenter pour AIX, le service chargeur de plug-in SnapCenter démarre automatiquement. Si le service du chargeur enfichable SnapCenter ne démarre pas automatiquement, vous devez :

- Assurez-vous que le répertoire dans lequel le plug-in fonctionne n'est pas supprimé
- Augmentez l'espace mémoire alloué à la machine virtuelle Java

Le fichier `spl.properties`, qui se trouve à `/Custom_location/NetApp/snapcenter/spl/etc/`, contient les paramètres suivants. Les valeurs par défaut sont attribuées à ces paramètres.

Nom du paramètre	Description
NIVEAU_JOURNAL	Affiche les niveaux de journaux pris en charge.  Les valeurs possibles sont TRACE, DEBUG, INFO, WARN, ERROR, ET FATAL.
SPL_PROTOCOL	Affiche le protocole pris en charge par le chargeur SnapCenter Plug-in.  Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.

Nom du paramètre	Description
SNAPCENTER_SERVER_PROTOCOL	<p>Affiche le protocole pris en charge par le serveur SnapCenter.</p> <p>Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.</p>
SKIP_JAVAHOME_UPDATE	<p>Par défaut, le service SPL détecte le chemin Java et met à jour LE paramètre JAVA_HOME.</p> <p>Par conséquent, la valeur par défaut est DÉFINIE sur FALSE. Vous pouvez définir LA valeur TRUE si vous souhaitez désactiver le comportement par défaut et corriger manuellement le chemin Java.</p>
SPL_KEYSTORE_PASS	<p>Affiche le mot de passe du fichier keystore.</p> <p>Vous ne pouvez modifier cette valeur que si vous modifiez le mot de passe ou si vous créez un nouveau fichier de magasin de clés.</p>
SPL_PORT	<p>Affiche le numéro de port sur lequel le service du chargeur enfichable SnapCenter est exécuté.</p> <p>Vous pouvez ajouter la valeur si la valeur par défaut est manquante.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p style="margin: 0;">Vous ne devez pas modifier la valeur après l'installation des modules externes.</p> </div>
SNAPCENTER_SERVER_HOST	<p>Affiche l'adresse IP ou le nom d'hôte du serveur SnapCenter.</p>
CHEMIN_DU_MAGASIN_DE_CLÉS SPL	<p>Affiche le chemin absolu du fichier de magasin de clés.</p>
SNAPCENTER_SERVER_PORT	<p>Affiche le numéro de port sur lequel le serveur SnapCenter s'exécute.</p>

Nom du paramètre	Description
LOGS_MAX_COUNT	<p>Affiche le nombre de fichiers journaux du chargeur de plug-in SnapCenter qui sont conservés dans le dossier <code>/Custom_location/snapcenter/spl/logs</code>.</p> <p>La valeur par défaut est 5000. Si le nombre est supérieur à la valeur spécifiée, les 5000 derniers fichiers modifiés sont conservés. La vérification du nombre de fichiers est effectuée automatiquement toutes les 24 heures à partir du démarrage du service du chargeur de plug-in SnapCenter.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si vous supprimez manuellement le fichier <code>spl.properties</code>, le nombre de fichiers à conserver est défini sur 9999.</p> </div>
JAVA_HOME	<p>Affiche le chemin absolu du répertoire <code>Java_HOME</code> utilisé pour démarrer le service SPL.</p> <p>Ce chemin est déterminé lors de l'installation et dans le cadre du démarrage de SPL.</p>
LOG_MAX_SIZE	<p>Affiche la taille maximale du fichier journal des travaux.</p> <p>Une fois la taille maximale atteinte, le fichier journal est compressé et les journaux sont écrits dans le nouveau fichier de ce travail.</p>
RETAIN_LOGS_OF_LAST_DAYS	<p>Affiche le nombre de jours jusqu'à lesquels les journaux sont conservés.</p>
ACTIVER_CERTIFICAT_VALIDATION	<p>Affiche <code>TRUE</code> lorsque la validation du certificat CA est activée pour l'hôte.</p> <p>Vous pouvez activer ou désactiver ce paramètre en modifiant le fichier <code>spl.properties</code> ou en utilisant l'interface graphique ou l'applet de commande SnapCenter.</p>

Si l'un de ces paramètres n'est pas affecté à la valeur par défaut ou si vous souhaitez attribuer ou modifier la valeur, vous pouvez modifier le fichier `spl.properties`. Vous pouvez également vérifier le fichier `spl.properties` et le modifier pour résoudre tous les problèmes liés aux valeurs qui sont affectées aux paramètres. Après avoir modifié le fichier `spl.properties`, vous devez redémarrer le service de chargeur de plug-in SnapCenter.

## Étapes

1. Effectuez l'une des opérations suivantes, si nécessaire :
  - Démarrez le service du chargeur de plug-in SnapCenter :
    - En tant qu'utilisateur `root`, exécutez :

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```

- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl start
```

- Arrêtez le service du chargeur enfichable SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl stop
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop
```



Vous pouvez utiliser l'option `-force` avec la commande `stop` pour arrêter le service SnapCenter Plug-in Loader avec force. Cependant, vous devez faire preuve de prudence avant de le faire car il met également fin aux opérations existantes.

- Redémarrez le service du chargeur Plug-in SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl restart
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart
```

- Rechercher l'état du service du chargeur enfichable SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl status
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl status
```

- Trouver le changement dans le service du chargeur Plug-in SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl change
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl change
```

## Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux

Vous devez gérer le mot de passe du magasin de clés SPL et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaire pour le magasin de confiance SPL et configurer la paire de clés signée CA pour le magasin de confiance SPL avec le service de chargeur de plug-in SnapCenter pour activer le certificat numérique installé.



SPL utilise le fichier « `keystore.jks` », qui se trouve dans `'/var/opt/snapcenter/spl/etc.'` en tant que magasin de confiance et clé.

### Gérer le mot de passe pour le magasin de clés SPL et l'alias de la paire de clés signée CA utilisée

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés SPL dans le fichier de propriétés SPL.

C'est la valeur correspondant à la clé 'PL\_KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Mettez à jour la même chose pour la clé SPL\_KEYSTORE\_PASS dans le fichier spl.properties.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés SPL et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

## Configurez les certificats racine ou intermédiaire sur le magasin de confiance SPL

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée dans le stockage de confiance SPL.

### Étapes

1. Accédez au dossier contenant le magasin de clés SPL : `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
. Ajouter un certificat racine ou intermédiaire :
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaire sur le stockage de confiance SPL.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurez la paire de clés signée CA sur le magasin de confiance SPL

Vous devez configurer la paire de clés signée CA dans le magasin de confiance SPL.

### Étapes

1. Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Répertoriez les certificats ajoutés dans le magasin de clés.
```

```
keytool -list -v -keystore keystore.jks
. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.
```

Le mot de passe du magasin de clés SPL par défaut est la valeur de la clé `SPL_KEYSTORE_PASS` dans le fichier `spl.properties`.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
. Si le nom d'alias du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("*", ",", "), remplacez le nom d'alias par un nom simple :
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
. Configurez le nom d'alias à partir du magasin de clés situé dans le fichier spl.properties.
```

Mettez à jour cette valeur par rapport à la clé `SPL_CERTIFICATE_ALIAS`.

4. Redémarrez le service après avoir configuré la paire de clés signée CA dans la boutique de confiance

SPL.

## Configurer la liste de révocation de certificats (CRL) pour SPL

Vous devez configurer la CRL pour SPL

### À propos de cette tâche

- SPL recherche les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour SPL est `/var/opt/snapcenter/spl/etc/crl`.

### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `spl.properties` par rapport à la clé `SPL_CRL_PATH`.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.

-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Importation des données depuis SnapManager for Oracle et SnapManager for SAP vers SnapCenter

Importer des données à partir de SnapManager pour Oracle et de SnapManager pour SAP vers SnapCenter vous permet de continuer à utiliser vos données des versions précédentes.

Vous pouvez importer des données de SnapManager for Oracle et de SnapManager for SAP vers SnapCenter en exécutant l'outil d'importation à partir de l'interface de ligne de commande (interface de ligne de commande hôte Linux).

L'outil d'importation crée des stratégies et des groupes de ressources dans SnapCenter. Les stratégies et les groupes de ressources créés dans SnapCenter correspondent aux profils et opérations effectués à l'aide de ces profils dans SnapManager for Oracle et SnapManager for SAP. L'outil d'importation SnapCenter interagit avec les bases de données du référentiel SnapManager pour Oracle et SnapManager pour SAP et avec la base de données que vous souhaitez importer.

- Récupère tous les profils, plannings et opérations effectués à l'aide des profils.
- Crée une politique de sauvegarde SnapCenter pour chaque opération et chaque planification attachée à un profil.
- Crée un groupe de ressources pour chaque base de données cible.

Vous pouvez exécuter l'outil d'importation en exécutant le script `sc-migration` situé à l'adresse `/opt/NetApp/snapcenter/spl/bin`. Lorsque vous installez le package de plug-ins SnapCenter pour Linux sur l'hôte de base de données que vous souhaitez importer, le script `sc-migration` est copié dans `/opt/NetApp/snapcenter/spl/bin`.



L'importation de données n'est pas prise en charge à partir de l'interface utilisateur graphique SnapCenter.

SnapCenter ne prend pas en charge Data ONTAP fonctionnant en 7-mode. Vous pouvez utiliser l'outil 7-mode transition Tool pour migrer vers un système ONTAP les données et les configurations stockées sur un système exécutant Data ONTAP 7-mode.

### Configurations prises en charge pour l'importation de données

Avant d'importer les données de SnapManager 3.4.x pour Oracle et de SnapManager 3.4.x pour SAP vers SnapCenter, nous vous recommandons de connaître les configurations prises en charge par le plug-in SnapCenter pour base de données Oracle.

Les configurations prises en charge par le plug-in SnapCenter pour la base de données Oracle sont répertoriées dans le "[Matrice d'interopérabilité NetApp](#)".

## Ce qui est importé dans SnapCenter

Vous pouvez importer des profils, des plannings et des opérations effectués à l'aide des profils.

Grâce à SnapManager for Oracle et SnapManager for SAP	À SnapCenter
Profils sans opération ni planification	Une stratégie est créée avec le type de sauvegarde par défaut en ligne et le champ d'application de sauvegarde complet.
Profils avec une ou plusieurs opérations	Plusieurs règles sont créées en fonction d'une combinaison unique d'un profil et d'opérations réalisées à l'aide de ce profil.  Les stratégies créées dans SnapCenter contiennent les détails d'élagage et de conservation du journal d'archivage extraits du profil et des opérations correspondantes.
Profils avec configuration Oracle Recovery Manager (RMAN)	Les stratégies sont créées avec l'option <b>sauvegarde catalogue avec Oracle Recovery Manager</b> activée.  Si le catalogage RMAN externe a été utilisé dans SnapManager, vous devez configurer les paramètres du catalogue RMAN dans SnapCenter. Vous pouvez sélectionner les informations d'identification existantes ou créer une nouvelle information d'identification.  Si RMAN a été configuré par le biais du fichier de contrôle dans SnapManager, vous n'avez pas besoin de configurer RMAN dans SnapCenter.
Calendrier joint à un profil	Une règle est créée uniquement pour le planning.
Base de données	Un groupe de ressources est créé pour chaque base de données importée.  Dans une configuration RAC (Real application clusters), le nœud sur lequel vous exécutez l'outil d'importation devient le nœud préféré après l'importation et le groupe de ressources est créé pour ce nœud.



Lorsqu'un profil est importé, une stratégie de vérification est créée avec la stratégie de sauvegarde.

Lorsque SnapManager pour Oracle et SnapManager pour SAP profils, planifications et toutes les opérations effectuées à l'aide des profils sont importées dans SnapCenter, les différentes valeurs de paramètres sont également importées.

SnapManager for Oracle et SnapManager for SAP : paramètres et valeurs	Paramètre et valeurs de SnapCenter	Remarques
<p>Étendue de la sauvegarde</p> <ul style="list-style-type: none"> <li>• Pleine</li> <li>• Les données</li> <li>• Journal</li> </ul>	<p>Étendue de la sauvegarde</p> <ul style="list-style-type: none"> <li>• Pleine</li> <li>• Les données</li> <li>• Journal</li> </ul>	
<p>Mode de sauvegarde</p> <ul style="list-style-type: none"> <li>• Auto</li> <li>• En ligne</li> <li>• Hors ligne</li> </ul>	<p>Type de sauvegarde</p> <ul style="list-style-type: none"> <li>• En ligne</li> <li>• Arrêt hors ligne</li> </ul>	<p>Si le mode de sauvegarde est Auto, l'outil d'importation vérifie alors l'état de la base de données lorsque l'opération a été effectuée et définit de manière appropriée le type de sauvegarde comme Arrêt en ligne ou hors ligne.</p>
<p>La conservation</p> <ul style="list-style-type: none"> <li>• Jours</li> <li>• Compte</li> </ul>	<p>La conservation</p> <ul style="list-style-type: none"> <li>• Jours</li> <li>• Compte</li> </ul>	<p>SnapManager pour Oracle et SnapManager pour SAP utilise à la fois des jours et des nombres pour définir les paramètres de conservation.</p> <p>Dans SnapCenter, il y a soit des jours <i>OU</i> comptes. La conservation est donc définie sur des jours car les jours de préférence ne sont plus nombreux dans SnapManager pour Oracle et SnapManager pour SAP.</p>
<p>Élagage pour les plannings</p> <ul style="list-style-type: none"> <li>• Tout</li> <li>• Numéro de changement du système (SCN)</li> <li>• Date</li> <li>• Journaux créés avant les heures, les jours, les semaines et les mois spécifiés</li> </ul>	<p>Élagage pour les plannings</p> <ul style="list-style-type: none"> <li>• Tout</li> <li>• Journaux créés avant les heures et les jours spécifiés</li> </ul>	<p>SnapCenter ne prend pas en charge l'élagage selon SCN, date, semaines et mois.</p>

SnapManager for Oracle et SnapManager for SAP : paramètres et valeurs	Paramètre et valeurs de SnapCenter	Remarques
<p>Notification</p> <ul style="list-style-type: none"> <li>• E-mails envoyés uniquement pour assurer la réussite des opérations</li> <li>• E-mails envoyés uniquement en cas d'échec</li> <li>• E-mails envoyés pour succès et échecs</li> </ul>	<p>Notification</p> <ul style="list-style-type: none"> <li>• Toujours</li> <li>• En cas de défaillance</li> <li>• Avertissement</li> <li>• Erreur</li> </ul>	<p>Les notifications par e-mail sont importées.</p> <p>Cependant, vous devez mettre à jour manuellement le serveur SMTP à l'aide de l'interface graphique SnapCenter. L'objet de l'e-mail reste vide pour que vous puissiez le configurer.</p>

### Ce qui n'est pas importé dans SnapCenter

L'outil d'importation n'importe pas tout dans SnapCenter.

Vous ne pouvez pas importer les éléments suivants dans SnapCenter :

- Les métadonnées de sauvegarde
- Sauvegardes partielles
- Sauvegardes relatives à Raw Device Mapping (RDM) et Virtual Storage Console (VSC)
- Rôles ou informations d'identification disponibles dans le référentiel SnapManager pour Oracle et SnapManager pour SAP
- Données liées aux opérations de vérification, de restauration et de clonage
- Des opérations de suppression
- Détails de réplication spécifiés dans le profil SnapManager pour Oracle et SnapManager pour SAP

Après l'importation, vous devez modifier manuellement la stratégie correspondante créée dans SnapCenter pour inclure les détails de la réplication.

- Informations de sauvegarde cataloguées

### Préparez-vous à importer des données

Avant d'importer des données dans SnapCenter, vous devez effectuer certaines tâches pour que l'opération d'importation puisse réussir.

#### Étapes

1. Identifiez la base de données à importer.
2. À l'aide de SnapCenter, ajoutez l'hôte de base de données et installez SnapCenter Plug-ins Package pour Linux.
3. SnapCenter permet de configurer les connexions des SVM utilisées par les bases de données sur l'hôte.
4. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
5. Dans la page Ressources, assurez-vous que la base de données à importer est découverte et affichée.

Lorsque vous souhaitez exécuter l'outil d'importation, la base de données doit être accessible ou la création du groupe de ressources échoue.

Si les informations d'identification de la base de données sont configurées, vous devez créer les informations d'identification correspondantes dans SnapCenter, attribuer les informations d'identification à la base de données, puis relancer la découverte de la base de données. Si la base de données réside dans ASM (Automatic Storage Management), vous devez créer des informations d'identification pour l'instance ASM et affecter ces informations d'identification à la base de données.

6. Assurez-vous que l'utilisateur exécutant l'outil d'importation dispose de privilèges suffisants pour exécuter des commandes CLI SnapManager pour Oracle ou SnapManager pour SAP (telles que la commande pour suspendre les planifications) à partir de l'hôte SnapManager pour Oracle ou SnapManager pour SAP.
7. Exécutez les commandes suivantes sur l'hôte SnapManager pour Oracle ou SnapManager pour SAP pour suspendre les planifications :

a. Si vous souhaitez suspendre les planifications sur l'hôte SnapManager pour Oracle, exécutez :

- `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smo credential set -profile -name profile_name`



Vous devez exécuter la commande d'ensemble d'informations d'identification smo pour chaque profil de l'hôte.

b. Si vous souhaitez suspendre les planifications sur l'hôte SnapManager pour SAP, exécutez :

- `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smsap credential set -profile -name profile_name`



Vous devez exécuter la commande smsap Credential set pour chaque profil de l'hôte.

8. Assurez-vous que le nom de domaine complet (FQDN) de l'hôte de la base de données s'affiche lorsque vous exécutez `hostname -F`.

Si le FQDN n'est pas affiché, vous devez modifier `/etc/hosts` pour spécifier le FQDN de l'hôte.

## Importer des données

Vous pouvez importer des données en exécutant l'outil d'importation à partir de l'hôte de la base de données.

## À propos de cette tâche

Les règles de sauvegarde SnapCenter créées après l'importation ont des formats de nommage différents :

- Les règles créées pour les profils sans opération ni planification ont le format `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRÉE`.

Lorsqu'aucune opération n'est effectuée à l'aide d'un profil, la règle correspondante est créée avec le type de sauvegarde par défaut en tant qu'étendue en ligne et la sauvegarde complète.

- Les règles créées pour les profils avec une ou plusieurs opérations ont le format `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRÉ`.
- Les règles créées pour les planifications attachées aux profils ont le format `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRÉ`.

## Étapes

1. Connectez-vous à l'hôte de base de données que vous souhaitez importer.
2. Exécutez l'outil d'importation en exécutant le script `sc-migrate` situé à `/opt/NetApp/snapcenter/spl/bin`.
3. Entrez le nom d'utilisateur et le mot de passe du serveur SnapCenter.

Une fois les informations d'identification valides, une connexion est établie avec SnapCenter.

4. Entrez les détails de la base de données du référentiel SnapManager pour Oracle ou SnapManager pour SAP.

La base de données du référentiel répertorie les bases de données disponibles sur l'hôte.

5. Entrez les détails de la base de données cible.

Si vous souhaitez importer toutes les bases de données de l'hôte, entrez tout.

6. Si vous souhaitez générer un journal système ou envoyer des messages ASUP pour les opérations ayant échoué, vous devez les activer soit en exécutant la commande `Add-SmStorageConnection` soit `set-SmStorageConnection`.



Si vous souhaitez annuler une opération d'importation, soit lors de l'exécution de l'outil d'importation, soit après l'importation, vous devez supprimer manuellement les stratégies SnapCenter, les informations d'identification et les groupes de ressources créés dans le cadre de l'opération d'importation.

## Résultats

Les stratégies de sauvegarde SnapCenter sont créées pour les profils, les planifications et les opérations effectuées à l'aide des profils. Des groupes de ressources sont également créés pour chaque base de données cible.

Une fois les données importées avec succès, les planifications associées à la base de données importée sont suspendues dans SnapManager pour Oracle et SnapManager pour SAP.



Après l'importation, vous devez gérer la base de données ou le système de fichiers importés à l'aide de SnapCenter.

Les journaux de chaque exécution de l'outil d'importation sont stockés dans le répertoire

`/var/opt/snapcenter/spl/logs` sous le nom `spl_migration_timestamp.log`. Vous pouvez consulter ce journal pour consulter les erreurs d'importation et les résoudre.

## Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM) ou si vous souhaitez protéger des VM et des datastores, vous devez déployer l'appliance virtuelle du plug-in SnapCenter pour VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section "[Présentation du déploiement](#)".

### Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Créez ou importez un certificat SSL](#)".

### Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est `/opt/netapp/config/crl`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

## Préparez-vous à la protection des bases de données Oracle

Avant d'effectuer des opérations de protection des données telles que la sauvegarde, le clonage ou la restauration, vous devez définir votre stratégie et configurer l'environnement. Vous pouvez également configurer le serveur SnapCenter pour qu'il utilise la technologie SnapMirror et SnapVault.

Pour profiter des avantages de SnapVault et de la technologie SnapMirror, vous devez configurer et initialiser une relation de protection des données entre les volumes source et destination sur le périphérique de stockage. Vous pouvez utiliser NetAppSystem Manager ou utiliser la ligne de commandes de la console de stockage pour effectuer ces tâches.

Avant d'utiliser le plug-in pour base de données Oracle, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches préalables.

- Installer et configurer SnapCenter Server. "[En savoir plus >>](#)"
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage. "[En savoir plus >>](#)"



SnapCenter ne prend pas en charge plusieurs SVM de même nom sur différents clusters. Chaque SVM enregistré avec SnapCenter via l'enregistrement de SVM ou de cluster doit être unique.

- Créez des informations d'identification avec le mode d'authentification sous Linux ou AIX pour l'utilisateur d'installation. "[En savoir plus >>](#)"

- Ajoutez des hôtes, installez les plug-ins et découvrez les ressources.
- Si vous utilisez SnapCenter Server pour protéger les bases de données Oracle résidant sur des LUN ou des VMDK VMware RDM, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter.
- Installez Java sur votre hôte Linux ou AIX.

Voir ["Configuration requise pour l'hôte Linux"](#) ou ["Configuration requise pour l'hôte AIX"](#) pour en savoir plus.

- Vous devez définir la valeur de délai d'exécution du pare-feu de l'application sur 3 heures ou plus.
- Si vous utilisez des bases de données Oracle sur des environnements NFS, vous devez avoir configuré au moins une LIF de données NFS pour le stockage primaire ou secondaire afin d'effectuer des opérations de montage, de clonage, de vérification et de restauration.
- Si vous disposez de plusieurs chemins d'accès aux données (LIF) ou d'une configuration dNFS, vous pouvez effectuer les opérations suivantes à l'aide de l'interface de ligne de commandes SnapCenter sur l'hôte de base de données :
  - Par défaut toutes les adresses IP de l'hôte de base de données sont ajoutées à la règle d'exportation du stockage NFS dans la machine virtuelle de stockage (SVM) pour les volumes clonés. Si vous souhaitez avoir une adresse IP spécifique ou restreindre à un sous-ensemble d'adresses IP, exécutez l'interface de ligne de commande `set-PreferredHostIPsInStorageExportPolicy`.
  - Si un SVM possède plusieurs chemins de données (LIF), SnapCenter choisit le chemin d'accès aux données (LIF) approprié pour le montage du volume cloné NFS. Toutefois, si vous souhaitez spécifier un chemin de données spécifique (LIF), vous devez exécuter l'interface de ligne de commande `set-SvmPreferredDataPath`. Le guide de référence des commandes contient plus d'informations.
- Si vous disposez de bases de données Oracle sur des environnements SAN, assurez-vous que l'environnement SAN est configuré selon les recommandations indiquées dans les guides suivants :
  - ["Utilisation d'hôtes Linux avec stockage ONTAP"](#)
  - ["Paramètres d'hôte affectés par les utilitaires hôtes AIX"](#)
- Si vous avez des bases de données Oracle sur LVM sous Oracle Linux ou RHEL, installez la dernière version de Logical Volume Management (LVM).
- Si vous utilisez SnapManager pour Oracle et que vous souhaitez migrer vers le plug-in SnapCenter pour Oracle Database, vous pouvez migrer les profils vers des stratégies et des groupes de ressources de SnapCenter à l'aide de la commande `sccli sc-migrate`.
- Configurez les fonctionnalités SnapMirror et SnapVault sur ONTAP, si vous souhaitez effectuer une sauvegarde de réplication

Pour les utilisateurs de SnapCenter 4.1.1, la documentation du plug-in SnapCenter pour VMware vSphere 4.1.1 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers. Pour les utilisateurs de SnapCenter 4.2.x, NetApp Data Broker 1.0 et 1.0.1, la documentation relative à la protection des bases de données et des systèmes de fichiers virtualisés à l'aide du plug-in SnapCenter pour VMware vSphere fourni par le dispositif virtuel NetApp Data Broker basé sur Linux (format Open Virtual Appliance). Pour les utilisateurs de SnapCenter 4.3.x, la documentation du plug-in SnapCenter pour VMware vSphere 4.3 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers à l'aide du plug-in SnapCenter basé sur Linux pour l'appliance virtuelle VMware vSphere (format Open Virtual Appliance).

## Plus d'informations

- ["Matrice d'interopérabilité"](#)

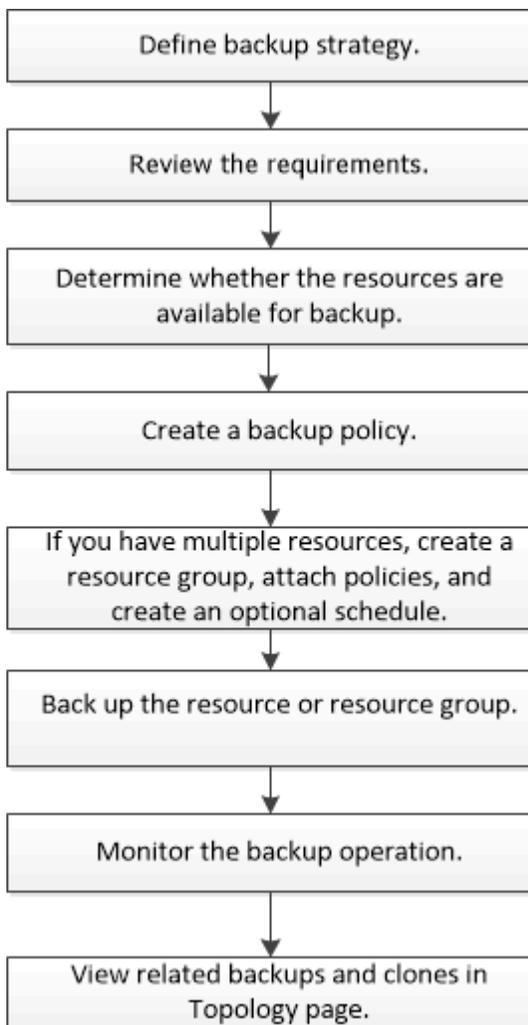
- "Documentation du plug-in SnapCenter pour VMware vSphere"
- "L'opération de protection des données échoue dans un environnement sans chemins d'accès multiples sous RHEL 7 et versions ultérieures"

## Sauvegarde des bases de données Oracle

### Présentation de la procédure de sauvegarde

Vous pouvez créer une sauvegarde d'une ressource (base de données) ou d'un groupe de ressources. La procédure de sauvegarde comprend la planification, l'identification des ressources pour la sauvegarde, la création de stratégies de sauvegarde, la création de groupes de ressources et de stratégies de connexion, la création de sauvegardes et la surveillance des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Lors de la création d'une sauvegarde pour les bases de données Oracle, un fichier de verrouillage opérationnel (*.sm\_lock\_dbsid*) est créé sur l'hôte de la base de données Oracle dans le répertoire */var/opt/snapcenter/sco/lock* pour éviter l'exécution de plusieurs opérations sur la base de données. Une fois la base de données sauvegardée, le fichier de verrouillage opérationnel est automatiquement supprimé.

Cependant, si la sauvegarde précédente a été terminée avec un avertissement, le fichier de verrouillage opérationnel peut ne pas être supprimé et l'opération de sauvegarde suivante est entrée dans la file d'attente. Il peut être annulé si le fichier `.sm_lock_dbsid` n'est pas supprimé. Dans ce scénario, vous devez supprimer manuellement le fichier de verrouillage opérationnel en procédant comme suit :

1. À l'invite de commandes, accédez à `/var/opt/snapcenter/sco/lock`.
2. Supprimez le verrouillage opérationnel : `rm -rf .sm_lock_dbsid`.

## Sauvegarder les informations de configuration

### Configurations de base de données Oracle prises en charge pour les sauvegardes

SnapCenter prend en charge la sauvegarde de différentes configurations de bases de données Oracle.

- Oracle autonome
- Oracle Real application clusters (RAC)
- Oracle autonome existant
- Base de données de conteneur autonome Oracle (CDB)
- Veille Oracle Data Guard

Vous ne pouvez créer que des sauvegardes de bases de données de secours Data Guard à montage hors ligne. La sauvegarde hors ligne, la sauvegarde du journal d'archivage uniquement et la sauvegarde complète ne sont pas prises en charge.

- Veille Oracle Active Data Guard

Vous pouvez uniquement créer des sauvegardes en ligne des bases de données de secours Active Data Guard. La sauvegarde et la sauvegarde complète du journal d'archivage uniquement ne sont pas prises en charge.

Avant de créer une sauvegarde de la base de données de secours Data Guard ou Active Data Guard, le processus de restauration géré (MRP) est arrêté et une fois la sauvegarde créée, le MRP est démarré.

- Gestion automatique du stockage (ASM)
  - ASM autonome et ASM RAC sur Virtual machine Disk (VMDK)

Parmi toutes les méthodes de restauration prises en charge pour les bases de données Oracle, vous pouvez effectuer uniquement la restauration de connexion et de copie des bases de données ASM RAC sur VMDK.

- ASM autonome et ASM RAC sur RDM (Raw Device Mapping) + vous pouvez effectuer des opérations de sauvegarde, de restauration et de clonage sur des bases de données Oracle sur ASM, avec ou sans ASMLib.
- Pilote de filtre Oracle ASM (ASMFD)

Les opérations de migration PDB et de clonage PDB ne sont pas prises en charge.

- Oracle Flex ASM

Pour obtenir les dernières informations sur les versions Oracle prises en charge, consultez le ["Matrice](#)

## Types de sauvegarde pris en charge pour les bases de données Oracle

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge les types de sauvegarde en ligne et hors ligne pour les bases de données Oracle.

### Sauvegarde en ligne

Une sauvegarde créée lorsque la base de données est en ligne est appelée sauvegarde en ligne. Également appelée sauvegarde à chaud, une sauvegarde en ligne vous permet de créer une sauvegarde de la base de données sans l'arrêter.

Dans le cadre de la sauvegarde en ligne, vous pouvez créer une sauvegarde des fichiers suivants :

- Fichiers de données et fichiers de contrôle uniquement
- Fichiers journaux d'archive uniquement (la base de données n'est pas mise en mode de sauvegarde dans ce scénario)
- Base de données complète comprenant les fichiers de données, les fichiers de contrôle et les fichiers journaux d'archivage

### Sauvegarde hors ligne

Une sauvegarde créée lorsque la base de données est à l'état monté ou arrêté est appelée sauvegarde hors ligne. Une sauvegarde hors ligne est également appelée sauvegarde à froid. Vous pouvez inclure uniquement les fichiers de données et les fichiers de contrôle dans les sauvegardes hors ligne. Vous pouvez créer une sauvegarde de montage hors ligne ou d'arrêt hors ligne.

- Lors de la création d'une sauvegarde de montage hors ligne, vous devez vous assurer que la base de données est à l'état monté.

Si la base de données est dans un autre état, l'opération de sauvegarde échoue.

- Lors de la création d'une sauvegarde d'arrêt hors ligne, la base de données peut être dans n'importe quel état.

L'état de la base de données passe à l'état requis pour créer une sauvegarde. Après avoir créé la sauvegarde, l'état de la base de données est rétabli à son état d'origine.

## Comment SnapCenter détecte les bases de données Oracle

Les ressources sont des bases de données Oracle gérées par SnapCenter sur l'hôte. Vous pouvez ajouter ces bases de données à des groupes de ressources pour exécuter des opérations de protection des données après avoir découvert les bases de données disponibles.

Les sections suivantes décrivent le processus utilisé par SnapCenter pour détecter les différents types et versions de bases de données Oracle.

## Pour Oracle versions 11g à 12cR1

### Base de données RAC

Les bases de données RAC ne sont découvertes que sur la base de `/etc/oratab` intrinsèques. Vous devez avoir les entrées de la base de données dans le fichier `/etc/oratab`.

### Autonome

Les bases de données autonomes ne sont découvertes que sur la base des entrées `/etc/oratab`.

### DE

L'entrée d'instance ASM doit être disponible dans le fichier `/etc/oratab`.

### RAC un nœud

Les bases de données RAC One Node ne sont découvertes que sur la base des entrées `/etc/oratab`. Les bases de données doivent être à l'état `nomount`, `mount` ou `open`. Vous devez avoir les entrées de la base de données dans le fichier `/etc/oratab`.

L'état de la base de données RAC One Node sera marqué comme renommé ou supprimé si la base de données est déjà découverte et que les sauvegardes sont associées à la base de données.

Si la base de données est déplacée, procédez comme suit :

1. Ajoutez manuellement l'entrée de base de données déplacée dans le fichier `/etc/oratab` sur le nœud RAC défaillant.
2. Actualisez manuellement les ressources.
3. Sélectionnez la base de données RAC One Node dans la page de ressources, puis cliquez sur Paramètres de base de données.
4. Configurez la base de données pour définir les nœuds de cluster préférés sur le nœud RAC qui héberge actuellement la base de données.
5. Effectuer les opérations SnapCenter.
6. Si vous avez déplacé une base de données d'un nœud vers un autre et si l'entrée `oratab` du nœud précédent n'est pas supprimée, supprimez manuellement l'entrée `oratab` pour éviter que la même base de données ne s'affiche deux fois.

## Pour les versions 12cR2 à 18c, 19c ou 21c d'Oracle

### Base de données RAC

Les bases de données RAC sont découvertes à l'aide de la commande `srvctl config`. Vous devez avoir les entrées de la base de données dans le fichier `/etc/oratab`.

### Autonome

Les bases de données autonomes sont découvertes en fonction des entrées du fichier `/etc/oratab` et de la sortie de la commande `srvctl config`.

### DE

L'entrée de l'instance ASM n'a pas besoin d'être dans le fichier `/etc/oratab`.

### RAC un nœud

Les bases de données RAC One Node sont découvertes à l'aide de la commande `srvctl config` uniquement. Les bases de données doivent être à l'état `nomount`, `mount` ou `open`. L'état de la base de données RAC One Node sera marqué comme renommé ou supprimé si la base de données est déjà découverte et que les

sauvegardes sont associées à la base de données.

Si la base de données est déplacée, procédez comme suit : . Actualisez manuellement les ressources. . Sélectionnez la base de données RAC One Node dans la page de ressources, puis cliquez sur Paramètres de base de données. . Configurez la base de données pour définir les nœuds de cluster préférés sur le nœud RAC qui héberge actuellement la base de données. . Effectuer les opérations SnapCenter.



S'il y a des entrées de base de données Oracle 12cR2 et 18c dans le fichier `/etc/oratab` et que la même base de données est enregistrée avec la commande `srvctl config`, SnapCenter éliminera les entrées de base de données dupliquées. Si des entrées de base de données obsolètes sont présentes, la base de données sera découverte mais la base de données sera inaccessible et son statut sera déconnecté.

## Nœuds préférés dans la configuration RAC

Dans le programme d'installation d'Oracle Real application clusters (RAC), vous pouvez spécifier les nœuds préférés que SnapCenter utilise pour effectuer l'opération de sauvegarde. Si vous ne spécifiez pas le nœud préféré, SnapCenter attribue automatiquement un nœud en tant que nœud préféré et la sauvegarde est créée sur ce nœud.

Les nœuds préférés peuvent être un ou tous les nœuds du cluster où les instances de base de données RAC sont présentes. L'opération de sauvegarde est déclenchée uniquement sur ces nœuds préférés dans l'ordre de préférence.

### Exemple

La base de données `cdbrac` comporte trois instances : `cdbrac1` sur le `node1`, `cdbrac2` sur le `node2` et `cdbrac3` sur le `node3`.

Les instances `node1` et `node2` sont configurées pour être les nœuds préférés, avec le nœud2 comme première préférence et le nœud1 comme seconde préférence. Lorsque vous effectuez une opération de sauvegarde, l'opération est d'abord tentée sur le nœud 2 car il s'agit du premier nœud préféré.

Si le nœud 2 n'est pas dans l'état de sauvegarde, ce qui peut être dû à plusieurs raisons, par exemple l'agent du plug-in ne s'exécute pas sur l'hôte, l'instance de base de données sur l'hôte n'est pas à l'état requis pour le type de sauvegarde spécifié, Ou l'instance de base de données sur `node2` dans une configuration FlexASM n'est pas traitée par l'instance ASM locale ; l'opération est alors tentée sur le nœud 1.

Le nœud 3 ne sera pas utilisé pour la sauvegarde, car il ne figure pas dans la liste des nœuds préférés.

### Configuration de Flex ASM

Dans une configuration Flex ASM, les nœuds Leaf ne seront pas répertoriés comme nœuds préférés si la cardinalité est inférieure au nombre de nœuds du cluster RAC. En cas de modification des rôles de nœud de cluster Flex ASM, vous devez découvrir manuellement afin que les nœuds préférés soient actualisés.

### État requis de la base de données

Les instances de base de données RAC sur les nœuds préférés doivent être dans l'état requis pour que la sauvegarde puisse se terminer correctement :

- L'une des instances de base de données RAC des nœuds préférés configurés doit être en état ouvert pour créer une sauvegarde en ligne.

- L'une des instances de base de données RAC des nœuds préférés configurés doit être en état de montage, et toutes les autres instances, y compris les autres nœuds préférés, doivent être en état de montage ou inférieures pour créer une sauvegarde de montage hors ligne.
- Les instances de base de données RAC peuvent être dans n'importe quel état, mais vous devez spécifier les nœuds préférés pour créer une sauvegarde d'arrêt hors ligne.

## Comment cataloguer les sauvegardes avec Oracle Recovery Manager

Vous pouvez cataloguer les sauvegardes de bases de données Oracle à l'aide d'Oracle Recovery Manager (RMAN) pour stocker les informations de sauvegarde dans le référentiel Oracle RMAN.

Les sauvegardes cataloguées peuvent être utilisées ultérieurement pour les opérations de restauration au niveau des blocs ou de restauration à un point dans le temps de l'espace de stockage. Lorsque vous n'avez pas besoin de ces sauvegardes cataloguées, vous pouvez supprimer les informations du catalogue.

La base de données doit être montée ou supérieure pour le catalogage. Vous pouvez cataloguer des sauvegardes de données, des sauvegardes de journaux d'archivage et des sauvegardes complètes. Si le catalogage est activé pour une sauvegarde d'un groupe de ressources possédant plusieurs bases de données, le catalogage est effectué pour chaque base de données. Pour les bases de données Oracle RAC, le catalogage s'effectue sur le nœud préféré où la base de données est au moins à l'état montée.

Si vous souhaitez cataloguer les sauvegardes d'une base de données RAC, assurez-vous qu'aucune autre tâche n'est en cours d'exécution pour cette base de données. Si un autre travail est en cours d'exécution, l'opération de catalogage échoue au lieu d'être mise en file d'attente.

### Base de données de catalogue externe

Par défaut, le fichier de contrôle de la base de données cible est utilisé pour le catalogage. Si vous souhaitez ajouter une base de données de catalogue externe, vous pouvez la configurer en spécifiant les informations d'identification et le nom de support réseau transparent (TNS) du catalogue externe à l'aide de l'assistant Paramètres de base de données de l'interface utilisateur graphique de SnapCenter. Vous pouvez également configurer la base de données du catalogue externe à partir de l'interface CLI en exécutant la commande `Configure-SmOracleDatabase` avec les options `-OracleRmanCatalCredentialName` et `-OracleRmanCatalTnsName`.

### Commande RMAN

Si vous avez activé l'option de catalogage lors de la création d'une stratégie de sauvegarde Oracle à partir de l'interface utilisateur graphique SnapCenter, les sauvegardes sont cataloguées à l'aide d'Oracle RMAN dans le cadre de l'opération de sauvegarde. Vous pouvez également procéder au catalogage différé des sauvegardes en exécutant `Catalog-SmBackupWithOracleRMAN` commande.

Une fois les sauvegardes cataloguées, vous pouvez exécuter `Get-SmBackupDetails` pour obtenir les informations de sauvegarde cataloguées, telles que la balise des fichiers de données catalogués, le chemin du catalogue de fichiers de contrôle et les emplacements des journaux d'archives catalogués.

### Format de dénomination

Si le nom du groupe de disques ASM est supérieur ou égal à 16 caractères, à partir de SnapCenter 3.0, le format de nommage utilisé pour la sauvegarde est `SC_HASHCODEofDISKGROUP_DBSID_BACKUPID`. Cependant, si le nom du groupe de disques est inférieur à 16 caractères, le format de nommage utilisé pour la sauvegarde est `DISKGROUPNAME_DBSID_BACKUPID`, qui est le même format que celui utilisé dans SnapCenter 2.0.

Le HASHCODEofDISKGROUP est un nombre généré automatiquement (2 à 10 chiffres) unique pour chaque groupe de disques ASM.

### Opérations de contre-vérification

Vous pouvez effectuer des vérifications croisées pour mettre à jour les informations de référentiel RMAN obsolètes concernant les sauvegardes dont les enregistrements de référentiel ne correspondent pas à leur état physique. Par exemple, si un utilisateur supprime les journaux archivés du disque à l'aide d'une commande du système d'exploitation, le fichier de contrôle indique toujours que les journaux sont sur le disque, alors qu'en fait ils ne le sont pas.

L'opération crosscheck vous permet de mettre à jour le fichier de contrôle avec les informations. Vous pouvez activer la fonction crosscheck en exécutant la commande set-SmConfigSettings et en attribuant la valeur TRUE au paramètre ENABLE\_CROSSCHECK. La valeur par défaut est FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

### Supprimer les informations du catalogue

Vous pouvez supprimer les informations de catalogue en exécutant la commande uncatolog-SmBackupWithOracleRMAN. Vous ne pouvez pas supprimer les informations du catalogue à l'aide de l'interface graphique de SnapCenter. Toutefois, les informations d'une sauvegarde cataloguée sont supprimées lors de la suppression de la sauvegarde ou lors de la suppression de la rétention et du groupe de ressources associés à cette sauvegarde cataloguée.



Lorsque vous forcez la suppression de l'hôte SnapCenter, les informations des sauvegardes cataloguées associées à cet hôte ne sont pas supprimées. Vous devez supprimer les informations de toutes les sauvegardes cataloguées de cet hôte avant de forcer la suppression de l'hôte.

Si le catalogage et le décatalogage échoue parce que le temps d'opération a dépassé la valeur de temporisation spécifiée pour le paramètre ORACLE\_PLUGIN\_RMAN\_CATALOG\_TIMEOUT, vous devez modifier la valeur du paramètre en exécutant la commande suivante :

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Après avoir modifié la valeur du paramètre, redémarrer le service SnapCenter Plug-in Loader (SPL) en exécutant la commande suivante :

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

Les informations concernant les paramètres qui peuvent être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant Get-Help nom\_commande. Vous pouvez également vous reporter à la ["Guide de référence sur les commandes du logiciel SnapCenter"](#).

### Variables d'environnement prédéfinies pour le prescripteur et le PostScript spécifiques à la sauvegarde

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez les scripts prescripteurs et postscripts lors de la création de stratégies de

sauvegarde. Cette fonctionnalité est prise en charge pour toutes les configurations Oracle, à l'exception de VMDK.

SnapCenter prédéfinit les valeurs des paramètres qui seront directement accessibles dans l'environnement où les scripts shell sont exécutés. Vous n'avez pas besoin de spécifier manuellement les valeurs de ces paramètres lors de l'exécution des scripts.

#### Variables d'environnement prédéfinies prises en charge pour la création de la stratégie de sauvegarde

- **SC\_JOB\_ID** indique l'ID de travail de l'opération.

Exemple : 256

- **SC\_ORACLE\_SID** spécifie l'identifiant système de la base de données.

Si l'opération implique plusieurs bases de données, le paramètre contient des noms de base de données séparés par un canal.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : NFSB32|NFSB31

- **SC\_HOST** spécifie le nom d'hôte de la base de données.

Pour RAC, le nom d'hôte sera le nom de l'hôte sur lequel la sauvegarde est effectuée.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : scsmohost2.gdl.englab.netapp.com

- **SC\_OS\_USER** spécifie le propriétaire du système d'exploitation de la base de données.

Les données seront formatées sous la forme <db1>@<osuser1>|<db2>@<osuser2>.

Exemple : NFSB31@oracle|NFSB32@oracle

- **SC\_OS\_GROUP** spécifie le groupe de systèmes d'exploitation de la base de données.

Les données seront formatées sous la forme <db1>@<osgroupe1>|<db2>@<osgroupe2>.

Exemple : NFSB31@install|NFSB32@oinstall

- **SC\_BACKUP\_TYPE** indique le type de sauvegarde (données en ligne complètes, données en ligne, journal en ligne, arrêt hors ligne, montage hors ligne)

Exemples :

- Pour une sauvegarde complète : ONLINEFULL
- Sauvegarde des données uniquement : ONLINEDEATA
- Pour la sauvegarde des journaux uniquement : ONLINELOG

- **SC\_BACKUP\_NAME** spécifie le nom de la sauvegarde.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : DATA@RG2\_scspr2417819002\_07-20-  
2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-  
2021\_12.16.48.9267\_1|AV@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267

- **SC\_BACKUP\_ID** spécifie l'ID de sauvegarde.

Ce paramètre sera renseigné pour les volumes d'application.

EXEMPLE : DATA@203|LOG@205|AV@207

- **SC\_ORACLE\_HOME** indique le chemin d'accès au répertoire racine Oracle.

Exemple :

NFSB32@/ora01/app/oracle/product/18.1.0/db\_1|NFSB31@/ora01/app/oracle/product/18.1.0/db\_1

- **SC\_BACKUP\_RETENTION** spécifie la période de conservation définie dans la stratégie.

Exemples :

- Pour une sauvegarde complète : toutes les heures|DONNÉES@JOURS:3|LOG@COUNT:4
- Pour la sauvegarde de données à la demande uniquement : OnDemand|DATA@COUNT:2
- Pour la sauvegarde du journal à la demande uniquement : OnDemand|LOG@COUNT:2

- **SC\_RESOURCE\_GROUP\_NAME** indique le nom du groupe de ressources.

Exemple : RG1

- **SC\_BACKUP\_POLICY\_NAME** indique le nom de la stratégie de sauvegarde.

Exemple : backup\_policy

- **SC\_AV\_NAME** spécifie les noms des volumes d'application.

Exemple : AV1|AV2

- **SC\_PRIMARY\_DATA\_VOLUME\_FULL\_PATH** spécifie le mappage de stockage du SVM vers le volume pour le répertoire des fichiers de données. Nom du volume parent des lun et des qtrees.

Les données sont formatées en tant que <db1>@<SVM1:volume Volume 1>|<db2>@<SVM2:Volume 2>.

Exemples :

- Pour 2 bases de données du même groupe de ressources :  
NFSB32@buck:/vol/svspr2417819002\_NFS\_CDB\_NFSB32\_DATA|NFSB31@buck:/vol/sspr2417819002\_NFS\_CDB\_NFSB31\_DATA
- Pour une base de données unique avec fichiers de données répartis sur plusieurs volumes :  
buck:/vol/sprs2417819002\_NFS\_CDB\_NFSB31\_DATA,herculus:/vol/sprs24819002\_NFS

- **SC\_PRIMARY\_ARCHIVELOGS\_VOLUME\_FULL\_PATH** spécifie le mappage de stockage du SVM vers le volume pour le répertoire des fichiers journaux. Nom du volume parent des lun et des qtrees.

Exemples :

- Pour une seule instance de base de données : buck:/vol/sprs24819002\_NFS\_CDB\_NFSB31\_REDO
- Pour plusieurs instances de base de données :

NFSB31@buck:/vol/svspr2417819002\_NFS\_CDB\_NFSB31\_REDO|NFSB32@buck:/vol/sspr24819002\_NFS\_CDB\_NFSB32\_REDO

- **SC\_PRIMARY\_FULL\_SNAPSHOT\_NAME\_FOR\_TAG** indique la liste des snapshots contenant le nom du système de stockage et le nom du volume.

Exemples :

- Pour une seule instance de base de données :  
buck:/vol/sprs24819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_sprs24819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/sprs2417819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_07\_21\_2021\_spr  
ice\_02.28.26.3973\_11\_1\_1\_1\_
- Pour plusieurs instances de base de données :  
NFSB32@buck:/vol/scros2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_spr24819002\_07-21-2021\_02.28.26.3973\_0,VOL/scrobuck:/vol/s24178002\_NFS\_CDB\_Sprick\_07\_21\_07\_Sprick\_2021\_Sm8241\_Sm82\_02.28.26.3973\_Sprick\_2021\_Sm802.28.26.3973\_Sm815001\_Smb\_SprickSprick\_21\_Sprick\_Sprick\_2021\_21\_Sm82Sprick\_Smb\_Sprick\_1241Sm82\_07\_02.28.26.3973\_Sprick\_1\_Sm82\_Smvol/Sprick\_Sprick\_Sprick\_SprickSprick

- **SC\_PRIMARY\_SNAPSHOT\_NAMES** spécifie les noms des snapshots primaires créés pendant la sauvegarde.

Exemples :

- Pour une seule instance de base de données : RG2\_scros2417819002\_07-21-2021\_02.28.26.3973\_0,RG2\_scrosspr2417819002\_07-21-2021\_02.28.26.3973\_1
- Pour plusieurs instances de base de données : NFSB32@RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,RG2\_scros2417819002\_07-21-2021\_02.28.26.3973\_1|NFSB31@RG2\_scspr2417819002\_07-21-2021\_02.28.26.3973\_0,RG2\_scrospr2417819002\_07-21-2021\_02.28.26.3973\_1
- Pour les instantanés de groupes de cohérence impliquant 2 volumes : cg3\_R80404CBEF5V1\_04-05-2021\_03.08.03.4945\_0\_bfc279cc-28ad-465c-9d60-5487ac17b25d\_2021\_4\_5\_3\_8\_58\_350

- **SC\_PRIMARY\_MOUNT\_POINTS** spécifie les détails du point de montage qui font partie de la sauvegarde.

Les détails incluent le répertoire sur lequel les volumes sont montés et non le parent immédiat du fichier en cours de sauvegarde. Dans le cas d'une configuration ASM, il s'agit du nom du groupe de disques.

Les données seront formatées sous la forme

<db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

Exemples :

- Pour une seule instance de base de données : /mnt/nfsdb3\_data,/mnt/nfsdb3\_log,/mnt/nfsdb3\_data1
- Pour plusieurs instances de base de données :  
NFSB31@/mnt/nfsdb31\_data,/mnt/nfsdb31\_log,/mnt/nfsdb31\_data1|NFSB32@/mnt/nfsdb32\_data,/mnt/nfsdb32\_log,/mnt/nfsdb32\_data1
- POUR ASM: +DATA2DG,+LOG2DG

- **SC\_PRIMARY\_SNAPSHOTS\_AND\_MOUNT\_POINTS** spécifie les noms des snapshots créés lors de la sauvegarde de chacun des points de montage.

Exemples :

- Pour une seule base de données, par exemple : RG2\_scros2417819002\_07-21-

2021\_02.28.26.3973\_0:/mnt/nfsb32\_data,RG2\_sms2417819002\_07-21-  
2021\_02.28.26.3973:/mnt/nfsb31\_log

- Pour plusieurs instances de base de données : NFSB32@RG2\_scspr2417819002\_07-21-  
2021\_02.28.26.3973\_0:/mnt/nfsb32\_data,RG2\_sms24819002\_07-21-  
2021\_02.28.26.3973:/mnt/nfsb31\_log|NFSB31@RG2\_scspr2417819002\_07-21-  
2021\_02.28.26.3973\_0:/mnt/nfsb31\_data,RG2\_sms24819002\_07\_21\_fnfn\_2021\_\_\_\_02.28.26.3973\_f  
mfn\_

- **SC\_ARCHIVELOGS\_LOCATIONS** indique l'emplacement du répertoire des journaux d'archives.

Les noms de répertoire seront le parent immédiat des fichiers journaux d'archive. Si les journaux d'archive sont placés à plusieurs emplacements, tous les emplacements seront capturés. Cela inclut également les scénarios de FRA. Si des liens logiciels sont utilisés pour le répertoire, le même nom sera renseigné.

Exemples :

- Pour une base de données unique sur NFS : /mnt/nfsdb2\_log
- Pour plusieurs bases de données sur NFS et pour les journaux d'archive de base de données NFSB31 qui sont placés à deux emplacements différents :  
NFSB31@/mnt/nfsdb31\_log1,/mnt/nfsdb31\_log2|NFSB32@/mnt/nfsdb32\_log
- POUR ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021\_07\_15

- **SC\_REDO\_LOGS\_LOCATIONS** indique l'emplacement du répertoire des journaux de reprise.

Les noms de répertoire seront le parent immédiat des fichiers journaux de reprise. Si des liens logiciels sont utilisés pour le répertoire, le même nom sera renseigné.

Exemples :

- Pour une base de données unique sur NFS : /mnt/nfsdb2\_data/newdb1
- Pour plusieurs bases de données sur NFS :  
NFSB31@/mnt/nfsdb31\_data/newdb31|NFSB32@/mnt/nfsdb32\_data/newdb32
- POUR ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC\_CONTROL\_FILES\_LOCATIONS** indique l'emplacement du répertoire des fichiers de contrôle.

Les noms de répertoire seront le parent immédiat des fichiers de contrôle. Si des liens logiciels sont utilisés pour le répertoire, le même nom sera renseigné.

Exemples :

- Pour une base de données unique sur NFS : /mnt/nfsdb2\_data/fra/newdb1,/mnt/nfsdb2\_data/newdb1
- Pour plusieurs bases de données sur NFS :  
NFSB31@/mnt/nfsdb31\_data/fra/newdb31,/mnt/nfsdb31\_data/newdb31|NFSB32@/mnt/nfsdb32\_data/f  
ra/newdb32,/mnt/nfsdb32\_data/newdb32
- POUR ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC\_DATA\_FILES\_LOCATIONS** indique l'emplacement du répertoire des fichiers de données.

Les noms de répertoire seront le parent immédiat des fichiers de données. Si des liens logiciels sont utilisés pour le répertoire, le même nom sera renseigné.

Exemples :

- Pour une base de données unique sur NFS : /mnt/nfsdb3\_data1,/mnt/nfsdb3\_data/NEWDB3/fichier de données
  - Pour plusieurs bases de données sur NFS : NFSB31@/mnt/nfsdb31\_data1,/mnt/nfsdb31\_data/NEWDB31/datafiles|NFSB32@/mnt/nfsdb32\_data1,/mnt/nfsdb32\_data/NEWDB32/datafiles
  - POUR ASM: +DATA2DG/ASMDB2/FICHER DE DONNÉES,+DATA2DG/ASMDB2/TEMPFILE
- **SC\_SNAPSHOT\_LABEL** spécifie le nom des étiquettes secondaires.

Exemples : étiquette horaire, quotidienne, hebdomadaire, mensuelle ou personnalisée.

#### Délimiteurs pris en charge

- : est utilisé pour séparer le nom du SVM et le nom du volume

Exemple : buck:/vol/scros2417819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_scrosspr2417819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/sprs24819002\_NFS\_SB32\_REDO/RG2\_scro8002\_07\_21\_2021\_02.28.26.3973\_\_1\_11\_1\_1\_1\_1\_1\_1

- @ est utilisé pour séparer les données de son nom de base de données et pour séparer la valeur de sa clé.

Exemples :

- NFSB32@buck:/vol/sspr24819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_sspr24819002\_07-21-2021\_0,buck:/vol/sspr24819002\_NFS\_NFS\_CDB\_NFS3232\_REDO/RG2\_RS19002\_21\_02.28.26.3973\_3\_Sprick\_07\_07\_02.28.26.3973\_Sprick\_02.28.26.3973\_2021\_2021\_Sprick\_2021\_1241\_Sm8241\_SB81Sprick21\_Sm821\_Sprick1241Smvol/Sprick\_Smvol/Sprick\_1241\_Sm8207\_Smvol/Sm82\_Smvol/Smb\_1241\_Sm82\_Smb\_\_02.28.26.3973
- NFSB31@oracle|NFSB32@oracle

- | est utilisé pour séparer les données entre deux bases de données différentes et pour séparer les données entre deux entités différentes pour les paramètres SC\_BACKUP\_ID, SC\_BACKUP\_RETENTION et SC\_BACKUP\_NAME.

Exemples :

- DATA@203|LOG@205
- HORAIRE|DATA@DAYS:3|LOG@COUNT:4
- DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1

- / est utilisé pour séparer le nom du volume de son instantané pour SC\_PRIMARY\_SNAPSHOT\_NAMES et les paramètres SC\_PRIMARY\_FULL\_SNAPSHOT\_NAME\_FOR\_TAG.

Exemple : NFSB32@buck:/vol/scrosspr24819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_sspr24819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/scros24819002\_NFS\_CDB\_NFSB32\_REDO/RG2\_07\_21\_2021\_02.28.26.39731\_11\_1\_1\_1\_fSC1\_fSC1\_fte

- , est utilisé pour séparer un ensemble de variables pour le même DB.

Exemple : NFSB32@buck:/vol/sspr24819002\_NFS\_CDB\_NFSB32\_DATA/RG2\_sspr24819002\_07-21-2021\_02.28.26.3973\_0,buck:/vol/sspr24819002\_NFS\_CDB\_RS242\_REDO/RS241\_21\_Sprick\_2021\_07\_07\_Sprick\_02.28.26.3973\_02.28.26.3973\_2021\_1241Sprick\_1241\_Sm82\_Sm82Sprick\_21\_Sm82Sprick\_07

## Options de conservation des sauvegardes

Vous pouvez choisir le nombre de jours pendant lesquels vous souhaitez conserver les copies de sauvegarde ou spécifier le nombre de copies de sauvegarde à conserver, dans un maximum de 255 copies ONTAP. Par exemple, votre entreprise peut avoir besoin de conserver 10 jours de copies de sauvegarde ou 130 copies de sauvegarde.

Lors de la création d'une stratégie, vous pouvez spécifier les options de rétention pour le type de sauvegarde et le type de planification.

Si vous configurez la réplication SnapMirror, la règle de conservation est mise en miroir sur le volume de destination.

SnapCenter supprime les sauvegardes conservées dont les étiquettes de conservation correspondent au type de planification. Si le type de planification a été modifié pour la ressource ou le groupe de ressources, les sauvegardes avec l'ancienne étiquette de type de planification peuvent rester sur le système.



Pour la conservation à long terme des copies de sauvegarde, nous vous recommandons d'utiliser la sauvegarde SnapVault.

## Planifications de sauvegarde

La fréquence de sauvegarde (type de planification) est spécifiée dans les stratégies ; un planning de sauvegarde est spécifié dans la configuration du groupe de ressources. Le facteur le plus important dans la détermination d'une fréquence ou d'un planning de sauvegarde est le taux de changement pour la ressource et l'importance des données. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. Parmi les autres facteurs figurent l'importance de la ressource pour votre organisation, votre contrat de niveau de service (SLA) et votre objectif de point de récupération (RPO).

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés au service, notamment la disponibilité et les performances de celui-ci. Un RPO définit la stratégie selon laquelle les fichiers doivent être récupérés à partir du stockage de sauvegarde afin que des opérations régulières puissent reprendre après une défaillance. Les SLA et RPO contribuent à la stratégie de protection des données.

Même avec une ressource largement utilisée, il n'est pas nécessaire d'exécuter une sauvegarde complète plus d'une fois ou deux fois par jour. Par exemple, des sauvegardes régulières du journal de transactions peuvent suffire pour vous assurer que vous disposez des sauvegardes dont vous avez besoin. Plus vous sauvegardez des bases de données, plus le nombre de journaux de transaction que SnapCenter doit utiliser au moment de la restauration est élevé, ce qui accélère les opérations de restauration.

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes

La fréquence de sauvegarde (fréquence d'exécution des sauvegardes), appelée *schedule type* pour certains plug-ins, fait partie d'une configuration de stratégie. Vous pouvez sélectionner la fréquence de

sauvegarde horaire, quotidienne, hebdomadaire ou mensuelle de la police. Si vous ne sélectionnez aucune de ces fréquences, la règle créée est une stratégie à la demande uniquement. Vous pouvez accéder aux stratégies en cliquant sur **Paramètres > stratégies**.

- Planifications de sauvegarde

Les planifications de sauvegarde (exactement quand les sauvegardes doivent être effectuées) font partie d'une configuration de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour sauvegarder chaque jeudi à 10 h 00. Vous pouvez accéder aux planifications de groupes de ressources en cliquant sur **Ressources > groupes de ressources**.

## Nomenclature établie des sauvegardes

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.
- *03-12-2015\_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, `clienttext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

## Conditions requises pour la sauvegarde d'une base de données Oracle

Avant de sauvegarder une base de données Oracle, assurez-vous que les prérequis sont terminés.

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « `napmirror All` ». Toutefois, si vous utilisez le rôle « `vsadmin` », le privilège « `napmirror all` » n'est pas requis.
- Vous devez avoir attribué l'agrégat utilisé par l'opération de sauvegarde à la machine virtuelle de stockage

(SVM) utilisée par la base de données.

- Vous devez avoir vérifié que tous les volumes de données et de journaux d'archivage appartenant à la base de données sont protégés si la protection secondaire est activée pour cette base de données.
- Vous devriez avoir vérifié que la base de données contenant des fichiers sur les groupes de disques ASM doit être à l'état "MONTANT" ou "OPEN" pour vérifier ses sauvegardes à l'aide de l'utilitaire DBVERIFY d'Oracle.
- Vous devez avoir vérifié que la longueur du point de montage du volume ne dépasse pas 240 caractères.
- Vous devez augmenter la valeur de RESTTimeout à 86400000 ms dans la valeur `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config` file de l'hôte SnapCenter Server, si la base de données en cours de sauvegarde est importante (taille en To).

Lors de la modification des valeurs, assurez-vous qu'il n'y a pas de travaux en cours d'exécution et redémarrez le service SnapCenter SMCore après avoir augmenté la valeur.

## Découvrez les bases de données Oracle disponibles pour la sauvegarde

Les ressources sont des bases de données Oracle sur l'hôte géré par SnapCenter. Vous pouvez ajouter ces bases de données à des groupes de ressources pour exécuter des opérations de protection des données après avoir découvert les bases de données disponibles.

### Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes, la création de connexions au système de stockage et l'ajout d'informations d'identification.
- Si les bases de données résident sur un VMDK (Virtual machine Disk) ou RDM (Raw Device Mapping), vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter.

Pour plus d'informations, voir "[Déployez le plug-in SnapCenter pour VMware vSphere](#)".

- Si les bases de données résident sur un système de fichiers VMDK, vous devez vous connecter à vCenter et naviguer vers **VM options > Advanced > Edit configuration** pour définir la valeur de `disk.enableUUID` sur true pour la machine virtuelle.
- Vous devez avoir examiné le processus qui suit par SnapCenter pour découvrir différents types et versions de bases de données Oracle.

## Étape 1 : empêcher SnapCenter de découvrir des entrées ne provenant pas de la base de données

Vous pouvez empêcher SnapCenter de découvrir les entrées non-base de données ajoutées dans le fichier `oratab`.

### Étapes

1. Après avoir installé le plug-in pour Oracle, l'utilisateur root doit créer le fichier `sc_oratab.config` sous le répertoire `/var/opt/snapcenter/sco/etc/`.

Accordez l'autorisation d'écriture au propriétaire et au groupe binaire Oracle afin que le fichier puisse être conservé à l'avenir.

2. L'administrateur de base de données doit ajouter les entrées non-base de données dans le fichier `sc_oratab.config`.

Il est recommandé de conserver le même format défini pour les entrées non-base de données dans le fichier `/etc/oratab` ou l'utilisateur peut simplement ajouter la chaîne d'entité non-base de données.



La chaîne est sensible à la casse. Tout texte avec `#` au début est traité comme un commentaire. Le commentaire peut être ajouté après le nom d'une autre base de données.

```
For example:

Sample entries
Each line can have only one non-database name
These are non-database name
oratar # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N

```

### 3. Découvrir les ressources.

Les entrées non-base de données ajoutées dans `sc_oratab.config` ne sont pas répertoriées dans la page Ressources.



Il est toujours recommandé de sauvegarder le fichier `sc_oratab.config` avant de mettre à niveau le plug-in SnapCenter.

## Étape 2 : découverte des ressources

Après avoir installé le plug-in, toutes les bases de données de cet hôte sont automatiquement découvertes et affichées sur la page Ressources.

Les bases de données doivent être au moins dans l'état monté ou au-dessus pour que la découverte des bases de données puisse réussir. Dans un environnement Oracle Real application clusters (RAC), l'instance de base de données RAC de l'hôte où la découverte est effectuée doit être au moins dans l'état montée ou au-dessus pour que la découverte de l'instance de base de données puisse réussir. Seules les bases de données découvertes avec succès peuvent être ajoutées aux groupes de ressources.

Si vous avez supprimé une base de données Oracle sur l'hôte, le serveur SnapCenter ne sera pas conscient et répertorie la base de données supprimée. Vous devez actualiser manuellement les ressources pour mettre à jour la liste des ressources SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.

Cliquez sur  [icône filtre], puis sélectionnez le nom d'hôte et le type de base de données pour filtrer les ressources. Vous pouvez alors cliquer sur l'icône `imagfilter_icon.gif[filter icon]_icon.png` pour fermer le volet de filtre.

### 3. Cliquez sur **Actualiser les ressources**.

Dans un scénario RAC One Node, la base de données est découverte comme base de données RAC sur le nœud où elle est actuellement hébergée.

## Résultats

Les bases de données s'affichent avec des informations telles que le type de base de données, le nom d'hôte ou de cluster, les groupes de ressources et les stratégies associés et l'état.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

- Si la base de données se trouve sur un système de stockage autre que NetApp, l'interface utilisateur affiche un message de sauvegarde non disponible dans la colonne État global.

Vous ne pouvez pas effectuer d'opérations de protection des données sur la base de données se résidant sur un système de stockage non NetApp.

- Si la base de données se trouve sur un système de stockage NetApp et qu'elle n'est pas protégée, l'interface utilisateur affiche un message non protégé dans la colonne Total Status.
- Si la base de données est sur un système de stockage NetApp et protégée, l'interface utilisateur affiche un message disponible pour la sauvegarde dans la colonne État global.



Si vous avez activé l'authentification d'une base de données Oracle, une icône de cadenas rouge s'affiche dans la vue Ressources. Vous devez configurer les informations d'identification de la base de données pour pouvoir protéger la base de données ou l'ajouter au groupe de ressources pour effectuer des opérations de protection des données.

## Créez des règles de sauvegarde pour les bases de données Oracle

Avant d'utiliser SnapCenter pour sauvegarder les ressources de la base de données Oracle, vous devez créer une stratégie de sauvegarde pour la ressource ou le groupe de ressources à sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes. Vous pouvez également spécifier les paramètres de réplication, de script et de type de sauvegarde. La création d'une stratégie permet de gagner du temps lorsque vous souhaitez réutiliser la stratégie sur une autre ressource ou un autre groupe de ressources.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.
- Vous devez être prêt pour la protection des données en exécutant des tâches telles que l'installation d'SnapCenter, l'ajout d'hôtes, la détection de bases de données et la création de connexions du système de stockage.
- Si vous répliquez des snapshots sur un stockage secondaire de copie miroir ou d'archivage sécurisé, l'administrateur SnapCenter doit vous avoir assigné les SVM pour les volumes source et de destination.
- Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

- Vérifiez les prérequis et les limites spécifiques de la synchronisation active SnapMirror. Pour plus d'informations, reportez-vous à "[Limites d'objet pour la synchronisation active SnapMirror](#)".

## Description de la tâche

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.

La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.

Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Sélectionnez **Oracle Database** dans la liste déroulante.
4. Cliquez sur **Nouveau**.
5. Dans la page Nom, entrez le nom et les détails de la stratégie.
6. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez votre type de stockage.
  - b. Sélectionner la portée de la règle :
    - Si vous souhaitez **créer une sauvegarde en ligne**, sélectionnez **sauvegarde en ligne**.

Vous devez indiquer si vous souhaitez sauvegarder tous les fichiers de données, les fichiers de contrôle et les fichiers journaux d'archivage, uniquement les fichiers de données et les fichiers de contrôle, ou uniquement les fichiers journaux d'archivage.
    - Si vous souhaitez **créer une sauvegarde hors ligne**, sélectionnez **sauvegarde hors ligne**, puis sélectionnez l'une des options suivantes :
      - Si vous souhaitez créer une sauvegarde hors ligne lorsque la base de données est à l'état monté, sélectionnez **Mount**.
      - Si vous souhaitez créer une sauvegarde d'arrêt hors ligne en changeant l'état d'arrêt de la base de données, sélectionnez **Shutdown**.
  - c. Si vous souhaitez cataloguer la sauvegarde à l'aide d'Oracle Recovery Manager (RMAN), sélectionnez **sauvegarde de catalogue avec Oracle Recovery Manager (RMAN)**.

Vous pouvez effectuer le catalogage différé d'une sauvegarde à la fois à l'aide de l'interface utilisateur graphique ou à l'aide de la commande SnapCenter CLI `Catalog-SmBackupWithOracleRMAN`.



Si vous souhaitez cataloguer les sauvegardes d'une base de données RAC, assurez-vous qu'aucune autre tâche n'est en cours d'exécution pour cette base de données. Si un autre travail est en cours d'exécution, l'opération de catalogage échoue au lieu d'être mise en file d'attente.

d. Si vous souhaitez élaguer les journaux d'archive après la sauvegarde, sélectionnez **Prune archive logs après la sauvegarde**.



L'élagage des journaux d'archive de la destination du journal d'archivage qui n'est pas configurée dans la base de données sera ignoré.



Si vous utilisez Oracle Standard Edition, vous pouvez utiliser LES paramètres `LOG_ARCHIVE_DEST` et `LOG_ARCHIVE_DUPLEX_DEST` lors de la sauvegarde du journal d'archivage.

- Vous ne pouvez supprimer les journaux d'archive que si vous avez sélectionné les fichiers journaux d'archive dans le cadre de votre sauvegarde.



Vous devez vous assurer que tous les nœuds d'un environnement RAC peuvent accéder à tous les emplacements du journal d'archivage pour que l'opération de suppression soit réussie.

Les fonctions que vous recherchez...	Alors...
Supprimer tous les journaux d'archive	Sélectionnez <b>Supprimer tous les journaux d'archive</b> .
Supprimer les journaux d'archive plus anciens	Sélectionnez <b>Supprimer les journaux d'archive plus anciens que</b> , puis spécifiez l'âge des journaux d'archive à supprimer en jours et en heures.
Supprimer les journaux d'archive de toutes les destinations	Sélectionnez <b>Supprimer les journaux d'archive de toutes les destinations</b> .
Supprimez les journaux d'archivage des destinations de journaux qui font partie de la sauvegarde	Sélectionnez <b>Supprimer les journaux d'archive des destinations qui font partie de la sauvegarde</b> .

+

Prune archive logs after backup

#### Prune log retention setting

Delete all archive logs

Delete archive logs older than

#### Prune log destination setting

Delete archive logs from all the destinations

Delete archive logs from the destinations which are part of backup

7. Dans la page instantané et réplication, effectuez les opérations suivantes :

a. Spécifiez la fréquence d'horaire en sélectionnant **sur demande, horaire, quotidien, hebdomadaire** ou **mensuel**.



Vous pouvez spécifier le planning (date de début et date de fin) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais vous permet d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

b. Dans la section Paramètres de rétention des instantanés de données, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionné dans la page Type de sauvegarde :

Les fonctions que vous recherchez...

Alors...

<p>Conserver un certain nombre d'instantanés</p>	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> <p> Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> </div>
<p>Conserver les instantanés pendant un certain nombre de jours</p>	<p>Sélectionnez <b>conserver les copies pour</b>, puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.</p>
<p>Période de verrouillage des copies Snapshot principales</p>	<p>Si vous souhaitez spécifier la période de verrouillage de la copie d'instantané principale, sélectionnez <b>période de verrouillage de la copie d'instantané principale</b> et sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>
<p>Période de verrouillage des copies Snapshot secondaires</p>	<p>Si vous souhaitez spécifier la période de verrouillage de la copie d'instantané secondaire, sélectionnez <b>période de verrouillage de la copie d'instantané secondaire</b>, puis sélectionnez jours, mois ou années.</p>



Vous ne pouvez conserver les sauvegardes du journal d'archivage que si vous avez sélectionné les fichiers journaux d'archive dans le cadre de votre sauvegarde.

- c. Dans la section Paramètres de conservation des instantanés du journal d'archivage, spécifiez les paramètres de conservation pour le type de sauvegarde et le type de planification sélectionnés dans la page Type de sauvegarde :

Les fonctions que vous recherchez...	Alors...
Conserver un certain nombre d'instantanés	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;"> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> <p> Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> </div>
Conserver les instantanés pendant un certain nombre de jours	Sélectionnez <b>conserver les copies pour</b> , puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage des copies Snapshot principales	<p>Si vous souhaitez spécifier la période de verrouillage de la copie d'instantané principale, sélectionnez <b>période de verrouillage de la copie d'instantané principale</b> et sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>

Période de verrouillage des copies Snapshot secondaires	Si vous souhaitez spécifier la période de verrouillage de la copie d'instantané secondaire, sélectionnez <b>période de verrouillage de la copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.
---------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Vous ne pouvez conserver les sauvegardes du journal d'archivage que si vous avez sélectionné les fichiers journaux d'archive dans le cadre de votre sauvegarde.

d. Sélectionnez le libellé de la stratégie.

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

8. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
Mettre à jour SnapMirror après la création d'un Snapshot local	<p>Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).</p> <p>Cette option doit être activée pour la synchronisation active SnapMirror.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p>

Pour ce champ...	Procédez comme ça...
Mettre à jour SnapVault après avoir créé un instantané local	<p>Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton <b>Actualiser</b> de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, voir <a href="#">"Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé"</a></p> <p>Voir <a href="#">"Afficher les sauvegardes et clones des bases de données Oracle sur la page topologie"</a>.</p>
Nombre de tentatives d'erreur	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

9. Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript que vous souhaitez exécuter avant ou après l'opération de sauvegarde, respectivement.

Vous devez stocker les scripts prescripteurs et postscripts dans `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin d'accès. Par défaut, le chemin `/var/opt/snapcenter/spl/scripts` est renseigné. Si vous avez créé des dossiers dans ce chemin pour stocker les scripts, vous devez spécifier ces dossiers dans le chemin d'accès.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est 60 secondes.

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript. ["En savoir plus >>"](#)

10. Dans la page Vérification, effectuez les opérations suivantes :
  - a. Sélectionnez le planning de sauvegarde pour lequel vous souhaitez effectuer l'opération de vérification.
  - b. Dans la section commandes du script de vérification, entrez le chemin et les arguments du prescripteur ou du PostScript que vous souhaitez exécuter avant ou après l'opération de vérification, respectivement.

Vous devez stocker les scripts prescripteurs et postscripts dans `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin d'accès. Par défaut, le chemin `/var/opt/snapcenter/spl/scripts` est renseigné. Si vous avez créé des dossiers dans ce chemin pour stocker les scripts, vous devez spécifier ces dossiers dans le chemin d'accès.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est 60 secondes.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et associez des stratégies pour les bases de données Oracle

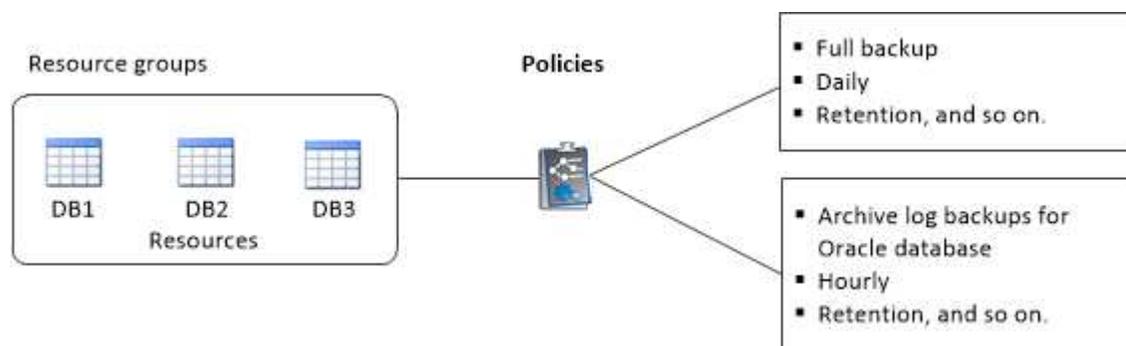
Un groupe de ressources est un conteneur dans lequel vous ajoutez des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée.

### Description de la tâche

- Une base de données contenant des fichiers dans des groupes de disques ASM doit être à l'état "MOUNT" ou "OPEN" pour vérifier ses sauvegardes à l'aide de l'utilitaire Oracle DBVERIFY.

Associez une ou plusieurs règles au groupe de ressources pour définir le type de tâche de protection des données à exécuter.

L'image suivante illustre la relation entre les ressources, les groupes de ressources et les politiques des bases de données :



- Pour les règles activées par SnapLock, pour ONTAP 9.12.1 et versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- L'ajout de nouvelles bases de données sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec la synchronisation active SnapMirror n'est pas pris en charge.
- L'ajout de nouvelles bases de données à un groupe de ressources existant en mode de basculement de la synchronisation active SnapMirror n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement à l'état normal ou de retour arrière.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans Oracle, y compris le préfixe.

4. Dans la page Ressources, sélectionnez un nom d'hôte de base de données Oracle dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources de la section Ressources disponibles et déplacez-les vers la section Ressources sélectionnées.



Vous pouvez ajouter des bases de données à partir d'hôtes Linux et AIX dans un seul groupe de ressources.

6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.

7. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.

- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec

les planifications de sauvegarde SnapCenter.

8. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.
- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire des ressources Oracle sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

## Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

- a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

- a. Sélectionnez le type de la règle de réplication.



Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.
- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.



Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .

Les fonctions que vous recherchez...	Procédez comme ça...
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.
- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Sauvegarder les ressources Oracle

Si une ressource ne fait pas partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste vue.
3. Cliquez sur , puis sélectionnez le nom d'hôte et le type de base de données pour filtrer les ressources.

Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

4. Sélectionnez la base de données à sauvegarder.

La page protéger la base de données s'affiche.

5. Dans la page Ressources, effectuez les opérations suivantes :
  - a. Cochez la case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple : `customtext_policy_hostname` ou `resource_hostname`. Par défaut, un horodatage est ajouté au nom du Snapshot.

- b. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.
6. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.

Vous pouvez créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer un planning pour la stratégie souhaitée.
- c. Dans la fenêtre Ajouter des plannings pour la règle *nom\_règle*, configurez la planification, puis sélectionnez OK.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Load locators** pour charger les volumes SnapMirror ou SnapVault afin de vérifier le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les programmes pour configurer le planning de vérification pour tous les types de planification de la stratégie. + dans la boîte de dialogue Ajouter des planifications de vérification *nom\_règle*, vous pouvez effectuer les opérations suivantes :
- c. Sélectionnez **Exécuter la vérification après la sauvegarde**.
- d. Sélectionnez **Exécuter la vérification planifiée**, puis sélectionnez le type de planification dans la liste déroulante.



Dans une configuration Flex ASM, vous ne pouvez pas effectuer d'opération de vérification sur les nœuds Leaf si la cardinalité est inférieure au nombre de nœuds dans le cluster RAC.

- e. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le stockage secondaire.
- f. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

8. Dans la page notification, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails dans la liste déroulante **préférence de messagerie**.

Vous devez spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de sauvegarde effectuée sur la ressource, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `Set-SmSmtServer`.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

La page topologie de la base de données s'affiche.

10. Cliquez sur **Sauvegarder maintenant**.

11. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante Stratégie, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Une fois que vous avez terminé

- Dans le programme d'installation AIX, vous pouvez utiliser le `lkdev` pour verrouiller et `rendev` commande permettant de renommer les disques sur lesquels la base de données sauvegardée résidait.

Le verrouillage ou le changement de nom des périphériques n'affecte pas l'opération de restauration lors de la restauration à l'aide de cette sauvegarde.

- Si l'opération de sauvegarde échoue parce que le temps d'exécution de la requête de base de données a dépassé la valeur du délai, vous devez modifier la valeur DES paramètres `ORACLE_SQL_QUERY_TIMEOUT` et `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` en exécutant le `Set-SmConfigSettings` cmdlet :

Après avoir modifié la valeur des paramètres, redémarrez le service SnapCenter Plug-in Loader (SPL) en exécutant la commande suivante `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si le fichier n'est pas accessible et que le point de montage n'est pas disponible pendant le processus de vérification, l'opération peut échouer avec le code d'erreur DBV-00100 fichier spécifié. Vous devez modifier les valeurs des paramètres `VERIFICATION_DELAY` et `VERIFICATION_RETRY_COUNT` dans `sco.properties`.

Après avoir modifié la valeur des paramètres, redémarrez le service SnapCenter Plug-in Loader (SPL) en exécutant la commande suivante `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.
- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer.

Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, le `do_start method Command` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante : `Java -jar -Xmx8192M -Xms4096M`.

### Trouvez plus d'informations

- ["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)
- ["La base de données Oracle RAC One Node est ignorée pour effectuer les opérations SnapCenter"](#)
- ["Impossible de modifier l'état d'une base de données Oracle 12c ASM"](#)

- "Paramètres personnalisables pour les opérations de sauvegarde, de restauration et de clonage sur les systèmes AIX" (Connexion requise)

## Sauvegarder les groupes de ressources de la base de données Oracle

Un groupe de ressources est un ensemble de ressources sur un hôte ou un cluster. L'opération de sauvegarde est effectuée sur toutes les ressources définies dans le groupe de ressources.

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont créées en fonction de la planification.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Entrez le nom du groupe de ressources dans la zone de recherche ou cliquez sur , puis sélectionnez la balise.

Cliquez sur  pour fermer le volet de filtre.

4. Dans la page Groupe de ressources, sélectionnez le groupe de ressources à sauvegarder.



Si vous disposez d'un groupe de ressources fédéré avec deux bases de données et que l'une d'entre elles contient des données sur un système de stockage non NetApp, l'opération de sauvegarde est abandonnée même si l'autre base de données se trouve sur un système de stockage NetApp.

5. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si plusieurs stratégies sont associées au groupe de ressources, sélectionnez la stratégie de sauvegarde que vous souhaitez utiliser dans la liste déroulante **Stratégie**.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

6. Surveillez la progression en sélectionnant **Monitor > Jobs**.

### Une fois que vous avez terminé

- Dans le programme d'installation AIX, vous pouvez utiliser le `lkdev` pour verrouiller et `rendev` commande permettant de renommer les disques sur lesquels la base de données sauvegardée résidait.

Le verrouillage ou le changement de nom des périphériques n'affecte pas l'opération de restauration lors de la restauration à l'aide de cette sauvegarde.

- Si l'opération de sauvegarde échoue parce que le temps d'exécution de la requête de base de données a dépassé la valeur du délai, vous devez modifier la valeur DES paramètres `ORACLE_SQL_QUERY_TIMEOUT` et `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` en exécutant le `Set-SmConfigSettings` cmdlet :

Après avoir modifié la valeur des paramètres, redémarrez le service SnapCenter Plug-in Loader (SPL) en exécutant la commande suivante `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Si le fichier n'est pas accessible et que le point de montage n'est pas disponible pendant le processus de vérification, l'opération peut échouer avec le code d'erreur DBV-00100 fichier spécifié. Vous devez modifier les valeurs des paramètres VERIFICATION\_DELAY\_ et VERIFICATION\_RETRY\_COUNT dans sco.properties.

Après avoir modifié la valeur des paramètres, redémarrez le service SnapCenter Plug-in Loader (SPL) en exécutant la commande suivante `/opt/NetApp/snapcenter/spl/bin/spl restart`

## Surveillez la sauvegarde de la base de données Oracle

Découvrez comment surveiller la progression des opérations de sauvegarde et de protection des données.

### Surveillez les opérations de sauvegarde des bases de données Oracle

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

#### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

### Surveiller les opérations de protection des données dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

## Autres opérations de sauvegarde

### Sauvegarder les bases de données Oracle à l'aide des commandes UNIX

Le workflow de sauvegarde comprend la planification, l'identification des ressources de sauvegarde, la création de stratégies de sauvegarde, la création de groupes de ressources et la connexion de stratégies, la création de sauvegardes et le contrôle des opérations.

#### Ce dont vous aurez besoin

- Vous devez avoir ajouté les connexions du système de stockage et créé les informations d'identification à l'aide des commandes *Add-SmStorageConnection* et *Add-SmCredential*.
- Vous devez avoir établi la session de connexion avec le serveur SnapCenter à l'aide de la commande *Open-SmConnection*.

Vous ne pouvez avoir qu'une seule session de connexion de compte SnapCenter et le token est stocké dans le répertoire d'accueil de l'utilisateur.



La session de connexion n'est valide que pendant 24 heures. Cependant, vous pouvez créer un jeton avec l'option *TokenNeverExpires* pour créer un jeton qui n'expire jamais et la session sera toujours valide.

#### À propos de cette tâche

Vous devez exécuter les commandes suivantes pour établir la connexion avec le serveur SnapCenter,

découvrir les instances de base de données Oracle, ajouter une stratégie et un groupe de ressources, sauvegarder et vérifier la sauvegarde.

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également vous reporter à la "[Guide de référence sur les commandes du logiciel SnapCenter](#)".

## Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié : *Open-SmConnection*
2. Effectuer une opération de découverte des ressources hôte : *get-SmResources*
3. Configurer les informations d'identification de la base de données Oracle et les nœuds préférés pour le fonctionnement de sauvegarde d'une base de données RAC (Real application Cluster) : *Configure-SmOracleDatabase*
4. Créez une stratégie de sauvegarde : *Add-SmPolicy*
5. Récupérez les informations sur l'emplacement de stockage secondaire (SnapVault ou SnapMirror) : *get-SmDeuxièmement\_Details*

Cette commande récupère les détails de mappage du stockage principal vers le stockage secondaire d'une ressource spécifiée. Vous pouvez utiliser les détails de mappage pour configurer les paramètres de vérification secondaires lors de la création d'un groupe de ressources de sauvegarde.

6. Ajoutez un groupe de ressources à SnapCenter : *Add-SmResourceGroup*
7. Créer une sauvegarde : *New-SmBackup*

Vous pouvez interroger le travail à l'aide de l'option `WaitForCompletion`. Si cette option est spécifiée, la commande continue à interroger le serveur jusqu'à la fin de la procédure de sauvegarde.

8. Récupérez les journaux depuis SnapCenter : *get-SmLogs*

## Annuler les opérations de sauvegarde des bases de données Oracle

Vous pouvez annuler les opérations de sauvegarde en cours d'exécution, en file d'attente ou non réactives.

Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâche pour annuler les opérations de sauvegarde.

### À propos de cette tâche

Lorsque vous annulez une opération de sauvegarde, le serveur SnapCenter arrête l'opération et supprime tous les snapshots du stockage si la sauvegarde créée n'est pas enregistrée auprès du serveur SnapCenter. Si la sauvegarde est déjà enregistrée avec le serveur SnapCenter, elle ne peut pas revenir à l'instantané déjà créé même après le déclenchement de l'annulation.

- Vous pouvez annuler uniquement le journal ou l'opération de sauvegarde complète en attente ou en cours d'exécution.
- Vous ne pouvez pas annuler l'opération après le début de la vérification.

Si vous annulez l'opération avant vérification, l'opération est annulée et l'opération de vérification ne sera pas effectuée.

- Vous ne pouvez pas annuler l'opération de sauvegarde après le démarrage des opérations de catalogue.
- Vous pouvez annuler une opération de sauvegarde à partir de la page moniteur ou du volet activité.
- Outre l'interface graphique de SnapCenter, vous pouvez utiliser les commandes de l'interface de ligne de commandes pour annuler des opérations.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

## Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>2. Sélectionnez l'opération et cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>1. Après avoir lancé la tâche de sauvegarde, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>2. Sélectionner l'opération.</li> <li>3. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

## Résultats

L'opération est annulée et la ressource est rétablie à l'état d'origine.

Si l'opération que vous avez annulée n'est pas réactive à l'état d'annulation ou d'exécution, vous devez exécuter `Annuler-SmJob -JobID <int> -forcer` pour arrêter l'opération de sauvegarde avec force.

## Afficher les sauvegardes et clones des bases de données Oracle sur la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire.

### À propos de cette tâche

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.

Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Si vous utilisez une relation secondaire comme SnapMirror actif Sync (initialement commercialisé sous la forme SnapMirror Business Continuity [SM-BC]), les icônes supplémentaires suivantes s'affichent :

-  Le site de réplica est en cours.
-  Le site de réplica est en panne.
-  La relation miroir ou coffre-fort secondaire n'a pas été rétablie.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologie de la ressource sélectionnée s'affiche.

4. Consultez la fiche récapitulative pour connaître le nombre de sauvegardes et de clones disponibles sur les stockages primaire et secondaire.

La section carte récapitulative affiche le nombre total de sauvegardes et de clones ainsi que le nombre total de sauvegardes de journaux.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration

SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Pour la synchronisation active SnapMirror, cliquez sur le bouton **Refresh** pour actualiser l'inventaire des sauvegardes SnapCenter en interrogeant ONTAP sur les sites principaux et de réplica. Une planification hebdomadaire effectue également cette activité pour toutes les bases de données contenant une relation de synchronisation active SnapMirror.

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations SnapMirror miroir asynchrone ou MirrorVault asynchrone vers la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir de ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.
  - Après le basculement, une sauvegarde doit être créée afin que SnapCenter puisse prendre connaissance du basculement. Vous ne pouvez cliquer sur **Rafraîchir** qu'après la création d'une sauvegarde.
5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer la restauration, le clonage, le montage, le démontage, le renommage, catalogue, décatalogue et suppression des opérations.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

- Si vous avez sélectionné une sauvegarde de journal, vous ne pouvez effectuer que renommer, monter, démonter, catalogue, décataloguer, les opérations de suppression et de suppression.
  - Si vous avez catalogué la sauvegarde à l'aide d'Oracle Recovery Manager (RMAN), vous ne pouvez pas renommer ces sauvegardes cataloguées.
7. Si vous souhaitez supprimer un clone, sélectionnez-le dans la table, puis cliquez sur .

Si la valeur attribuée à SnapmirrorStatusUpdateWaitTime est inférieure, les copies de sauvegarde Mirror et Vault ne sont pas répertoriées sur la page topologique, même si les volumes de données et de journaux sont protégés avec succès. Vous devez augmenter la valeur attribuée à SnapmirrorStatusUpdateWaitTime à l'aide de l'applet de commande `set-SmConfigSettings` PowerShell.

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`.

Vous pouvez également vous reporter à "[Guide de référence sur les commandes du logiciel SnapCenter](#)" ou "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Monter et démonter les sauvegardes de base de données

Vous pouvez monter une ou plusieurs sauvegardes de données et de journaux uniquement si vous souhaitez accéder aux fichiers de la sauvegarde. Vous pouvez

monter la sauvegarde sur le même hôte où la sauvegarde a été créée ou sur un hôte distant ayant le même type de configuration Oracle et d'hôte. Si vous avez monté les sauvegardes manuellement, vous devez les démonter manuellement une fois l'opération terminée. Dans n'importe quelle instance donnée, une sauvegarde d'une base de données peut être montée sur n'importe quel hôte. Lors de l'exécution d'une opération, vous ne pouvez monter qu'une seule sauvegarde.



Dans une configuration Flex ASM, vous ne pouvez pas effectuer une opération de montage sur les nœuds Leaf si la cardinalité est inférieure au nombre de nœuds dans le cluster RAC.

## Montez une sauvegarde de base de données

Vous devez monter manuellement une sauvegarde de base de données si vous souhaitez accéder aux fichiers de la sauvegarde.

### Ce dont vous aurez besoin

- Si vous disposez d'une instance de base de données ASM (Automatic Storage Management) dans un environnement NFS et souhaitez monter les sauvegardes ASM, vous devez avoir ajouté le chemin de disque ASM `/var/opt/snapcenter/sco/backup*///__` au chemin existant défini dans le paramètre `asm_diskstring`.
- Si vous disposez d'une instance de base de données ASM dans un environnement NFS et que vous souhaitez monter les sauvegardes de journaux ASM dans le cadre d'une opération de récupération, vous devez avoir ajouté le chemin de disque ASM `/var/opt/snapcenter/scu/clones//` au chemin existant défini dans le paramètre `asm_diskstring`.
- Dans le paramètre `asm_diskstring`, vous devez configurer `AFD:*` si vous utilisez ASMFD ou `ORCL:*` si vous utilisez ASMLIB.



Pour plus d'informations sur la modification du paramètre `asm_diskstring`, reportez-vous à la section "[Comment ajouter des chemins de disque à `asm\_diskstring`](#)".

- Vous devez configurer les informations d'identification ASM et le port ASM s'il diffère de l'hôte de la base de données source lors du montage de la sauvegarde.
- Si vous souhaitez monter sur un autre hôte, vous devez vérifier que l'autre hôte répond aux exigences suivantes :
  - Mêmes UID et GID que l'hôte d'origine
  - Même version Oracle que celle de l'hôte d'origine
  - Même distribution et version du système d'exploitation que celle de l'hôte d'origine
  - Pour NVMe, vous devez installer NVMe util
- Vous devez vous assurer que la LUN n'est pas mappée sur l'hôte AIX à l'aide d'iGroup composé de protocoles mixtes iSCSI et FC. Pour plus d'informations, voir "[L'opération échoue avec une erreur impossible de détecter le périphérique pour la LUN](#)".

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.

3. Sélectionnez la base de données dans la vue Détails de la base de données ou dans la vue Détails du groupe de ressources.

La page topologie de la base de données s'affiche.

4. Dans la vue gérer les copies, sélectionnez **sauvegardes** dans le système de stockage principal ou secondaire (en miroir ou répliqué).

5.

Sélectionnez la sauvegarde dans la table, puis cliquez sur .

6. Dans la page Mount Backups, sélectionnez l'hôte sur lequel vous souhaitez monter la sauvegarde dans la liste déroulante **Choisissez l'hôte pour monter la sauvegarde**.

Le chemin de montage `/var/opt/snapcenter/sco/backup_mount/backup_name/database_name` s'affiche.

Si vous montez la sauvegarde d'une base de données ASM, le chemin de montage `+diskgroupname_SID_backupid` s'affiche.

7. Cliquez sur **Mount**.

## Après la fin

- Vous pouvez exécuter la commande suivante pour extraire les informations relatives à la sauvegarde montée :

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- Si vous avez monté une base de données ASM, vous pouvez exécuter la commande suivante pour extraire les informations relatives à la sauvegarde montée :

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- Pour récupérer l'ID de sauvegarde, exécutez la commande suivante :

```
./sccli Get-Smbbackup-BackupNamebackup_name
```

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également vous reporter à "[Guide de référence sur les commandes du logiciel SnapCenter](#)".

## Démontez une sauvegarde de base de données

Vous pouvez démonter manuellement une sauvegarde de base de données montée lorsque vous ne souhaitez plus accéder aux fichiers de la sauvegarde.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données dans la vue Détails de la base de données ou dans la vue Détails du groupe de ressources.

La page topologie de la base de données s'affiche.

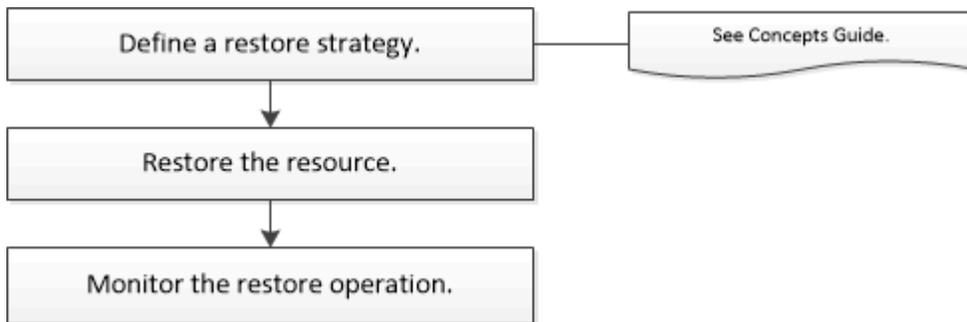
4. Sélectionnez la sauvegarde montée, puis cliquez sur .
5. Cliquez sur **OK**.

## Restaurez et récupérez les bases de données Oracle

### Restaurer le flux de travail

Le workflow de restauration inclut la planification, l'exécution des opérations de restauration et le contrôle des opérations.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



### Définissez une stratégie de restauration et de reprise pour les bases de données Oracle

Vous devez définir une stratégie avant de restaurer et de récupérer votre base de données pour que les opérations de restauration et de récupération soient effectuées avec succès.

#### Types de sauvegardes pris en charge pour les opérations de restauration et de restauration

SnapCenter prend en charge la restauration et la restauration de différents types de sauvegardes de bases de données Oracle.

- Sauvegarde des données en ligne
- Sauvegarde des données d'arrêt hors ligne
- Monter la sauvegarde des données hors ligne



Si vous restaurez un arrêt hors ligne ou une sauvegarde des données de montage hors ligne, SnapCenter conserve l'état hors ligne de la base de données. Vous devez récupérer manuellement la base de données et réinitialiser les journaux.

- Sauvegarde complète
- Sauvegardes hors ligne des bases de données de secours Data Guard
- Sauvegardes en ligne des bases de données de secours Active Data Guard uniquement



Vous ne pouvez pas effectuer la récupération des bases de données de secours Active Data Guard.

- Les sauvegardes de données en ligne, les sauvegardes complètes en ligne, les sauvegardes de montage hors ligne et les sauvegardes hors ligne dans une configuration RAC (Real application clusters)
- Sauvegardes de données en ligne, sauvegardes complètes en ligne, sauvegardes de montage hors ligne et sauvegardes d'arrêt hors ligne dans une configuration ASM (Automatic Storage Management)

## Types de méthodes de restauration pris en charge pour les bases de données Oracle

SnapCenter prend en charge la connexion et la copie ou la restauration sur place des bases de données Oracle. Lors d'une opération de restauration, SnapCenter détermine la méthode de restauration appropriée pour le système de fichiers à utiliser pour la restauration sans perte de données.



SnapCenter ne prend pas en charge la SnapRestore basée sur les volumes.

### Restauration de connexion et de copie

Si la disposition de la base de données diffère de celle de la sauvegarde ou si de nouveaux fichiers ont été créés après la création de la sauvegarde, la restauration de la connexion et de la copie est effectuée. Dans la méthode de restauration de connexion et de copie, les tâches suivantes sont effectuées :

#### Étapes

1. Le volume est cloné à partir de la copie Snapshot et la pile du système de fichiers est construite sur l'hôte à l'aide des LUN ou des volumes clonés.
2. Les fichiers sont copiés depuis les systèmes de fichiers clonés vers les systèmes de fichiers d'origine.
3. Les systèmes de fichiers clonés sont ensuite démontés de l'hôte et les volumes clonés sont supprimés de ONTAP.



Dans le cas d'une configuration Flex ASM (où la cardinalité est inférieure au nombre de nœuds dans le cluster RAC) ou de bases de données RAC ASM sur VMDK ou RDM, seule la méthode de restauration de connexion et de copie est prise en charge.

Même si vous avez activé avec force la restauration sur place, SnapCenter effectue des restaurations de connexion et de copie dans les scénarios suivants :

- Restauration à partir d'un système de stockage secondaire
- Restauration des groupes de disques ASM présents sur les nœuds d'une configuration Oracle RAC sur laquelle l'instance de base de données n'est pas configurée
- Dans la configuration d'Oracle RAC, sur l'un des nœuds homologues si l'instance ASM ou l'instance de cluster n'est pas exécutée ou si le nœud homologue est arrêté
- Restauration des fichiers de contrôle uniquement
- Restaurer un sous-ensemble d'espaces de stockage résidant sur un groupe de disques ASM
- Le groupe de disques est partagé entre les fichiers de données, le fichier sp et le fichier de mot de passe
- Le service SnapCenter Plug-in Loader (SPL) n'est pas installé ou ne s'exécute pas sur le nœud distant dans un environnement RAC
- Les nouveaux nœuds sont ajoutés à Oracle RAC et le serveur SnapCenter ne connaît pas les nouveaux

nœuds ajoutés

## Restauration sur place

Si l'infrastructure de la base de données est similaire à la sauvegarde et qu'aucune modification de configuration n'a été apportée sur la pile de stockage et de base de données, une restauration sur place est effectuée, dans laquelle la restauration du fichier ou de la LUN est effectuée sur ONTAP. SnapCenter prend uniquement en charge SFSR (Single File SnapRestore) dans le cadre de la méthode de restauration sur place.



NetApp ONTAP prend en charge la restauration sur place à partir d'un emplacement secondaire.

Si vous souhaitez effectuer une restauration sur place sur la base de données, assurez-vous que vous ne disposez que de fichiers de données sur le groupe de disques ASM. Vous devez créer une sauvegarde après avoir apporté des modifications au groupe de disques ASM ou à la structure physique de la base de données. Une fois la restauration sur place effectuée, le groupe de disques contiendra le même nombre de fichiers de données qu'au moment de la sauvegarde.

La restauration sur place sera automatiquement appliquée lorsque le groupe de disques ou le point de montage correspond aux critères suivants :

- Aucun nouveau fichier de données n'est ajouté après la sauvegarde (vérification de fichiers étrangers)
- Pas d'ajout, de suppression ou de création d'un disque ASM ou d'un LUN après sauvegarde (vérification des modifications structurelles du groupe de disques ASM)
- Pas d'ajout, de suppression ou de création de LUN au groupe de disques LVM (vérification des modifications structurelles du groupe de disques LVM)



Vous pouvez également activer avec force la restauration sur place à l'aide de l'interface graphique, de l'interface de ligne de commande SnapCenter ou de l'applet de commande PowerShell pour ignorer la vérification des fichiers étrangers et la vérification des modifications structurelles du groupe de disques LVM.

## Exécution d'une restauration sur place sur le RAC ASM

Dans SnapCenter, le nœud sur lequel vous effectuez la restauration est appelé nœud principal et tous les autres nœuds du RAC sur lequel réside le groupe de disques ASM sont appelés nœuds homologues. SnapCenter modifie l'état du groupe de disques ASM afin de démonter sur tous les nœuds où le groupe de disques ASM est à l'état de montage avant d'effectuer l'opération de restauration du stockage. Une fois la restauration du stockage terminée, SnapCenter modifie l'état du groupe de disques ASM comme il était avant l'opération de restauration.

Dans les environnements SAN, SnapCenter supprime les périphériques des nœuds homologues et effectue une opération de mappage des LUN avant l'opération de restauration du stockage. Une fois la restauration du stockage effectuée, SnapCenter exécute une opération de mappage de LUN et construit des périphériques sur tous les nœuds homologues. Dans un environnement SAN, si la disposition d'Oracle RAC ASM se trouve sur des LUN, pendant la restauration de SnapCenter effectue des opérations de mappage de LUN, de restauration de LUN et de mappage de LUN sur tous les nœuds du cluster RAC où réside le groupe de disques ASM. Avant de restaurer, même si tous les initiateurs des nœuds RAC n'étaient pas utilisés pour les LUN, après restauration de SnapCenter, crée un nouveau iGroup avec tous les initiateurs de tous les nœuds RAC.

- En cas d'échec lors de l'activité de pré-stockage sur les nœuds homologues, SnapCenter rétablit automatiquement l'état du groupe de disques ASM comme il était avant d'effectuer la restauration sur les nœuds homologues sur lesquels l'opération de pré-stockage a réussi. La restauration n'est pas prise en

charge pour le nœud principal et le nœud homologue sur lequel l'opération a échoué. Avant de tenter une autre restauration, vous devez corriger manuellement le problème sur le nœud homologue et ramener le groupe de disques ASM sur le nœud principal à l'état de montage.

- En cas d'échec pendant l'activité de restauration, l'opération de restauration échoue et aucune restauration n'est effectuée. Avant de tenter une autre restauration, vous devez corriger manuellement le problème de restauration du stockage et rétablir l'état de montage du groupe de disques ASM sur le nœud principal.
- En cas de défaillance au cours de l'activité postrestore sur l'un des nœuds homologues, SnapCenter poursuit l'opération de restauration sur les autres nœuds homologues. Vous devez corriger manuellement le problème de post-restauration sur le nœud homologue.

## Types d'opérations de restauration pris en charge pour les bases de données Oracle

SnapCenter vous permet d'effectuer différents types d'opérations de restauration pour les bases de données Oracle.

Avant de restaurer la base de données, les sauvegardes sont validées pour déterminer si des fichiers sont manquants par rapport aux fichiers réels de la base de données.

### Restauration complète

- Restaure uniquement les fichiers de données
- Restaure uniquement les fichiers de contrôle
- Restaure les fichiers de données et les fichiers de contrôle
- Restaure les fichiers de données, les fichiers de contrôle et les fichiers journaux de reprise dans les bases de données de secours Data Guard et Active Data Guard

### Restauration partielle

- Restaure uniquement les espaces de stockage sélectionnés
- Restaure uniquement les bases de données enfichables sélectionnées (PDB)
- Restaure uniquement les espaces de stockage sélectionnés d'un PDB

## Types d'opérations de restauration pris en charge pour les bases de données Oracle

SnapCenter vous permet d'effectuer différents types d'opérations de restauration pour les bases de données Oracle.

- La base de données jusqu'à la dernière transaction (tous les journaux)
- La base de données jusqu'à un numéro de changement de système spécifique (SCN)
- La base de données jusqu'à une date et une heure précises

Vous devez spécifier la date et l'heure de la récupération en fonction du fuseau horaire de l'hôte de la base de données.

SnapCenter fournit également l'option pas de récupération pour les bases de données Oracle.



Le plug-in pour base de données Oracle ne prend pas en charge la récupération si vous avez restauré à l'aide d'une sauvegarde créée avec le rôle de base de données en tant que secours. Vous devez toujours effectuer une restauration manuelle pour les bases de données de secours physiques.

## Restrictions liées à la restauration et à la restauration des bases de données Oracle

Avant d'effectuer des opérations de restauration et de restauration, vous devez connaître les limites.

Si vous utilisez une version d'Oracle de 11.2.0.4 à 12.1.0.1, l'opération de restauration sera à l'état suspendu lorsque vous exécutez la commande *renamedg*. Vous pouvez appliquer le correctif Oracle 19544733 pour résoudre ce problème.

Les opérations de restauration et de reprise suivantes ne sont pas prises en charge :

- Restauration et récupération des espaces de stockage de la base de données du conteneur racine (CDB)
- Restauration des espaces de stockage temporaires et des espaces de stockage temporaires associés aux BDD
- Restauration et restauration simultanées de tablespaces à partir de plusieurs bases de données PDB
- Restauration des sauvegardes des journaux
- Restauration des sauvegardes dans un emplacement différent
- Restauration des fichiers journaux de reprise dans toute configuration autre que les bases de données de secours Data Guard ou Active Data Guard
- Restauration des fichiers SPFILE et Password
- Lorsque vous effectuez une opération de restauration sur une base de données qui a été recrée à l'aide du nom de base de données préexistante sur le même hôte, qui a été géré par SnapCenter et dont les sauvegardes sont valides, l'opération de restauration écrase les fichiers de base de données nouvellement créés, même si les DBID sont différents.

Cela peut être évité en effectuant l'une des actions suivantes :

- Découvrez les ressources SnapCenter après la recréation de la base de données
- Créez une sauvegarde de la base de données recréée

## Limitations liées à la restauration instantanée des tablespaces

- La récupération ponctuelle (PITI) des espaces système, SYSAUX et UNDO n'est pas prise en charge
- Les PITI des espaces de stockage ne peuvent pas être effectués avec d'autres types de restauration
- Si un espace de table est renommé et que vous souhaitez le restaurer à un point avant son changement de nom, vous devez spécifier le nom antérieur de l'espace de table
- Si les contraintes pour les tables d'un espace table sont contenues dans un autre espace table, vous devez restaurer les deux espaces de table
- Si une table et ses index sont stockés dans des espaces de stockage différents, les index doivent être supprimés avant d'effectuer le PITR
- PITI ne peut pas être utilisé pour restaurer l'espace de table par défaut actuel
- Le PITI ne peut pas être utilisé pour récupérer des espaces de stockage contenant l'un des objets suivants :
  - Objets contenant des objets sous-jacents (tels que des vues matérialisées) ou des objets contenus (tels que des tables partitionnées), sauf si tous les objets sous-jacents ou contenus se trouvent dans le jeu de récupération

En outre, si les partitions d'une table partitionnée sont stockées dans des espaces de stockage différents, vous devez soit supprimer la table avant d'exécuter PITR, soit déplacer toutes les partitions

vers le même espace de table avant d'effectuer PITR.

- Annuler ou annuler les segments
- Files d'attente avancées compatibles avec Oracle 8 avec plusieurs destinataires
- Objets appartenant à l'utilisateur SYS

Les exemples de ces types d'objets sont PL/SQL, les classes Java, les programmes d'appel, les vues, les synonymes, utilisateurs, privilèges, dimensions, répertoires et séquences.

## Sources et destinations pour la restauration de bases de données Oracle

Vous pouvez restaurer une base de données Oracle à partir d'une copie de sauvegarde sur le stockage primaire ou secondaire. Vous ne pouvez restaurer les bases de données qu'au même emplacement sur la même instance de base de données. Cependant, dans la configuration RAC (Real application Cluster), vous pouvez restaurer les bases de données vers d'autres nœuds.

### Sources des opérations de restauration

Vous pouvez restaurer les bases de données à partir d'une sauvegarde sur un stockage primaire ou secondaire. Si vous souhaitez restaurer à partir d'une sauvegarde sur le stockage secondaire dans une configuration à plusieurs miroirs, vous pouvez sélectionner le miroir de stockage secondaire comme source.

### Destinations des opérations de restauration

Vous ne pouvez restaurer les bases de données qu'au même emplacement sur la même instance de base de données.

Dans une configuration RAC, vous pouvez restaurer des bases de données RAC à partir de n'importe quel nœud du cluster.

## Des variables d'environnement prédéfinies pour restaurer des scripts prescripteurs et PostScript spécifiques

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript lors de la restauration d'une base de données.

### Variables d'environnement prédéfinies prises en charge pour la restauration d'une base de données

- **SC\_JOB\_ID** indique l'ID de travail de l'opération.

Exemple : 257

- **SC\_ORACLE\_SID** spécifie l'identifiant système de la base de données.

Si l'opération implique plusieurs bases de données, cela contiendra des noms de bases de données séparés par un canal.

Exemple : NFSB31

- **SC\_HOST** spécifie le nom d'hôte de la base de données.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : scsmohost2.gdl.englabe.netapp.com

- **SC\_OS\_USER** spécifie le propriétaire du système d'exploitation de la base de données.

Exemple : oracle

- **SC\_OS\_GROUP** spécifie le groupe de systèmes d'exploitation de la base de données.

Exemple : oinstall

- **SC\_BACKUP\_NAME** spécifie le nom de la sauvegarde.

Ce paramètre sera renseigné pour les volumes d'application.

Exemples :

- Si la base de données n'est pas en mode ARCHIVELOG : DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- Si la base de données est exécutée en mode ARCHIVELOG : DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1, RG2\_scro819002\_07-22-2021\_12.16.48.9267\_1

- **SC\_BACKUP\_ID** spécifie l'ID de la sauvegarde.

Ce paramètre sera renseigné pour les volumes d'application.

Exemples :

- Si la base de données n'est pas exécutée en mode ARCHIVELOG : DATA@203|LOG@205
- Si la base de données est exécutée en mode ARCHIVELOG : DATA@203|LOG@205,206,207

- **SC\_RESOURCE\_GROUP\_NAME** indique le nom du groupe de ressources.

Exemple : RG1

- **SC\_ORACLE\_HOME** indique le chemin d'accès au répertoire racine Oracle.

Exemple : /ora01/app/oracle/product/18.1.0/db\_1

- **SC\_RECOVERY\_TYPE** spécifie les fichiers qui sont récupérés ainsi que la portée de récupération.

Exemple :

RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Pour plus d'informations sur les délimiteurs, reportez-vous à la section "[Délimiteurs pris en charge](#)".

## Conditions requises pour la restauration d'une base de données Oracle

Avant de restaurer une base de données Oracle, vous devez vous assurer que les prérequis sont terminés.

- Vous devez avoir défini votre stratégie de restauration et de récupération.

- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir attribué les machines virtuelles de stockage (SVM) des volumes source et de destination.
- Si les journaux d'archive sont élagués dans le cadre de la sauvegarde, vous devez avoir monté manuellement les sauvegardes de journaux d'archive requises.
- Si vous souhaitez restaurer les bases de données Oracle résidant sur un VMDK (Virtual machine Disk), assurez-vous que l'ordinateur invité dispose du nombre requis de slots libres pour allouer les VMDK clonés.
- Vous devez vous assurer que tous les volumes de données et de journaux d'archives appartenant à la base de données sont protégés si la protection secondaire est activée pour cette base de données.
- Assurez-vous que la base de données RAC One Node est à l'état "nomount" pour effectuer la restauration du fichier de contrôle ou de la base de données complète.
- Si vous disposez d'une instance de base de données ASM dans l'environnement NFS, vous devez ajouter le chemin du disque ASM `/var/opt/snapcenter/scu/clones//` au chemin existant défini dans le paramètre `asm_diskstring` pour monter correctement les sauvegardes du journal ASM dans le cadre de l'opération de récupération.
- Dans le paramètre `asm_diskstring`, vous devez configurer `AFD:*` si vous utilisez ASMFD ou `ORCL:*` si vous utilisez ASMLIB.



Pour plus d'informations sur la modification du paramètre `asm_diskstring`, reportez-vous à la section ["Comment ajouter des chemins de disque à asm\\_diskstring"](#)

- Vous devez configurer l'écouteur statique dans le fichier `listener.ora` disponible à `$ORACLE_HOME/network/admin` pour les bases de données non ASM et `$GRID_HOME/network/admin` pour les bases de données ASM si vous avez désactivé l'authentification du système d'exploitation et activé l'authentification de base de données Oracle pour une base de données Oracle, et que vous souhaitez restaurer les fichiers de données et les fichiers de contrôle de cette base de données.
- Vous devez augmenter la valeur du paramètre `SCORestoreTimeout` en exécutant la commande `set-SmConfigSettings` si la taille de la base de données est en téraoctets (To).
- Vous devez vous assurer que toutes les licences requises pour vCenter sont installées et à jour.

Si les licences ne sont pas installées ou à jour, un message d'avertissement s'affiche. Si vous ignorez l'avertissement et continuez, la restauration à partir de RDM échoue.

- Vous devez vous assurer que la LUN n'est pas mappée sur l'hôte AIX à l'aide d'iGroup composé de protocoles mixtes iSCSI et FC. Pour plus d'informations, voir ["L'opération échoue avec une erreur Impossible de détecter le périphérique pour la LUN"](#).

## Restaurez et récupérez la base de données Oracle

En cas de perte de données, vous pouvez utiliser SnapCenter pour restaurer les données d'une ou plusieurs sauvegardes sur votre système de fichiers actif, puis restaurer la base de données.

### Avant de commencer

Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

### À propos de cette tâche

- La récupération est effectuée à l'aide des journaux d'archivage disponibles à l'emplacement configuré du journal d'archivage. Si la base de données est exécutée en mode ARCHIVELOG, la base de données Oracle enregistre les groupes remplis de fichiers journaux de reprise vers une ou plusieurs destinations hors ligne, appelées collectivement le journal de reprise archivé. SnapCenter identifie et monte le nombre optimal de sauvegardes de journaux en fonction du SCN spécifié, de la date et de l'heure sélectionnées ou de tous les journaux.

Si les journaux d'archivage requis pour la restauration ne sont pas disponibles à l'emplacement configuré, vous devez monter le snapshot contenant les journaux et spécifier le chemin comme journaux d'archivage externes.

Si vous migrez la base de données ASM d'ASMLIB vers ASMFD, les sauvegardes créées avec ASMLIB ne peuvent pas être utilisées pour restaurer la base de données. Vous devez créer des sauvegardes dans la configuration ASMFD et utiliser ces sauvegardes pour les restaurer. De même, si la base de données ASM est migrée d'ASMFD vers ASMLIB, vous devez créer des sauvegardes dans la configuration ASMLIB pour restaurer.

Lors de la restauration d'une base de données, un fichier de verrouillage opérationnel (.sm\_lock\_dbsid) est créé sur l'hôte de la base de données Oracle dans le répertoire `/var/opt/snapcenter/sco/lock` pour éviter l'exécution de plusieurs opérations sur la base de données. Une fois la base de données restaurée, le fichier de verrouillage opérationnel est automatiquement supprimé.



La restauration des fichiers SPFILE et Password n'est pas prise en charge.

- Pour les règles activées par SnapLock, pour ONTAP 9.12.1 et versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données dans la vue Détails de la base de données ou dans la vue Détails du groupe de ressources.

La page topologie de la base de données s'affiche.

4. Dans la vue gestion des copies, sélectionnez **backups** dans les systèmes de stockage principal ou secondaire (mis en miroir ou répliqué).
5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur .
6. Dans la page objectif de restauration, effectuez les tâches suivantes :
  - a. Si vous avez sélectionné une sauvegarde d'une base de données dans un environnement RAC (Real application clusters), sélectionnez le nœud RAC.
  - b. Lorsque vous sélectionnez des données mises en miroir ou de coffre-fort:
    - s'il n'y a pas de sauvegarde de journaux sur le miroir ou le coffre-fort, rien n'est sélectionné et les localisateurs sont vides.
    - si des sauvegardes de journaux existent dans le miroir ou le coffre-fort, la dernière sauvegarde du journal est sélectionnée et le localisateur correspondant s'affiche.



Si la sauvegarde du journal sélectionné existe à la fois à l'emplacement miroir et à l'emplacement du coffre-fort, les deux localisateurs sont affichés.

c. Effectuez les opérations suivantes :

Si vous voulez restaurer...	Procédez comme ça...
Tous les fichiers de données de la base de données	<p>Sélectionnez <b>tous les fichiers de données</b>.</p> <p>Seuls les fichiers de données de la base de données sont restaurés. Les fichiers de contrôle, les journaux d'archivage ou les fichiers journaux de reprise ne sont pas restaurés.</p>
Espaces de stockage	<p>Sélectionnez <b>tablespaces</b>.</p> <p>Vous pouvez indiquer les espaces de stockage à restaurer.</p>
Fichiers de contrôle	<p>Sélectionnez <b>fichiers de contrôle</b>.</p> <p> Lors de la restauration des fichiers de contrôle, assurez-vous que la structure de répertoires existe ou doit être créée avec les utilisateurs et les groupes appropriés, le cas échéant, pour permettre la copie des fichiers vers l'emplacement cible par le processus de restauration. Si le répertoire n'existe pas, la tâche de restauration échouera.</p>
Rétablir les fichiers journaux	<p>Sélectionnez <b>Redo log files</b>.</p> <p>Cette option est disponible uniquement pour les bases de données de secours Data Guard ou Active Data Guard.</p> <p> Les fichiers journaux de reprise ne sont pas sauvegardés pour les bases de données non Data Guard. Pour les bases de données non Data Guard, la récupération est effectuée à l'aide de journaux d'archivage.</p>
Bases de données enfichables (BDD)	<p>Sélectionnez <b>Pluggable Databases</b>, puis spécifiez les PDB que vous souhaitez restaurer.</p>

Si vous voulez restaurer...	Procédez comme ça...
Espaces de stockage de base de données enfichables (PDB)	<p>Sélectionnez <b>Pluggable database (PDB) tablespaces</b>, puis spécifiez le PDB et les espaces de stockage de ce PDB que vous souhaitez restaurer.</p> <p>Cette option n'est disponible que si vous avez sélectionné un PDB à restaurer.</p>

- d. Sélectionnez **changer l'état de la base de données si nécessaire pour restaurer et restaurer** pour changer l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de reprise.

Les différents États d'une base de données de niveau supérieur à inférieur sont ouverts, montés, démarrés et shutdown. Vous devez cocher cette case si la base de données est dans un état plus élevé mais que l'état doit être inférieur pour effectuer une opération de restauration. Si la base de données est dans un état inférieur mais que l'état doit être supérieur pour effectuer l'opération de restauration, l'état de la base de données est automatiquement modifié, même si vous ne cochez pas la case.

Si une base de données est à l'état ouvert et que pour restaurer la base de données doit être à l'état monté, l'état de la base de données n'est modifié que si vous cochez cette case.

- a. Sélectionnez **forcer la restauration sur place** si vous souhaitez effectuer une restauration sur place dans les scénarios où de nouveaux fichiers de données sont ajoutés après la sauvegarde ou lorsque des LUN sont ajoutées, supprimés ou recrées à un groupe de disques LVM.

7. Dans la page étendue de la récupération, effectuez les opérations suivantes :

Si...	Procédez comme ça...
Que vous souhaitez restaurer à la dernière transaction	Sélectionnez <b>tous les journaux</b> .
Que vous souhaitez récupérer à un numéro de changement de système (SCN) spécifique	Sélectionnez <b>jusqu'à ce que SCN (numéro de changement du système)</b> .
Veulent restaurer des données et un temps spécifique	<p>Sélectionnez <b>Date et heure</b>.</p> <p>Vous devez spécifier la date et l'heure du fuseau horaire de l'hôte de la base de données.</p>
Ne pas récupérer	Sélectionnez <b>pas de récupération</b> .

Si...	Procédez comme ça...
<p>Vous souhaitez spécifier les emplacements de journaux d'archives externes</p>	<p>Si la base de données est exécutée en mode ARCHIVELOG, SnapCenter identifie et monte le nombre optimal de sauvegardes de journaux en fonction du SCN spécifié, de la date et de l'heure sélectionnées, ou de tous les journaux.</p> <p>Si vous voulez toujours spécifier l'emplacement des fichiers journaux d'archives externes, sélectionnez <b>spécifier les emplacements des journaux d'archives externes</b>.</p> <p>Si les journaux d'archives sont élagués dans le cadre de la sauvegarde et que vous avez monté manuellement les sauvegardes de journaux d'archives requises, vous devez spécifier le chemin de sauvegarde monté comme emplacement de journal d'archivage externe pour la restauration.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Vous devez vérifier le chemin et le contenu du chemin de montage avant de le répertorier en tant qu'emplacement de journal externe.</p> <ul style="list-style-type: none"> <li>• <a href="#">"Protection des données Oracle avec ONTAP"</a></li> <li>• <a href="#">"L'opération échoue avec l'erreur ORA-00308"</a></li> </ul> </div>

Vous ne pouvez pas effectuer une restauration avec restauration à partir de sauvegardes secondaires si les volumes du journal d'archivage ne sont pas protégés, mais si les volumes de données sont protégés. Vous ne pouvez restaurer que si vous sélectionnez **pas de récupération**.

Si vous restaurez une base de données RAC avec l'option ouvrir base de données sélectionnée, seule l'instance RAC sur laquelle l'opération de restauration a été lancée est remise à l'état ouvert.



La récupération n'est pas prise en charge pour les bases de données de secours Data Guard et Active Data Guard.

8. Dans la page PreOps, entrez le chemin d'accès et les arguments du prescripteur que vous voulez exécuter avant l'opération de restauration.

Vous devez stocker les prescripteurs dans le chemin `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin. Par défaut, le chemin `/var/opt/snapcenter/spl/scripts` est renseigné. Si vous avez créé des dossiers dans ce chemin pour stocker les scripts, vous devez spécifier ces dossiers dans le chemin d'accès.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est 60 secondes.

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript. ["En savoir plus >>"](#)

9. Dans la page PostOps, effectuez les opérations suivantes :

- a. Entrez le chemin d'accès et les arguments du script PostScript que vous souhaitez exécuter après l'opération de restauration.

Vous devez stocker les scripts dans `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin. Par défaut, le chemin `/var/opt/snapcenter/spl/scripts` est renseigné. Si vous avez créé des dossiers dans ce chemin pour stocker les scripts, vous devez spécifier ces dossiers dans le chemin d'accès.



Si l'opération de restauration échoue, les postscripts ne seront pas exécutés et les activités de nettoyage seront déclenchées directement.

- b. Cochez la case si vous souhaitez ouvrir la base de données après la récupération.

Après la restauration d'une base de données de conteneur (CDB) avec ou sans fichiers de contrôle, ou après la restauration des fichiers de contrôle CDB uniquement, si vous spécifiez d'ouvrir la base de données après la récupération, seul le CDB est ouvert et non les bases de données enfichables (PDB) dans ce CDB.

Dans une configuration RAC, seule l'instance RAC utilisée pour la restauration s'ouvre après une restauration.



Après la restauration d'un espace table utilisateur avec des fichiers de contrôle, d'un espace table système avec ou sans fichiers de contrôle, ou d'un PDB avec ou sans fichiers de contrôle, seul l'état du PDB associé à l'opération de restauration est modifié à l'état d'origine. L'état des autres PDB qui n'ont pas été utilisés pour la restauration n'est pas modifié à l'état d'origine car l'état de ces PDB n'a pas été enregistré. Vous devez modifier manuellement l'état des PDB qui n'ont pas été utilisés pour la restauration.

10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les notifications par e-mail.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de restauration effectuée, vous devez sélectionner **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface utilisateur graphique ou de la commande PowerShell `set-SmtpServer`.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.
12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Pour plus d'informations

- ["La base de données Oracle RAC One Node est ignorée pour effectuer les opérations SnapCenter"](#)
- ["Impossible de restaurer le système à partir d'un emplacement SnapMirror ou SnapVault secondaire"](#)
- ["Échec de la restauration à partir d'une sauvegarde d'une incarnation orpheline"](#)
- ["Paramètres personnalisables pour les opérations de sauvegarde, de restauration et de clonage sur les systèmes AIX"](#)

## Restauration et restauration d'espaces de stockage à partir d'une restauration instantanée

Vous pouvez restaurer un sous-ensemble d'espaces de stockage qui a été corrompu ou supprimé sans affecter les autres espaces de stockage de la base de données. SnapCenter utilise RMAN pour effectuer une restauration instantanée (PITR) des tablespaces.

### Avant de commencer

- Les sauvegardes requises pour effectuer le PITR des espaces de stockage doivent être cataloguées et montées.
- Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

### À propos de cette tâche

Au cours de l'opération PITI, RMAN crée une instance auxiliaire à la destination auxiliaire spécifiée. La destination auxiliaire peut être un point de montage ou un groupe de disques ASM. Si l'espace est suffisant à l'emplacement monté, vous pouvez réutiliser un des emplacements montés au lieu d'un point de montage dédié.

Vous devez spécifier la date et l'heure ou SCN et l'espace table est restauré dans la base de données source.

Vous pouvez sélectionner et restaurer plusieurs espaces de stockage résidant sur les environnements ASM, NFS et SAN. Par exemple, si les espaces de stockage TS2 et TS3 résident sur NFS et TS4 se trouvent sur SAN, vous pouvez effectuer une opération PITI unique pour restaurer tous les espaces de stockage.



Dans une configuration RAC, vous pouvez effectuer le PITI des espaces de stockage à partir de n'importe quel nœud du RAC.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données de type instance unique (multitenant) dans la vue détaillée de la base de données ou dans la vue détaillée du groupe de ressources.

La page topologie de la base de données s'affiche.

4. Dans la vue gestion des copies, sélectionnez **backups** dans les systèmes de stockage principal ou secondaire (mis en miroir ou répliqué).

Si la sauvegarde n'est pas cataloguée, sélectionnez la sauvegarde et cliquez sur **Catalogue**.

5. Sélectionnez la sauvegarde cataloguée, puis cliquez sur .
6. Dans la page objectif de restauration, effectuez les tâches suivantes :
  - a. Si vous avez sélectionné une sauvegarde d'une base de données dans un environnement RAC (Real application clusters), sélectionnez le nœud RAC.

b. Sélectionnez **tablespaces**, puis spécifiez les espaces de stockage à restaurer.



Vous ne pouvez pas exécuter PITI sur SYSAUX, LE SYSTÈME et ANNULER les espaces de table.

c. Sélectionnez **changer l'état de la base de données si nécessaire pour restaurer et restaurer** pour changer l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de reprise.

7. Dans la page étendue de la récupération, effectuez l'une des opérations suivantes :

- Si vous souhaitez restaurer un numéro de changement de système (SCN) spécifique, sélectionnez **jusqu'à SCN** et spécifiez le SCN et la destination auxiliaire.
- Pour restaurer une date et une heure spécifiques, sélectionnez **Date et heure** et spécifiez la date et l'heure ainsi que la destination auxiliaire.

SnapCenter identifie, puis monte et catalogue le nombre optimal de sauvegardes de données et de journaux requis pour effectuer le transfert de données en fonction du SCN spécifié ou de la date et de l'heure sélectionnées.

8. Dans la page PreOps, entrez le chemin d'accès et les arguments du prescripteur que vous voulez exécuter avant l'opération de restauration.

Vous devez stocker les prescripteurs dans le chemin `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin. Par défaut, le chemin `/var/opt/snapcenter/SPL/scripts` est renseigné. Si vous avez créé des dossiers dans ce chemin pour stocker les scripts, vous devez spécifier ces dossiers dans le chemin d'accès.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est 60 secondes.

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript. "[En savoir plus >>](#)"

9. Dans la page PostOps, effectuez les opérations suivantes :

- a. Entrez le chemin d'accès et les arguments du script PostScript que vous souhaitez exécuter après l'opération de restauration.



Si l'opération de restauration échoue, les postscripts ne seront pas exécutés et les activités de nettoyage seront déclenchées directement.

- b. Cochez la case si vous souhaitez ouvrir la base de données après la récupération.

10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les notifications par e-mail.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.

12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Restaurez et récupérez une base de données enfichable à l'aide d'une récupération ponctuelle

Vous pouvez restaurer et récupérer une base de données enfichable (PDB) qui a été corrompue ou supprimée sans affecter les autres PDB dans la base de données du

conteneur (CDB). SnapCenter utilise RMAN pour effectuer une récupération ponctuelle (PITI) du PDB.

### Avant de commencer

- Les sauvegardes requises pour effectuer le PITR d'un PDB doivent être cataloguées et montées.



Dans une configuration RAC, vous devez fermer manuellement le boîtier de distribution électrique (en changeant son état sur MONTÉ) sur tous les nœuds de la configuration RAC.

- Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

### À propos de cette tâche

Au cours de l'opération PITI, RMAN crée une instance auxiliaire à la destination auxiliaire spécifiée. La destination auxiliaire peut être un point de montage ou un groupe de disques ASM. Si l'espace est suffisant à l'emplacement monté, vous pouvez réutiliser un des emplacements montés au lieu d'un point de montage dédié.

Vous devez spécifier la date et l'heure ou le SCN pour effectuer le PITR du PDB. RMAN permet de récupérer DES bases de données en LECTURE, EN LECTURE SEULE ou en échec, y compris les fichiers de données.

Vous ne pouvez restaurer et récupérer que :

- Un PDB à la fois
- Un espace table dans un PDB
- Plusieurs espaces de stockage d'un même PDB



Dans une configuration RAC, vous pouvez effectuer le PITI des espaces de stockage à partir de n'importe quel nœud du RAC.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données de type instance unique (multitenant) dans la vue détaillée de la base de données ou dans la vue détaillée du groupe de ressources.

La page topologie de la base de données s'affiche.

4. Dans la vue gestion des copies, sélectionnez **backups** dans les systèmes de stockage principal ou secondaire (mis en miroir ou répliqué).

Si la sauvegarde n'est pas cataloguée, sélectionnez la sauvegarde et cliquez sur **Catalogue**.

5. Sélectionnez la sauvegarde cataloguée, puis cliquez sur .
6. Dans la page objectif de restauration, effectuez les tâches suivantes :
  - a. Si vous avez sélectionné une sauvegarde d'une base de données dans un environnement RAC (Real

application clusters), sélectionnez le nœud RAC.

- b. Selon que vous souhaitez restaurer le PDB ou les espaces de stockage dans un PDB, effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Étapes...
Restaurer un PDB	<p>i. Sélectionnez <b>bases de données enfichables (PDB)</b>.</p> <p>ii. Spécifiez le PDB à restaurer.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Vous ne pouvez pas effectuer le PITR sur la base de données PDB\$SEED.</div>
Restaurer les espaces de stockage dans un PDB	<p>i. Sélectionnez <b>bases de données enfichables (PDB) tablespaces</b>.</p> <p>ii. Spécifiez le PDB.</p> <p>iii. Spécifiez un espace table ou plusieurs espaces de stockage à restaurer.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Vous ne pouvez pas exécuter PITI sur SYSAUX, LE SYSTÈME et ANNULER les espaces de table.</div>

- c. Sélectionnez **changer l'état de la base de données si nécessaire pour restaurer et restaurer** pour changer l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de reprise.

7. Dans la page étendue de la récupération, effectuez l'une des opérations suivantes :

- Si vous souhaitez restaurer un numéro de changement de système (SCN) spécifique, sélectionnez **jusqu'à SCN** et spécifiez le SCN et la destination auxiliaire.
- Pour restaurer une date et une heure spécifiques, sélectionnez **Date et heure** et spécifiez la date et l'heure ainsi que la destination auxiliaire.

SnapCenter identifie, puis monte et catalogue le nombre optimal de sauvegardes de données et de journaux requis pour effectuer le transfert de données en fonction du SCN spécifié ou de la date et de l'heure sélectionnées.

8. Dans la page PreOps, entrez le chemin d'accès et les arguments du prescripteur que vous voulez exécuter avant l'opération de restauration.

Vous devez stocker les prescripteurs dans le chemin `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin. Par défaut, le chemin `/var/opt/snapcenter/SPL/scripts` est renseigné. Si vous avez créé des dossiers dans ce chemin pour stocker les scripts, vous devez spécifier ces dossiers dans le chemin d'accès.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est 60 secondes.

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript. "[En savoir plus >>](#)"

9. Dans la page PostOps, effectuez les opérations suivantes :
  - a. Entrez le chemin d'accès et les arguments du script PostScript que vous souhaitez exécuter après l'opération de restauration.



Si l'opération de restauration échoue, les postscripts ne seront pas exécutés et les activités de nettoyage seront déclenchées directement.

- b. Cochez la case si vous souhaitez ouvrir la base de données après la récupération.

Dans une configuration RAC, le PDB est ouvert uniquement sur le nœud où la base de données a été récupérée. Vous devez ouvrir manuellement le PDB récupéré sur tous les autres nœuds de la configuration RAC.

10. Sur la page notification, dans la liste déroulante Préférences **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les notifications par e-mail.
11. Vérifiez le résumé, puis cliquez sur **Terminer**.
12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Restaurez et récupérez des bases de données Oracle à l'aide des commandes UNIX

Le flux de travail de restauration et de reprise comprend une planification, des opérations de restauration et de reprise, ainsi que la surveillance des opérations.

### À propos de cette tâche

- Vous devez exécuter les commandes suivantes pour établir la connexion avec le serveur SnapCenter, répertorier les sauvegardes et récupérer ses informations, et restaurer la sauvegarde.

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également vous reporter à "[Guide de référence sur les commandes du logiciel SnapCenter](#)".

- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié : `Open-SmConnection`
2. Récupérez les informations sur les sauvegardes que vous souhaitez restaurer : `get-SmBackup`
3. Récupérez les informations détaillées sur la sauvegarde spécifiée : `get-SmBackupDetails`

Cette commande récupère les informations détaillées relatives à la sauvegarde d'une ressource spécifiée avec un ID de sauvegarde donné. Ces informations comprennent le nom de la base de données, la version, le domicile, le SCN de début et de fin, les espaces de stockage, les bases de données enfichables et ses espaces de stockage.

4. Restaurez les données à partir de la sauvegarde : *Restore-SmBackup*

## Surveillez les opérations de restauration des bases de données Oracle

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Annuler les opérations de restauration de la base de données Oracle

Vous pouvez annuler les travaux de restauration mis en file d'attente.

Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâche pour annuler les opérations de restauration.

### Description de la tâche

- Vous pouvez annuler une opération de restauration en file d'attente à partir de la page **Monitor** ou du volet

### Activity.

- Vous ne pouvez pas annuler une opération de restauration en cours.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes de l'interface de ligne de commande pour annuler les opérations de restauration en attente.
- Le bouton **Annuler tâche** est désactivé pour les opérations de restauration qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de restauration en file d'attente d'autres membres tout en utilisant ce rôle.

### Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>2. Sélectionnez le travail et cliquez sur <b>Annuler le travail</b>.</li></ol>
Volet activité	<ol style="list-style-type: none"><li>1. Après avoir lancé l'opération de restauration, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li><li>2. Sélectionner l'opération.</li><li>3. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li></ol>

## Cloner la base de données Oracle

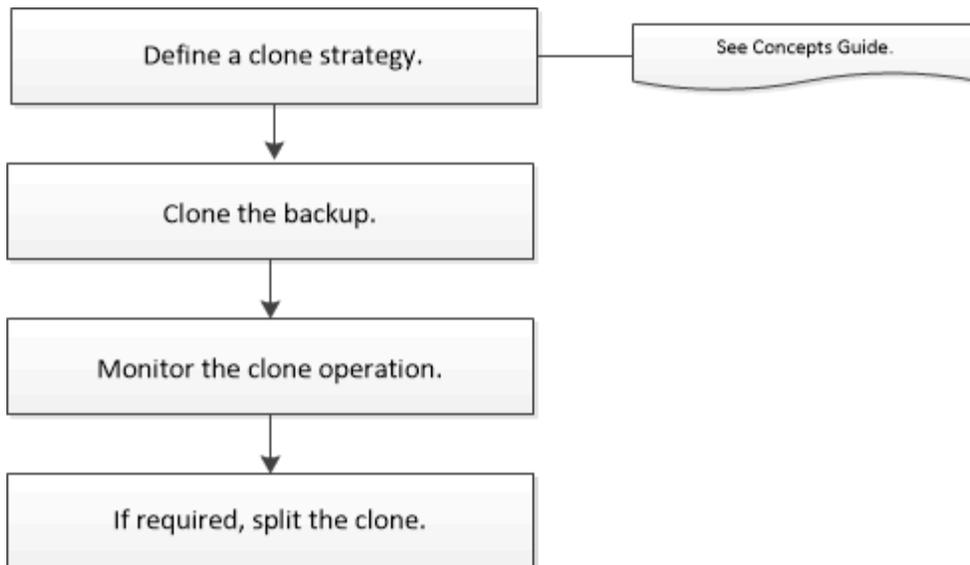
### Workflow de clonage

Le workflow de clonage inclut la planification, la réalisation de l'opération de clonage et le contrôle de l'opération.

Il est possible de cloner des bases de données pour les raisons suivantes :

- Tester les fonctionnalités à implémenter à l'aide de la structure et du contenu actuels de la base de données au cours des cycles de développement d'applications.
- Pour renseigner les data warehouses à l'aide d'outils d'extraction et de manipulation de données.
- Pour récupérer les données qui ont été supprimées ou modifiées par erreur.

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



## Définissez une stratégie de clonage pour les bases de données Oracle

La définition d'une stratégie avant le clonage de votre base de données garantit la réussite de l'opération de clonage.

### Types de sauvegardes pris en charge pour le clonage

SnapCenter prend en charge le clonage de différents types de sauvegardes de bases de données Oracle.

- Sauvegarde des données en ligne
- Sauvegarde complète en ligne
- Monter la sauvegarde hors ligne
- Arrêter la sauvegarde hors ligne
- Sauvegardes des bases de données de secours Data Guard et des bases de données de secours Active Data Guard
- Les sauvegardes de données en ligne, les sauvegardes complètes en ligne, les sauvegardes de montage hors ligne et les sauvegardes hors ligne dans une configuration RAC (Real application clusters)
- Sauvegardes de données en ligne, sauvegardes complètes en ligne, sauvegardes de montage hors ligne et sauvegardes d'arrêt hors ligne dans une configuration ASM (Automatic Storage Management)



Les configurations SAN ne sont pas prises en charge si l'option `User_friendly_Names` du fichier de configuration multichemin est définie sur `yes`.



Le clonage des sauvegardes du journal d'archivage n'est pas pris en charge.

### Types de clonage pris en charge pour les bases de données Oracle

Dans un environnement de base de données Oracle, SnapCenter prend en charge le clonage d'une sauvegarde de base de données. La sauvegarde peut être clonée à partir de systèmes de stockage primaires et secondaires.

Le serveur SnapCenter s'appuie sur la technologie NetApp FlexClone pour cloner des sauvegardes.

Vous pouvez actualiser un clone en exécutant la commande « Refresh-SmClone ». Cette commande crée une sauvegarde de la base de données, supprime le clone existant et crée un clone portant le même nom.



L'opération d'actualisation des clones ne peut être effectuée qu'à l'aide des commandes UNIX.

### Nomenclature établie des clones pour les bases de données Oracle

À partir de SnapCenter 3.0, la convention de nommage utilisée pour les clones de systèmes de fichiers est différente des clones de groupes de disques ASM.

- la convention de dénomination des systèmes de fichiers SAN ou NFS est `FileSystemNamedesourcedatabase_CLONESID`.
- la convention de nommage des groupes de disques ASM est `SC_HASHCODEofDISKGROUP_CLONESID`.

`HASHCODEofDISKGROUP` est un nombre généré automatiquement (2 à 10 chiffres) unique pour chaque groupe de disques ASM.

### Limitations du clonage des bases de données Oracle

Avant de cloner les bases de données, vous devez connaître les limites des opérations de clonage.

- Si vous utilisez une version d'Oracle de 11.2.0.4 à 12.1.0.1, l'opération clone sera à l'état suspendu lorsque vous exécutez la commande `renamedg`. Vous pouvez appliquer le correctif Oracle 19544733 pour résoudre ce problème.
- Le clonage de bases de données à partir d'une LUN directement connectée à un hôte (par exemple, en utilisant l'initiateur iSCSI Microsoft sur un hôte Windows) vers un VMDK ou une LUN RDM sur le même hôte Windows, ou un autre hôte Windows, ou vice versa, n'est pas pris en charge.
- Le répertoire racine du point de montage du volume ne peut pas être un répertoire partagé.
- Si vous déplacez une LUN contenant un clone vers un nouveau volume, le clone ne peut pas être supprimé.

### Variables d'environnement prédéfinies pour le prescripteur et le post-script spécifiques au clone

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript lors du clonage d'une base de données.

#### Variables d'environnement prédéfinies prises en charge pour le clonage d'une base de données

- **SC\_ORIGINAL\_SID** spécifie le SID de la base de données source.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : NFSB32

- **SC\_ORIGINAL\_HOST** spécifie le nom de l'hôte source.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : asmrac1.gdl.englab.netapp.com

- **SC\_ORACLE\_HOME** indique le chemin du répertoire racine Oracle de la base de données cible.

Exemple : /ora01/app/oracle/product/18.1.0/db\_1

- **SC\_BACKUP\_NAME** indique le nom de la sauvegarde.

Ce paramètre sera renseigné pour les volumes d'application.

Exemples :

- Si la base de données n'est pas en mode ARCHIVELOG : DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_1
- Si la base de données est exécutée en mode ARCHIVELOG : DATA@RG2\_scspr2417819002\_07-20-2021\_12.16.48.9267\_0|LOG:RG2\_scrospr2417819002\_07-20-2021\_12.16.48.9267\_1, RG2\_spr2417819002\_07-21-2021\_1, RG2\_sprspr24819002\_07-12.16.48.9267-22-12.16.48.9267 2021\_1

- **SC\_AV\_NAME** spécifie les noms des volumes d'application.

Exemple : AV1|AV2

- **SC\_ORIGINAL\_OS\_USER** spécifie le propriétaire du système d'exploitation de la base de données source.

Exemple : oracle

- **SC\_ORIGINAL\_OS\_GROUP** spécifie le groupe de systèmes d'exploitation de la base de données source.

Exemple : oinstall

- **SC\_TARGET\_SID** spécifie le SID de la base de données clonée.

Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : clonedb

- **SC\_TARGET\_HOST** spécifie le nom de l'hôte sur lequel la base de données sera clonée.

Ce paramètre sera renseigné pour les volumes d'application.

Exemple : asmrac1.gdl.englab.netapp.com

- **SC\_TARGET\_OS\_USER** spécifie le propriétaire du système d'exploitation de la base de données clonée.

Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie.

Exemple : oracle

- **SC\_TARGET\_OS\_GROUP** spécifie le groupe de systèmes d'exploitation de la base de données clonée.

Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie.

Exemple : oinstall

- **SC\_TARGET\_DB\_PORT** spécifie le port de base de données de la base de données clonée.

Pour le workflow de clonage PDB, la valeur de ce paramètre n'est pas prédéfinie.

Exemple : 1521

Pour plus d'informations sur les délimiteurs, reportez-vous à la section "[Délimiteurs pris en charge](#)".

## Conditions requises pour le clonage d'une base de données Oracle

Avant de cloner une base de données Oracle, vous devez vous assurer que les prérequis sont terminés.

- Vous devez avoir créé une sauvegarde de la base de données à l'aide de SnapCenter.

Vous devez avoir créé avec succès les sauvegardes de journaux et de données en ligne ou les sauvegardes hors ligne (montage ou arrêt) pour que l'opération de clonage puisse réussir.

- Si vous souhaitez personnaliser les chemins du fichier de contrôle ou du fichier journal de reprise, vous devez avoir préprovisionné le système de fichiers requis ou le groupe de disques ASM (Automatic Storage Management).

Par défaut, les fichiers de reprise et de contrôle de la base de données clonée sont créés sur le groupe de disques ASM ou le système de fichiers provisionné par SnapCenter pour les fichiers de données de la base de données clone.

- Si vous utilisez ASM sur NFS, vous devez ajouter `/var/opt/snapcenter/scu/clones/*/*` au chemin existant défini dans le paramètre `asm_diskstring`.
- Dans le paramètre `asm_diskstring`, vous devez configurer `AFD:*` si vous utilisez ASMFD ou `ORCL:*` si vous utilisez ASMLIB.

Pour plus d'informations sur la modification du paramètre `asm_diskstring`, reportez-vous à la section "[Comment ajouter des chemins de disque à asm\\_diskstring](#)".

- Si vous créez le clone sur un autre hôte, celui-ci doit répondre aux exigences suivantes :
  - Le plug-in SnapCenter pour base de données Oracle doit être installé sur l'hôte secondaire.
  - L'hôte clone doit pouvoir détecter les LUN à partir du stockage primaire ou secondaire.
    - Si vous effectuez le clonage depuis le stockage primaire ou le stockage secondaire (Vault ou Mirror) vers un autre hôte, assurez-vous qu'une session iSCSI est soit établie entre le stockage secondaire et l'hôte secondaire, ou bien zonée correctement pour FC.
    - Si vous effectuez un clonage depuis le stockage Vault ou Mirror vers le même hôte, assurez-vous qu'une session iSCSI est soit établie entre le stockage Vault ou Mirror et l'hôte, soit zonée correctement pour FC.
    - Si vous effectuez le clonage dans un environnement virtualisé, assurez-vous qu'une session iSCSI est soit établie entre le stockage primaire ou secondaire et le serveur ESX qui héberge l'hôte secondaire, ou bien zonée correctement pour FC.

Pour plus d'informations, reportez-vous à la section "[documentation des utilitaires hôtes](#)".

- Si la base de données source est une base de données ASM :
  - L'instance ASM doit être active sur l'hôte sur lequel le clone sera exécuté.

- Le groupe de disques ASM doit être provisionné avant l'opération de clonage si vous souhaitez placer les fichiers journaux d'archive de la base de données clonée dans un groupe de disques ASM dédié.
- Le nom du groupe de disques de données peut être configuré, mais assurez-vous que le nom n'est pas utilisé par tout autre groupe de disques ASM sur l'hôte où le clone sera effectué.

Les fichiers de données résidant sur le groupe de disques ASM sont provisionnés dans le cadre du workflow de clonage SnapCenter.

- Pour NVMe, vous devez installer NVMe util

- Le type de protection de la LUN de données et de la LUN de journal, tel que miroir, coffre-fort ou miroir-vault, doit être le même pour détecter les dispositifs de localisation secondaires lors du clonage sur un autre hôte à l'aide des sauvegardes de journaux.
- Vous devez définir LA valeur `exclude_seed_cdb_View` sur `FALSE` dans le fichier de paramètres de la base de données source pour récupérer les informations relatives au PDB de départ pour cloner une sauvegarde de la base de données `12_c_.`

Le PDB de semences est un modèle fourni par le système que le CDB peut utiliser pour créer des PDB. Le PDB de semences est nommé `PDB$SEED`. Pour plus d'informations sur `PDB$SEED`, consultez le document Oracle Doc ID 1940806.1.



Vous devez définir la valeur avant de sauvegarder la base de données `12_c_.`

- SnapCenter prend en charge la sauvegarde des systèmes de fichiers gérés par le sous-système autofs. Si vous procédez au clonage de la base de données, assurez-vous que les points de montage de données ne sont pas sous la racine du point de montage de l'autofs car l'utilisateur racine de l'hôte du plug-in n'est pas autorisé à créer des répertoires sous la racine du point de montage de l'autofs.

Si les fichiers journaux de contrôle et de reprise sont sous le point de montage des données, modifiez le chemin du fichier de contrôle, puis refaites le chemin du fichier journal en conséquence.



Vous pouvez enregistrer manuellement les nouveaux points de montage clonés avec le sous-système autofs. Les nouveaux points de montage clonés ne seront pas enregistrés automatiquement.

- Si vous avez un TDE (connexion automatique) et que vous souhaitez cloner la base de données sur le même hôte ou un autre hôte, vous devez copier le porte-monnaie (fichiers clés) sous `/etc/ORACLE/PORTEFEUILLE/$ORACLE_SID` de la base de données source vers la base de données clonée.
- Vous devez définir la valeur de `use_lvmetag = 0` dans `/etc/lvm/lvm.conf` et arrêter le service `lvm2-lvmetad` pour effectuer le clonage dans les environnements SAN sous Oracle Linux 7 ou version ultérieure ou Red Hat Enterprise Linux (RHEL) 7 ou version ultérieure.
- Vous devez installer le correctif Oracle 13366202 si vous utilisez la base de données Oracle 11.2.0.3 ou une version ultérieure et si l'ID de base de données de l'instance auxiliaire est modifié à l'aide d'un script NID.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Pour NVMe, si un port cible doit être exclu de la connexion, vous devez ajouter le nom du nœud cible et le nom du port dans le fichier `/var/opt/snapcenter/scu/etc/nvme.conf`.

Si le fichier n'existe pas, vous devez créer le fichier comme indiqué dans l'exemple ci-dessous :

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- Vous devez vous assurer que la LUN n'est pas mappée sur l'hôte AIX à l'aide d'iGroup composé de protocoles mixtes iSCSI et FC. Pour plus d'informations, voir "[L'opération échoue avec une erreur Impossible de détecter le périphérique pour la LUN](#)".

## Cloner une sauvegarde de base de données Oracle

Vous pouvez utiliser SnapCenter pour cloner une base de données Oracle à l'aide de la sauvegarde de la base de données.

### Avant de commencer

Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

### À propos de cette tâche

- L'opération de clonage crée une copie des fichiers de données de la base de données et crée de nouveaux fichiers journaux de reprise en ligne et fichiers de contrôle. La base de données peut être éventuellement restaurée à une heure spécifiée, en fonction des options de restauration spécifiées.



Le clonage échoue si vous tentez de cloner une sauvegarde créée sur un hôte Linux vers un hôte AIX ou vice-versa.

SnapCenter crée une base de données autonome lorsqu'elle est clonée à partir d'une sauvegarde de base de données Oracle RAC. SnapCenter prend en charge la création de clone à partir de la sauvegarde d'une base de données de secours Data Guard et Active Data Guard.

Lors du clonage, SnapCenter monte le nombre optimal de sauvegardes de journaux en fonction de SCN ou dat, et de la durée des opérations de restauration. Après la récupération, la sauvegarde du journal est démonté. Tous ces clones sont montés sous `/var/opt/snapcenter/scu/clones/`. Si vous utilisez ASM sur NFS, vous devez ajouter `/var/opt/snapcenter/scu/clones/*/*` au chemin existant défini dans le paramètre `asm_diskstring`.

Lors du clonage d'une sauvegarde d'une base de données ASM dans un environnement SAN, les règles udev pour les périphériques hôtes clonés sont créées à l'adresse `/etc/udev/rules.d/999-scu-netapp.rules`. Ces règles udev associées aux périphériques hôtes clonés sont supprimées lorsque vous supprimez le clone.



Dans une configuration Flex ASM, vous ne pouvez pas effectuer d'opération de clonage sur les nœuds Leaf si la cardinalité est inférieure au nombre de nœuds dans le cluster RAC.

- Pour les règles activées par SnapLock, pour ONTAP 9.12.1 et versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données dans la vue Détails de la base de données ou dans la vue Détails du groupe de ressources.

La page topologie de la base de données s'affiche.

4. Dans la vue gérer les copies, sélectionnez les sauvegardes depuis les copies locales (primaires), les copies miroir (secondaires) ou les copies de coffre-fort (secondaires).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page Nom, effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez...	Étapes...
Cloner une base de données (CDB ou non CDB)	<p>a. Spécifiez la SID du clone.</p> <p>Le SID de clone n'est pas disponible par défaut et la longueur maximale du SID est de 8 caractères.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><p> Vous devez vous assurer qu'aucune base de données avec le même SID n'existe sur l'hôte sur lequel le clone sera créé.</p></div>
Cloner une base de données enfichable (PDB)	<p>a. Sélectionnez <b>PDB Clone</b>.</p> <p>b. Spécifiez le PDB à cloner.</p> <p>c. Spécifiez le nom du PDB cloné. Pour connaître les étapes détaillées de clonage d'un PDB, reportez-vous à la section "<a href="#">Cloner une base de données enfichable</a>".</p>

Lorsque vous sélectionnez des données mises en miroir ou de coffre-fort:

- s'il n'y a pas de sauvegarde de journaux sur le miroir ou le coffre-fort, rien n'est sélectionné et les localisateurs sont vides.
- si des sauvegardes de journaux existent dans le miroir ou le coffre-fort, la dernière sauvegarde du journal est sélectionnée et le localisateur correspondant s'affiche.



Si la sauvegarde du journal sélectionné existe à la fois à l'emplacement miroir et à l'emplacement du coffre-fort, les deux localisateurs sont affichés.

7. Dans la page emplacements, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Hôte clone	<p>Par défaut, l'hôte de la base de données source est renseigné.</p> <p>Si vous souhaitez créer le clone sur un autre hôte, sélectionnez l'hôte ayant la même version d'Oracle et de système d'exploitation que celle de l'hôte de base de données source.</p>
Emplacement des fichiers de données	<p>Par défaut, l'emplacement du fichier de données est renseigné.</p> <p>la convention de nommage par défaut de SnapCenter pour les systèmes de fichiers SAN ou NFS est <code>FileSystemNamedesourcedatabase_CLONESID</code>.</p> <p>la convention de nommage par défaut de SnapCenter pour les groupes de disques ASM est <code>SC_HASHCODEofDISKGROUP_CLONESID</code>. Le <code>HASHCODEofDISKGROUP</code> est un nombre généré automatiquement (2 à 10 chiffres) unique pour chaque groupe de disques ASM.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Si vous personnalisez le nom du groupe de disques ASM, assurez-vous que la longueur du nom respecte la longueur maximale prise en charge par Oracle.</p> </div> <p>Si vous souhaitez définir un autre chemin, vous devez entrer les points de montage des fichiers de données ou les noms de groupe de disques ASM pour cloner la base de données. Lorsque vous personnalisez le chemin du fichier de données, vous devez également modifier le fichier de contrôle et le fichier journal de reprise noms de groupe de disques ASM ou de système de fichiers au même nom que celui utilisé pour les fichiers de données ou pour les groupes de disques ASM existants ou un système de fichiers.</p>

Pour ce champ...	Procédez comme ça...
Fichiers de contrôle	<p>Par défaut, le chemin du fichier de contrôle est renseigné.</p> <p>Les fichiers de contrôle sont placés dans le même groupe de disques ASM ou système de fichiers que ceux des fichiers de données. Si vous souhaitez remplacer le chemin du fichier de contrôle, vous pouvez fournir un chemin différent pour le fichier de contrôle.</p> <p> Le système de fichiers ou le groupe de disques ASM doit exister sur l'hôte.</p> <p>Par défaut, le nombre de fichiers de contrôle est identique à celui de la base de données source. Vous pouvez modifier le nombre de fichiers de contrôle, mais un minimum d'un fichier de contrôle est nécessaire pour cloner la base de données.</p> <p>Vous pouvez personnaliser le chemin du fichier de contrôle vers un système de fichiers (existant) différent de celui de la base de données source.</p>

Pour ce champ...	Procédez comme ça...
Journaux de reprise	<p>Par défaut, le groupe de fichiers du journal de reprise, le chemin d'accès et leur taille sont renseignés.</p> <p>Les journaux de reprise sont placés dans le même groupe de disques ASM ou système de fichiers que les fichiers de données de la base de données clonée. Si vous souhaitez remplacer le chemin du fichier journal de reprise, vous pouvez personnaliser le chemin du fichier journal de reprise sur un système de fichiers différent de celui de la base de données source.</p> <p> Le nouveau système de fichiers ou le groupe de disques ASM doit exister sur l'hôte.</p> <p>Par défaut, le nombre de groupes de journaux de reprise, de fichiers journaux de reprise et de leurs tailles seront identiques à ceux de la base de données source. Vous pouvez modifier les paramètres suivants :</p> <ul style="list-style-type: none"> <li>• Nombre de groupes du journal de reprise</li> </ul> <p> Un minimum de deux groupes de fichiers journaux de reprise sont nécessaires pour cloner la base de données.</p> <ul style="list-style-type: none"> <li>• Rétablir les fichiers journaux de chaque groupe et leur chemin d'accès</li> </ul> <p>Vous pouvez personnaliser le chemin du fichier journal de reprise sur un système de fichiers (existant) différent de celui de la base de données source.</p> <p> Un minimum d'un fichier journal de reprise est requis dans le groupe de journaux de reprise pour cloner la base de données.</p> <ul style="list-style-type: none"> <li>• Tailles du fichier journal de reprise</li> </ul>

8. Sur la page informations d'identification, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom des informations d'identification de l'utilisateur sys	<p>Sélectionnez les informations d'identification à utiliser pour définir le mot de passe utilisateur sys de la base de données clone.</p> <p>Si SQLNET.AUTHENTICATION_SERVICES est défini sur NONE dans le fichier sqlnet.ora de l'hôte cible, vous ne devez pas sélectionner <b>None</b> comme informations d'identification dans l'interface utilisateur graphique de SnapCenter.</p>
Nom des informations d'identification de l'instance ASM	<p>Sélectionnez <b>aucun</b> si l'authentification OS est activée pour la connexion à l'instance ASM sur l'hôte clone.</p> <p>Sinon, sélectionnez les informations d'identification Oracle ASM configurées avec l'utilisateur "sys" ou un utilisateur disposant du privilège "ssysasm" applicable à l'hôte clone.</p>

Les informations relatives au domicile Oracle, au nom d'utilisateur et au groupe sont automatiquement renseignées à partir de la base de données source. Vous pouvez modifier les valeurs en fonction de l'environnement Oracle de l'hôte sur lequel le clone sera créé.

9. Dans la page opérations préopérationnelles, effectuez les opérations suivantes :

- a. Entrez le chemin d'accès et les arguments du prescripteur que vous souhaitez exécuter avant l'opération de clonage.

Vous devez stocker le prescripteur dans `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin. Par défaut, le chemin `/var/opt/snapcenter/spl/scripts` est renseigné. Si vous avez placé le script dans un dossier de ce chemin, vous devez fournir le chemin complet vers le dossier où le script est placé.

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript. ["En savoir plus >>"](#)

- b. Dans la section Paramètres de base de données, modifiez les valeurs des paramètres de base de données préremplis utilisés pour initialiser la base de données.

Vous pouvez ajouter des paramètres supplémentaires en cliquant sur \*\*  .

Si vous utilisez Oracle Standard Edition et que la base de données est exécutée en mode Journal d'archive ou si vous souhaitez restaurer une base de données à partir du journal de reprise d'archive, ajoutez les paramètres et spécifiez le chemin d'accès.

- LOG\_ARCHIVE\_DEST
- LOG\_ARCHIVE\_DUPLEX\_DEST



La zone de récupération rapide (FRA) n'est pas définie dans les paramètres de la base de données préremplie. Vous pouvez configurer FRA en ajoutant les paramètres associés.



La valeur par défaut de `log_archive_dest_1` est `$ORACLE_HOME/clone_sid` et les journaux d'archive de la base de données clonée sont créés à cet emplacement. Si vous avez supprimé le paramètre `log_archive_dest_1`, l'emplacement du journal d'archives est déterminé par Oracle. Vous pouvez définir un nouvel emplacement pour le journal d'archives en éditant `log_archive_dest_1` mais vous devez vous assurer que le système de fichiers ou le groupe de disques doit être existant et mis à disposition sur l'hôte.

a. Cliquez sur **Réinitialiser** pour obtenir les paramètres par défaut de la base de données.

10. Dans la page opérations postales, **récupérer la base de données et jusqu'à Annuler** sont sélectionnés par défaut pour effectuer la récupération de la base de données clonée.

SnapCenter effectue la restauration en montant la dernière sauvegarde des journaux qui présentent la séquence incassée des journaux d'archivage qui ont été sélectionnés pour le clonage. La sauvegarde des journaux et des données doit se trouver sur le système de stockage principal afin d'effectuer le clonage sur le stockage primaire et la sauvegarde des journaux, et la sauvegarde des données doit se trouver sur un système de stockage secondaire pour effectuer le clonage sur le stockage secondaire.

Les options **récupérer base de données et jusqu'à Annuler** ne sont pas sélectionnées si SnapCenter ne trouve pas les sauvegardes de journal appropriées. Vous pouvez indiquer l'emplacement du journal d'archivage externe si la sauvegarde du journal n'est pas disponible dans **spécifier les emplacements du journal d'archivage externe**. Vous pouvez spécifier plusieurs emplacements de journaux.



Si vous souhaitez cloner une base de données source configurée pour prendre en charge la zone de récupération flash (FRA) et les fichiers gérés Oracle (OMF), la destination du journal pour la récupération doit également adhérer à la structure de répertoires OMF.

La page PostOps ne s'affiche pas si la base de données source est une base de données de secours Data Guard ou active Data Guard. Pour une base de données de secours Data Guard ou Active Data Guard, SnapCenter ne fournit pas d'option pour sélectionner le type de récupération dans l'interface graphique SnapCenter, mais la base de données est récupérée à l'aide de jusqu'à annuler le type de récupération sans appliquer de journaux.

Nom du champ	Description
Jusqu'à Annuler	SnapCenter effectue les restaurations en installant la dernière sauvegarde des journaux, puis en suivant cette sauvegarde de données sélectionnée pour le clonage, qui suit la séquence indéfinie des journaux d'archivage. La base de données clonée est restaurée jusqu'au fichier journal manquant ou corrompu.

Nom du champ	Description
Date et heure	<p>SnapCenter restaure la base de données jusqu'à une date et une heure spécifiées. Le format accepté est mm/jj/aaaa hh:mm:ss</p> <p> L'heure peut être spécifiée au format 24 heures.</p>
Jusqu'à SCN (numéro de changement du système)	<p>SnapCenter restaure la base de données jusqu'à un numéro de modification du système (SCN) spécifié.</p>
Spécifiez les emplacements des journaux d'archives externes	<p>Si la base de données est exécutée en mode ARCHIVELOG, SnapCenter identifie et monte le nombre optimal de sauvegardes de journaux en fonction du SCN spécifié ou de la date et de l'heure sélectionnées.</p> <p>Vous pouvez également spécifier l'emplacement du journal d'archivage externe.</p> <p> SnapCenter n'identifie pas et ne monte pas automatiquement les sauvegardes de journaux si vous avez sélectionné jusqu'à ce que Annuler.</p>
Créer un nouveau DBID	<p>Par défaut, la case à cocher <b>Créer un nouveau DBID</b> est sélectionnée pour générer un numéro unique (DBID) pour la base de données clonée la distinguant de la base de données source.</p> <p>Décochez la case si vous souhaitez affecter le DBID de la base de données source à la base de données clonée. Dans ce scénario, si vous souhaitez enregistrer la base de données clonée avec le catalogue RMAN externe où la base de données source est déjà enregistrée, l'opération échoue.</p>
Créez un fichier tempfile pour l'espace de table temporaire	<p>Cochez la case si vous souhaitez créer un fichier tempfile pour le tablespace temporaire par défaut de la base de données clonée.</p> <p>Si la case n'est pas cochée, le clone de la base de données est créé sans le fichier tempfile.</p>
Entrez les entrées sql à appliquer lors de la création du clone	<p>Ajoutez les entrées sql que vous souhaitez appliquer lors de la création du clone.</p>

Nom du champ	Description
Entrez les scripts à exécuter après l'opération de clonage	<p>Spécifiez le chemin d'accès et les arguments du script PostScript que vous souhaitez exécuter après l'opération de clonage.</p> <p>Vous devez stocker le script PostScript dans <i>/var/opt/snapcenter/spl/scripts</i> ou dans n'importe quel dossier de ce chemin. Par défaut, le chemin <i>/var/opt/snapcenter/spl/scripts</i> est renseigné.</p> <p>Si vous avez placé le script dans un dossier de ce chemin, vous devez fournir le chemin complet vers le dossier où le script est placé.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si l'opération de clonage échoue, les scripts postaux ne sont pas exécutés et les activités de nettoyage sont déclenchées directement.</p> </div>

- Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

- Vérifiez le résumé, puis cliquez sur **Terminer**.



Lors de l'exécution de la restauration dans le cadre de l'opération de création de clones, même en cas de défaillance de la restauration, le clone est créé avec un avertissement. Vous pouvez effectuer une restauration manuelle sur ce clone pour assurer la cohérence de la base de données clone.

- Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Résultat

Après le clonage de la base de données, vous pouvez actualiser la page de ressources pour afficher la base de données clonée comme l'une des ressources disponibles pour la sauvegarde. La base de données clonée peut être protégée comme toute autre base de données grâce au workflow de sauvegarde standard ou être incluse dans un groupe de ressources (nouvellement créé ou existant). La base de données clonée peut être davantage clonée (clone).

Après le clonage, vous ne devez jamais renommer la base de données clonée.



Si vous n'avez pas effectué de restauration lors du clonage, la sauvegarde de la base de données clonée peut échouer en raison d'une restauration incorrecte, et vous devrez donc effectuer une restauration manuelle. La sauvegarde du journal peut également échouer si l'emplacement par défaut renseigné pour les journaux d'archivage est dans un stockage non NetApp ou si le système de stockage n'est pas configuré avec SnapCenter.

Dans la configuration AIX, vous pouvez utiliser la commande `lkdev` pour verrouiller et la commande `rendev` pour renommer les disques sur lesquels réside la base de données clonée.

Le verrouillage ou le changement de nom des périphériques n'affecte pas l'opération de suppression du clone. Pour les mises en page LVM d'AIX construites sur des périphériques SAN, le changement de nom des périphériques ne sera pas pris en charge pour les périphériques SAN clonés.

### Plus d'informations

- ["Échec de la restauration ou du clonage avec le message d'erreur ORA-00308"](#)
- ["Impossible de restaurer une base de données clonée"](#)
- ["Paramètres personnalisables pour les opérations de sauvegarde, de restauration et de clonage sur les systèmes AIX"](#)

### Mettez à jour l'adresse IP préférée sur l'hôte

Une fois l'opération de clonage terminée, le chemin fourni par la couche d'accès au stockage (SAL) vers le clone sera au format `<nfs_lif_IP>:<JunctionPath>`. Pour fournir l'adresse IP préférée, vous devez la configurer sur l'hôte à l'aide des commandes SCCLI.

#### Étapes

1. Connectez-vous à l'hôte de la base de données.
2. Lancez une session de connexion PowerShell avec SnapCenter pour un utilisateur spécifié.

```
Open-SmConnection
```

3. Créez un fichier vide.

```
appuyez sur /var/opt/SnapCenter/scu/etc/storagepreference.properties
```

4. Configurer la LIF de données préférée pour le SVM

```
Add-SvmPreferredDataPath -SVM <SVM Name> -DataPath <adresse IP ou FQDN>
```

5. Vérifiez le chemin préféré.

```
Get-SvmPreferredDataPath
```

### Cloner une base de données enfichable

Vous pouvez cloner une base de données enfichable (PDB) sur un CDB cible différent ou identique sur le même hôte ou un autre hôte. Vous pouvez également récupérer le PDB cloné sur un SCN ou une date et une heure souhaités.

### Avant de commencer

Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données de type instance unique (multitenant) dans la vue détaillée de la base de données ou dans la vue détaillée du groupe de ressources.

La page topologie de la base de données s'affiche.

4. Dans la vue gérer les copies, sélectionnez les sauvegardes depuis les copies locales (primaires), les copies miroir (secondaires) ou les copies de coffre-fort (secondaires).
5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur .
6. Dans la page Nom, effectuez les opérations suivantes :
  - a. Sélectionnez **PDB Clone**.
  - b. Spécifiez le PDB à cloner.



Vous ne pouvez cloner qu'un seul boîtier de distribution électrique à la fois.

- c. Spécifiez le nom du PDB clone.

7. Dans la page emplacements, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Hôte clone	Par défaut, l'hôte de la base de données source est renseigné.  Si vous souhaitez créer le clone sur un autre hôte, sélectionnez l'hôte ayant la même version d'Oracle et de système d'exploitation que celle de l'hôte de base de données source.
CDB cible	Sélectionnez le CDB dans lequel vous souhaitez inclure le PDB cloné.  Vous devez vous assurer que le CDB cible est en cours d'exécution.
État de la base de données	Cochez la case <b>Ouvrir le PDB cloné en mode LECTURE-ÉCRITURE</b> si vous souhaitez ouvrir le PDB en mode LECTURE-ÉCRITURE.

<p>Emplacement des fichiers de données</p>	<p>Par défaut, l'emplacement du fichier de données est renseigné.</p> <p>la convention de nommage par défaut de SnapCenter pour les systèmes de fichiers SAN ou NFS est FileSystemNamedesourcedatabase_SCJOBID.</p> <p>la convention de nommage par défaut de SnapCenter pour les groupes de disques ASM est SC_HASHCODEofDISKGROUP_SCJOBID. Le HASHCODEofDISKGROUP est un nombre généré automatiquement (2 à 10 chiffres) unique pour chaque groupe de disques ASM.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>Si vous personnalisez le nom du groupe de disques ASM, assurez-vous que la longueur du nom respecte la longueur maximale prise en charge par Oracle.</p> </div> <p>Si vous souhaitez définir un autre chemin, vous devez entrer les points de montage des fichiers de données ou les noms de groupe de disques ASM pour cloner la base de données.</p>
--------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Les informations relatives au domicile Oracle, au nom d'utilisateur et au groupe sont automatiquement renseignées à partir de la base de données source. Vous pouvez modifier les valeurs en fonction de l'environnement Oracle de l'hôte sur lequel le clone sera créé.

8. Dans la page opérations préopérationnelles, effectuez les opérations suivantes :

- a. Entrez le chemin d'accès et les arguments du prescripteur que vous souhaitez exécuter avant l'opération de clonage.

Vous devez stocker le prescripteur dans `/var/opt/snapcenter/spl/scripts` ou dans n'importe quel dossier de ce chemin d'accès. Par défaut, le chemin `/var/opt/snapcenter/SPL/scripts` est renseigné. Si vous avez placé le script dans un dossier de ce chemin, vous devez fournir le chemin complet vers le dossier où le script est placé.

SnapCenter vous permet d'utiliser les variables d'environnement prédéfinies lorsque vous exécutez le prescripteur et le PostScript. ["En savoir plus >>"](#)

- a. Dans la section Paramètres de la base de données de clonage CDB auxiliaire, modifiez les valeurs des paramètres de base de données préremplis utilisés pour initialiser la base de données.

9. Cliquez sur **Réinitialiser** pour obtenir les paramètres par défaut de la base de données.

10. Dans la page opérations postales, **jusqu'à ce que Annuler** soit sélectionné par défaut pour effectuer la récupération de la base de données clonée.

L'option **jusqu'à Annuler** n'est pas sélectionnée si SnapCenter ne trouve pas les sauvegardes de journal appropriées. Vous pouvez indiquer l'emplacement du journal d'archivage externe si la sauvegarde du journal n'est pas disponible dans **spécifier les emplacements du journal d'archivage externe**. Vous

pouvez spécifier plusieurs emplacements de journaux.



Si vous souhaitez cloner une base de données source configurée pour prendre en charge la zone de récupération flash (FRA) et les fichiers gérés Oracle (OMF), la destination du journal pour la récupération doit également adhérer à la structure de répertoires OMF.

Nom du champ	Description
Jusqu'à Annuler	<p>SnapCenter effectue les restaurations en installant la dernière sauvegarde des journaux, puis en suivant cette sauvegarde de données sélectionnée pour le clonage, qui suit la séquence indéfinie des journaux d'archivage.</p> <p>La sauvegarde des journaux et des données doit se trouver sur le système de stockage principal afin d'effectuer le clonage sur le stockage primaire et la sauvegarde des journaux, et la sauvegarde des données doit se trouver sur un système de stockage secondaire pour effectuer le clonage sur le stockage secondaire. La base de données clonée est restaurée jusqu'au fichier journal manquant ou corrompu.</p>
Date et heure	<p>SnapCenter restaure la base de données jusqu'à une date et une heure spécifiées.</p> <p> L'heure peut être spécifiée au format 24 heures.</p>
Jusqu'à SCN (numéro de changement du système)	SnapCenter restaure la base de données jusqu'à un numéro de modification du système (SCN) spécifié.
Spécifiez les emplacements des journaux d'archives externes	Spécifiez l'emplacement du journal d'archivage externe.
Créer un nouveau DBID	<p>Par défaut, la case à cocher <b>Créer un nouveau DBID</b> n'est pas sélectionnée pour la base de données de clonage auxiliaire.</p> <p>Cochez la case si vous souhaitez générer un numéro unique (DBID) pour la base de données clonée auxiliaire la différencie de la base de données source.</p>
Créer un fichier tempfile pour l'espace de table temporaire	<p>Cochez la case si vous souhaitez créer un fichier tempfile pour le tablespace temporaire par défaut de la base de données clonée.</p> <p>Si la case n'est pas cochée, le clone de la base de données est créé sans le fichier tempfile.</p>

Nom du champ	Description
Entrez les entrées sql à appliquer lors de la création du clone	Ajoutez les entrées sql que vous souhaitez appliquer lors de la création du clone.
Entrez les scripts à exécuter après l'opération de clonage	<p>Spécifiez le chemin d'accès et les arguments du script PostScript que vous souhaitez exécuter après l'opération de clonage.</p> <p>Vous devez stocker le script PostScript dans <code>/var/opt/snapcenter/spl/scripts</code> ou dans n'importe quel dossier de ce chemin.</p> <p>Par défaut, le chemin <code>/var/opt/snapcenter/spl/scripts</code> est renseigné. Si vous avez placé le script dans un dossier de ce chemin, vous devez fournir le chemin complet vers le dossier où le script est placé.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Si l'opération de clonage échoue, les scripts postaux ne sont pas exécutés et les activités de nettoyage sont déclenchées directement. </div>

11. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

12. Vérifiez le résumé, puis cliquez sur **Terminer**.
13. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Après la fin

Si vous souhaitez créer une sauvegarde du PDB cloné, vous devez sauvegarder le CDB cible dans lequel le PDB est cloné, car la sauvegarde ne peut être effectuée que par le PDB cloné. Vous devez créer une relation secondaire pour le CDB cible si vous souhaitez créer la sauvegarde avec la relation secondaire.

Dans une configuration RAC, le stockage pour PDB cloné est uniquement relié au nœud sur lequel le clone PDB a été effectué. Les PDB sur les autres nœuds du RAC sont en état DE MONTAGE. Si vous souhaitez que le PDB cloné soit accessible à partir des autres nœuds, vous devez connecter manuellement le stockage aux autres nœuds.

### Plus d'informations

- ["Échec de la restauration ou du clonage avec le message d'erreur ORA-00308"](#)
- ["Paramètres personnalisables pour les opérations de sauvegarde, de restauration et de clonage sur les systèmes AIX"](#)

## Cloner les sauvegardes de bases de données Oracle à l'aide des commandes UNIX

Le workflow de clonage inclut la planification, la réalisation de l'opération de clonage et le contrôle de l'opération.

### À propos de cette tâche

Vous devez exécuter les commandes suivantes pour créer le fichier de spécification du clone de base de données Oracle et lancer l'opération de clonage.

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également vous reporter à la ["Guide de référence sur les commandes du logiciel SnapCenter"](#).

### Étapes

1. Créez une spécification de clone de base de données Oracle à partir d'une sauvegarde spécifiée : *New-SmOracleCloneSpecification*



Si la règle de protection des données secondaire est unifiée mirror-vault, spécifiez uniquement `-IncludeAppuyDetails`. Vous n'avez pas besoin de spécifier `-Deuxièmement.StorageType`.

Cette commande crée automatiquement un fichier de spécification de clone de base de données Oracle pour la base de données source spécifiée et sa sauvegarde. Vous devez également fournir un SID de base de données clone afin que le fichier de spécifications créé ait les valeurs générées automatiquement pour la base de données clone que vous allez créer.



Le fichier de spécifications du clone est créé à l'adresse `/var/opt/snapcenter/sco/clone_specs`.

2. Lancez une opération de clonage à partir d'un groupe de ressources clone ou d'une sauvegarde existante : *New-SmClone*

Cette commande démarre une opération de clonage. Vous devez également fournir un chemin d'accès au fichier de spécification de clone Oracle pour l'opération de clonage. Vous pouvez également spécifier les options de récupération, l'hôte où l'opération de clonage doit être effectuée, les prescripteurs, les postscripts et d'autres détails.

Par défaut, le fichier de destination du journal d'archivage de la base de données clone est automatiquement renseigné à `$ORACLE_HOME/CLONE_SID`.

## Séparer un clone de base de données Oracle

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### À propos de cette tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé `clone1` à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de `clone1`, puis cloner cette sauvegarde (`clone2`). Après avoir créé `clone2`, `clone1` est un

clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde du clone sont supprimées.
- Pour plus d'informations sur les opérations de répartition des volumes FlexClone, voir, "[Séparer un volume FlexClone de son volume parent](#)"
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.
3. Sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur .
4. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement de clone cesse de répondre si le service SMCore redémarre et si les bases de données sur lesquelles l'opération de fractionnement de clone ont été exécutées sont répertoriées sous forme de clones dans la page Ressources. Vous devez exécuter l'applet de commande *Stop-SmJob* pour arrêter l'opération de fractionnement du clone, puis relancer l'opération de fractionnement du clone.

Si vous souhaitez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre CloneSplitStatusCheckPollTime dans le fichier SMCoreServiceHost.exe.config afin de définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou le fractionnement d'un autre clone est en cours. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

## Séparer le clone d'une base de données enfichable

Vous pouvez utiliser SnapCenter pour diviser une base de données clonée enfichable (PDB).

### À propos de cette tâche

Si vous avez créé une sauvegarde du CDB cible dans laquelle le PDB est cloné, lorsque vous fractionnez le clone PDB, le PDB cloné est également supprimé de toutes les sauvegardes du BCD cible contenant le PDB

cloné.



Les clones PDB ne sont pas affichés dans la vue Inventaire ou ressources.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Sélectionnez la base de données du conteneur source (CDB) dans la vue ressource ou groupe de ressources.
3. Dans la vue gérer les copies, sélectionnez **clones** dans les systèmes de stockage primaire ou secondaire (mis en miroir ou répliqué).
4. Sélectionnez le clone PDB (targetCDB:PDBClone), puis cliquez sur .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Surveillez les opérations de clonage de bases de données Oracle

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.

4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Actualiser un clone

Vous pouvez actualiser le clone en exécutant la commande *Refresh-SmClone*. Cette commande crée une sauvegarde de la base de données, supprime le clone existant et crée un clone portant le même nom.



Vous ne pouvez pas actualiser un clone PDB.

### Ce dont vous aurez besoin

- Créez une sauvegarde complète en ligne ou une stratégie de sauvegarde des données hors ligne sans que les sauvegardes planifiées soient activées.
- Configurez la notification par e-mail dans la stratégie pour les échecs de sauvegarde uniquement.
- Définissez le nombre de rétention pour les sauvegardes à la demande de façon appropriée pour garantir qu'il n'y a pas de sauvegardes non souhaitées.
- Assurez-vous que seule une sauvegarde complète en ligne ou une stratégie de sauvegarde des données hors ligne est associée au groupe de ressources identifié pour l'opération d'actualisation du clone.
- Créez un groupe de ressources avec une seule base de données.
- Si une tâche cron est créée pour la commande d'actualisation de clone, assurez-vous que les planifications SnapCenter et cron ne se chevauchent pas pour le groupe de ressources de base de données.

Pour une tâche cron créée pour la commande d'actualisation de clone, assurez-vous d'exécuter *Open-SmConnection* après toutes les 24 heures.

- Assurez-vous que le SID de clone est unique pour un hôte.

Si plusieurs opérations d'actualisation de clone utilisent le même fichier de spécifications de clone ou utilisent le fichier de spécifications de clone avec le même SID de clone, le clone existant avec le SID sur l'hôte est supprimé et le clone est alors créé.

- Assurez-vous que la politique de sauvegarde est activée avec une protection secondaire et que le fichier de spécifications du clone est créé avec `"-IncludeDeuetaryDetailss"` pour créer les clones à l'aide de sauvegardes secondaires.
  - Si le fichier de spécification du clone principal est spécifié mais que l'option de mise à jour secondaire de la règle est sélectionnée, la sauvegarde est créée et la mise à jour est transférée vers le fichier secondaire. Cependant, le clone sera créé à partir de la sauvegarde principale.
  - Si le fichier de spécification du clone principal est spécifié et que l'option de mise à jour secondaire de la règle n'est pas sélectionnée, la sauvegarde est créée sur le fichier principal et le clone est créé à partir du fichier principal.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié : *Open-SmConnection*
2. Créez une spécification de clone de base de données Oracle à partir d'une sauvegarde spécifiée : *New-*



Si la règle de protection des données secondaire est unifiée mirror-vault, spécifiez uniquement `-IncludeAppuyDetails`. Vous n'avez pas besoin de spécifier `-Deuxièmement.StorageType`.

Cette commande crée automatiquement un fichier de spécification de clone de base de données Oracle pour la base de données source spécifiée et sa sauvegarde. Vous devez également fournir un SID de base de données clone afin que le fichier de spécifications créé ait les valeurs générées automatiquement pour la base de données clone que vous allez créer.



Le fichier de spécifications du clone est créé à l'adresse `/var/opt/snapcenter/sco/clone_specs`.

### 3. Exécutez `Refresh-SmClone`.

Si l'opération échoue avec les messages d'erreur "PL-SCO-20032: CanExecute a échoué avec l'erreur: PL-SCO-30031: Redo log file +SC\_2959770772\_clmdb/clmdb/redo01\_01.log existe", spécifiez une valeur plus élevée pour `-WaitToTriggerClone`.

Pour plus d'informations sur les commandes UNIX, reportez-vous au ["Guide de référence sur les commandes du logiciel SnapCenter"](#).

## Supprimer le clone d'une base de données enfichable

Vous pouvez supprimer le clone d'une base de données enfichable (PDB) si vous n'en avez plus besoin.

Si vous avez créé une sauvegarde du CDB cible dans laquelle le PDB est cloné, lorsque vous supprimez le clone PDB, le PDB cloné est également supprimé de la sauvegarde du CDB cible.



Les clones PDB ne sont pas affichés dans la vue Inventaire ou ressources.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Sélectionnez la base de données du conteneur source (CDB) dans la vue ressource ou groupe de ressources.
3. Dans la vue gérer les copies, sélectionnez **clones** dans les systèmes de stockage primaire ou secondaire (mis en miroir ou répliqué).
4. Sélectionnez le clone PDB (targetCDB:PDBClone), puis cliquez sur .
5. Cliquez sur **OK**.

## Gestion des volumes d'applications

### Que sont les volumes d'applications

Les volumes d'application sont des volumes de stockage dans lesquels sont stockées

des informations telles que la configuration, le programme d'installation et d'autres fichiers autres que des données liés à la base de données Oracle.

Le plug-in SnapCenter pour bases de données Oracle vous permet de créer une sauvegarde cohérente des volumes applicatifs (volumes non-données) avec les bases de données Oracle.

Ce plug-in automatise la sauvegarde et le clonage des volumes d'applications.

- Protégez les volumes d'application et les volumes de base de données Oracle au sein d'un seul groupe de ressources.
- Création de sauvegardes des volumes applicatifs
- Créez des sauvegardes des bases de données Oracle avec les volumes d'application.
- Créez des clones de bases de données et de volumes applicatifs jusqu'à un point dans le temps.
- Planifiez les opérations de sauvegarde.
- Contrôle de toutes les opérations.
- Afficher des rapports sur les opérations de sauvegarde et de clonage

## Ajout de volumes d'application

SnapCenter prend en charge la sauvegarde et le clonage des volumes d'applications de base de données Oracle. Vous devez ajouter manuellement les volumes d'application. La découverte automatique des volumes d'application n'est pas prise en charge.



Les volumes d'application ne prennent en charge que les connexions NFS directes et iSCSI.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Cliquez sur **Ajouter un volume d'application**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - Dans le champ Nom, entrez le nom du volume de l'application.
  - Dans le champ Nom d'hôte, entrez le nom de l'hôte.
4. Dans la page Storage Footprint, entrez le nom du système de stockage, sélectionnez un ou plusieurs volumes, puis spécifiez les LUN ou qtrees associés.

Vous pouvez ajouter plusieurs systèmes de stockage.

5. Vérifiez le résumé, puis cliquez sur **Terminer**.
6. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage** pour afficher tous les volumes d'application que vous avez ajoutés.

### Modifier le volume de l'application

Vous pouvez modifier toutes les valeurs que vous avez spécifiées lors de l'ajout du volume d'application, si aucune sauvegarde n'est créée. Si la sauvegarde est créée, vous ne pouvez modifier que les détails du système de stockage.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage**.
3. Cliquez sur  pour modifier les valeurs.
4. Cliquez sur  pour modifier les valeurs.

## Supprimer le volume de l'application

Lorsque vous supprimez un volume d'application, en cas de sauvegardes associées au volume d'application, le volume d'application est mis en mode maintenance. Aucune sauvegarde nouvelle n'est créée et aucune sauvegarde antérieure n'est conservée. Si aucune sauvegarde n'est associée, toutes les métadonnées seront supprimées.

Si nécessaire, SnapCenter vous permet d'annuler l'opération de suppression.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage**.
3. Cliquez sur  [l'icône Supprimer] pour modifier les valeurs.

## Sauvegarder les volumes d'applications

### Sauvegarder le volume d'application

Si le volume d'application ne fait partie d'aucun groupe de ressources, vous pouvez sauvegarder le volume d'application à partir de la page Ressources.

### À propos de cette tâche

Par défaut, des sauvegardes de groupe de cohérence sont créées. Si vous souhaitez créer des sauvegardes basées sur des volumes, définissez la valeur de **EnableOracleNdvVolumeBasedBackup** sur true dans le fichier *web.config*.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage**.
3. Cliquez sur \* , puis sélectionnez le nom d'hôte et le type de base de données pour filtrer les ressources.  
  
Vous pouvez alors cliquer sur \*  pour fermer le volet de filtre.
4. Sélectionnez le volume d'application à sauvegarder.

La page protection du volume de l'application s'affiche.

5. Dans la page ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Utilisez le format de nom personnalisé pour la copie Snapshot	Cochez cette case, puis entrez un format de nom personnalisé à utiliser pour le nom du snapshot.  Par exemple, clienttext__policy_hostname ou Resource_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.
Exclure les destinations du journal d'archivage de la sauvegarde	Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.

6. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Cliquez sur  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer une planification.

c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de sauvegarde effectuée sur la ressource, puis sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell set-SmSmtServer.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

La page topologie du volume de l'application s'affiche.

9. Cliquez sur **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.
- b. Cliquez sur **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Sauvegarder le groupe de ressources des volumes d'application

Vous pouvez sauvegarder le groupe de ressources contenant uniquement des volumes d'application ou une combinaison de volumes d'application et de bases de données. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

Si le groupe de ressources possède plusieurs volumes d'application, tous les volumes d'application doivent avoir une règle de réplication SnapMirror ou SnapVault.

### À propos de cette tâche

Par défaut, des sauvegardes de groupe de cohérence sont créées. Si vous souhaitez créer des sauvegardes basées sur des volumes, définissez la valeur de **EnableOracleNdvVolumeBasedBackup** sur true dans le fichier *web.config*.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en cliquant sur \*\*, puis en sélectionnant la balise. Vous pouvez alors cliquer sur \* pour fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis cliquez sur **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.



L'opération de vérification sera effectuée uniquement pour les bases de données et non pour les volumes d'application.

## Sauvegarde des volumes des applications clonées

Vous pouvez cloner les sauvegardes de volumes d'applications à l'aide de SnapCenter.

## Avant de commencer

Si vous avez installé le plug-in en tant qu'utilisateur non root, vous devez attribuer manuellement les autorisations d'exécution aux répertoires prescripteur et postscript.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage**.
3. Sélectionnez le volume d'application dans la vue Détails du volume d'application ou dans la vue Détails du groupe de ressources.

La page topologie du volume de l'application s'affiche.

4. Dans la vue gérer les copies, sélectionnez les sauvegardes depuis les copies locales (primaires), les copies miroir (secondaires) ou les copies de coffre-fort (secondaires).

5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur .

6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Hôte de plug-in	Sélectionnez l'hôte dans lequel vous souhaitez créer le clone.
Nom de la ressource cible	Spécifiez le nom de la ressource.

7. Dans la page scripts, spécifiez les noms des scripts à exécuter avant le clonage, les commandes de montage d'un système de fichiers et les noms des scripts à exécuter après le clonage.
8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Séparer un clone de volume d'application

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.

2. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage**.
3. Sélectionnez la ressource clonée et cliquez sur .
4. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Supprime un clone de volume d'application

Vous pouvez supprimer les clones si vous les trouvez devenus superflus. Vous ne pouvez pas supprimer des clones qui agissent comme la source pour d'autres clones.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Oracle Database dans la liste.
2. Dans la page Ressources, sélectionnez **Volume d'application** dans la liste **Affichage**.
3. Sélectionnez la ressource ou le groupe de ressources dans la liste.  
  
La page topologie de ressource ou de groupe de ressources s'affiche.
4. Dans la vue gérer les copies, sélectionnez **clones** dans les systèmes de stockage primaire ou secondaire (mis en miroir ou répliqué).
5. Sélectionnez le clone, puis cliquez sur .
6. Sur la page Supprimer le clone, effectuez les opérations suivantes :
  - a. Dans le champ **Pre clone delete**, entrez les noms des scripts à exécuter avant de supprimer le clone.
  - b. Dans le champ **Unmount**, entrez les commandes permettant de démonter le clone avant de supprimer le clone.
7. Cliquez sur **OK**.

# Protection des systèmes de fichiers Windows

## Le plug-in SnapCenter pour Microsoft Windows concepts

### Présentation du plug-in SnapCenter pour Microsoft Windows

Le plug-in SnapCenter pour Microsoft Windows est un composant côté hôte du logiciel NetApp SnapCenter qui permet de gérer la protection des données et les applications des ressources du système de fichiers Microsoft. De plus, il assure le provisionnement du stockage, la cohérence Snapshot et la récupération d'espace pour les systèmes de fichiers Windows. Le plug-in pour Windows automatise les opérations de sauvegarde, de restauration et de clonage des systèmes de fichiers dans votre environnement SnapCenter.

Lorsque le plug-in pour Windows est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume et grâce à la technologie NetApp SnapVault afin d'effectuer une réplication de sauvegarde disque à disque à des fins d'archivage ou de conformité aux normes.

- Protège les données respectueuses des applications pour les autres plug-ins exécutés dans les hôtes Windows de votre environnement SnapCenter
- Automatise les opérations de sauvegarde, de restauration et de clonage respectueuses des applications pour les systèmes de fichiers Microsoft dans votre environnement SnapCenter
- Prend en charge le provisionnement du stockage, la cohérence Snapshot et la récupération d'espace pour les hôtes Windows



Le plug-in pour Windows provisionne les partages SMB et les systèmes de fichiers Windows sur les LUN physiques et RDM, mais ne prend pas en charge les opérations de sauvegarde pour les systèmes de fichiers Windows sur les partages SMB.

### Ce que vous pouvez faire avec le plug-in SnapCenter pour Microsoft Windows

Lorsque le plug-in pour Windows est installé dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner les systèmes de fichiers Windows. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Découvrir les ressources
- Sauvegarder les systèmes de fichiers Windows
- Planifiez les opérations de sauvegarde
- Restaurer les sauvegardes du système de fichiers
- Cloner les sauvegardes du système de fichiers
- Contrôle des opérations de sauvegarde, de restauration et de clonage



Le plug-in pour Windows ne prend pas en charge la sauvegarde et la restauration des systèmes de fichiers sur les partages SMB.

## Le plug-in SnapCenter pour Windows

Le plug-in pour Windows s'intègre à la technologie NetApp Snapshot sur le système de stockage. Pour utiliser le plug-in pour Windows, utilisez l'interface SnapCenter.

Le plug-in pour Windows inclut les principales fonctionnalités suivantes :

- **Interface graphique utilisateur unifiée optimisée par SnapCenter**

L'interface SnapCenter vous permet de standardiser et d'assurer une cohérence entre les plug-ins et les environnements. L'interface SnapCenter vous permet d'effectuer des sauvegardes et des restaurations cohérentes dans l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues du tableau de bord en un coup d'œil, de configurer le contrôle d'accès basé sur les rôles et de surveiller les tâches dans tous les plug-ins. SnapCenter propose également une planification et une gestion centralisées des règles pour prendre en charge les opérations de sauvegarde et de clonage.

- **Administration centrale automatisée**

Vous pouvez planifier des sauvegardes de routine des systèmes de fichiers, configurer la conservation des sauvegardes basée sur des règles et configurer des opérations de restauration. Vous pouvez également surveiller de manière proactive votre environnement de système de fichiers en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie snapshot NetApp non disruptive**

Le plug-in pour Windows utilise la technologie Snapshot de NetApp. Vous pouvez ainsi sauvegarder vos systèmes de fichiers en quelques secondes et les restaurer rapidement sans mettre l'hôte hors ligne. Les copies Snapshot consomment un espace de stockage minimal.

Outre ces fonctionnalités principales, le plug-in pour Windows offre les avantages suivants :

- Prise en charge des flux de travail relatifs aux sauvegardes, aux restaurations et aux clones
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles
- Création de copies compactes de systèmes de fichiers de production à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Pour obtenir des informations sur les licences FlexClone, reportez-vous à la section "[Licences SnapCenter](#)".

- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs serveurs
- Les applets de commande PowerShell pour créer des scripts pour les opérations de sauvegarde, de restauration et de clonage
- Prise en charge des sauvegardes des systèmes de fichiers et des disques de machines virtuelles (VMDK)
- Prise en charge des infrastructures physiques et virtualisées
- Prise en charge des protocoles iSCSI, Fibre Channel, FCoE, Raw Device Mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK over NFS et VMFS, et du protocole FC virtuel
- Prise en charge de NVMe (non-volatile Memory Express) sur Windows Server 2022
  - Workflows de sauvegarde, de restauration, de clonage et de vérification sur une disposition VMDK créée sur NVMe over TCP/IP.
  - Prend en charge la version 1.3 du firmware NVMe à partir de la mise à jour 2 d'ESX 8.0 et requiert la

version 21 du matériel virtuel.

- Windows Server Failover Clustering (WSFC) n'est pas pris en charge pour les applications sur VMDK sur NVMe over TCP/IP.
- Prise en charge de la synchronisation active SnapMirror (initialement lancée sous la forme de SnapMirror Business Continuity [SM-BC]) qui assure la continuité des services de l'entreprise même en cas de défaillance complète du site, permettant ainsi aux applications de basculer en toute transparence au moyen d'une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

## Sauvegarde des systèmes de fichiers Windows par SnapCenter

SnapCenter utilise la technologie Snapshot pour sauvegarder les ressources du système de fichiers Windows qui résident sur des LUN, des CSV (volumes partagés de clusters), des volumes RDM (mappage de périphériques bruts), ALM (mappage de LUN asymétrique) dans des clusters Windows et des VMDK basés sur VMFS/NFS (VMware Virtual machine File System utilisant NFS).

SnapCenter crée des sauvegardes en créant des snapshots des systèmes de fichiers. Les sauvegardes fédérées, dans lesquelles un volume contient des LUN provenant de plusieurs hôtes, sont plus rapides et plus efficaces que les sauvegardes de chaque LUN, car une seule copie Snapshot du volume est créée par rapport aux snapshots individuels de chaque système de fichiers.

Lorsque SnapCenter crée une copie Snapshot, l'intégralité du volume du système de stockage est capturée dans la copie Snapshot. Cependant, la sauvegarde n'est valide que pour le serveur hôte pour lequel la sauvegarde a été créée.

Si les données d'autres serveurs hôtes résident sur le même volume, elles ne peuvent pas être restaurées à partir du Snapshot.



Si un système de fichiers Windows contient une base de données, la sauvegarde du système de fichiers n'est pas la même que la sauvegarde de la base de données. Pour sauvegarder une base de données, vous devez utiliser l'un des plug-ins de base de données.

## Types de stockage pris en charge par le plug-in SnapCenter pour Microsoft Windows

SnapCenter prend en charge un large éventail de types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier si la prise en charge de votre type de stockage est disponible avant d'installer le package pour votre hôte.

Le provisionnement et la protection des données SnapCenter sont pris en charge par Windows Server. Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp](#)".

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur physique	LUN connectés via FC	Interface graphique SnapCenter ou applets de commande PowerShell	

<b>Machine</b>	<b>Type de stockage</b>	<b>Provisionnement avec</b>	<b>Notes de support</b>
Serveur physique	LUN connectées à l'iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	
Serveur physique	Partages SMB3 (CIFS) résidant sur un SVM (Storage Virtual machine)	Interface graphique SnapCenter ou applets de commande PowerShell	Prise en charge du provisionnement uniquement.
VM VMware	LUN RDM connectés par un HBA FC ou iSCSI	Applets de commande PowerShell	
VM VMware	LUN iSCSI connectés directement au système invité par l'initiateur iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	
VM VMware	Datastores VMFS (Virtual machine File Systems) ou NFS	VMware vSphere	
VM VMware	Système invité connecté à des partages SMB3 résidant sur un SVM	Interface graphique SnapCenter ou applets de commande PowerShell	Prise en charge du provisionnement uniquement.
VM VMware	Datastores vVol sur NFS et SAN	Outils ONTAP pour VMware vSphere	

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur virtuel Hyper-V.	LUN FC virtuels (VFC) connectés par un commutateur Fibre Channel virtuel	Interface graphique SnapCenter ou applets de commande PowerShell	<p data-bbox="1156 151 1489 361">Vous devez utiliser Hyper-V Manager pour provisionner les LUN FC virtuels (VFC) connectés par un commutateur Fibre Channel virtuel.</p> <div data-bbox="1188 394 1461 961" style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p data-bbox="1307 403 1455 953">Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>
Serveur virtuel Hyper-V.	LUN iSCSI connectés directement au système invité par l'initiateur iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	<div data-bbox="1188 1024 1461 1570" style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p data-bbox="1307 1024 1455 1562">Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur virtuel Hyper-V.	Système invité connecté à des partages SMB3 résidant sur un SVM	Interface graphique SnapCenter ou applets de commande PowerShell	Prise en charge du provisionnement uniquement. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">  <p>Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>

## Privilèges ONTAP minimum requis pour le plug-in Windows

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - suppression de la lun
  - lun igroup add
  - créez un groupe initiateur lun
  - suppression du groupe initiateur lun
  - renommer la lun igroup
  - affichage de la lun igroup
  - lun mapping des nœuds supplémentaires
  - création d'un mappage de lun
  - suppression du mappage de lun
  - mappage de lun supprimer-rapports-nœuds

- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes
- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume

- suppression du snapshot de volume
- modification de snapshot de volume
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau
  - interface réseau affiche
  - un vserver

## **Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault**

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Définir une stratégie de sauvegarde pour les systèmes de fichiers Windows

En définissant une stratégie de sauvegarde avant de créer vos sauvegardes, vous obtenez les sauvegardes dont vous avez besoin pour restaurer ou cloner vos systèmes de fichiers. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

### Planifications de sauvegarde pour les systèmes de fichiers Windows

La fréquence de sauvegarde est spécifiée dans les stratégies ; un planning de sauvegarde est spécifié dans la configuration du groupe de ressources. Le facteur le plus important dans la détermination d'une fréquence ou d'un planning de sauvegarde est le taux de changement pour la ressource et l'importance des données. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. Parmi les autres facteurs figurent l'importance de la ressource pour votre organisation, votre contrat de niveau de service (SLA) et votre objectif de point de récupération (RPO).

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés au service, notamment la disponibilité et les performances de celui-ci. Un RPO définit la stratégie selon laquelle les fichiers doivent être récupérés à partir du stockage de sauvegarde afin que des opérations régulières puissent reprendre après une défaillance. Les SLA et RPO contribuent à la stratégie de protection des données.

Même avec une ressource largement utilisée, il n'est pas nécessaire d'exécuter une sauvegarde complète plus d'une fois ou deux fois par jour.

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes

La fréquence de sauvegarde (fréquence d'exécution des sauvegardes), appelée *schedule type* pour

certaines plug-ins, fait partie d'une configuration de stratégie. Par exemple, vous pouvez configurer la fréquence de sauvegarde en tant qu'heures, quotidiennes, hebdomadaires ou mensuelles, ou vous pouvez spécifier **aucun** qui fait de la stratégie une stratégie à la demande uniquement. Vous pouvez accéder aux stratégies en cliquant sur **Paramètres > stratégies**.

- Planifications de sauvegarde

Les planifications de sauvegarde (exactement quand les sauvegardes doivent être effectuées) font partie d'une configuration de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour sauvegarder chaque jeudi à 10 h 00. Vous pouvez accéder aux planifications de groupes de ressources en cliquant sur **Ressources > groupes de ressources**.

## Nombre de sauvegardes nécessaires pour les systèmes de fichiers Windows

Les facteurs déterminant le nombre de sauvegardes nécessaires incluent la taille du système de fichiers Windows, le nombre de volumes utilisés, le taux de changement du système de fichiers et votre contrat de niveau de service.

## convention de dénomination des sauvegardes pour les systèmes de fichiers Windows

Les sauvegardes du système de fichiers Windows utilisent la nomenclature établie par défaut des snapshots. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le snapshot utilise la convention de nommage par défaut suivante :  
resourcegroupname\_hostname\_timestamp

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dtst1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- dtst1 est le nom du groupe de ressources.
- mach1x88 est le nom d'hôte.
- 03-12-2015\_23.17.26 est la date et l'horodatage.

Lors de la création d'une sauvegarde, vous pouvez également ajouter une balise descriptive pour vous aider à identifier la sauvegarde. En revanche, si vous souhaitez utiliser une convention de dénomination de sauvegarde personnalisée, vous devez renommer la sauvegarde une fois l'opération terminée.

## Options de conservation des sauvegardes

Vous pouvez choisir le nombre de jours pendant lesquels vous souhaitez conserver les copies de sauvegarde ou spécifier le nombre de copies de sauvegarde à conserver, dans un maximum de 255 copies ONTAP. Par exemple, votre entreprise peut avoir besoin de conserver 10 jours de copies de sauvegarde ou 130 copies de sauvegarde.

Lors de la création d'une stratégie, vous pouvez spécifier les options de rétention pour le type de sauvegarde

et le type de planification.

Si vous configurez la réplication SnapMirror, la règle de conservation est mise en miroir sur le volume de destination.

SnapCenter supprime les sauvegardes conservées dont les étiquettes de conservation correspondent au type de planification. Si le type de planification a été modifié pour la ressource ou le groupe de ressources, les sauvegardes avec l'ancienne étiquette de type de planification peuvent rester sur le système.



Pour la conservation à long terme des copies de sauvegarde, nous vous recommandons d'utiliser la sauvegarde SnapVault.

## Sources et destinations des clones pour les systèmes de fichiers Windows

Vous pouvez cloner une sauvegarde du système de fichiers à partir d'un stockage primaire ou secondaire. Vous pouvez également choisir la destination qui répond à vos besoins : l'emplacement de sauvegarde d'origine ou une destination différente sur le même hôte ou sur un hôte différent. La destination doit se trouver sur le même volume que la sauvegarde source clone.

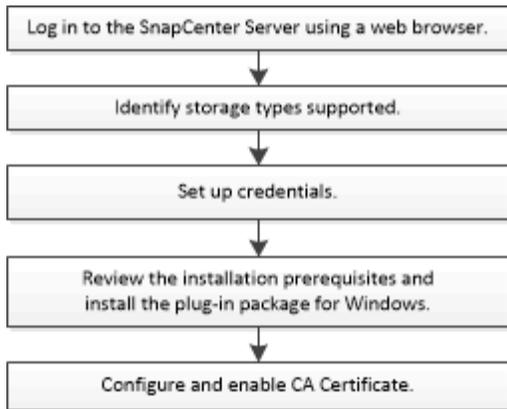
Destination des clones	Description
Original, source, emplacement	Par défaut, SnapCenter stocke le clone au même emplacement et sur le même hôte que la sauvegarde clonée.
Emplacement différent	Vous pouvez stocker le clone sur un autre emplacement sur le même hôte ou sur un autre hôte. L'hôte doit disposer d'une connexion configurée au SVM (Storage Virtual machine).

Vous pouvez renommer le clone une fois l'opération de clonage terminée.

## Installez le plug-in SnapCenter pour Microsoft Windows

### Workflow d'installation du plug-in SnapCenter pour Microsoft Windows

Vous devez installer et configurer le plug-in SnapCenter pour Microsoft Windows si vous souhaitez protéger les fichiers Windows qui ne sont pas des fichiers de base de données.



## Conditions d'installation requises pour le plug-in SnapCenter pour Microsoft Windows

Avant d'installer le plug-in pour Windows, vous devez connaître certaines conditions d'installation.

Avant de commencer à utiliser le plug-in pour Windows, l'administrateur SnapCenter doit installer et configurer SnapCenter Server et effectuer les tâches préalables.

- Vous devez disposer des privilèges d'administrateur SnapCenter pour installer le plug-in pour Windows.  
Le rôle d'administrateur SnapCenter doit disposer de privilèges d'administrateur.
- Vous devez avoir installé et configuré le serveur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Si vous souhaitez sauvegarder la réplication, vous devez configurer SnapMirror et SnapVault.

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systemes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p> <p>Si vous utilisez une configuration de cluster Windows, vous devez également installer et configurer la gestion à distance Windows (WinRM).</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO

Élément	De formation
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <p> Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

## Configurez vos informations d'identification pour le plug-in pour Windows

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter, ainsi que des informations d'identification supplémentaires pour exécuter les opérations de protection des données sur les systèmes de fichiers Windows.

### Ce dont vous aurez besoin

- Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.
- Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur, sur l'hôte distant.
- Si vous configurez des informations d'identification pour des groupes de ressources individuels et que l'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde à l'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.

3. Cliquez sur **Nouveau**.

4. Dans la page informations d'identification, procédez comme suit :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.
Nom d'utilisateur/Mot de passe	<p>Entrez le nom d'utilisateur et le mot de passe utilisés pour l'authentification.</p> <ul style="list-style-type: none"><li>Administrateur de domaine ou tout membre du groupe d'administrateurs</li></ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"><li>NetBIOS\UserName</li><li>Domain FQDN\UserName</li><li>UserName@upn</li></ul> <ul style="list-style-type: none"><li>Administrateur local (groupes de travail uniquement)</li></ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format du champ Nom d'utilisateur est le suivant :</p> <p>UserName</p> <p>N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.

5. Cliquez sur **OK**.

Une fois que vous avez terminé la configuration des informations d'identification, vous pouvez affecter la

maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs sur la page utilisateur et accès.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

### Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

### Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediately
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

Par exemple :

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :
  - a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Ajoutez des hôtes et installez le plug-in SnapCenter pour Microsoft Windows

Vous pouvez utiliser la page Ajouter un hôte SnapCenter pour ajouter des hôtes Windows. Le plug-in SnapCenter pour Microsoft Windows est automatiquement installé sur l'hôte spécifié. Il s'agit de la méthode recommandée pour installer les plug-ins. Vous pouvez ajouter un hôte et installer un plug-in pour un hôte individuel ou un cluster.

### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur

l'hôte.

- L'utilisateur SnapCenter doit être ajouté au rôle « se connecter en tant que service » du serveur Windows.
- Vous devez vous assurer que le service de mise en file d'attente des messages est en cours d'exécution.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

["Configurez le compte de service géré par groupe sur Windows Server 2016 ou version ultérieure pour Windows File System"](#)

### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.
- Plug-ins Windows
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installation des plug-ins sur un cluster

Si vous installez des plug-ins sur un cluster (WSFC, Oracle RAC ou Exchange DAG), ils sont installés sur tous les noeuds du cluster.

- Stockage E-Series

Vous ne pouvez pas installer le plug-in pour Windows sur un hôte Windows connecté au stockage E-Series.



SnapCenter ne prend pas en charge l'ajout du même hôte (hôte de plug-in) à SnapCenter si l'hôte fait déjà partie d'un groupe de travail et est modifié vers un autre domaine ou vice versa. Si vous souhaitez ajouter le même hôte, vous devez supprimer l'hôte de SnapCenter et l'ajouter à nouveau.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Assurez-vous que **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, procédez comme suit :

Pour ce champ...	Procédez comme ça...
Type d'hôte	Sélectionnez le type d'hôte <b>Windows</b> .  Le serveur SnapCenter ajoute l'hôte, puis installe le plug-in pour Windows s'il n'est pas déjà installé sur l'hôte.

Pour ce champ...	Procédez comme ça...
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le nom de domaine complet (FQDN).</p> <p>Vous pouvez entrer les adresses IP ou FQDN de l'un des éléments suivants :</p> <ul style="list-style-type: none"> <li>• Hôte autonome</li> <li>• Windows Server Failover Clustering (WSFC)</li> </ul> <p>Si vous ajoutez un hôte à l'aide de SnapCenter et qu'il fait partie d'un sous-domaine, vous devez fournir le FQDN.</p>
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez les nouvelles informations d'identification.</p> <p>Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus d'informations, reportez-vous à la section informations sur la création d'informations d'identification.</p> <p>Les informations d'identification, notamment le nom d'utilisateur, le domaine et le type d'hôte, s'affichent en plaçant votre curseur sur le nom d'identification fourni.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le mode d'authentification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

Pour les nouveaux déploiements, aucun plug-in n'est répertorié.

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port.</p> <p>Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue. </div>
Chemin d'installation	<p>Le chemin par défaut est C:\Program Files\NetApp\SnapCenter.</p> <p>Vous pouvez éventuellement personnaliser le chemin. Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Toutefois, si vous le souhaitez, vous pouvez personnaliser le chemin par défaut.</p>
Ajoutez tous les hôtes du cluster	Cochez cette case pour ajouter tous les nœuds du cluster dans un WSFC.
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	<p>Cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <p>Indiquez le nom GMSA dans le format suivant : <i>domainName\accountName\$</i>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows. </div>

7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case **Skip précontrôles**, l'hôte est validé pour vérifier s'il répond aux conditions requises pour installer le plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET et l'emplacement sont validés par rapport aux exigences minimales. Si la configuration minimale

requis n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier `web.config` situé à `C:\Program Files\NetApp\SnapCenter WebApp` pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier `web.config`, vous devez le mettre à jour sur les deux nœuds.

8. Surveillez la progression de l'installation.

## Installation du plug-in SnapCenter pour Microsoft Windows sur plusieurs hôtes distants à l'aide d'applets de commande PowerShell

Si vous souhaitez installer le plug-in SnapCenter pour Microsoft Windows sur plusieurs hôtes simultanément, vous pouvez le faire en utilisant le `Install-SmHostPackage` Cmdlet PowerShell.

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer les plug-ins.

### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de `Open-SmConnection` cmdlet, puis saisissez vos informations d'identification.
3. Ajoutez l'hôte autonome ou le cluster au système SnapCenter à l'aide du `Add-SmHost` cmdlet et les paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

4. Installez le plug-in sur plusieurs hôtes à l'aide de `Install-SmHostPackage` cmdlet et les paramètres requis.

Vous pouvez utiliser le `-skipprecheck` option lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

## Installez le plug-in SnapCenter pour Microsoft Windows silencieusement à partir de la ligne de commande

Vous pouvez installer le plug-in SnapCenter pour Microsoft Windows localement sur un hôte Windows si vous ne pouvez pas installer le plug-in à distance à partir de l'interface graphique SnapCenter. Vous pouvez exécuter le programme d'installation du plug-in SnapCenter pour Microsoft Windows sans surveillance, en mode silencieux, à partir de la ligne de commande Windows.

### Avant de commencer

- Vous devez avoir installé ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle.

- Vous devez avoir installé PowerShell 7.4.2 ou une version ultérieure.
- Vous devez être un administrateur local sur l'hôte.

## Étapes

1. Téléchargez le plug-in SnapCenter pour Microsoft Windows à partir de votre emplacement d'installation.

Par exemple, le chemin d'installation par défaut est C:\ProgramData\NetApp\SnapCenter\Package Repository.

Ce chemin est accessible à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. Copiez le fichier d'installation sur l'hôte sur lequel vous souhaitez installer le plug-in.
3. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez téléchargé le fichier d'installation.
4. Entrez la commande suivante en remplaçant les variables par vos données :

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
ISFeatureInstall=SCW
```

Par exemple :

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCW_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW`
```



Tous les paramètres transmis lors de l'installation de Plug-in pour Windows sont sensibles à la casse.

Entrez les valeurs des variables suivantes :

Variable	Valeur
<code>/debuglog »&lt;Debug_Log_Path&gt;</code>	Spécifiez le nom et l'emplacement du fichier journal du programme d'installation de la suite, comme dans l'exemple suivant : <code>setup.exe /debuglog"C:\PathToLog\setupexe.log"</code> .
<code>BI_SNAPCENTER_PORT</code>	Spécifiez le port sur lequel SnapCenter communique avec SMCORE.
<code>SUITE_INSTALLDIR</code>	Spécifiez le répertoire d'installation du module de plug-in hôte.

Variable	Valeur
BI_SERVICEACCOUNT	Spécifiez le compte de service Web SnapCenter Plug-in pour Microsoft Windows.
BI_SERVICEPWD	Spécifiez le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows.
Installation de ISFeatureInstall	Spécifier la solution à déployer par SnapCenter sur un hôte distant

Le paramètre *debuglog* inclut le chemin du fichier journal pour SnapCenter. L'écriture dans ce fichier journal est la méthode recommandée pour obtenir des informations de dépannage, car le fichier contient les résultats des vérifications effectuées par l'installation pour les prérequis du plug-in.

Si nécessaire, vous trouverez des informations de dépannage supplémentaires dans le fichier journal du package SnapCenter pour Windows. Les fichiers journaux du package sont répertoriés (le plus ancien d'abord) dans le dossier *%Temp%*, par exemple, *C:\temp\*.



L'installation du plug-in pour Windows enregistre le plug-in sur l'hôte et non sur le serveur SnapCenter. Vous pouvez enregistrer le plug-in sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Une fois l'hôte ajouté, le plug-in est automatiquement découvert.

## Contrôler l'état d'installation du module d'extension SnapCenter

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.

- b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
  5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

### Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

#### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.

6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

### Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

#### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
  - a. Double-cliquez sur le certificat.
  - b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
  - c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
  - d. Copiez les caractères hexadécimaux de la zone.
  - e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :
  - a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

## Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte
Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent

être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

## Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

# Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM) ou si vous souhaitez protéger des VM et des datastores, vous devez déployer l'appliance virtuelle du plug-in SnapCenter pour VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section ["Présentation du déploiement"](#).

## Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section ["Créez ou importez un certificat SSL"](#).

## Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est `/opt/netapp/config/crl`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

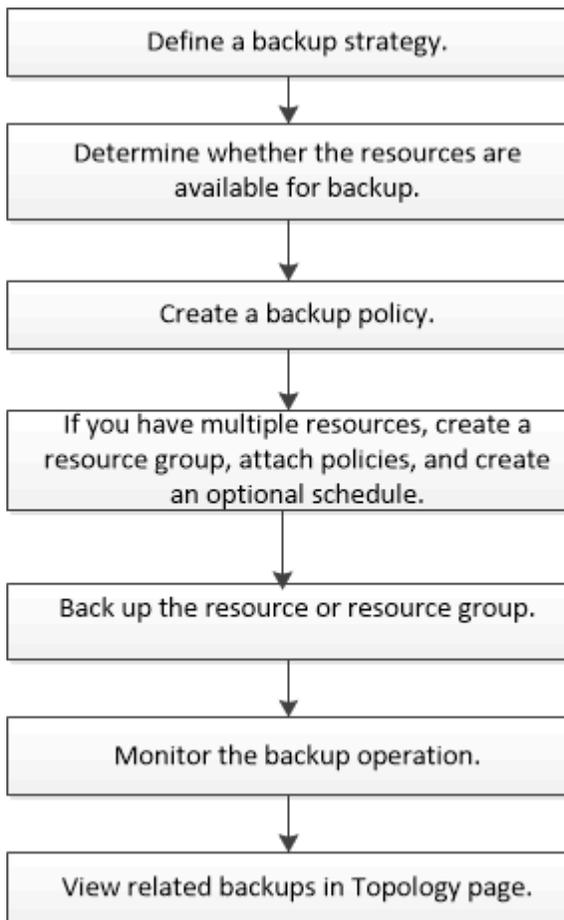
# Sauvegarder les systèmes de fichiers Windows

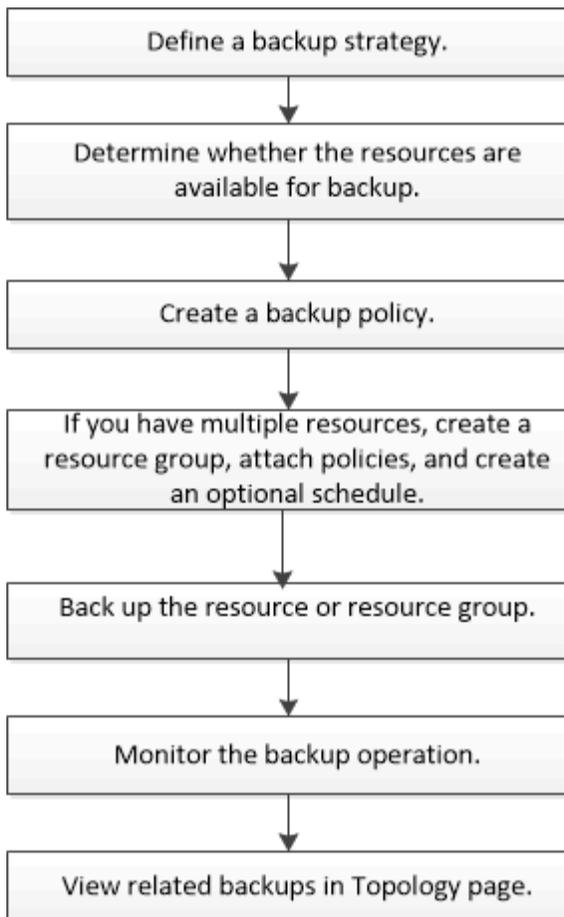
## Sauvegarder les systèmes de fichiers Windows

Lorsque vous installez le plug-in SnapCenter pour Microsoft Windows dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder les systèmes de fichiers Windows. Vous pouvez sauvegarder un seul système de fichiers ou un groupe de ressources contenant plusieurs systèmes de fichiers. Vous pouvez effectuer des sauvegardes à la demande ou selon un planning de protection défini.

Vous pouvez planifier plusieurs sauvegardes pour les exécuter simultanément sur plusieurs serveurs. Les opérations de sauvegarde et de restauration ne peuvent pas être effectuées simultanément sur la même ressource.

Le workflow suivant montre l'ordre dans lequel vous devez effectuer les opérations de sauvegarde :





Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide du cmdlet SnapCenter ou le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#) contient des informations détaillées sur les applets de commande PowerShell.

## Déterminez la disponibilité des ressources pour les systèmes de fichiers Windows

Les ressources sont les LUN et les composants similaires de votre système de fichiers gérés par les plug-ins que vous avez installés. Vous pouvez ajouter ces ressources aux groupes de ressources de sorte que vous puissiez effectuer des tâches de protection des données sur plusieurs ressources. Toutefois, vous devez d'abord identifier les ressources disponibles. La détection des ressources disponibles permet également de vérifier que l'installation du plug-in a bien été effectuée.

### Avant de commencer

- Vous devez déjà avoir terminé certaines tâches, telles que l'installation d'SnapCenter Server, l'ajout d'hôtes, la création de connexions SVM et l'ajout d'identifiants.
- Si les fichiers résident sur des LUN RDM ou des VMDK VMware, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter. Pour plus d'informations, voir ["Documentation du plug-in SnapCenter pour VMware vSphere"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.

2. Dans la page Ressources, sélectionnez **systèmes de fichiers** dans la liste.
3. Sélectionnez l'hôte pour filtrer la liste des ressources, puis cliquez sur **Actualiser les ressources**.

Les systèmes de fichiers récemment ajoutés, renommés ou supprimés sont mis à jour dans l'inventaire du serveur SnapCenter.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

## Créez des stratégies de sauvegarde pour les systèmes de fichiers Windows

Vous pouvez créer une nouvelle stratégie de sauvegarde pour les ressources avant d'utiliser SnapCenter pour sauvegarder des systèmes de fichiers Windows, ou vous pouvez créer une nouvelle stratégie de sauvegarde au moment de créer un groupe de ressources ou de sauvegarder une ressource.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde. "[En savoir plus >>](#)"
- Vous devez avoir préparé pour la protection des données,

Pour préparer la protection des données, vous devez réaliser des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la détection de ressources et la création de connexions de serveurs virtuels de stockage (SVM).

- Si vous répliquez des snapshots sur un stockage secondaire de copie miroir ou d'archivage sécurisé, l'administrateur SnapCenter doit vous avoir assigné les SVM pour les volumes source et de destination.
- Si vous souhaitez exécuter les scripts PowerShell dans les scripts prescripteurs et postscripts, définissez la valeur du paramètre usePowerProcessforScripts sur true dans le fichier web.config.

La valeur par défaut est FALSE

- Vérifiez les prérequis et les limites spécifiques de la synchronisation active SnapMirror. Pour plus d'informations, reportez-vous à "[Limites d'objet pour la synchronisation active SnapMirror](#)".

### Description de la tâche

- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots

jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Paramètres**.
2. Dans la page Paramètres, sélectionnez **stratégies**.
3. Sélectionnez **Nouveau**.
4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page sauvegarde et réplication, effectuez les tâches suivantes :
  - a. Sélectionnez un paramètre de sauvegarde.

Option	Description
Sauvegarde cohérente avec le système de fichiers	Choisissez cette option si vous souhaitez que SnapCenter arrête le lecteur sur lequel réside le système de fichiers avant le début de l'opération de sauvegarde, puis reprenne le lecteur après la fin de l'opération de sauvegarde.
Sauvegarde cohérente en cas de panne du système de fichiers	Choisissez cette option si vous ne souhaitez pas que SnapCenter arrête le lecteur de disque sur lequel réside le système de fichiers.

- b. Sélectionnez une fréquence de planification (également appelée type de stratégie).

La stratégie spécifie uniquement la fréquence de sauvegarde. La planification de protection spécifique pour la sauvegarde est définie dans le groupe de ressources. Par conséquent, au moins deux groupes de ressources peuvent partager la même stratégie et la même fréquence de sauvegarde, mais ont des programmes de sauvegarde différents.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

- c. Sélectionnez un libellé de stratégie.

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

6. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
Mettez à jour SnapMirror après avoir créé une copie Snapshot locale	<p>Sélectionnez cette option pour créer des copies miroir des jeux de sauvegarde sur un autre volume (SnapMirror).</p> <p>Cette option doit être activée pour la synchronisation active SnapSnapMirror.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir "<a href="#">Afficher les sauvegardes et clones associés sur la page topologie</a>".</p>
Mettez à jour la SnapVault après la création d'une copie Snapshot	<p>Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton Actualiser de la page topologie, l'heure d'expiration du SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquer sur le bouton Actualiser de la page topologie permet d'actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, voir "<a href="#">Archivage des copies Snapshot sur WORM sur une destination d'archivage sécurisé</a>".</p>
Nombre de tentatives d'erreur	Saisissez le nombre de tentatives de réplication qui doivent se produire avant l'interruption du processus.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

7. Dans la page Paramètres de conservation, spécifiez les paramètres de conservation des sauvegardes à la

demande et pour chaque fréquence de planification sélectionnée.

Option	Description
Copies Snapshot totales à conserver	Choisissez cette option si vous souhaitez spécifier le nombre de magasins SnapCenter d'instantanés avant de les supprimer automatiquement.
Conservation des copies Snapshot pour	Sélectionnez cette option si vous souhaitez spécifier le nombre de jours pendant lesquels SnapCenter conserve une copie de sauvegarde avant de la supprimer.
Période de verrouillage des copies Snapshot principales	Sélectionnez période de verrouillage des instantanés, puis sélectionnez jours, mois ou années.  La période de conservation SnapLock doit être inférieure à 100 ans.
Période de verrouillage des copies Snapshot secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.



Vous devez définir le nombre de rétention sur 2 ou plus. La valeur minimale pour le nombre de rétention est 2.



La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.

8. Dans la page script, entrez le chemin d'accès du prescripteur ou du PostScript que vous souhaitez que le serveur SnapCenter s'exécute avant ou après l'opération de sauvegarde, respectivement, et un délai d'attente que SnapCenter attend pour que le script s'exécute avant l'expiration du délai.

Par exemple, vous pouvez exécuter un script pour mettre à jour les traps SNMP, automatiser les alertes et envoyer des logs.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources pour les systèmes de fichiers Windows

Un groupe de ressources est le conteneur auquel vous pouvez ajouter plusieurs systèmes de fichiers que vous souhaitez protéger. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de tâche de protection des données que vous souhaitez exécuter, puis spécifier la planification de sauvegarde.

## Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- L'ajout de nouveaux systèmes de fichiers sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec la synchronisation active SnapMirror n'est pas pris en charge.
- L'ajout de nouveaux systèmes de fichiers à un groupe de ressources existant en mode de basculement de la synchronisation active SnapMirror n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement à l'état normal ou de retour arrière.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **systèmes de fichiers** dans la liste.



Si vous avez récemment ajouté un système de fichiers à SnapCenter, cliquez sur **Actualiser les ressources** pour afficher la nouvelle ressource ajoutée.

3. Cliquez sur **Nouveau groupe de ressources**.
4. Dans la page Nom de l'assistant, procédez comme suit :

Pour ce champ...	Procédez comme ça...
Nom	Entrez le nom du groupe de ressources.   Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Utilisez le format de nom personnalisé pour la copie Snapshot	Facultatif : entrez un nom et un format de snapshot personnalisés.  Par exemple, clienttext_resourcegroup_policy_hostname ou resourcegroup_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.
Balise	Entrez une balise descriptive pour faciliter la recherche d'un groupe de ressources.

5. Dans la page Ressources, effectuez les tâches suivantes :

- a. Sélectionnez l'hôte pour filtrer la liste des ressources.

Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

- b. Dans la section Ressources disponibles, cliquez sur les systèmes de fichiers à sauvegarder, puis cliquez sur la flèche vers la droite pour les déplacer vers la section ajoutée.

Si vous sélectionnez l'option **Autosélectionner toutes les ressources sur le même volume de stockage**, toutes les ressources du même volume sont sélectionnées. Lorsque vous les déplacez vers la section ajoutée, toutes les ressources du volume sont déplacées simultanément.

Pour ajouter un système de fichiers unique, désactivez l'option **Autosélectionner toutes les ressources sur le même volume de stockage**, puis sélectionnez les systèmes de fichiers que vous souhaitez déplacer vers la section ajoutée.

6. Dans la page stratégies, effectuez les tâches suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.

Vous pouvez sélectionner une stratégie existante et cliquer sur **Détails** pour déterminer si vous pouvez utiliser cette stratégie.

Si aucune politique existante ne répond à vos exigences, vous pouvez créer une nouvelle politique en cliquant sur  pour démarrer l'assistant de règles.

Les stratégies sélectionnées sont répertoriées dans la colonne Stratégie de la section configurer les plannings pour les stratégies sélectionnées.

b.

Dans la section configurer les plannings des stratégies sélectionnées, cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer le planning.

c. Si la stratégie est associée à plusieurs types d'horaires (fréquences), sélectionnez la fréquence à configurer.

d. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez la planification en spécifiant la date de début, la date d'expiration et la fréquence, puis cliquez sur **Finish**.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués de la section configurer les planifications pour les stratégies sélectionnées.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter. Vous ne devez pas modifier les planifications à partir du planificateur de tâches Windows et de SQL Server Agent.

7. Dans la page notification, fournissez les informations de notification comme suit :

Pour ce champ...	Procédez comme ça...
Préférence de courrier électronique	Sélectionnez <b>Always</b> , <b>On Failure</b> ou <b>On Failure ou warning</b> pour envoyer des e-mails aux destinataires après la création de groupes de ressources de sauvegarde, la connexion de stratégies et la configuration des planifications. Entrez le serveur SMTP, la ligne d'objet de l'e-mail par défaut, ainsi que les adresses e-mail de à et de.
De	Adresse électronique
À	Adresse e-mail

Pour ce champ...	Procédez comme ça...
Objet	Ligne d'objet de l'e-mail par défaut

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

Vous pouvez effectuer une sauvegarde à la demande ou attendre que la sauvegarde planifiée soit effectuée.

## Créez des groupes de ressources et activez la protection secondaire pour les systèmes de fichiers Windows sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.

6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.

7. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

a. Sélectionnez le type de la règle de réplication.



Règle de réplication synchrone non prise en charge.

b. Indiquez le suffixe du groupe de cohérence à utiliser.

c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.



Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.
- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell set-SmSmtServer.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell

Vous devez créer une connexion SVM (Storage Virtual machine) et une identifiant avant d'utiliser les applets de commande PowerShell pour réaliser les opérations de protection des données.

## Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de gestion unique.

## Étapes

1. Lancez une session de connexion PowerShell Core à l'aide de l'applet de commande `Open-SmConnection`.

Cet exemple ouvre une session PowerShell :

```
PS C:\> Open-SmConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-SmStorageConnection`.

Dans cet exemple, une nouvelle connexion au système de stockage est créée :

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande `Add-SmCredential`.

Cet exemple crée un nouvel identifiant nommé `FinanceAdmin` avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarder une seule ressource à la demande pour les systèmes de fichiers Windows

Si une ressource ne se trouve pas dans un groupe de ressources, vous pouvez sauvegarder la ressource à la demande à partir de la page Ressources.

### Description de la tâche

Si vous souhaitez sauvegarder une ressource avec un système de stockage secondaire ayant une relation SnapMirror, le rôle attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.



Lors de la sauvegarde d'un système de fichiers, SnapCenter ne sauvegarde pas les LUN montées sur un point de montage de volume (VMP) dans le système de fichiers en cours de sauvegarde.



Si vous travaillez dans un contexte de système de fichiers Windows, ne sauvegardez pas les fichiers de base de données. La sauvegarde est ainsi incohérente et risque de perte de données lors de la restauration. Pour protéger les fichiers de base de données, vous devez utiliser le plug-in SnapCenter approprié pour la base de données (par exemple, le plug-in SnapCenter pour Microsoft SQL Server ou le plug-in SnapCenter pour Microsoft Exchange Server).

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource système de fichiers, puis sélectionnez la ressource à sauvegarder.
3. Si l'assistant système de fichiers - protection ne démarre pas automatiquement, cliquez sur **protéger** pour lancer l'assistant.

Spécifiez les paramètres de protection, comme décrit dans les tâches création de groupes de ressources.

4. Facultatif : dans la page ressource de l'assistant, entrez un format de nom personnalisé pour l'instantané.

Par exemple, `clienttext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page stratégies, effectuez les tâches suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.

Vous pouvez sélectionner une stratégie existante, puis cliquer sur **Détails** pour déterminer si vous pouvez utiliser cette stratégie.

Si aucune stratégie existante ne répond à vos exigences, vous pouvez copier une stratégie existante et la modifier ou créer une nouvelle stratégie en cliquant sur  pour lancer l'assistant de stratégie. Si aucune stratégie existante ne répond à vos exigences, vous pouvez copier une stratégie existante et la modifier ou créer une nouvelle stratégie en cliquant sur  pour lancer l'assistant de stratégie.

Les stratégies sélectionnées sont répertoriées dans la colonne Stratégie de la section configurer les plannings pour les stratégies sélectionnées.

- b. Dans la section configurer les planifications pour les stratégies sélectionnées, cliquez sur  dans la colonne configurer les planifications de la stratégie pour laquelle vous souhaitez configurer la planification.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez la planification en spécifiant la date de début, la date d'expiration et la fréquence, puis cliquez sur **Finish**.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués de la section configurer les planifications pour les stratégies sélectionnées.

["Les opérations planifiées peuvent échouer"](#)

6. Dans la page notification, effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Préférence de courrier électronique	Sélectionnez <b>Always</b> , ou <b>On Failure</b> , ou <b>On Failure ou warning</b> , pour envoyer des e-mails aux destinataires après la création de groupes de ressources de sauvegarde, la connexion de stratégies et la configuration des planifications.  Entrez les informations sur le serveur SMTP, la ligne d'objet par défaut des e-mails et les adresses e-mail « à » et « de ».
De	Adresse électronique
À	Adresse e-mail
Objet	Ligne d'objet de l'e-mail par défaut

7. Vérifiez le résumé, puis cliquez sur **Terminer**.

La page topologie de la base de données s'affiche.

8. Cliquez sur **Sauvegarder maintenant**.

9. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante Stratégie, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.

Cet exemple crée une nouvelle stratégie de sauvegarde avec un type de sauvegarde SQL fullbackup :

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Cet exemple crée une nouvelle stratégie de sauvegarde avec un type de sauvegarde de système de fichiers Windows de CrashConsistent :

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

### 3. Découvrez les ressources hôte à l'aide de l'applet de commande Get-SmResources.

Cet exemple recherche les ressources du plug-in Microsoft SQL sur l'hôte spécifié :

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

Cet exemple détecte les ressources des systèmes de fichiers Windows sur l'hôte spécifié :

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

### 4. Ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.

Cet exemple crée un nouveau groupe de ressources de sauvegarde de base de données SQL avec la stratégie et les ressources spécifiées :

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

Cet exemple crée un nouveau groupe de ressources de sauvegarde du système de fichiers Windows avec la stratégie et les ressources spécifiées :

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet `New-SmBackup`.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Affichez l'état de la tâche de sauvegarde à l'aide de l'applet de commande `Get-SmBackupReport`.

Cet exemple affiche un rapport récapitulatif de tous les travaux exécutés à la date spécifiée :

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarder des groupes de ressources pour les systèmes de fichiers Windows

Un groupe de ressources est un ensemble de ressources sur un hôte ou un cluster. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources. Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror sur un système de stockage secondaire, le rôle attribué à l'utilisateur de stockage doit inclure le privilège « `napmirror All` ». Toutefois, si vous utilisez le rôle « `vsadmin` », le privilège « `napmirror all` » n'est pas requis.
- Si un groupe de ressources contient plusieurs bases de données provenant de différents hôtes, l'opération de sauvegarde sur certains hôtes peut se déclencher tardivement en raison de problèmes réseau. Vous devez configurer la valeur de `MaxRetryForUninitializedHoots` dans `web.config` à l'aide de l'applet de commande `set-SmConfigSettings PowerShell`



Lors de la sauvegarde d'un système de fichiers, SnapCenter ne sauvegarde pas les LUN montées sur un point de montage de volume (VMP) dans le système de fichiers en cours de sauvegarde.



Si vous travaillez dans un contexte de système de fichiers Windows, ne sauvegardez pas les fichiers de base de données. La sauvegarde est ainsi incohérente et risque de perte de données lors de la restauration. Pour protéger les fichiers de base de données, vous devez utiliser le plug-in SnapCenter approprié pour la base de données (par exemple, le plug-in SnapCenter pour Microsoft SQL Server ou le plug-in SnapCenter pour Microsoft Exchange Server).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en cliquant sur et en  sélectionnant la balise. Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis cliquez sur **Sauvegarder maintenant**.



Pour le plug-in SnapCenter pour base de données Oracle, si vous disposez d'un groupe de ressources fédéré contenant deux bases de données et que l'un de ces fichiers est placé sur un stockage non NetApp, l'opération de sauvegarde est abandonnée, même si l'autre base de données se trouve sur un stockage NetApp.

4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

"Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer. Pour augmenter la taille du segment de mémoire Java, localisez le fichier script `/opt/netapp/init_scripts/scvservice`. Dans ce script, le `do_start method Command` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante : `Java -jar -Xmx8192M -Xms4096M`.

## Surveiller les opérations de sauvegarde

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès

-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Surveiller les opérations dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

## Annuler les opérations de sauvegarde

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

## Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

## Étapes

1. Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>a. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>b. Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>a. Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>b. Sélectionner l'opération.</li> <li>c. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Afficher les sauvegardes et clones associés sur la page topologie

Lorsque vous préparez une ressource à sauvegarder ou à cloner une ressource, vous pouvez afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire. Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

### Description de la tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

- 



affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.

-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes du miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.

- Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie pour ne conserver que 4 sauvegardes, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes du miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Si vous utilisez une relation secondaire comme SnapMirror actif Sync (initialement commercialisé sous la forme SnapMirror Business Continuity [SM-BC]), les icônes supplémentaires suivantes s'affichent :

-  Le site de réplica est en cours.
-  Le site de réplica est en panne.
-  La relation miroir ou coffre-fort secondaire n'a pas été rétablie.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la fiche récapitulative pour connaître le nombre de sauvegardes et de clones disponibles sur les stockages primaire et secondaire.

La section carte récapitulative affiche le nombre total de sauvegardes et de clones. Pour la base de données Oracle uniquement, la section carte de résumé affiche également le nombre total de sauvegardes de journaux.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Pour la synchronisation active SnapMirror, cliquez sur le bouton **Refresh** pour actualiser l'inventaire des sauvegardes SnapCenter en interrogeant ONTAP sur les sites principaux et de réplica. Une planification hebdomadaire effectue également cette activité pour toutes les bases de données contenant une relation de synchronisation active SnapMirror.

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations SnapMirror miroir asynchrone ou MirrorVault asynchrone vers la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir de ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.
  - Après le basculement, une sauvegarde doit être créée afin que SnapCenter puisse prendre connaissance du basculement. Vous ne pouvez cliquer sur **Rafraîchir** qu'après la création d'une sauvegarde.
5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage, de renommage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le système de stockage secondaire.

7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur  pour supprimer le clone.

## Exemple de sauvegardes et de clones sur le stockage primaire

### Manage Copies



## Nettoyez le nombre de sauvegardes secondaires à l'aide des applets de commande PowerShell

Vous pouvez utiliser l'applet de commande Remove-SmBackup pour nettoyer le nombre de sauvegardes secondaires sans instantané. Vous pouvez utiliser cette applet de commande lorsque le nombre total de snapshots affichés dans la topologie gérer les

copies ne correspond pas au paramètre de conservation des snapshots de stockage secondaire.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Nettoyez le nombre de sauvegardes secondaires à l'aide du paramètre `-CleanupSecondaryBackups`.

Cet exemple nettoie le nombre de sauvegardes secondaires sans snapshots :

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

# Restauration des systèmes de fichiers Windows

## Restaurez les sauvegardes du système de fichiers Windows

Vous pouvez utiliser SnapCenter pour restaurer les sauvegardes du système de fichiers. La restauration du système de fichiers est un processus en plusieurs phases qui copie toutes les données d'une sauvegarde spécifiée vers l'emplacement d'origine du système de fichiers.

### Avant de commencer

- Vous devez avoir sauvegardé le système de fichiers.
- Si une opération planifiée, telle qu'une opération de sauvegarde, est en cours pour un système de fichiers, cette opération doit être annulée avant de pouvoir lancer une opération de restauration.
- Vous pouvez uniquement restaurer une sauvegarde du système de fichiers à l'emplacement d'origine, et non à un chemin alternatif.

Vous ne pouvez pas restaurer un seul fichier à partir d'une sauvegarde car le système de fichiers restauré écrase les données à l'emplacement d'origine du système de fichiers. Pour restaurer un seul fichier à partir d'une sauvegarde de système de fichiers, vous devez cloner la sauvegarde et accéder au fichier dans le clone.

- Vous ne pouvez pas restaurer un système ou un volume d'amorçage.
- SnapCenter peut restaurer des systèmes de fichiers dans un cluster Windows sans mettre le groupe de clusters hors ligne.

### Description de la tâche

- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Pour filtrer la liste des ressources, sélectionnez les options système de fichiers et Groupe de ressources.
3. Sélectionnez un groupe de ressources dans la liste, puis cliquez sur **Restaurer**.
4. Sur la page sauvegardes, sélectionnez si vous souhaitez effectuer une restauration à partir des systèmes de stockage primaire ou secondaire, puis sélectionnez une sauvegarde à restaurer.
5. Sélectionnez vos options dans l'assistant de restauration.
6. Vous pouvez entrer le chemin et les arguments du prescripteur ou du PostScript que vous souhaitez exécuter SnapCenter avant ou après l'opération de restauration, respectivement.

Vous pouvez par exemple exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer les journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

7. Dans la page notification, sélectionnez l'une des options suivantes :

Pour ce champ...	Procédez comme ça...
Consigner les événements du serveur SnapCenter dans le journal système de stockage	Sélectionnez cette option pour consigner les événements du serveur SnapCenter dans le syslog du système de stockage.
Envoyez une notification AutoSupport pour les opérations ayant échoué au système de stockage	Sélectionnez cette option pour envoyer des informations concernant les opérations qui ont échoué à NetApp utilisant AutoSupport.
Préférence de courrier électronique	Sélectionnez <b>toujours, en cas d'échec</b> ou <b>en cas d'échec ou d'avertissement</b> pour envoyer des e-mails aux destinataires après la restauration des sauvegardes. Entrez le serveur SMTP, la ligne d'objet de l'e-mail par défaut, ainsi que les adresses e-mail de et à partir.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.
9. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.



Si le système de fichiers restauré contient une base de données, vous devez également restaurer la base de données. Si vous ne restaurez pas la base de données, votre base de données est peut-être dans un état non valide. Pour plus d'informations sur la restauration des bases de données, reportez-vous au Guide de protection des données correspondant à cette base de données.

### Applets de commande PowerShell

## Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1 '
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurer des ressources à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de ressources inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande `Get-SmBackup` and `get-SmBackupReport`.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
-----	-----	-----
-----		
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveiller les opérations de restauration

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours

-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Annuler les opérations de restauration

Vous pouvez annuler les travaux de restauration mis en file d'attente.

Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâche pour annuler les opérations de restauration.

### Description de la tâche

- Vous pouvez annuler une opération de restauration en file d'attente à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de restauration en cours.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes de l'interface de ligne de commande pour annuler les opérations de restauration en attente.
- Le bouton **Annuler tâche** est désactivé pour les opérations de restauration qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de restauration en file d'attente d'autres membres tout en utilisant ce rôle.

### Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>2. Sélectionnez le travail et cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>1. Après avoir lancé l'opération de restauration, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>2. Sélectionner l'opération.</li> <li>3. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

## Clonage des systèmes de fichiers Windows

### Clonage à partir d'une sauvegarde du système de fichiers Windows

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde du système de fichiers Windows. Pour copier un fichier qui a été supprimé ou modifié par erreur, vous pouvez cloner une sauvegarde et accéder à ce fichier dans le clone.

#### Avant de commencer

- Vous devez être prêt à préparer la protection des données en effectuant des tâches telles que l'ajout d'hôtes, l'identification des ressources et la création de connexions de machines virtuelles de stockage (SVM).
- Vous devez avoir une sauvegarde du système de fichiers.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Vous ne pouvez pas cloner un groupe de ressources. Vous ne pouvez cloner que des sauvegardes de systèmes de fichiers individuels.
- Si une sauvegarde réside sur une machine virtuelle dotée d'un disque VMDK, SnapCenter ne peut pas cloner la sauvegarde sur un serveur physique.
- Si vous clonez un cluster Windows (par exemple une LUN partagée ou une LUN CSV (Cluster Shared volume), le clone est stocké en tant que LUN dédiée sur l'hôte que vous spécifiez.
- Pour une opération de clonage, le répertoire racine du point de montage du volume ne peut pas être un répertoire partagé.
- Le clone ne peut pas être créé sur un nœud qui n'est pas le home node de l'agrégat.
- Vous ne pouvez pas planifier d'opérations de clonage récurrentes (ou de cycle de vie des clones) pour les systèmes de fichiers Windows ; vous pouvez uniquement cloner une sauvegarde à la demande.
- Si vous déplacez une LUN contenant un clone vers un nouveau volume, SnapCenter ne peut plus prendre en charge le clone. Par exemple, vous ne pouvez pas utiliser SnapCenter pour supprimer le clone.
- Vous ne pouvez pas cloner des environnements. Par exemple, le clonage d'un disque physique vers un disque virtuel ou vice versa.

## Description de la tâche

- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **systèmes de fichiers** dans la liste.
3. Sélectionnez l'hôte.

La vue topologique s'affiche automatiquement si la ressource est protégée.

4. Dans la liste des ressources, sélectionnez la sauvegarde à cloner, puis cliquez sur l'icône cloner.
5. Dans la page Options, procédez comme suit :

Pour ce champ...	Procédez comme ça...
Serveur clone	Choisissez l'hôte sur lequel le clone doit être créé.
« Attribuer automatiquement un point de montage » ou « attribuer automatiquement un point de montage de volume sous la trajectoire »	<p>Choisissez d'attribuer automatiquement un point de montage ou un point de montage de volume sous un chemin d'accès.</p> <p>Affectation automatique d'un point de montage de volume sous le chemin : le point de montage sous un chemin vous permet de fournir un répertoire spécifique dans lequel les points de montage seront créés. Avant de choisir cette option, vous devez vérifier que le répertoire est vide. Si une sauvegarde est effectuée dans le répertoire, la sauvegarde sera dans un état non valide après l'opération de montage.</p>
Emplacement d'archivage	Choisissez un emplacement d'archivage si vous procédez au clonage d'une sauvegarde secondaire.

6. Dans la page script, spécifiez les prescripteurs ou les postscripts que vous souhaitez exécuter.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

7. Vérifiez le résumé, puis cliquez sur **Terminer**.
8. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Répertoriez les sauvegardes pouvant être clonées à l'aide de l'applet de commande `Get-SmBackup` ou `Get-SmResourceGroup`.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

Cet exemple affiche des informations sur un groupe de ressources spécifié, ses ressources et les stratégies associées :

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
```

SearchResources : False  
ByPassCredential : False  
IsCustomSnapshot :  
MaintenanceStatus : Production  
PluginProtectionGroupTypes : {SMSQL}  
Name : Payrolldataset  
Type : Group  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
ApplySnapvaultUpdate : False  
ApplyRetention : False  
RetentionCount : 0  
RetentionDays : 0  
ApplySnapMirrorUpdate : False  
SnapVaultLabel :  
MirrorVaultUpdateRetryCount : 7  
AppPolicies : {}  
Description : FinancePolicy  
PreScriptPath :  
PreScriptArguments :  
PostScriptPath :  
PostScriptArguments :  
ScriptTimeOut : 60000  
DateModified : 8/4/2015 3:43:30 PM  
DateCreated : 8/4/2015 3:43:30 PM  
Schedule : SMCoreContracts.SmSchedule  
PolicyType : Backup  
PluginPolicyType : SMSQL  
Name : FinancePolicy  
Type :  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
clab-a13-13.sddev.lab.netapp.com  
DatabaseGUID :

```
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Lancez une opération de clonage à partir d'une sauvegarde existante à l'aide de l'applet de commande `New-SmClone`.

Dans cet exemple, un clone est créé à partir d'une sauvegarde spécifiée avec tous les journaux :

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

Dans cet exemple, un clone est créé dans une instance Microsoft SQL Server spécifiée :

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

#### 4. Affichez l'état du travail clone à l'aide de l'applet de commande Get-SmCloneReport.

Cet exemple affiche un rapport de clonage pour l'ID de tâche spécifié :

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
 Sally_DRAPER}
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveillance des opérations de clonage

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Annuler les opérations de clonage

Vous pouvez annuler les opérations de clonage mises en file d'attente.

Pour annuler les opérations de clonage, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâches.

### Description de la tâche

- Vous pouvez annuler une opération de clonage en file d'attente à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de clonage en cours d'exécution.
- Vous pouvez utiliser l'interface utilisateur graphique SnapCenter, les applets de commande PowerShell ou les commandes de l'interface de ligne de commande pour annuler les opérations de clonage mises en attente.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de clonage en file d'attente d'autres membres tout en utilisant ce rôle.

### Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>2. Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>1. Après avoir lancé l'opération de clonage, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>2. Sélectionner l'opération.</li> <li>3. Dans la page <b>Détails du travail</b>, cliquez sur <b>Annuler le travail</b>.</li> </ol>

## Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur \* \* .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

#### Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

# Protection des bases de données Microsoft Exchange Server

## Concepts du plug-in SnapCenter pour Microsoft Exchange Server

### Présentation du plug-in SnapCenter pour Microsoft Exchange Server

Le plug-in SnapCenter pour Microsoft Exchange Server est un composant côté hôte du logiciel NetApp SnapCenter qui permet de gérer la protection des données des bases de données Exchange avec reconnaissance des applications. Le plug-in pour Exchange automatise la sauvegarde et la restauration des bases de données Exchange dans votre environnement SnapCenter.

Lorsque le plug-in pour Exchange est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume et, grâce à la technologie NetApp SnapVault, exécuter une réplication de sauvegarde disque à disque à des fins de conformité et d'archivage.

Si vous souhaitez restaurer et récupérer des messages ou des boîtes aux lettres à la place de la base de données Exchange complète, vous pouvez utiliser le logiciel Single Mailbox Recovery (SMBR). NetApp® Single Mailbox Recovery a pris fin le 12 mai 2023. NetApp continuera d'assurer le support des clients ayant acheté une capacité de boîte aux lettres, des services de maintenance et un support via des références marketing introduites le 24 juin 2020, pendant la durée du support souscrit.

NetApp Single Mailbox Recovery est un produit partenaire fourni par Ontrack. OnTrack PowerControls offre des fonctionnalités similaires à celles de NetApp Single Mailbox Recovery. Les clients peuvent se procurer de nouvelles licences logicielles Ontrack PowerControls et des renouvellements de maintenance et de support Ontrack PowerControls depuis Ontrack (jusqu'à [licensingteam@ontrack.com](mailto:licensingteam@ontrack.com)) pour une récupération granulaire des boîtes aux lettres.

Le plug-in pour Exchange prend en charge la synchronisation active SnapMirror (initialement commercialisée sous le nom de SnapMirror Business Continuity [SM-BC]), qui permet aux services de l'entreprise de continuer de fonctionner même en cas de défaillance complète du site, et prend en charge le basculement transparent des applications via une copie secondaire. Aucune intervention manuelle, ni script supplémentaire n'est nécessaire pour déclencher un basculement avec la synchronisation active SnapMirror.

Il prend en charge le mode asymétrique, de basculement ou non duplex de SnapMirror Active Sync. Cela se rapporte à la solution dans laquelle le chemin optimisé se trouve uniquement à partir du nœud propriétaire de la LUN côté principal. Toutes les E/S arrivant sur les chemins du cluster secondaire sont servies par proxy sur le cluster principal. La réplication synchrone est unidirectionnelle, dans la direction du primaire vers le secondaire.

- Automatise les opérations de sauvegarde et de restauration respectueuses des applications pour les bases de données Microsoft Exchange Server et les groupes de disponibilité de base de données (DAG) dans votre environnement SnapCenter
- Prend en charge les serveurs Exchange virtualisés sur les LUN RDM lorsque vous déployez le plug-in SnapCenter pour VMware vSphere et enregistrez le plug-in avec SnapCenter.

## Avantages du plug-in SnapCenter pour Microsoft Exchange Server

Vous pouvez utiliser le plug-in pour Exchange pour sauvegarder et restaurer les bases de données Exchange Server.

- Afficher et gérer un inventaire actif des groupes de disponibilité de base de données Exchange (DAG), des bases de données et des ensembles de répliques
- Définissez des règles fournissant les paramètres de protection pour l'automatisation des sauvegardes
- Affecter des stratégies à des groupes de ressources
- Protéger les fichiers DAG et les bases de données individuelles
- Sauvegarder les bases de données primaires et secondaires des boîtes aux lettres Exchange
- Restaurer des bases de données à partir de sauvegardes primaires et secondaires

## Types de stockage pris en charge par le plug-in SnapCenter pour Microsoft Windows et pour Microsoft Exchange Server

SnapCenter prend en charge un large éventail de types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier si la prise en charge de votre type de stockage est disponible avant d'installer le package pour votre hôte.

Le provisionnement et la protection des données SnapCenter sont pris en charge par Windows Server. Pour obtenir les dernières informations sur les versions prises en charge, consultez la <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT> [matrice d'interopérabilité NetApp^].

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur physique	LUN connectés via FC	Interface graphique SnapCenter ou applets de commande PowerShell	
Serveur physique	LUN connectées à l'iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	
VM VMware	LUN RDM connectés par un HBA FC ou iSCSI	Applets de commande PowerShell	Compatibilité physique uniquement   Les VMDK ne sont pas pris en charge.
VM VMware	LUN iSCSI connectés directement au système invité par l'initiateur iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	 Les VMDK ne sont pas pris en charge.

Machine	Type de stockage	Provisionnement avec	Notes de support
Serveur virtuel Hyper-V.	LUN FC virtuels (VFC) connectés par un commutateur Fibre Channel virtuel	Interface graphique SnapCenter ou applets de commande PowerShell	<p data-bbox="1156 151 1487 361">Vous devez utiliser Hyper-V Manager pour provisionner les LUN FC virtuels (VFC) connectés par un commutateur Fibre Channel virtuel.</p> <div data-bbox="1188 394 1461 961" style="border: 1px solid #ccc; padding: 10px;">  <p data-bbox="1305 403 1455 953">Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>
Serveur virtuel Hyper-V.	LUN iSCSI connectés directement au système invité par l'initiateur iSCSI	Interface graphique SnapCenter ou applets de commande PowerShell	<div data-bbox="1188 1024 1461 1570" style="border: 1px solid #ccc; padding: 10px;">  <p data-bbox="1305 1024 1455 1562">Hyper-V ne prend pas en charge les disques pass-through et les bases de données sauvegardées sur les disques VHD(x) provisionnés sur le stockage NetApp.</p> </div>

## Privilèges ONTAP minimum requis pour le plug-in Exchange

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log

- l'historique des tâches s'affiche
- fin de la tâche
- lun
- la création de lun
- la création de lun
- la création de lun
- suppression de la lun
- lun igroup add
- créez un groupe initiateur lun
- suppression du groupe initiateur lun
- renommer la lun igroup
- renommer la lun igroup
- affichage de la lun igroup
- lun mapping des nœuds supplémentaires
- création d'un mappage de lun
- suppression du mappage de lun
- mappage de lun supprimer-rapports-nœuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- suppression de la réservation persistante de lun
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version

- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes
- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- volume snapshot modify-snaplock-expiration-time
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show

- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau
  - interface réseau affiche
  - un vserver

## Préparez les systèmes de stockage pour la réplication SnapMirror et SnapVault

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le ["Documentation ONTAP"](#).

## Définir une stratégie de sauvegarde pour les ressources Exchange Server

La définition d'une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous permet de vous assurer que vous disposez des sauvegardes dont vous avez besoin pour restaurer correctement vos bases de données. Votre accord de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de récupération (RPO) déterminent largement votre stratégie de sauvegarde.

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés au service, notamment la disponibilité et les performances de celui-ci. Le RTO est le moment par où un processus métier doit être

restauré suite à une interruption de service. Un RPO définit la stratégie selon laquelle les fichiers doivent être récupérés à partir du stockage de sauvegarde afin que des opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de sauvegarde.

### Types de sauvegardes pris en charge pour la base de données Exchange

Pour sauvegarder des boîtes aux lettres Exchange avec SnapCenter, il vous faut choisir le type de ressource, comme les bases de données et les groupes de disponibilité de base de données. Elle permet de créer des copies en ligne en lecture seule des volumes sur lesquels résident les ressources.

Type de sauvegarde	Description
Sauvegarde complète et journal	<p>Sauvegarde les bases de données et tous les journaux de transactions, y compris les journaux tronqués.</p> <p>Une fois la sauvegarde complète terminée, Exchange Server tronque les journaux de transactions déjà engagés dans la base de données.</p> <p>Généralement, vous devez choisir cette option. Toutefois, si votre temps de sauvegarde est court, vous pouvez choisir de ne pas exécuter de sauvegarde complète du journal de transactions.</p>
Sauvegarde complète	<p>Sauvegarde des bases de données et des journaux de transactions.</p> <p>Les journaux de transactions tronqués ne sont pas sauvegardés.</p>
Sauvegarde des journaux	<p>Sauvegarde tous les journaux de transactions.</p> <p>Les journaux tronqués déjà engagés dans la base de données ne sont pas sauvegardés. Si vous planifiez des sauvegardes fréquentes du journal des transactions entre des sauvegardes complètes de base de données, vous pouvez choisir des points de restauration granulaires.</p>

### Planifications de sauvegarde pour les plug-ins de bases de données

La fréquence de sauvegarde (type de planification) est spécifiée dans les stratégies ; un planning de sauvegarde est spécifié dans la configuration du groupe de ressources. Le facteur le plus important dans la détermination d'une fréquence ou d'un planning de sauvegarde est le taux de changement pour la ressource et l'importance des données. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. Parmi les autres facteurs figurent l'importance de la ressource pour votre organisation, votre contrat de niveau de service (SLA) et votre objectif de point de récupération (RPO).

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés au service, notamment la disponibilité et les performances de celui-ci. Un RPO définit la stratégie selon laquelle les fichiers doivent être récupérés à partir du stockage de sauvegarde afin que des opérations régulières puissent reprendre après une

défaillance. Les SLA et RPO contribuent à la stratégie de protection des données.

Même avec une ressource largement utilisée, il n'est pas nécessaire d'exécuter une sauvegarde complète plus d'une fois ou deux fois par jour. Par exemple, des sauvegardes régulières du journal de transactions peuvent suffire pour vous assurer que vous disposez des sauvegardes dont vous avez besoin. Plus vous sauvegardez des bases de données, plus le nombre de journaux de transaction que SnapCenter doit utiliser au moment de la restauration est élevé, ce qui accélère les opérations de restauration.

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes

La fréquence de sauvegarde (fréquence d'exécution des sauvegardes), appelée *schedule type* pour certains plug-ins, fait partie d'une configuration de stratégie. Vous pouvez sélectionner la fréquence de sauvegarde horaire, quotidienne, hebdomadaire ou mensuelle de la police. Si vous ne sélectionnez aucune de ces fréquences, la règle créée est une stratégie à la demande uniquement. Vous pouvez accéder aux stratégies en cliquant sur **Paramètres > stratégies**.

- Planifications de sauvegarde

Les planifications de sauvegarde (exactement quand les sauvegardes doivent être effectuées) font partie d'une configuration de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour sauvegarder chaque jeudi à 10 h 00. Vous pouvez accéder aux planifications de groupes de ressources en cliquant sur **Ressources > groupes de ressources**.

## Nombre de tâches de sauvegarde nécessaires pour les bases de données

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

## Nomenclature établie des sauvegardes

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.
- *03-12-2015\_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, clienttext\_resourcegroup\_policy\_hostname ou resourcegroup\_hostname. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

### Options de conservation des sauvegardes

Vous pouvez choisir le nombre de jours pendant lesquels vous souhaitez conserver les copies de sauvegarde ou spécifier le nombre de copies de sauvegarde à conserver, dans un maximum de 255 copies ONTAP. Par exemple, votre entreprise peut avoir besoin de conserver 10 jours de copies de sauvegarde ou 130 copies de sauvegarde.

Lors de la création d'une stratégie, vous pouvez spécifier les options de rétention pour le type de sauvegarde et le type de planification.

Si vous configurez la réplication SnapMirror, la règle de conservation est mise en miroir sur le volume de destination.

SnapCenter supprime les sauvegardes conservées dont les étiquettes de conservation correspondent au type de planification. Si le type de planification a été modifié pour la ressource ou le groupe de ressources, les sauvegardes avec l'ancienne étiquette de type de planification peuvent rester sur le système.



Pour la conservation à long terme des copies de sauvegarde, nous vous recommandons d'utiliser la sauvegarde SnapVault.

### Durée de conservation des sauvegardes du journal des transactions sur le volume de stockage source pour Exchange Server

Le plug-in SnapCenter pour Microsoft Exchange Server nécessite des sauvegardes de journal de transactions pour effectuer des opérations de restauration à chaud, qui restaurent votre base de données à un moment donné entre deux sauvegardes complètes.

Par exemple, si le plug-in pour Exchange a pris une sauvegarde complète du journal de transactions à 8:00 et une autre sauvegarde complète du journal de transactions plus à 5:00, elle pourrait utiliser la dernière sauvegarde du journal de transactions pour restaurer la base de données à n'importe quel moment entre 8:00 et 5:00. Si les journaux de transactions ne sont pas disponibles, le plug-in pour Exchange peut uniquement effectuer des opérations de restauration à un point dans le temps, ce qui permet de restaurer une base de données à l'heure où le plug-in pour Exchange a terminé une sauvegarde complète.

En règle générale, les opérations de restauration sont réalisées en moins d'une journée ou deux. Par défaut, SnapCenter conserve un minimum de deux jours.

### Définir une stratégie de restauration pour les bases de données Exchange

La définition d'une stratégie de restauration pour Exchange Server vous permet de restaurer votre base de données avec succès.

### Sources pour une opération de restauration dans Exchange Server

Vous pouvez restaurer une base de données Exchange Server à partir d'une copie de sauvegarde sur le stockage primaire.

Les bases de données ne peuvent être restaurées qu'à partir d'un système de stockage primaire.

## Types d'opérations de restauration pris en charge pour Exchange Server

Vous pouvez utiliser SnapCenter pour effectuer différents types d'opérations de restauration sur les ressources Exchange.

- Restaurez vos données en moins d'une minute
- Restauration à un point précédent dans le temps

### Restaurez vos données en quelques minutes

Dans le cadre d'une opération de restauration en moins d'une minute, les bases de données sont récupérées jusqu'au point de défaillance. Pour cela, SnapCenter effectue la séquence suivante :

1. Restaure les bases de données à partir de la sauvegarde de base de données complète que vous sélectionnez.
2. Applique tous les journaux de transactions sauvegardés, ainsi que tous les nouveaux journaux créés depuis la sauvegarde la plus récente.

Les journaux de transactions sont déplacés vers l'avant et appliqués à toute base de données sélectionnée.

Exchange crée une nouvelle chaîne de journaux une fois la restauration terminée.

**Meilleure pratique:** il est recommandé d'effectuer une nouvelle sauvegarde complète et du journal une fois la restauration terminée.

Une opération de restauration en moins d'une minute nécessite un ensemble contigu de journaux de transaction.

Après avoir effectué une restauration en moins d'une minute, la sauvegarde que vous avez utilisée pour la restauration n'est disponible que pour les opérations de restauration à un point dans le temps.

Si vous n'avez pas besoin de conserver une capacité de restauration à la minute pour toutes les sauvegardes, vous pouvez configurer la conservation de la sauvegarde du journal des transactions de votre système à l'aide des stratégies de sauvegarde.

### Restauration à un point précédent dans le temps

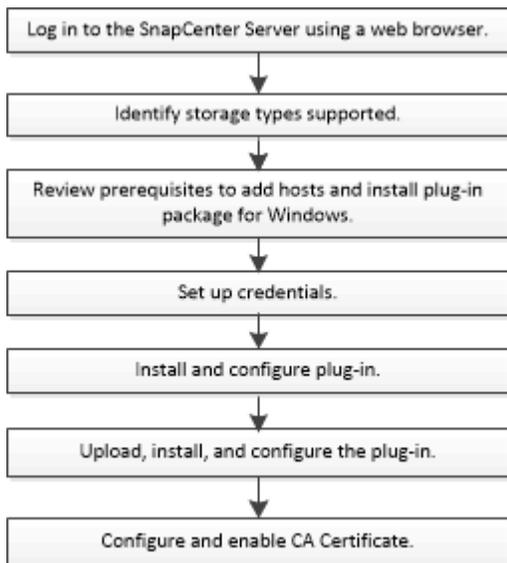
Dans le cadre d'une opération de restauration instantanée, les bases de données ne sont restaurées qu'à une heure spécifique par le passé. Une opération de restauration à un point dans le temps se produit dans les situations de restauration suivantes :

- La base de données est restaurée à une heure donnée dans un journal de transactions sauvegardé.
- La base de données est restaurée et seul un sous-ensemble des journaux de transactions sauvegardés y est appliqué.

## Installez le plug-in SnapCenter pour Microsoft Exchange Server

## Workflow d'installation du plug-in SnapCenter pour Microsoft Exchange Server

Vous devez installer et configurer le plug-in SnapCenter pour Microsoft Exchange Server si vous souhaitez protéger les bases de données Exchange.



## Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour Microsoft Exchange Server

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Vous devez utiliser Microsoft Exchange Server 2013, 2016 ou 2019 pour les configurations autonomes et de groupes de disponibilité de base de données.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Si vous gérez des nœuds de cluster dans SnapCenter, vous devez disposer d'un utilisateur disposant de privilèges d'administration sur tous les nœuds du cluster.
- Vous devez disposer d'un utilisateur avec des autorisations d'administration sur le serveur Exchange.
- Si SnapManager pour Microsoft Exchange Server et SnapDrive pour Windows sont déjà installés, vous devez annuler l'enregistrement du fournisseur de matériel VSS utilisé par SnapDrive pour Windows avant d'installer le plug-in pour Exchange sur le même serveur Exchange pour assurer la protection des données à l'aide de SnapCenter.
- Si SnapManager pour Microsoft Exchange Server et le plug-in pour Exchange sont installés sur le même serveur, vous devez interrompre ou supprimer du planificateur Windows tous les planifications créés par SnapManager pour Microsoft Exchange Server.
- L'hôte doit être résolu au nom de domaine complet (FQDN) du serveur. Si le fichier hosts est modifié pour le rendre résolu et si le nom abrégé et le FQDN sont spécifiés dans le fichier hosts, créez une entrée dans le fichier hosts SnapCenter au format suivant : `<adresse_ip> <nom_hôte> <nom_hôte>`.

- Assurez-vous que les ports suivants ne sont pas bloqués dans le pare-feu, sinon l'opération d'ajout d'hôte échoue. Pour résoudre ce problème, vous devez configurer la plage de ports dynamiques. Pour plus d'informations, voir "[Documentation Microsoft](#)".
  - Plage de ports 50000 - 51000 pour Windows 2016 et Exchange 2016
  - Plage de ports 6000 - 6500 pour Windows 2012 R2 et Exchange 2013
  - Plage de ports 49152 - 65536 pour Windows 2019

Pour identifier la plage de ports, exécutez les commandes suivantes :



- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

### Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	Microsoft Windows  Pour obtenir les dernières informations sur les versions prises en charge, consultez le " <a href="#">Matrice d'interopérabilité NetApp</a> ".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	5 GO  <div style="border: 1px solid #ccc; padding: 10px; margin-left: 20px;"> <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>

Élément	De formation
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java et OpenJDK</li> </ul> <p>Java 11 Oracle Java et OpenJDK sont requis uniquement pour SAP HANA, IBM DB2, PostgreSQL, MySQL, les plug-ins pris en charge par NetApp et d'autres applications personnalisées qui peuvent être installées sur l'hôte Windows.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

### Privilèges Exchange Server requis

Pour permettre à SnapCenter d'ajouter un serveur Exchange ou un DAG et d'installer le plug-in SnapCenter pour Microsoft Exchange Server sur un hôte ou un DAG, vous devez configurer SnapCenter avec les informations d'identification d'un utilisateur disposant d'un ensemble minimal de privilèges et d'autorisations.

Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local et d'autorisations de connexion locales sur l'hôte Exchange distant, ainsi que de droits d'administration sur tous les nœuds du DAG. L'utilisateur du domaine requiert les autorisations minimales suivantes :

- Add-MailboxDatabaseCopy
- Démonter-base de données
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- GET-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true

- Montage de la base de données
- New-MailboxDatabase
- New-PublicFolderDatabase
- Supprimer-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Supprimer-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Définir-AdServerSettings
- Set-MailboxDatabase -allofilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

### Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systemes d'exploitation	Microsoft Windows  Pour obtenir les dernières informations sur les versions prises en charge, consultez le " <a href="#">Matrice d'interopérabilité NetApp</a> ".
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	5 GO  <div style="border: 1px solid #ccc; padding: 10px; margin-left: 20px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>

Élément	De formation
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java et OpenJDK</li> </ul> <p>Java 11 Oracle Java et OpenJDK sont requis uniquement pour SAP HANA, IBM DB2, PostgreSQL, MySQL, les plug-ins pris en charge par NetApp et d'autres applications personnalisées qui peuvent être installées sur l'hôte Windows.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

## Configuration des informations d'identification pour le plug-in SnapCenter pour Windows

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation du module d'extension et des informations d'identification supplémentaires pour effectuer des opérations de protection des données sur les bases de données.

### Description de la tâche

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Windows. Bien que vous puissiez créer des identifiants pour Windows après le déploiement d'hôtes et l'installation de plug-ins, il est conseillé de créer des identifiants après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

Configurez les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.

La fenêtre Credential s'affiche.

4. Dans la page informations d'identification, procédez comme suit :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Entrez un nom pour l'identifiant.
Nom d'utilisateur	<p>Entrez le nom d'utilisateur utilisé pour l'authentification.</p> <ul style="list-style-type: none"><li>Administrateur de domaine ou tout membre du groupe d'administrateurs</li></ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"><li>◦ NetBIOS\UserName</li><li>◦ Domain FQDN\UserName</li></ul> <ul style="list-style-type: none"><li>Administrateur local (groupes de travail uniquement)</li></ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : UserName</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Authentification	Sélectionnez Windows comme mode d'authentification.

5. Cliquez sur **OK**.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

**Avant de commencer**

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

## Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediely
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

Par exemple :

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :
  - a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```

PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name Name Install State

[] Active Directory Domain Services AD-Domain-Services Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code Feature Result

True No Success {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.

```

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Ajoutez des hôtes et installez le plug-in pour Exchange

Vous pouvez utiliser la page Ajouter un hôte SnapCenter pour ajouter des hôtes Windows. Le plug-in pour Exchange est automatiquement installé sur l'hôte spécifié. Il s'agit de la méthode recommandée pour installer les plug-ins. Vous pouvez ajouter un hôte et installer un plug-in pour un hôte individuel ou un cluster.

### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, telles que SnapCenter Admin.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur

l'hôte.

- Le service de mise en file d'attente des messages doit être en cours d'exécution.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration. Pour plus d'informations, voir "[Configurez le compte de service géré par groupe sous Windows Server 2016 ou version ultérieure pour Microsoft Exchange Server](#)".

### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.
- Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte ou un cluster individuel.
- Si un nœud Exchange fait partie d'un DAG, vous ne pouvez pas ajouter qu'un seul nœud dans le serveur SnapCenter.
- Si vous installez des plug-ins sur un cluster (Exchange DAG), ils sont installés sur tous les nœuds du cluster, même si certains nœuds ne possèdent pas de bases de données sur des LUN NetApp.

Depuis SnapCenter 4.6, SCE prend en charge la colocation et vous pouvez ajouter un hôte en utilisant les méthodes suivantes :

Ajout d'une opération d'hôte	4.5 et versions antérieures	4.6 et versions ultérieures
Ajoutez un DAG sans IP dans un domaine transversal ou différent	Non pris en charge	Pris en charge
Ajoutez plusieurs groupes de travail IP avec des noms uniques, résidant dans le même domaine ou entre les domaines	Pris en charge	Pris en charge
Ajoutez plusieurs groupes DAG sans IP ou sans IP qui ont les mêmes noms d'hôte et/ou nom de base de données dans le domaine transversal	Non pris en charge	Pris en charge
Ajoutez plusieurs groupes DAG sans IP avec le même nom et le même domaine	Non pris en charge	Pris en charge
Ajoutez plusieurs hôtes autonomes avec le même nom et le même domaine	Non pris en charge	Pris en charge

Le plug-in pour Exchange dépend du package de plug-ins SnapCenter pour Windows et les versions doivent être identiques. Lors de l'installation du plug-in pour Exchange, le module SnapCenter Plug-ins Package pour Windows est sélectionné par défaut et est installé avec le fournisseur de matériel VSS.

Si SnapManager pour Microsoft Exchange Server et SnapDrive pour Windows sont déjà installés, Et que vous souhaitez installer le plug-in pour Exchange sur le même serveur Exchange, vous devez annuler l'enregistrement du fournisseur de matériel VSS utilisé par SnapDrive pour Windows car il est incompatible avec le fournisseur de matériel VSS installé avec le module Plug-in pour Exchange et le module de plug-ins SnapCenter pour Windows. Pour plus d'informations, voir "[Comment enregistrer manuellement le fournisseur de matériel Data ONTAP VSS](#)".

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, procédez comme suit :

<b>Pour ce champ...</b>	<b>Procédez comme ça...</b>
Type d'hôte	<p>Sélectionnez <b>Windows</b> comme type d'hôte.</p> <p>SnapCenter Server ajoute l'hôte, puis installe le plug-in pour Windows sur l'hôte et le plug-in pour Exchange s'ils ne sont pas déjà installés.</p> <p>Le plug-in pour Windows et le plug-in pour Exchange doivent être de la même version. Si une version différente de Plug-in pour Windows était déjà installée, SnapCenter met à jour la version dans le cadre de l'installation.</p>

Pour ce champ...	Procédez comme ça...
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le nom de domaine complet (FQDN).</p> <p>Une adresse IP n'est prise en charge pour les hôtes de domaine non approuvés que si elle résout le FQDN.</p> <p>Si vous ajoutez un hôte à l'aide de SnapCenter et qu'il fait partie d'un sous-domaine, vous devez fournir le FQDN.</p> <p>Vous pouvez saisir des adresses IP ou le FQDN de l'une des adresses suivantes :</p> <ul style="list-style-type: none"><li>• Hôte autonome</li><li>• DAG Exchange</li></ul> <p>Pour un DAG Exchange, vous pouvez :</p> <ul style="list-style-type: none"><li>◦ Ajoutez un DAG en indiquant le nom du DAG, l'adresse IP du DAG, le nom du noeud ou l'adresse IP du noeud.</li><li>◦ Ajoutez le cluster DAG sans IP en fournissant l'adresse IP ou le FQDN de l'un des nœuds du cluster DAG.</li><li>◦ Ajoutez un DAG sans IP qui réside dans le même domaine ou dans un domaine différent. Vous pouvez également ajouter plusieurs groupes de travail IP/IP moins avec le même nom, mais des domaines différents.</li></ul> <div data-bbox="873 1520 928 1577"></div> <p>Pour un hôte autonome ou un DAG Exchange (cross-domain ou même domaine), il est recommandé de fournir un FQDN ou l'adresse IP de l'hôte ou du DAG.</p>

Pour ce champ...	Procédez comme ça...
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez les nouvelles informations d'identification.</p> <p>Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus d'informations, reportez-vous à la section informations sur la création d'informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom d'identification que vous avez spécifié.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

Lorsque vous sélectionnez Plug-in pour Exchange, le plug-in SnapCenter pour Microsoft SQL Server est automatiquement désélectionné. Microsoft recommande que SQL Server et Exchange Server ne soient pas installés sur le même système en raison de la quantité de mémoire utilisée et de toute autre utilisation des ressources requise par Exchange.

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port.</p> <p>Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p> </div>

Pour ce champ...	Procédez comme ça...
Chemin d'installation	Le chemin par défaut est C:\Program Files\NetApp\SnapCenter.  Vous pouvez éventuellement personnaliser le chemin.
Ajoutez tous les hôtes dans le DAG	Cochez cette case lorsque vous ajoutez un DAG.
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	Cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.  Indiquez le nom GMSA dans le format suivant : <i>domainName\accountName\$</i> .  <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">  GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows. </div>

7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour déterminer s'il répond aux conditions requises pour installer le plug-in. Si la configuration minimale requise n'est pas respectée, les messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à C:\Program Files\NetApp\SnapCenter\WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Surveillez la progression de l'installation.

### Configurer le port personnalisé pour les communications TCP NET

Par défaut, à partir de la version SnapCenter 6.0, le plug-in SnapCenter pour Windows utilise le port 909 pour les communications TCP NET. Si le port 909 est utilisé, vous pouvez configurer un autre port pour les communications TCP NET.

#### Étapes

1. Modifiez la valeur de la clé *NetTCPPort* située dans *C:\Program Files\NetApp\SnapCenter\SnapCenter\SnapCenter Plug-in pour Microsoft*

*Windows\vssproviders\navssprv.exe.config* au numéro de port requis.

```
<add key="NetTCPPort" value="new_port_number" />
```

2. Modifiez la valeur de la clé *NetTCPPort* située dans *C:\Program Files\NetApp\SnapCenter\SnapCenter\SnapCenter Plug-in pour Microsoft Windows\SnapDriveService.dll.config* au numéro de port requis.

```
<add key="NetTCPPort" value="new_port_number" />
```

3. Annulez l'enregistrement du service *Data ONTAP VSS Hardware Provider* en exécutant la commande ci-dessous :

```
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u
```

Vérifiez que le service ne s'affiche pas dans la liste des services dans *services.msc*.

4. Enregistrez le service *Data ONTAP VSS Hardware Provider* en exécutant la commande ci-dessous :

```
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem" `
```

Vérifiez si le service est maintenant affiché dans la liste des services dans *services.msc*.

5. Redémarrez le service *Plug-in pour Windows*.

## Installez le plug-in pour Exchange à partir de l'hôte SnapCenter Server à l'aide des applets de commande PowerShell

Vous devez installer le plug-in pour Exchange à partir de l'interface utilisateur graphique de SnapCenter. Si vous ne souhaitez pas utiliser l'interface graphique, vous pouvez utiliser les applets de commande PowerShell sur l'hôte SnapCenter Server ou sur un hôte distant.

### Avant de commencer

- Le serveur SnapCenter doit avoir été installé et configuré.
- Vous devez être un administrateur local sur l'hôte ou un utilisateur disposant de privilèges d'administration.
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations de plug-in, d'installation et de désinstallation, telles que SnapCenter Admin.
- Vous devez avoir vérifié les conditions d'installation requises et les types de configurations prises en charge avant d'installer le plug-in pour Exchange.
- L'hôte sur lequel vous souhaitez installer le plug-in pour Exchange doit être un hôte Windows.

### Étapes

1. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande *Open-SmConnection*, puis saisissez vos informations d'identification.
2. Ajoutez l'hôte sur lequel vous souhaitez installer le plug-in pour Exchange à l'aide de l'applet de commande *Add-SmHost* avec les paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

L'hôte peut être un hôte autonome ou un DAG. Si vous spécifiez un DAG, le paramètre *-IsDAG* est requis.

3. Installez le plug-in pour Exchange à l'aide de l'applet de commande *Install-SmHostPackage* avec les paramètres requis.

Cette commande installe le plug-in pour Exchange sur l'hôte spécifié, puis enregistre le plug-in avec SnapCenter.

## Installez le plug-in SnapCenter pour l'échange silencieusement à partir de la ligne de commande

Vous devez installer le plug-in pour Exchange à partir de l'interface utilisateur SnapCenter. Cependant, si vous ne pouvez pas pour une raison quelconque, vous pouvez exécuter le programme d'installation de Plug-in pour Exchange sans surveillance en mode silencieux à partir de la ligne de commande Windows.

### Avant de commencer

- Vous devez avoir sauvegardé vos ressources Microsoft Exchange Server.
- Vous devez avoir installé les modules du plug-in SnapCenter.
- Vous devez supprimer la version antérieure du plug-in SnapCenter pour Microsoft SQL Server avant de procéder à l'installation.

Pour plus d'informations, voir ["Comment installer un plug-in SnapCenter manuellement et directement à partir de l'hôte du plug-in"](#).

### Étapes

1. Vérifiez si le dossier *C:\temp* existe sur l'hôte du plug-in et que l'utilisateur connecté dispose d'un accès complet.
2. Téléchargez le plug-in SnapCenter pour Microsoft Windows depuis le site *C:\ProgramData\NetApp\SnapCenter\Package Repository*.

Ce chemin est accessible à partir de l'hôte sur lequel le serveur SnapCenter est installé.

3. Copiez le fichier d'installation sur l'hôte sur lequel vous souhaitez installer le plug-in.
4. À partir d'une invite de commande Windows sur l'hôte local, accédez au répertoire dans lequel vous avez enregistré les fichiers d'installation du plug-in.
5. Entrez la commande suivante pour installer le plug-in.

```
_Snapcenter_Windows_host_plugin.exe"/muet /debuglog"<Debug_Log_Path>" /log"<Log_Path>«
BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLSCE=« Install_Directory_Path> »
EPBI_SEREACCOUNT=<SERVICONTAP__PRODUCT_install_SICMADE>
```

Par exemple :

```
_C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_Windows_host_plugin.exe »/Silent
/debuglog« C:\HPPSCSQL_Install.log » /log« C:\temp » BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR=« C:\Program
Files\utilisateur_d'installation_de_HP_SICentrer=ISPs_SICentrer_SICentrer=s_SICentrer_SICentrer_SICe
ntrer=s_SICentrer_SICentrer_SICentrer=s_SICentrer_SICentrer=s
```



Tous les paramètres transmis lors de l'installation du plug-in pour Exchange sont sensibles à la casse.

Entrez les valeurs suivantes pour les variables :

Variable	Valeur
<code>/debuglog »&lt;Debug_Log_Path&gt;</code>	Spécifiez le nom et l'emplacement du fichier journal du programme d'installation de la suite, comme dans l'exemple suivant :  <code>Setup.exe /debuglog"C:\PathToLog\setupexe.log</code>
<code>BI_SNAPCENTER_PORT</code>	Spécifiez le port sur lequel SnapCenter communique avec SMCORE.
<code>SUITE_INSTALLDIR</code>	Spécifiez le répertoire d'installation du module de plug-in hôte.
<code>BI_SERVICEACCOUNT</code>	Spécifiez le compte de service Web SnapCenter Plug-in pour Microsoft Windows.
<code>BI_SERVICEPWD</code>	Spécifiez le mot de passe du compte de service Web SnapCenter Plug-in pour Microsoft Windows.
Installation de ISFeatureInstall	Spécifier la solution à déployer par SnapCenter sur un hôte distant

- Surveillez le planificateur de tâches Windows, le fichier journal d'installation principal `C:\Installdebug.log` et les fichiers d'installation supplémentaires dans `C:\Temp`.
- Surveillez le répertoire `%temp%` pour vérifier si les programmes d'installation `msiexe.exe` installent le logiciel sans erreur.



L'installation du plug-in pour Exchange enregistre le plug-in sur l'hôte et non sur le serveur SnapCenter. Vous pouvez enregistrer le plug-in sur le serveur SnapCenter en ajoutant l'hôte à l'aide de l'interface graphique de SnapCenter ou de l'applet de commande PowerShell. Une fois l'hôte ajouté, le plug-in est automatiquement découvert.

## Contrôler l'état d'installation du module d'extension SnapCenter

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours

-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

## Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

### Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
  - a. Double-cliquez sur le certificat.
  - b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
  - c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.

- d. Copiez les caractères hexadécimaux de la zone.
- e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :
  - a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

### Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

#### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCORE 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte
Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_{certificate thumbprint}_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:_{SMCore Port}_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:_{SMCore Port}_ certhash=$cert
appid="$guid"
```

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Configurez SnapManager 7.x pour Exchange et SnapCenter afin qu'ils coexistent

Pour permettre au plug-in SnapCenter pour Microsoft Exchange Server de coexister avec SnapManager pour Microsoft Exchange Server, vous devez installer le plug-in SnapCenter pour Microsoft Exchange Server sur le même serveur Exchange sur lequel SnapManager pour Microsoft Exchange Server est installé, désactiver les planifications SnapManager pour Exchange, Et configurer de nouvelles planifications et de nouvelles sauvegardes à l'aide du plug-in SnapCenter pour Microsoft Exchange Server.

### Avant de commencer

- SnapManager pour Microsoft Exchange Server et SnapDrive pour Windows sont déjà installés. De plus, SnapManager pour les sauvegardes Microsoft Exchange Server est présent sur le système et dans le

répertoire SnapInfo.

- Vous devez avoir supprimé ou récupéré les sauvegardes effectuées par SnapManager pour Microsoft Exchange Server dont vous n'avez plus besoin.
- Vous devez avoir suspendu ou supprimé tous les programmes créés par SnapManager pour Microsoft Exchange Server à partir du planificateur Windows.
- Le plug-in SnapCenter pour Microsoft Exchange Server et SnapManager pour Microsoft Exchange Server peuvent coexister sur le même serveur Exchange, mais vous ne pouvez pas mettre à niveau les installations SnapManager existantes pour Microsoft Exchange Server vers SnapCenter.

SnapCenter ne propose pas d'option de mise à niveau.

- SnapCenter ne prend pas en charge la restauration des bases de données Exchange à partir de SnapManager pour sauvegarde Microsoft Exchange Server.

Si vous ne désinstallez pas SnapManager pour Microsoft Exchange Server après l'installation du plug-in SnapCenter pour Microsoft Exchange Server et que vous souhaitez restaurer une sauvegarde SnapManager pour Microsoft Exchange Server, vous devez effectuer des étapes supplémentaires.

## Étapes

1. En utilisant PowerShell sur tous les nœuds DAG, déterminez si SnapDrive pour Windows VSS Hardware Provider est enregistré : `vssadmin list fournisseurs`

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
 Provider type: Hardware
 Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
 Version: 7. 1. 4. 6845
```

2. A partir du répertoire SnapDrive, désenregistrez le fournisseur de matériel VSS à partir de SnapDrive pour Windows : `navssprv.exe -r service -u`
3. Vérifiez que le fournisseur de matériel VSS a été supprimé : `vssadmin list fournisseurs`
4. Ajoutez l'hôte Exchange à SnapCenter, puis installez le plug-in SnapCenter pour Microsoft Windows et le plug-in SnapCenter pour Microsoft Exchange Server.
5. Dans le répertoire Plug-in SnapCenter pour Microsoft Windows de tous les nœuds DAG, vérifiez que le fournisseur de matériel VSS est enregistré : `vssadmin list fournisseurs`

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
 Provider type: Hardware
 Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
 Version: 7. 0. 0. 5561
```

6. Arrêtez les planifications de sauvegarde SnapManager pour Microsoft Exchange Server.
7. À l'aide de l'interface graphique SnapCenter, créez des sauvegardes à la demande, configurez des sauvegardes planifiées et configurez les paramètres de conservation.
8. Désinstallez SnapManager pour Microsoft Exchange Server.

Si vous ne désinstallez pas SnapManager pour Microsoft Exchange Server maintenant et ultérieurement souhaitez restaurer une sauvegarde SnapManager pour Microsoft Exchange Server :

- a. Annuler l'enregistrement du plug-in SnapCenter pour Microsoft Exchange Server à partir de tous les nœuds DAG : `navssprv.exe -r service -u`

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. Dans le répertoire `C:\Program Files\NetApp\SnapDrive\`, enregistrez SnapDrive pour Windows sur tous les nœuds du DAG : `navssprv.exe -r service -a hostname\username -p password`

## Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM) ou si vous souhaitez protéger des VM et des datastores, vous devez déployer l'appliance virtuelle du plug-in SnapCenter pour VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section "[Présentation du déploiement](#)".

### Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Créez ou importez un certificat SSL](#)".

### Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est `/opt/netapp/config/crl`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour

chaque CRL.

## Préparation à la protection des données

Avant d'effectuer des opérations de protection des données telles que la sauvegarde, le clonage ou la restauration, vous devez définir votre stratégie et configurer l'environnement. Vous pouvez également configurer le serveur SnapCenter pour qu'il utilise la technologie SnapMirror et SnapVault.

Pour profiter des avantages de SnapVault et de la technologie SnapMirror, vous devez configurer et initialiser une relation de protection des données entre les volumes source et destination sur le périphérique de stockage. Vous pouvez utiliser NetAppSystem Manager ou utiliser la ligne de commandes de la console de stockage pour effectuer ces tâches.

### Plus d'informations

["Mise en route de l'API REST"](#)

## Conditions préalables à l'utilisation du plug-in SnapCenter pour Microsoft Exchange Server

Avant d'utiliser le plug-in pour Exchange, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches préalables.

- Installer et configurer SnapCenter Server.
- Connectez-vous à SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant ou en attribuant des connexions au système de stockage et en créant des identifiants.



SnapCenter ne prend pas en charge plusieurs SVM de même nom sur différents clusters. Chaque SVM pris en charge par SnapCenter doit avoir un nom unique.

- Ajoutez des hôtes, installez le plug-in SnapCenter pour Microsoft Windows et le plug-in SnapCenter pour Microsoft Exchange Server et découvrez (actualisez) les ressources.
- Provisionnez le stockage côté hôte à l'aide du plug-in SnapCenter pour Microsoft Windows.
- Si vous utilisez SnapCenter Server pour protéger les bases de données Exchange résidant sur des LUN RDM VMware, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter. La documentation du plug-in SnapCenter pour VMware vSphere contient des informations supplémentaires.



Les VMDK ne sont pas pris en charge.

- Déplacer une base de données Microsoft Exchange Server existante d'un disque local vers un stockage pris en charge à l'aide des outils Microsoft Exchange.
- Configurez les relations SnapMirror et SnapVault, si vous souhaitez effectuer une répllication de sauvegarde.

Pour les utilisateurs de SnapCenter 4.1.1, la documentation du plug-in SnapCenter pour VMware vSphere 4.1.1 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers. Pour les utilisateurs de SnapCenter 4.2.x, NetApp Data Broker 1.0 et 1.0.1, la documentation relative

à la protection des bases de données et des systèmes de fichiers virtualisés à l'aide du plug-in SnapCenter pour VMware vSphere fourni par le dispositif virtuel NetApp Data Broker basé sur Linux (format Open Virtual Appliance). Pour les utilisateurs de SnapCenter 4.3.x, la documentation du plug-in SnapCenter pour VMware vSphere 4.3 contient des informations sur la protection des bases de données virtualisées et des systèmes de fichiers à l'aide du plug-in SnapCenter basé sur Linux pour l'appliance virtuelle VMware vSphere (format Open Virtual Appliance).

["Documentation du plug-in SnapCenter pour VMware vSphere"](#)

## Mode d'utilisation des ressources, des groupes de ressources et des stratégies pour la protection d'Exchange Server

Avant d'utiliser SnapCenter, il est utile de comprendre les concepts de base associés aux opérations de sauvegarde, de restauration et de réamorçage que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des bases de données de boîtes aux lettres ou des groupes de disponibilité de base de données Microsoft Exchange que vous sauvegardez avec SnapCenter.
- Un groupe de ressources SnapCenter, est un ensemble de ressources d'un DAG hôte ou Exchange, et le groupe de ressources peut inclure un DAG entier ou des bases de données individuelles.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

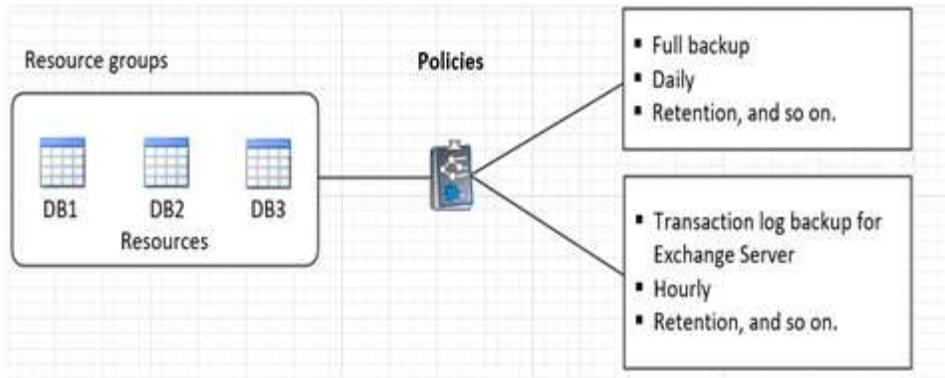
Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

Les groupes de ressources étaient auparavant appelés ensembles de données.

- Les stratégies définissent la fréquence de sauvegarde, la conservation des copies, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une ou plusieurs stratégies lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

Pensez à un groupe de ressources comme définissant *quoi* vous voulez protéger et quand vous voulez le protéger en termes de jour et de temps. Pensez à une stratégie comme définir *comment* vous voulez la protéger. Si vous sauvegardez toutes les bases de données d'un hôte, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources pour effectuer une sauvegarde complète tous les jours et un autre programme qui effectue des sauvegardes de journaux toutes les heures. L'image suivante illustre la relation entre les ressources, les groupes de ressources et les politiques des bases de données :



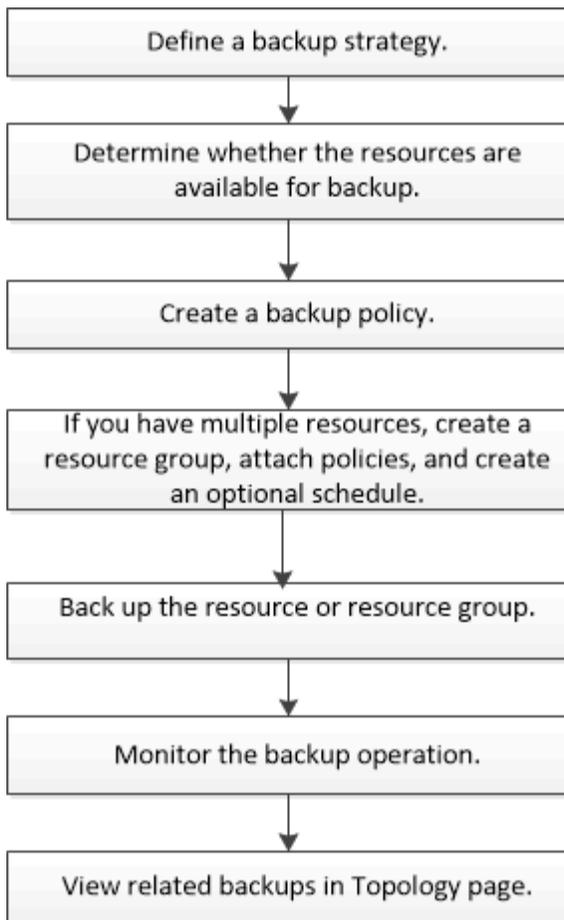
## Sauvegarder les ressources Exchange

### Workflow de sauvegarde

Lorsque vous installez le plug-in SnapCenter pour Microsoft Exchange Server dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder les ressources Exchange.

Vous pouvez planifier plusieurs sauvegardes pour les exécuter simultanément sur plusieurs serveurs. Les opérations de sauvegarde et de restauration ne peuvent pas être effectuées simultanément sur la même ressource. Les copies de sauvegarde actives et passives sur le même volume ne sont pas prises en charge.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



## Vérification des sauvegardes et des bases de données Exchange

Le plug-in SnapCenter pour Microsoft Exchange Server ne permet pas de vérifier les sauvegardes. Toutefois, vous pouvez utiliser l'outil SSET fourni avec Exchange pour vérifier les bases de données et les sauvegardes Exchange.

L'outil Microsoft Exchange Eseutil est un utilitaire de ligne de commande inclus avec votre serveur Exchange. L'utilitaire vous permet d'effectuer des contrôles de cohérence pour vérifier l'intégrité des bases de données et des sauvegardes Exchange.

**Meilleure pratique:** il n'est pas nécessaire d'effectuer des contrôles de cohérence sur les bases de données faisant partie d'une configuration DAG (Database Availability Group) avec au moins deux répliques.

Pour plus d'informations, reportez-vous à la section "[Documentation Microsoft Exchange Server](#)".

## Déterminez si des ressources Exchange sont disponibles pour la sauvegarde

Les ressources sont les bases de données, les groupes de disponibilité de base de données Exchange gérés par les plug-ins que vous avez installés. Vous pouvez ajouter ces ressources aux groupes de ressources de sorte que vous puissiez effectuer des tâches de protection des données, mais vous devez d'abord identifier les ressources disponibles. La détermination des ressources disponibles permet également de vérifier que l'installation du plug-in s'est déroulée correctement.

## Avant de commencer

- Vous devez avoir déjà terminé des tâches telles que l'installation de SnapCenter Server, l'ajout d'hôtes, la création de connexions au système de stockage, l'ajout d'informations d'identification et l'installation du plug-in pour Exchange.
- Pour tirer parti des fonctionnalités du logiciel Single Mailbox Recovery, vous devez avoir localisé votre base de données active sur le serveur Exchange Server sur lequel le logiciel Single Mailbox Recovery est installé.
- Si les bases de données résident sur des LUN RDM VMware, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter. Le "[Documentation du plug-in SnapCenter pour VMware vSphere](#)" a plus d'informations.

## Description de la tâche

- Vous ne pouvez pas sauvegarder les bases de données lorsque l'option **Etat général** de la page Détails est définie sur non disponible pour la sauvegarde. L'option **Etat général** est définie sur non disponible pour la sauvegarde lorsque l'un des éléments suivants est vrai :

- Les bases de données ne se trouvent pas sur un LUN NetApp.
- Les bases de données ne sont pas dans un état normal.

Les bases de données ne sont pas à l'état normal lorsqu'elles sont en montage, démontage, réamorçage ou récupération en attente.

- Si vous disposez d'un groupe de disponibilité de base de données (DAG), vous pouvez sauvegarder toutes les bases de données du groupe en exécutant la tâche de sauvegarde à partir du DAG.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez **Microsoft Exchange Server** dans la liste déroulante des plug-ins située dans le coin supérieur gauche de la page Ressources.
2. Dans la page Ressources, sélectionnez **Database**, **Database Availability Group** ou **Resource Group** dans la liste déroulante **View**.

Toutes les bases de données et les fichiers DAG sont affichés avec leurs noms DAG ou d'hôte au format FQDN, ce qui vous permet de distinguer entre plusieurs bases de données.

Cliquez sur  et sélectionnez le nom d'hôte et le serveur Exchange pour filtrer les ressources. Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

3. Cliquez sur **Actualiser les ressources**.

Les ressources récemment ajoutées, renommées ou supprimées sont mises à jour dans l'inventaire du serveur SnapCenter.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

Les ressources s'affichent avec des informations telles que le nom de la ressource, le nom du groupe de disponibilité de la base de données, le serveur dans lequel la base de données est actuellement active, le serveur avec copies, l'heure de la dernière sauvegarde et l'état global.

- Si la base de données se trouve sur un stockage non-NetApp, la colonne État global n'est pas disponible pour la sauvegarde.

Dans un DAG, si la copie de la base de données active se trouve sur un stockage non NetApp et si au moins une copie de base de données passive se trouve sur un stockage NetApp, elle n'est pas protégée dans la colonne **global Status**.

Vous ne pouvez pas effectuer d'opérations de protection des données sur une base de données se résidant sur un type de stockage non NetApp.

- Si la base de données se trouve sur du stockage NetApp et n'est pas protégée, elle ne sera pas protégée dans la colonne **global Status**.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée, l'interface utilisateur affiche le message Backup not run dans la colonne **global Status**.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée et si la sauvegarde est déclenchée pour la base de données, l'interface utilisateur affiche le message Backup succeeded (sauvegarde réussie) dans la colonne **global Status** (État général).

## Créer des stratégies de sauvegarde pour les bases de données Exchange Server

Vous pouvez créer une stratégie de sauvegarde pour les ressources Exchange ou pour les groupes de ressources avant d'utiliser SnapCenter pour sauvegarder les ressources Microsoft Exchange Server, ou vous pouvez créer une stratégie de sauvegarde au moment de créer un groupe de ressources ou de sauvegarder une seule ressource.

### Avant de commencer

- Vous devez avoir défini votre stratégie de protection des données.

Pour en savoir plus, consultez les informations sur la définition d'une stratégie de protection des données pour les bases de données Exchange.

- Vous devez être prêt à préparer la protection des données en exécutant des tâches telles que l'installation d'SnapCenter, l'ajout d'hôtes, l'identification des ressources et la création de connexions du système de stockage.
- Vous devez avoir actualisé (découvert) les ressources Exchange Server.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir attribué des machines virtuelles de stockage (SVM) pour les volumes source et de destination.
- Si vous voulez exécuter les scripts PowerShell dans les prescripteurs et les postscripts, vous devez définir la valeur de `usePowershellProcessforScripts` paramètre à vrai dans le `web.config` fichier.

La valeur par défaut est FALSE.

- Vérifiez les prérequis et les limites spécifiques de la synchronisation active SnapMirror. Pour plus d'informations, reportez-vous à "[Limites d'objet pour la synchronisation active SnapMirror](#)".

### Description de la tâche

- Une stratégie de sauvegarde est un ensemble de règles qui régit la façon dont vous gérez et conservez les sauvegardes, ainsi que la fréquence de sauvegarde de la ressource ou du groupe de ressources. En outre, vous pouvez spécifier des paramètres de script. La définition d'options dans une stratégie permet de gagner du temps lorsque vous souhaitez réutiliser la stratégie pour un autre groupe de ressources.
- La conservation complète des sauvegardes est spécifique à une règle donnée. Une base de données ou une ressource utilisant la stratégie A avec une conservation de sauvegarde complète de 4 conserve 4 sauvegardes complètes et n'a aucun effet sur la stratégie B pour la même base de données ou ressource, qui peut avoir une rétention de 3 pour conserver 3 sauvegardes complètes.

- La conservation des sauvegardes de journaux est efficace pour toutes les stratégies et s'applique à toutes les sauvegardes de journaux d'une base de données ou d'une ressource. Par conséquent, lorsqu'une sauvegarde complète est effectuée à l'aide de la stratégie B, le paramètre de conservation des journaux affecte les sauvegardes des journaux créées par la stratégie A sur la même base de données ou ressource. De même, le paramètre de rétention des journaux de la stratégie A affecte les sauvegardes des journaux créées par la stratégie B sur la même base de données.
- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreServiceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

**Meilleure pratique:** il est préférable de configurer la stratégie de rétention secondaire en fonction du nombre de sauvegardes complètes et de journaux, globalement, que vous voulez conserver. Lorsque vous configurez des règles de conservation secondaires, gardez à l'esprit que lorsque les bases de données et les journaux situés sur des volumes différents, chaque sauvegarde peut avoir trois copies Snapshot. Lorsque les bases de données et les journaux se trouvent dans le même volume, chaque sauvegarde peut avoir deux copies Snapshot.

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.

La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.

Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page Type de sauvegarde et réplication, effectuez les opérations suivantes :
  - a. Choisissez un type de sauvegarde :

Les fonctions que vous recherchez...	Procédez comme ça...
Sauvegardez les fichiers de base de données et les journaux de transactions requis	<p>Sélectionnez <b>sauvegarde complète et sauvegarde du journal</b>.</p> <p>Les bases de données sont sauvegardées par troncature de journaux, et tous les journaux sont sauvegardés, notamment les journaux tronqués.</p> <p> Il s'agit du type de sauvegarde recommandé.</p>
Sauvegardez les fichiers de base de données et les journaux de transactions non validés	<p>Sélectionnez <b>sauvegarde complète</b>.</p> <p>Les bases de données sont sauvegardées par troncature de journal, et les journaux tronqués ne sont pas sauvegardés.</p>
Sauvegardez tous les journaux de transaction	<p>Sélectionnez <b>sauvegarde journal</b>.</p> <p>Tous les journaux de transactions du système de fichiers actif sont sauvegardés et il n'y a pas de troncature de journal.</p> <p>Un répertoire <i>scebackupinfo</i> est créé sur le même disque que le journal live. Ce répertoire contient le pointeur vers les modifications incrémentielles de la base de données Exchange et il n'est pas équivalent aux fichiers journaux complets.</p>
Sauvegardez tous les fichiers de base de données et les journaux de transactions sans tronquer les fichiers journaux de transaction	<p>Sélectionnez <b>Copier sauvegarde</b>.</p> <p>Toutes les bases de données et tous les journaux sont sauvegardés, et il n'y a pas de troncature de journal. Généralement, ce type de sauvegarde est utilisé pour le réamorçage d'une réplique, pour le test ou le diagnostic d'un problème.</p>



Vous devez définir l'espace requis pour les sauvegardes de journaux en fonction de la conservation complète des sauvegardes et non pas en fonction de la conservation à chaud (UTM).



Créez des règles de copie distinctes pour les journaux et les bases de données lors du traitement des volumes Exchange (LUN), et définissez la conservation (conservation) de la règle de journalisation sur deux fois le nombre pour chaque étiquette de la règle de base de données, en utilisant les mêmes étiquettes. Pour plus d'informations, voir "[Les sauvegardes SnapCenter pour Exchange ne conservent que la moitié des snapshots sur le volume du journal de destination du coffre-fort](#)"

b. Dans la section Database Availability Group Settings, sélectionnez une action :

Pour ce champ...	Procédez comme ça...
Sauvegarde des copies actives	<p>Sélectionnez cette option pour sauvegarder uniquement les copies actives de la base de données sélectionnée.</p> <p>Pour les groupes de disponibilité de base de données (DAG), cette option sauvegarde uniquement les copies actives de toutes les bases de données du DAG.</p> <p>Les copies passives ne sont pas sauvegardées.</p>
Sauvegarder les copies sur les serveurs à sélectionner au moment de la création des tâches de sauvegarde	<p>Sélectionnez cette option pour sauvegarder toutes les copies des bases de données sur les serveurs sélectionnés, actifs et passifs.</p> <p>Pour les fichiers DAG, cette option sauvegarde les copies actives et passives de toutes les bases de données des serveurs sélectionnés.</p>



Dans les configurations en cluster, les sauvegardes sont conservées sur chaque nœud du cluster en fonction des paramètres de conservation définis dans la règle. Si le nœud propriétaire du cluster change, les sauvegardes du nœud propriétaire précédent seront conservées. La conservation s'applique uniquement au niveau des nœuds.

- c. Dans la section fréquence d'horaires, sélectionnez un ou plusieurs types de fréquence : **sur demande, horaire, quotidien, hebdomadaire et mensuel**.



Vous pouvez spécifier le planning (date de début, date de fin) des opérations de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais vous permet d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

- d. Sélectionnez le libellé police.

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

- e. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif. L'option **période de verrouillage de copie d'instantané secondaire** est disponible sur la page Retention.

Pour ce champ...	Procédez comme ça...
Mettre à jour SnapMirror après la création d'un Snapshot local	<p>Sélectionnez cette option pour conserver des copies en miroir des jeux de sauvegarde sur un autre volume (SnapMirror).</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Cette option doit être activée pour la synchronisation active SnapMirror.</p> <div data-bbox="873 772 932 829" data-label="Image"></div> <p>La règle primaire uniquement ne peut pas être utilisée si la synchronisation active SnapMirror est configurée pour des volumes Exchange ONTAP. SnapCenter n'autorise pas cela. Vous devez activer l'option « miroir ».</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir "<a href="#">Afficher les sauvegardes Exchange sur la page topologie</a>".</p>
Mettre à jour SnapVault après avoir créé un instantané local	Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque.
Nombre de tentatives d'erreur	Saisissez le nombre de tentatives de réplication qui doivent se produire avant l'interruption du processus.

+



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

6. Dans la page Retention, configurez les paramètres de rétention.

Les options affichées dépendent du type de sauvegarde et du type de fréquence que vous avez précédemment sélectionnés.



La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.



Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.

- a. Dans la section Paramètres de conservation des sauvegardes de journaux, sélectionnez l'une des options suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
<p>Conservation d'un nombre spécifique de sauvegardes de journaux</p>	<p>Sélectionnez <b>nombre de sauvegardes complètes pour lesquelles les journaux sont conservés</b> et spécifiez le nombre de sauvegardes complètes pour lesquelles vous souhaitez pouvoir être restaurées à la minute.</p> <p>La conservation des données en moins d'une minute s'applique à la sauvegarde des journaux créée via une sauvegarde complète ou une sauvegarde des journaux. Par exemple, si les paramètres de conservation UTM sont configurés pour conserver les sauvegardes des journaux des 5 dernières sauvegardes complètes, les sauvegardes des journaux des 5 dernières sauvegardes complètes sont conservées.</p> <p>Les dossiers de journaux créés dans le cadre de sauvegardes complètes et de journaux sont automatiquement supprimés dans le cadre d'UTM. Vous ne pouvez pas supprimer les dossiers de journal manuellement. Par exemple, si le paramètre de conservation de sauvegarde complète ou complète et de sauvegarde des journaux est défini sur 1 mois et que la rétention UTM est définie sur 10 jours, le dossier de journaux créé dans le cadre de ces sauvegardes sera supprimé conformément à UTM. Par conséquent, seuls les dossiers journaux de 10 jours seront présents et toutes les autres sauvegardes sont marquées pour la restauration à un point dans le temps.</p> <p>Vous pouvez définir la valeur de rétention UTM sur 0, si vous ne souhaitez pas effectuer une restauration en moins d'une minute. Cela active l'opération de restauration instantanée.</p> <p><b>Meilleure pratique</b> : il est préférable que le paramètre soit égal au paramètre Total snapshots (sauvegardes complètes) dans la section Paramètres de rétention complète des sauvegardes. Cela permet de s'assurer que les fichiers journaux sont conservés pour chaque sauvegarde complète.</p>

Les fonctions que vous recherchez...	Procédez comme ça...
Conservation des copies de sauvegarde pendant un nombre spécifique de jours	<p>Sélectionnez l'option <b>conserver les sauvegardes du journal pour le dernier</b> et indiquez le nombre de jours pour conserver les copies de sauvegarde du journal.</p> <p>Les sauvegardes de journaux ne prennent pas plus de jours, mais sont conservées.</p>
Période de verrouillage des snapshots	<p>Sélectionnez <b>période de verrouillage des copies Snapshot</b>, puis sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>

Si vous avez sélectionné **Log backup** comme type de sauvegarde, les sauvegardes de journaux sont conservées dans le cadre des paramètres de conservation à la minute pour les sauvegardes complètes.

- b. Dans la section Paramètres de conservation des sauvegardes complètes, sélectionnez l'une des options suivantes pour les sauvegardes à la demande, puis sélectionnez-en une pour les sauvegardes complètes :

Pour ce champ...	Procédez comme ça...
Conservez uniquement un nombre spécifique d'instantanés	<p>Si vous souhaitez spécifier le nombre de sauvegardes complètes à conserver, sélectionnez l'option <b>nombre total de copies Snapshot à conserver</b> et spécifiez le nombre de snapshots (sauvegardes complètes) à conserver.</p> <p>Si le nombre de sauvegardes complètes dépasse le nombre spécifié, les sauvegardes complètes dépassant le nombre spécifié sont supprimées, les copies les plus anciennes étant supprimées en premier.</p>
Conservation des sauvegardes complètes pendant un nombre spécifique de jours	<p>Sélectionnez l'option <b>conserver les copies Snapshot pour</b> et spécifiez le nombre de jours de conservation des snapshots (sauvegardes complètes).</p>
Période de verrouillage du snapshot principal	<p>Sélectionnez <b>période de verrouillage des copies d'instantanés primaires</b>, puis sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>

Pour ce champ...	Procédez comme ça...
Période de verrouillage des snapshots secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.

Si vous disposez d'une base de données avec uniquement des sauvegardes de journaux et qu'aucune sauvegarde complète sur un hôte dans une configuration DAG, les sauvegardes de journaux sont conservées de la manière suivante :

- Par défaut, SnapCenter trouve la sauvegarde complète la plus ancienne pour cette base de données dans tous les autres hôtes du DAG, et supprime toutes les sauvegardes des journaux de cet hôte qui ont été effectuées avant la sauvegarde complète.
- Vous pouvez ignorer le comportement de conservation par défaut ci-dessus pour une base de données sur un hôte d'un DAG avec uniquement des sauvegardes de journaux en ajoutant la clé **MaxBackupLogOnlyCountWithoutFullBackup** dans le fichier *C:\Program Files\NetApp\SnapCenter WebApp\web.config*.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

Dans l'exemple, la valeur 10 signifie que vous conservez jusqu'à 10 sauvegardes de journaux sur l'hôte.

7. Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript qui doivent être exécutés avant ou après l'opération de sauvegarde, respectivement.

- Les arguments de sauvegarde du prescripteur incluent « »\$Database' et « »\$ServerInstance' ».
- Les arguments de sauvegarde PostScript incluent ""\$Database"", ""\$ServerInstance"", ""\$BackupName"", ""\$logDirectory"" et ""\$Logsnapshot"".

Vous pouvez exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer des journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et associez des stratégies pour les serveurs Exchange

Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de tâche de protection des données que vous souhaitez exécuter et la planification de protection.

### Description de la tâche

- Le CHEMIN\_SCRIPTS est défini à l'aide de la clé pré-défini WindowsScriptsDirectory située dans le fichier SMCoreserviceHost.exe.Config de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service SMcore. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : API /4.7/configsettings

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- L'ajout de nouvelles bases de données sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec la synchronisation active SnapMirror n'est pas pris en charge.
- L'ajout de nouvelles bases de données à un groupe de ressources existant en mode de basculement de la synchronisation active SnapMirror n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement à l'état normal ou de retour arrière.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in Microsoft Exchange Server dans la liste.
2. Dans la page Ressources, sélectionnez **Database** dans la liste **View**.



Si vous avez récemment ajouté une ressource à SnapCenter, cliquez sur **Actualiser les ressources** pour afficher la nouvelle ressource ajoutée.

3. Cliquez sur **Nouveau groupe de ressources**.
4. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez le nom du groupe de ressources.   Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.  Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.
Utilisez le format de nom personnalisé pour la copie Snapshot	Facultatif : entrez un nom et un format de snapshot personnalisés.  Par exemple, <i>clienttext_resourcegroup_policy_hostname</i> ou <i>resourcegroup_hostname</i> . Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page Ressources, effectuez les opérations suivantes :

- a. Sélectionnez le type de ressource et le groupe de disponibilité de base de données dans les listes déroulantes pour filtrer la liste des ressources disponibles.



Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

Dans les sections Ressources disponibles et Ressources sélectionnées, le nom de la base de données s'affiche avec le FQDN de l'hôte. Ce FQDN indique uniquement que la base de données est active sur cet hôte spécifique et peut ne pas effectuer de sauvegarde sur cet hôte. Vous devez sélectionner un ou plusieurs serveurs de sauvegarde dans l'option de sélection du serveur, où vous souhaitez effectuer une sauvegarde au cas où vous avez sélectionné l'option **Sauvegarder les copies sur les serveurs à sélectionner au moment de la création de la tâche de sauvegarde** dans la stratégie.

- b. Saisissez le nom de la ressource dans la zone de texte de recherche ou faites défiler pour rechercher une ressource.
- c. Pour déplacer des ressources de la section Ressources disponibles vers la section Ressources sélectionnées, effectuez l'une des opérations suivantes :
  - Sélectionnez **Autosélectionner toutes les ressources sur le même volume de stockage** pour déplacer toutes les ressources du même volume vers la section Ressources sélectionnées.
  - Sélectionnez les ressources dans la section Ressources disponibles, puis cliquez sur la flèche droite pour les déplacer vers la section Ressources sélectionnées.

Les groupes de ressources de SnapCenter pour Microsoft Exchange Server ne peuvent pas avoir plus de 30 bases de données par instantané. S'il y a plus de 30 bases de données dans un groupe de ressources, un deuxième instantané est créé pour les bases de données supplémentaires. Par conséquent, 2 sous-tâches sont créées sous la tâche de sauvegarde principale. Pour les sauvegardes ayant une réplication secondaire, lorsque SnapMirror ou SnapVault est en cours de mise à jour, il peut arriver que la mise à jour pour les sous-tâches se chevauchent. La tâche de sauvegarde principale reste en cours d'exécution permanente même si les journaux indiquent que la tâche est terminée.

6. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .



Si une stratégie contient l'option **Sauvegarder les copies sur les serveurs à sélectionner au moment de la création de la tâche de sauvegarde**, une option de sélection de serveur s'affiche pour sélectionner un ou plusieurs serveurs. L'option de sélection du serveur répertorie uniquement le serveur sur lequel la base de données sélectionnée se trouve sur du stockage NetApp.

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Dans la section configurer les plannings des stratégies sélectionnées, cliquez sur  Dans la colonne **configurer les programmes** pour la stratégie pour laquelle vous souhaitez configurer le

planning.

- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez la planification en spécifiant la date de début, la date d'expiration et la fréquence, puis cliquez sur **OK**.

Vous devez le faire pour chaque fréquence répertoriée dans la police. Les planifications configurées sont répertoriées dans la colonne **programmes appliqués** de la section configurer les planifications pour les stratégies sélectionnées.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.

Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `Set-SmSmtPServer`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell pour Exchange Server

Vous devez créer une connexion SVM (Storage Virtual machine) et une identifiant avant d'utiliser les applets de commande PowerShell pour sauvegarder et restaurer.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

### Étapes

1. Démarrer une session de connexion PowerShell à l'aide de `Open-SmConnection` applet de commande.

Cet exemple ouvre une session PowerShell :

```
PS C:\> Open-SmConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de `Add-SmStorageConnection` applet de commande.

Dans cet exemple, une nouvelle connexion au système de stockage est créée :

```
PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
-Timeout 60
```

3. Créez un nouveau compte Run as en utilisant le `Add-Credential` applet de commande.

Cet exemple crée un nouveau compte Run as nommé `ExchangeAdmin` avec des informations d'identification Windows :

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
-Credential sddev\administrator
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Sauvegarde des bases de données Exchange

Si une base de données ne fait pas partie d'un groupe de ressources, vous pouvez sauvegarder la base de données ou le groupe de disponibilité de base de données à partir de la page Ressources.

### Avant de commencer

- Vous devez avoir créé une stratégie de sauvegarde.
- On doit avoir attribué l'agrégat utilisé par l'opération de sauvegarde à la SVM utilisée par la base de données.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un stockage secondaire, le rôle attribué à l'utilisateur de stockage doit inclure le privilège « `napmirror All` ». Toutefois, si vous utilisez le rôle « `vsadmin` », le privilège « `napmirror all` » n'est pas requis.
- Si vous souhaitez effectuer une sauvegarde de la base de données ou d'un groupe de disponibilité de base de données doté d'une copie de base de données active/passive sur un système de stockage NetApp et non-NetApp, Et vous avez sélectionné l'option **Sauvegarder les copies actives** ou **Sauvegarder les copies sur les serveurs à sélectionner lors de la création de la tâche de sauvegarde temps** dans la stratégie, puis les tâches de sauvegarde passent à l'état d'avertissement. La sauvegarde réussira si la copie de base de données active/passive sur le stockage NetApp. La sauvegarde échouera pour la copie de base de données active/passive sur un système de stockage non

NetApp.

**Meilleure pratique:** n'exécutez pas les sauvegardes des bases de données actives et passives en même temps. Un problème de course peut se produire et l'une des sauvegardes peut échouer.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in **Microsoft Exchange Server** dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Database Availability Group** dans la liste **View**.

Dans la page Ressources, l'  icône indique que la base de données se trouve sur un stockage non-NetApp.



Dans un DAG, si une copie active de la base de données se trouve sur un stockage non-NetApp et qu'au moins une copie de base de données passive réside sur un stockage NetApp, vous pouvez protéger la base de données.

Cliquez sur \* , puis sélectionnez le nom d'hôte et le type de base de données pour filtrer les ressources. Vous pouvez alors cliquer sur \*  pour fermer le volet de filtre.

- Si vous souhaitez sauvegarder une base de données, cliquez sur son nom.
    - i. Si la vue topologie est affichée, cliquez sur **protéger**.
    - ii. Si l'assistant base de données - protection des ressources s'affiche, passez à l'étape 3.
  - Si vous souhaitez sauvegarder un groupe de disponibilité de base de données, cliquez sur le nom du groupe de disponibilité de base de données.
3. Si vous souhaitez spécifier un nom d'instantané personnalisé, dans la page Ressources, cochez la case **utiliser le format de nom personnalisé pour la copie d'instantané**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom d'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

4. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \* \* .



Si une stratégie contient l'option **Sauvegarder les copies sur les serveurs à sélectionner au moment de la création de la tâche de sauvegarde**, une option de sélection de serveur s'affiche pour sélectionner un ou plusieurs serveurs. L'option de sélection du serveur répertorie uniquement le serveur sur lequel la base de données sélectionnée se trouve sur un système de stockage NetApp.

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

5. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de sauvegarde effectuée sur la ressource, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

6. Vérifiez le résumé, puis cliquez sur **Terminer**.

La page topologie de la base de données s'affiche.

7. Cliquez sur **Sauvegarder maintenant**.

8. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

9. Contrôlez la progression de la sauvegarde en double-cliquant sur le travail dans le volet activité au bas de la page pour afficher la page Détails du travail.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

Pour plus d'informations, voir : ["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer.

Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, la commande `do_start method` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante :  
`Java -jar -Xmx8192M -Xms4096M`

## Applets de commande PowerShell

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

## 2. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.

Cet exemple crée une nouvelle stratégie de sauvegarde avec un type de sauvegarde Exchange de sauvegarde complète et de sauvegarde des journaux :

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

Cet exemple crée une nouvelle stratégie de sauvegarde avec un type de sauvegarde Exchange de sauvegarde complète et de sauvegarde des journaux toutes les heures :

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

Cet exemple crée une nouvelle stratégie de sauvegarde pour sauvegarder uniquement les journaux Exchange :

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

## 3. Découvrez les ressources hôte à l'aide de l'applet de commande Get-SmResources.

Cet exemple recherche les ressources du plug-in Microsoft Exchange Server sur l'hôte spécifié :

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

## 4. Ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.

Cet exemple crée un nouveau groupe de ressources de sauvegarde de la base de données Exchange Server avec la stratégie et les ressources spécifiées :

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Lo
g_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange
Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-
w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

Cet exemple crée un nouveau groupe de ressources de sauvegarde DAG (Exchange Database Availability Group) avec la stratégie et les ressources spécifiées :

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Lo
g_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet `New-SmBackup`.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

Dans cet exemple, une nouvelle sauvegarde est créée sur un système de stockage secondaire :

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Affichez l'état de la tâche de sauvegarde à l'aide de l'applet de commande `Get-SmBackupReport`.

Cet exemple affiche un rapport récapitulatif de tous les travaux exécutés à la date spécifiée :

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Cet exemple affiche un rapport récapitulatif des travaux pour un ID de travail spécifique :

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également consulter la section ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegardez les groupes de ressources Exchange

Un groupe de ressources est un ensemble de ressources sur un hôte ou un DAG Exchange, et le groupe de ressources peut inclure un DAG entier ou des bases de données individuelles. Vous pouvez sauvegarder les groupes de ressources à partir de la page Ressources.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Vous devez avoir attribué l'agrégat utilisé par l'opération de sauvegarde à la machine virtuelle de stockage (SVM) utilisée par la base de données.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un stockage secondaire, le rôle attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.
- Si un groupe de ressources possède plusieurs bases de données provenant de différents hôtes, l'opération de sauvegarde sur certains hôtes peut démarrer en retard en raison de problèmes de réseau. Vous devez configurer la valeur de `MaxRetryForUninitializedHosts` dans `web.config` à l'aide du `Set-SmConfigSettings Cmdlet PowerShell`.
- Dans un groupe de ressources, si vous incluez une base de données ou un groupe de disponibilité de base de données qui dispose d'une copie de base de données active/passive sur un stockage NetApp et non-NetApp, et que vous avez sélectionné **Sauvegarder les copies actives** ou **Sauvegarder les copies sur serveurs à sélectionner lors de la création des tâches de sauvegarde** dans la règle, les tâches de sauvegarde passent alors en état d'avertissement.

La sauvegarde réussira si la copie de base de données active/passive sur le stockage NetApp. La sauvegarde échouera pour la copie de base de données active/passive sur un système de stockage non NetApp.

### Description de la tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in **Microsoft Exchange Server** dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en cliquant sur \* \*, puis en  sélectionnant la balise. Vous pouvez alors cliquer sur \*  pour fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis cliquez sur **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de

sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

b. Cliquez sur **Backup**.

5. Contrôlez la progression de la sauvegarde en double-cliquant sur le travail dans le volet activité au bas de la page pour afficher la page Détails du travail.

## Surveiller les opérations de sauvegarde

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Surveiller les opérations dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s’affiche également lorsque l’opération a été lancée et que l’état de l’opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l’une des opérations, les détails de l’opération sont répertoriés dans la page **Détails du travail**.

## Annuler les opérations de sauvegarde pour la base de données Exchange

Vous pouvez annuler les opérations de sauvegarde mises en file d’attente.

### Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu’administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d’exécution.
- Vous pouvez utiliser l’interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d’autres objets membres** dans la page utilisateurs\groupes lors de la création d’un rôle, vous pouvez annuler les opérations de sauvegarde en file d’attente d’autres membres tout en utilisant ce rôle.

### Étapes

1. Effectuez l’une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>a. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>b. Sélectionnez l’opération, puis cliquez sur <b>Annuler le travail</b>.</li></ol>

Du...	Action
Volet activité	<ol style="list-style-type: none"> <li>Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>Sélectionner l'opération.</li> <li>Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Afficher les sauvegardes Exchange sur la page topologie

Lorsque vous préparez à sauvegarder une ressource, il est parfois utile d'afficher une représentation graphique de toutes les sauvegardes des stockages primaire et secondaire.

### Description de la tâche

Dans la page topologie, vous pouvez voir toutes les sauvegardes disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes, puis les sélectionner pour effectuer des opérations de protection des données.

Vous pouvez consulter l'icône suivante dans la vue gérer les copies pour déterminer si les sauvegardes sont disponibles sur le stockage principal ou secondaire (copies miroir ou copies Vault).

-  affiche le nombre de sauvegardes disponibles sur le stockage principal.
-  Affiche le nombre de sauvegardes mises en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
-  Affiche le nombre de sauvegardes répliquées sur le système de stockage secondaire à l'aide de la technologie SnapVault.

- Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire.

Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.

**Meilleure pratique** : pour vous assurer que le nombre correct de sauvegardes répliquées est affiché, nous vous recommandons d'actualiser la topologie.

Si vous utilisez une relation secondaire comme SnapMirror actif Sync (initialement commercialisé sous la forme SnapMirror Business Continuity [SM-BC]), les icônes supplémentaires suivantes s'affichent :

-



Le site de réplica est en cours.



Le site de réplica est en panne.



La relation miroir ou coffre-fort secondaire n'a pas été rétablie.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la base de données, la ressource ou le groupe de ressources dans la liste déroulante **View**.
3. Sélectionnez la ressource dans la vue Détails de la base de données ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologie de la ressource sélectionnée s'affiche.

4. Consultez la section « Récapitulatif » pour afficher un récapitulatif du nombre de sauvegardes disponibles sur les stockages primaire et secondaire.

La section carte récapitulative affiche le nombre total de sauvegardes et le nombre total de sauvegardes de journaux.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Pour la synchronisation active SnapMirror, cliquez sur le bouton **Refresh** pour actualiser l'inventaire des sauvegardes SnapCenter en interrogeant ONTAP sur les sites principaux et de réplica. Une planification hebdomadaire effectue également cette activité pour toutes les bases de données contenant une relation de synchronisation active SnapMirror.

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations SnapMirror miroir asynchrone ou MirrorVault asynchrone vers la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir de ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.After failover.
  - Après le basculement, une sauvegarde doit être créée afin que SnapCenter puisse prendre connaissance du basculement. Vous ne pouvez cliquer sur **Rafraîchir** qu'après la création d'une sauvegarde.
5. Dans la vue gérer les copies, cliquez sur **sauvegardes** dans le stockage principal ou secondaire pour afficher les détails d'une sauvegarde.

Les détails des sauvegardes s'affichent sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour

effectuer des opérations de restauration, de renommage et de suppression.



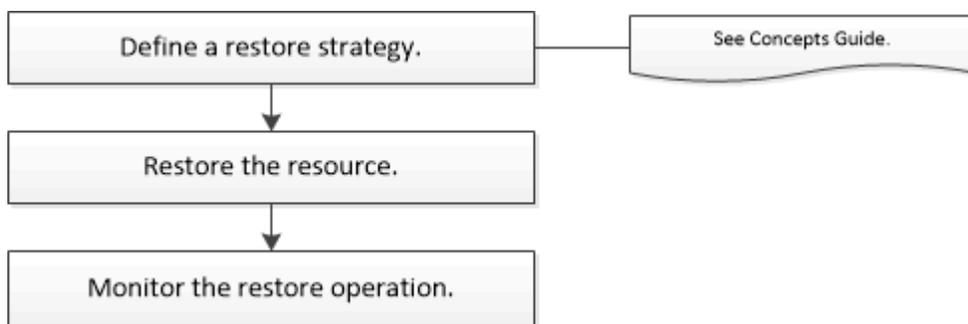
Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire. La suppression des snapshots est gérée par les paramètres de conservation ONTAP.

## Restaurer les ressources Exchange

### Restaurer le flux de travail

Vous pouvez utiliser SnapCenter pour restaurer les bases de données Exchange en restaurant une ou plusieurs sauvegardes sur votre système de fichiers actif.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer les opérations de restauration de la base de données Exchange :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde et de restauration. Pour plus d'informations sur les applets de commande PowerShell, consultez l'aide du cmdlet SnapCenter ou consultez le "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

### Conditions requises pour la restauration d'une base de données Exchange

Avant de restaurer une base de données Exchange Server à partir d'un plug-in SnapCenter pour sauvegarde Microsoft Exchange Server, vous devez vous assurer que plusieurs conditions sont respectées.



Pour utiliser complètement la fonctionnalité de restauration, vous devez mettre à niveau SnapCenter Server et le plug-in SnapCenter pour base de données Exchange vers la version 4.6.

- Le serveur Exchange doit être en ligne et en cours d'exécution avant de pouvoir restaurer une base de données.
- Les bases de données doivent exister sur le serveur Exchange.



La restauration des bases de données supprimées n'est pas prise en charge.

- Les planifications SnapCenter pour la base de données doivent être suspendues.
- Le serveur SnapCenter et le plug-in SnapCenter pour l'hôte Microsoft Exchange Server doivent être

connectés au stockage principal et secondaire contenant les sauvegardes que vous souhaitez restaurer.

## Restaurer les bases de données Exchange

Vous pouvez utiliser SnapCenter pour restaurer des bases de données Exchange sauvegardées.

### Avant de commencer

- Vous devez avoir sauvegardé les groupes de ressources, la base de données ou les groupes de disponibilité de base de données (DAG).
- Lorsque la base de données Exchange est migrée vers un autre emplacement, l'opération de restauration ne fonctionne pas pour les anciennes sauvegardes.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir attribué les SVM pour les volumes source et de destination.
- Dans un DAG, si une copie active de la base de données se trouve sur un stockage non NetApp et que vous souhaitez restaurer à partir de la sauvegarde passive de copie de base de données sur un stockage NetApp, faire la copie passive (stockage NetApp) comme copie active, actualiser les ressources et exécuter l'opération de restauration.

Exécutez le `Move-ActiveMailboxDatabase` commande pour faire de la copie passive de la base de données une copie active de la base de données.

Le "[Documentation Microsoft](#)" contient des informations sur cette commande.

### Description de la tâche

- Lorsque l'opération de restauration est effectuée sur une base de données, la base de données est remontée sur le même hôte et aucun nouveau volume n'est créé.
- Les sauvegardes de niveau DAG doivent être restaurées à partir de bases de données individuelles.
- La restauration complète du disque n'est pas prise en charge lorsque des fichiers autres que le fichier de base de données Exchange (.edb) existent.

Le plug-in pour Exchange n'effectue pas de restauration complète sur un disque si celui-ci contient des fichiers Exchange tels que ceux utilisés pour la réplication. Lorsqu'une restauration complète peut avoir un impact sur les fonctionnalités d'Exchange, le plug-in pour Exchange effectue une seule opération de restauration de fichiers.

- Le plug-in pour Exchange ne peut pas restaurer les disques cryptés BitLocker.
- Le `CHEMIN_SCRIPTS` est défini à l'aide de la clé pré-défini `WindowsScriptsDirectory` située dans le fichier `SMCoreServiceHost.exe.Config` de l'hôte du plug-in.

Si nécessaire, vous pouvez modifier ce chemin et redémarrer le service `SMcore`. Il est recommandé d'utiliser le chemin par défaut pour la sécurité.

La valeur de la clé peut être affichée à partir de Swagger via l'API : `API /4.7/configsettings`

Vous pouvez utiliser L'API GET pour afficher la valeur de la clé. L'API DÉFINIE n'est pas prise en charge.

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources** dans le coin supérieur gauche de la page ressource.
2. Sélectionnez le plug-in Exchange Server dans la liste déroulante.
3. Dans la page Ressources, sélectionnez **Database** dans la liste vue.
4. Sélectionnez la base de données dans la liste.
5. Dans la vue gestion des copies, sélectionnez **backups** dans la table sauvegardes primaires, puis cliquez sur .
6. Dans la page Options, sélectionnez l'une des options de sauvegarde des journaux suivantes :

Option	Description
Toutes les sauvegardes de journaux	Choisissez <b>toutes les sauvegardes de journaux</b> pour effectuer une opération de restauration de sauvegarde à la minute afin de restaurer toutes les sauvegardes de journaux disponibles après la sauvegarde complète.
En journaliser les sauvegardes jusqu'à	Choisissez <b>par sauvegardes de journaux jusqu'à</b> pour effectuer une opération de restauration ponctuelle, qui restaure la base de données en fonction des sauvegardes de journaux jusqu'au journal sélectionné.  <div style="border: 1px solid #ccc; padding: 10px;"><p>Le nombre de journaux affichés dans la liste déroulante est basé sur UTM. Par exemple, si la conservation complète des sauvegardes est 5 et que la conservation UTM est 3, le nombre de sauvegardes de journaux disponibles est 5, mais dans la liste déroulante, seulement 3 journaux sont répertoriés pour effectuer l'opération de restauration.</p></div>
Par date spécifique jusqu'à	Choisissez <b>par date spécifique jusqu'à</b> pour spécifier la date et l'heure auxquelles les journaux de transactions sont appliqués à la base de données restaurée. Cette opération de restauration ponctuelle restaure les entrées du journal de transactions enregistrées jusqu'à la dernière sauvegarde à la date et à l'heure spécifiées.

Option	Description
Aucune	Choisissez <b>aucun</b> si vous devez restaurer uniquement la sauvegarde complète sans sauvegarde de journaux.

Vous pouvez effectuer l'une des opérations suivantes :

- **Récupérer et monter la base de données après la restauration** - cette option est sélectionnée par défaut.
- **Ne pas vérifier l'intégrité des journaux de transactions dans la sauvegarde avant restauration** - par défaut, SnapCenter vérifie l'intégrité des journaux de transactions dans une sauvegarde avant d'effectuer une opération de restauration.

**Meilleure pratique:** vous ne devez pas sélectionner cette option.

7. Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript qui doivent être exécutés avant ou après l'opération de restauration, respectivement.

Les arguments de restauration du prescripteur incluent \$Database et \$Serverinstance.

Les arguments Restore PostScript incluent \$Database, \$ServerInstance, \$BackupName, \$logDirectory et \$TargetServerInstance.

Vous pouvez exécuter un script pour mettre à jour les interruptions SNMP, automatiser les alertes, envoyer des journaux, etc.



Le chemin prescripteurs ou postscripts ne doit pas inclure de disques ou de partages. Le chemin doit être relatif au CHEMIN\_SCRIPTS.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

10. Vous pouvez afficher l'état du travail de restauration en développant le panneau activité au bas de la page.

Vous devez contrôler le processus de restauration à l'aide de la page **moniteur > travaux**.

Lorsque vous restaurez une base de données active à partir d'une sauvegarde, la base de données passive peut passer à l'état suspendu ou en échec s'il y a un décalage entre la réplique et la base de données active.

Le changement d'état peut se produire lorsque la chaîne de logs de la base de données active va et commence une nouvelle branche qui rompt la réplification. Exchange Server tente de corriger le réplica, mais s'il ne parvient pas à le faire, après la restauration, vous devez créer une nouvelle sauvegarde, puis réamorcer le réplica.

### Applets de commande PowerShell

## Étapes

1. Démarrez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié en utilisant le `Open-SmConnection` applet de commande.

```
Open-smconnection -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

2. Récupérez les informations relatives à une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide de la `Get-SmBackup` applet de commande.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup

BackupId BackupName
BackupTime BackupType

341 ResourceGroup_36304978_UTM...
12/8/2017 4:13:24 PM Full Backup
342 ResourceGroup_36304978_UTM...
12/8/2017 4:16:23 PM Full Backup
355 ResourceGroup_06140588_UTM...
12/8/2017 6:32:36 PM Log Backup
356 ResourceGroup_06140588_UTM...
12/8/2017 6:36:20 PM Full Backup
```

3. Restaurez les données à partir de la sauvegarde à l'aide du `Restore-SmBackup` applet de commande.

Cet exemple restaure une sauvegarde en moins d'une minute :

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

Cet exemple restaure une sauvegarde instantanée :

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

Cet exemple restaure une sauvegarde sur un système de stockage secondaire dans l'histoire principale :

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'
-BackupId 81 -IsRecoverMount:$true -Confirm:$false
-archive @{Primary="paw_vs:voll";Secondary="paw_vs:voll_mirror"}
-logrestoretype All
```

Le `-archive` paramètre vous permet de spécifier les volumes primaire et secondaire que vous souhaitez utiliser pour la restauration.

Le `-IsRecoverMount:$true` paramètre vous permet de monter la base de données après la restauration.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Restauration granulaire des e-mails et des boîtes aux lettres

Le logiciel Single Mailbox Recovery (SMBR) vous permet de restaurer et de récupérer des messages ou des boîtes aux lettres à la place de la base de données Exchange complète.

La restauration d'une base de données complète simplement pour restaurer un courrier spécifique prendra beaucoup de temps et de ressources. SMBR permet de restaurer rapidement les courriers électroniques en créant une copie clone du Snapshot, puis en utilisant des API Microsoft pour monter la boîte aux lettres dans SMBR. Pour plus d'informations sur l'utilisation de SMBR, consultez "[Guide d'administration de SMBR](#)".

Pour plus d'informations sur SMBR, reportez-vous aux documents suivants :

- "[Restauration manuelle d'un élément unique avec SMBR \(également applicable pour les restaurations Ontrack Power Control\)](#)"
- "[Comment restaurer à partir d'un stockage secondaire dans SMBR avec SnapCenter](#)"
- "[Restauration de Microsoft Exchange Mail à partir de SnapVault à l'aide de SMBR](#)"

## Restaurer une base de données Exchange Server à partir du stockage secondaire

Vous pouvez restaurer une base de données Exchange Server sauvegardée à partir du stockage secondaire (miroir ou coffre-fort).

Vous devez avoir répliqué les snapshots du stockage primaire vers un stockage secondaire.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez **le plug-in Microsoft Exchange Server** dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste déroulante **View**.
3. Sélectionnez la base de données ou le groupe de ressources.

La page topologie de la base de données ou du groupe de ressources s'affiche.

4. Dans la section gérer les copies, sélectionnez **sauvegardes** dans le système de stockage secondaire (miroir ou coffre-fort).
5. Sélectionnez la sauvegarde dans la liste, puis cliquez sur .
6. Dans la page emplacement, choisissez le volume de destination pour restaurer la ressource sélectionnée.
7. Terminez l'assistant Restaurer, vérifiez le résumé, puis cliquez sur **Terminer**.

## Réamorçage d'un réplica de nœud Exchange passif

Si vous devez réamorcer une copie de réplica, par exemple lorsqu'une copie est corrompue, vous pouvez réamorcer la dernière sauvegarde à l'aide de la fonction de réamorçage dans SnapCenter.

### Avant de commencer

Vous devez avoir créé une sauvegarde de la base de données à réamorçage.

+ pour éviter de prendre du retard entre les nœuds, vous pouvez soit créer une nouvelle sauvegarde avant d'effectuer une opération de réamorçage, soit choisir l'hôte avec la dernière sauvegarde.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez **le plug-in Microsoft Exchange Server** dans la liste.
2. Sur la page Ressources, sélectionnez l'option appropriée dans la liste Afficher :

Option	Description
Pour réamorcer une seule base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour réamorcer les bases de données dans un DAG	Sélectionnez <b>Database Availability Group</b> dans la liste View.

3. Sélectionnez la ressource à réamorçage.
4. Dans la page gérer les copies, cliquez sur **Reseed**.
5. Dans la liste des copies de bases de données malsaines de l'assistant de réamorçage, sélectionnez celle que vous voulez réamorcer, puis cliquez sur **Suivant**.
6. Dans la fenêtre hôte, sélectionnez l'hôte avec la sauvegarde à partir de laquelle vous souhaitez réamorcer, puis cliquez sur **Suivant**.
7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.
9. Vous pouvez afficher l'état du travail en développant le panneau activité au bas de la page.



L'opération de réamorçage n'est pas prise en charge si la copie passive de la base de données réside sur une solution de stockage non NetApp.

## Réamorçage d'une réplique à l'aide des applets de commande PowerShell pour la base de données Exchange

Vous pouvez utiliser les applets de commande PowerShell pour restaurer une réplique défectueuse en utilisant la copie la plus récente sur le même hôte ou la copie la plus récente depuis un autre hôte.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Démarrez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié en utilisant le `Open-SmConnection` applet de commande.

```
Open-smconnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. Réamorçage de la base de données à l'aide du `reseed-SmDagReplicaCopy` applet de commande.

Cet exemple replace la copie échouée de la base de données appelée `execdb` sur l'hôte "mva-rx200.netapp.com" en utilisant la dernière sauvegarde sur cet hôte.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

Cet exemple replace la copie échouée de la base de données appelée `execdb` en utilisant la dernière sauvegarde de la base de données (production/copie) sur un autre hôte "mva-rx201.netapp.com."

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

## Surveiller les opérations de restauration

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

## Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Annuler les opérations de restauration de la base de données Exchange

Vous pouvez annuler les travaux de restauration mis en file d'attente.

Vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire de tâche pour annuler les opérations de restauration.

## Description de la tâche

- Vous pouvez annuler une opération de restauration en file d'attente à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de restauration en cours.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes de l'interface de ligne de commande pour annuler les opérations de restauration en attente.
- Le bouton **Annuler tâche** est désactivé pour les opérations de restauration qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets**

**membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de restauration en file d'attente d'autres membres tout en utilisant ce rôle.

### Étape

Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>1. Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>2. Sélectionnez le travail et cliquez sur <b>Annuler le travail</b>.</li></ol>
Volet activité	<ol style="list-style-type: none"><li>1. Après avoir lancé l'opération de restauration, cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.</li><li>2. Sélectionner l'opération.</li><li>3. Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li></ol>

# Protégez IBM DB2

## Plug-in SnapCenter pour IBM DB2

### Présentation du plug-in SnapCenter pour IBM DB2

Le plug-in SnapCenter pour IBM DB2 Database est un composant côté hôte du logiciel NetApp SnapCenter qui permet la gestion de la protection des données orientée applications des bases de données IBM DB2. Le plug-in pour IBM DB2 Database automatise la sauvegarde, la restauration et le clonage des bases de données IBM DB2 dans votre environnement SnapCenter.

- SnapCenter 6.0 prend en charge IBM DB2 10.5 et versions ultérieures.
- SnapCenter 6.0.1 prend en charge IBM DB2 9.7.x et versions ultérieures. De plus, à partir de SnapCenter 6.0.1, IBM DB2 sous AIX est pris en charge.

SnapCenter prend en charge les configurations DB2 à instance unique et à instances multiples. Vous pouvez utiliser le plug-in pour IBM DB2 Database dans les environnements Linux et Windows. Dans les environnements Windows, DB2 sera pris en charge en tant que ressource manuelle.



L'environnement DB2 pureScale et les systèmes DB2 multinoeuds (DPF) ne sont pas pris en charge.

Lorsque le plug-in pour IBM DB2 Database est installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies miroir des jeux de sauvegarde sur un autre volume. Vous pouvez également utiliser le plug-in doté de la technologie SnapVault de NetApp pour effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes.

Le plug-in SnapCenter pour DB2 prend en charge NFS et SAN sur les infrastructures de stockage de fichiers ONTAP et Azure NetApp.

L'organisation du stockage virtuel VMDK, vVol et RDM est prise en charge.

### Ce que vous pouvez faire avec le plug-in SnapCenter pour IBM DB2

Lorsque vous installez le plug-in pour IBM DB2 Database dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner les bases de données IBM DB2 et leurs ressources. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Ajouter des bases de données.
- Création de sauvegardes.
- Effectuez des restaurations à partir des sauvegardes.
- Sauvegardes clones.
- Planifiez les opérations de sauvegarde.
- Contrôle des opérations de sauvegarde, de restauration et de clonage
- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.

## Plug-in SnapCenter pour fonctionnalités IBM DB2

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour utiliser le plug-in pour IBM DB2 Database, vous utilisez l'interface utilisateur graphique de SnapCenter.

- **Interface utilisateur graphique unifiée**

L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

Vous pouvez planifier des opérations de sauvegarde, configurer la conservation des sauvegardes basée sur des règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie de copie snapshot NetApp non disruptive**

SnapCenter utilise la technologie de snapshot NetApp avec le plug-in pour IBM DB2 Database pour sauvegarder les ressources.

L'utilisation du plug-in pour IBM DB2 offre également les avantages suivants :

- Prise en charge des workflows de sauvegarde, de restauration et de clonage
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Création de copies compactes et ponctuelles de ressources à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonctionnalité de snapshot de groupe de cohérence (CG) de ONTAP dans le cadre de la création des sauvegardes.
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

En une seule opération, les snapshots sont consolidés lorsque les ressources d'un hôte unique partagent le même volume.

- Possibilité de créer des instantanés à l'aide de commandes externes.
- Prise en charge de Linux LVM sur le système de fichiers XFS.

## Types de stockage pris en charge par le plug-in SnapCenter pour IBM DB2

SnapCenter prend en charge de nombreux types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier le support de votre type de stockage avant d'installer le

## plug-in SnapCenter pour IBM DB2.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"><li>• LUN connectés via FC</li><li>• LUN connectées à l'iSCSI</li><li>• Volumes connectés par NFS</li></ul>
VMware ESXi	<ul style="list-style-type: none"><li>• L'exécution des LUN RDM connectés par un HBA FC ou iSCSI ESXi peut prendre du temps car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte.</li></ul> <p>Vous pouvez modifier le fichier <b>LinuxConfig.pm</b> situé à <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> à 1 pour analyser uniquement les HBA répertoriés dans les NOMS de PILOTE HBA.</p> <ul style="list-style-type: none"><li>• LUN iSCSI connectés directement au système invité par l'initiateur iSCSI</li><li>• VMDK sur des datastores NFS</li><li>• VMDK sur VMFS créés</li><li>• Volumes NFS connectés directement au système invité</li><li>• Datastores vVol sur NFS et SAN</li></ul> <p>Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>

## Privilèges ONTAP minimum requis pour le plug-in IBM DB2

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - la création de lun
  - la création de lun

- suppression de la lun
- lun igroup add
- créez un groupe initiateur lun
- suppression du groupe initiateur lun
- renommer la lun igroup
- renommer la lun igroup
- affichage de la lun igroup
- lun mapping des nœuds supplémentaires
- création d'un mappage de lun
- suppression du mappage de lun
- mappage de lun supprimer-rapports-nœuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- suppression de la réservation persistante de lun
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes

- création d'un clone de fichiers de volumes
- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- volume snapshot modify-snaplock-expiration-time
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau

- interface réseau affiche
- un vservers

## Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour IBM DB2

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire > miroir > coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le ["Documentation ONTAP"](#).

## Stratégie de sauvegarde pour IBM DB2

### Définir une stratégie de sauvegarde pour IBM DB2

Définir une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous aide à disposer des sauvegardes dont vous avez besoin pour restaurer ou cloner vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

#### Description de la tâche

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

#### Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.
2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décidez si vous souhaitez créer une règle basée sur les copies Snapshot pour sauvegarder des copies Snapshot cohérentes au niveau des applications de la base de données.
5. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
6. Déterminer la période de conservation des snapshots sur le système de stockage source et la destination SnapMirror.
7. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescripteur ou un PostScript.

### **Découverte automatique des ressources sur l'hôte Linux**

Les ressources sont des bases de données et des instances IBM DB2 sur l'hôte Linux qui sont gérées par SnapCenter. Après avoir installé le plug-in SnapCenter pour IBM DB2, les bases de données IBM DB2 de toutes les instances de cet hôte Linux sont automatiquement découvertes et affichées dans la page Ressources.

### **Types de sauvegardes pris en charge**

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge le type de sauvegarde snapshot basé sur la copie pour les bases de données IBM DB2.

### **Sauvegarde basée sur des copies Snapshot**

Les sauvegardes basées sur des copies Snapshot s'appuient sur la technologie snapshot de NetApp pour créer des copies en ligne en lecture seule des volumes sur lesquels résident les bases de données IBM DB2.

### **Comment le plug-in SnapCenter pour IBM DB2 utilise les snapshots de groupes de cohérence**

Vous pouvez utiliser le plug-in pour créer des snapshots de groupes de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes, de sorte que vous puissiez les gérer comme une entité unique. Un groupe de cohérence est une copie instantanée de plusieurs volumes, fournissant ainsi des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente nécessaire au contrôleur de stockage pour regrouper les snapshots de manière cohérente. Les options de temps d'attente disponibles sont **urgent**, **Moyen** et **détendu**. Vous pouvez également activer ou désactiver la synchronisation WAFL (Write Anywhere File Layout) lors d'une opération de snapshot de groupe cohérente. WAFL Sync améliore les performances d'un snapshot de groupe de cohérence.

### **Comment SnapCenter gère la gestion de la gestion des sauvegardes de données**

SnapCenter gère la gestion des sauvegardes de données au niveau du système de stockage et du système de fichiers.

Les snapshots du stockage primaire ou secondaire et leurs entrées correspondantes dans le catalogue IBM DB2 sont supprimés en fonction des paramètres de rétention.

### **Considérations relatives à la détermination des plannings de sauvegarde pour IBM DB2**

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes (fréquence des sauvegardes)

La fréquence de sauvegarde, également appelée type de planification pour certains plug-ins, fait partie d'une configuration de règles. Par exemple, vous pouvez configurer la fréquence des sauvegardes sous forme horaire, quotidienne, hebdomadaire ou mensuelle.

- Plannings de sauvegarde (exactement au moment où les sauvegardes doivent être effectuées)

Les planifications de sauvegarde font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour la sauvegarder tous les jeudis à 10 h 00

### **Nombre de tâches de sauvegarde nécessaires pour IBM DB2**

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

### **Conventions de dénomination des sauvegardes pour le plug-in pour les bases de données IBM DB2**

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.
- *03-12-2015\_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, `clienttext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

## Stratégie de restauration et de récupération pour IBM DB2

### Définir une stratégie de restauration et de récupération pour les ressources IBM DB2

Vous devez définir une stratégie avant de restaurer et de récupérer votre base de données pour que vous puissiez effectuer correctement les opérations de restauration et de récupération.



Seule la récupération manuelle de la base de données est prise en charge.

#### Étapes

1. Déterminez les stratégies de restauration prises en charge pour les ressources IBM DB2 ajoutées manuellement
2. Déterminez les stratégies de restauration prises en charge pour les bases de données IBM DB2 découvertes automatiquement

### Types de stratégies de restauration pris en charge pour les ressources IBM DB2 ajoutées manuellement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les ressources IBM DB2 ajoutées manuellement.



Vous ne pouvez pas récupérer les ressources IBM DB2 ajoutées manuellement.

#### Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

### Type de stratégie de restauration pris en charge pour IBM DB2 détecté automatiquement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter.

La restauration complète des ressources est la stratégie de restauration prise en charge pour les bases de

données IBM DB2 découvertes automatiquement. Cette opération restaure tous les volumes, qtree et LUN d'une ressource.

### Types d'opérations de restauration pour IBM DB2 détecté automatiquement

Le plug-in SnapCenter pour IBM DB2 prend en charge les types de restauration Single File SnapRestore et Connect-and-copy pour les bases de données IBM DB2 découvertes automatiquement.

Single File SnapRestore s'effectue dans des environnements NFS pour les scénarios suivants :

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde sélectionnée provient d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Complete Resource** est sélectionnée

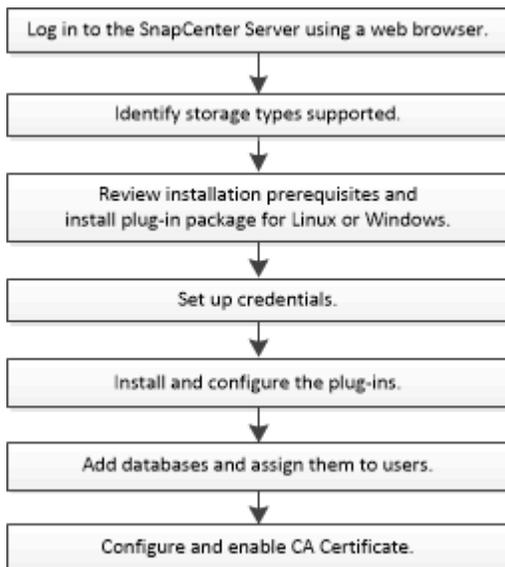
Single File SnapRestore s'effectue dans des environnements SAN pour les scénarios suivants :

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée depuis un emplacement secondaire SnapMirror ou SnapVault et l'option **Complete Resource** est sélectionnée

## Préparez l'installation du plug-in SnapCenter pour IBM DB2

### Workflow d'installation du plug-in SnapCenter pour IBM DB2

Vous devez installer et configurer le plug-in SnapCenter pour IBM DB2 si vous souhaitez protéger les bases de données IBM DB2.



### Conditions préalables à l'ajout d'hôtes et à l'installation du module Plug-ins pour Windows, Linux ou AIX

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises. Plug-in SnapCenter pour IBM DB2 pris en charge dans les

## environnements Windows, Linux et AIX.

- Vous devez avoir installé Java 11 sur votre hôte.



IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Pour Windows, le service de création de plug-in doit être exécuté à l'aide de l'utilisateur Windows « LocalSystem », qui est le comportement par défaut lorsque le plug-in pour IBM DB2 est installé en tant qu'administrateur de domaine.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in IBM DB2 sur les hôtes Windows.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte IBM DB2.

### Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour IBM DB2 sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Windows.

["Télécharger JAVA pour Windows"](#)

["Matrice d'interopérabilité NetApp"](#)

### Hôtes Linux et AIX

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

["Télécharger JAVA pour Linux"](#)

["Télécharger JAVA pour AIX"](#)

["Matrice d'interopérabilité NetApp"](#)

- Pour les bases de données IBM DB2 exécutées sur un hôte Linux, lors de l'installation de Plug-in pour IBM DB2, SnapCenter Plug-in pour UNIX est installé automatiquement.
- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

### Commandes supplémentaires

Pour exécuter une commande supplémentaire sur le plug-in SnapCenter pour IBM DB2, vous devez l'inclure dans le fichier *allowed\_commands.config*.

- Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*

- Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`

Pour autoriser des commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier `allowed_commands.config` dans un éditeur. Entrez chaque commande sur une ligne distincte et les commandes ne sont pas sensibles à la casse. Assurez-vous de spécifier le chemin d'accès complet et de le joindre entre guillemets (") s'il contient des espaces.

Par exemple :

commande : `mount`

commande : `umount`

Commande : « `C:\Program Files\NetApp\SnapCreator commands\sdcli.exe` »

commande : `myscript.bat`

Si le fichier `allowed_commands.config` n'est pas présent, les commandes ou l'exécution du script seront bloquées et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »

Si la commande ou le script n'est pas présent dans `allowed_commands.config`, l'exécution de la commande ou du script sera bloquée et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »



Vous ne devez pas utiliser de caractère générique (\*) pour autoriser toutes les commandes.

## Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux

SnapCenter permet à un utilisateur non root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/*LINUX\_USER*/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /Custom\_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom\_location/NetApp/snapcenter/spl/bin/spl

## Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`LINUX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte AIX

SnapCenter 4.4 et version ultérieure permet à un utilisateur non-root d'installer le module de plug-ins SnapCenter pour AIX et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.

- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

### À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- `/Home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/Custom_location/NetApp/snapcenter/spl/installation/plugins/désinstaller`
- `/Custom_location/NetApp/snapcenter/spl/bin/spl`

### Étapes

1. Connectez-vous à l'hôte AIX sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour AIX.
2. Ajoutez les lignes suivantes au fichier `/etc/sudoers` à l'aide de l'utilitaire visudo Linux.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`AIX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java et OpenJDK</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

## Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux

Avant d'installer le module de plug-ins SnapCenter pour Linux, vous devez connaître certains besoins en espace système hôte de base et en dimensionnement.

Élément	De formation
<p>Systemes d'exploitation</p>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>
<p>RAM minimale pour le plug-in SnapCenter sur l'hôte</p>	<p>1 GO</p>
<p>Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte</p>	<p>2 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
<p>Packs logiciels requis</p>	<p>Java 11 Oracle Java et OpenJDK</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>

## Configurez les informations d'identification du plug-in SnapCenter pour IBM DB2

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

### Description de la tâche

- Hôtes Linux

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

**Meilleure pratique:** bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>Administrateur de domaine ou tout membre du groupe d'administrateurs</li> </ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li><i>NetBIOS\username</i></li> <li><i>Domain FQDN\username</i></li> </ul> <ul style="list-style-type: none"> <li>Administrateur local (groupes de travail uniquement)</li> </ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p> <p>N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-right: 10px;"> <span style="font-size: 18px; font-weight: bold;">i</span> </div> <div> <p>Applicable uniquement aux utilisateurs Linux.</p> </div> </div>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

### Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

### Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediately
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

Par exemple :

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :
  - a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Installez le plug-in SnapCenter pour IBM DB2

### Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour un cluster.

#### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.

- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

["Configurez le compte de service géré de groupe sur Windows Server 2016 ou version ultérieure pour IBM DB2"](#)

### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez le type d'hôte :</p> <ul style="list-style-type: none"> <li>• Répertoires de base</li> <li>• Linux</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le plug-in pour IBM DB2 est installé sur l'hôte client IBM DB2 et cet hôte peut se trouver sur un système Windows ou Linux.</p> </div>
Nom d'hôte	<p>Entrez le nom d'hôte de communication. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p>

Pour ce champ...	Procédez comme ça...
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez fourni.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

Lorsque vous utilisez l'API REST pour installer Plug-in pour DB2, vous devez transmettre la version 3.0. Par exemple, DB2:3.0

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p> </div>

Pour ce champ...	Procédez comme ça...
Chemin d'installation	<p>Le plug-in pour IBM DB2 est installé sur l'hôte client IBM DB2 et cet hôte peut se trouver sur un système Windows ou Linux.</p> <ul style="list-style-type: none"> <li>• Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin.</li> <li>• Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.</li> </ul>
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	<p>Pour l'hôte Windows, cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Indiquez le nom GMSA au format suivant : domainname\accountName\$.</p> <p> GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.</p> </div>

7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les précontrôles, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, RAM, version de PowerShell, . La version NET, l'emplacement (pour les plug-ins Windows) et Java 11 (pour les plug-ins Windows et Linux) sont validés en fonction des exigences minimales. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse C:\Program Files\NetApp\SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l’empreinte de chacun des nœuds du cluster.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l’empreinte a été confirmée.

9. Surveillez la progression de l’installation.

- Pour le plug-in Windows, les journaux d’installation et de mise à niveau se trouvent à l’adresse suivante : `C:\Windows\SnapCenter plugin\Install<JOBID>\`
- Pour le plug-in Linux, les journaux d’installation se trouvent à l’adresse suivante : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log`. Les journaux de mise à niveau se trouvent à l’adresse : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log`

### Une fois que vous avez terminé

Si vous souhaitez effectuer une mise à niveau vers SnapCenter 6.0 ou une version ultérieure, le plug-in PERL existant pour DB2 sera désinstallé du serveur de plug-in distant.

### Installez les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes distants à l’aide d’applets de commande

Vous pouvez installer simultanément les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes à l’aide de l’applet de commande `Install-SmHostPackage` PowerShell.

#### Avant de commencer

Vous devez vous connecter à SnapCenter en tant qu’utilisateur de domaine disposant des droits d’administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

#### Étapes

1. Lancer PowerShell.
2. Sur l’hôte du serveur SnapCenter, établissez une session à l’aide de l’applet de commande `Open-SmConnection`, puis saisissez vos informations d’identification.
3. Installez le plug-in sur plusieurs hôtes à l’aide de l’applet de commande `Install-SmHostPackage` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l’applet de commande du logiciel SnapCenter"](#).

Vous pouvez utiliser l’option `-skipreccheck` lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l’hôte répond aux exigences d’installation du plug-in.

4. Saisissez vos informations d’identification pour l’installation à distance.

### Installez le plug-in SnapCenter pour IBM DB2 sur les hôtes Linux à l’aide de l’interface de ligne de commande

Vous devez installer le plug-in SnapCenter pour IBM DB2 Database à l’aide de l’interface utilisateur SnapCenter. Si votre environnement ne permet pas l’installation à distance du plug-in à partir de l’interface utilisateur SnapCenter, vous pouvez installer le plug-in pour

la base de données IBM DB2 en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

### Avant de commencer

- Vous devez installer le plug-in pour IBM DB2 Database sur chaque hôte Linux sur lequel réside le client IBM DB2.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour IBM DB2 Database doit répondre à la configuration logicielle, de base de données et de système d'exploitation.

La matrice d'interopérabilité (IMT) contient les dernières informations sur les configurations prises en charge.

#### "Matrice d'interopérabilité NetApp"

- Le plug-in SnapCenter pour IBM DB2 Database fait partie du module de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé SnapCenter sur un hôte Windows.

### Description de la tâche

Si les paramètres ne sont pas mentionnés, SnapCenter est installé avec les valeurs par défaut.

### Étapes

1. Copiez le fichier d'installation du pack de plug-ins SnapCenter pour Linux (snapcenter\_linux\_host\_plugin.bin) depuis C:\ProgramData\NetApp\SnapCenter\Package Repository vers l'hôte sur lequel vous souhaitez installer le plug-in pour IBM DB2.

Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in :

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server
```

  - -DPORT spécifie le port de communication SMCORE HTTPS.
  - -DSERVER\_IP spécifie l'adresse IP du serveur SnapCenter.
  - -DSERVER\_HTTPS\_PORT spécifie le port HTTPS du serveur SnapCenter.
  - -DUSER\_INSTALL\_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
  - DINSTALL\_LOG\_NAME indique le nom du fichier journal.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Modifiez le fichier /<installation directory>/NetApp/snapcenter/scc/etc/SC\_SMS\_Services.properties, puis ajoutez le paramètre PLUGINS\_ENABLED = DB2:3.0.

5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveillez l'état d'installation du plug-in pour IBM DB2

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité

de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

## Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

### Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

#### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :

- a. Double-cliquez sur le certificat.
- b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
- c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
- d. Copiez les caractères hexadécimaux de la zone.
- e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :

- a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

### Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

#### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte
Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Configurez le certificat CA pour le service de plug-ins IBM DB2 SnapCenter sur un hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier « keystore.jks », qui se trouve dans `/opt/NetApp/snapcenter/scc/etc` à la fois comme magasin de confiance et magasin de clés.

**Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation**

### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Procédez de même pour la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in : `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaires pour le plug-in trust-store.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Répertorier les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.

7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Si le nom d'alias du certificat de l'autorité de certification est
long et contient de l'espace ou des caractères spéciaux ("*", ",", "),
remplacez le nom d'alias par un nom simple :
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurez le nom d'alias à partir du certificat CA dans le fichier
agent.properties.
```

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in `trust-store`.

### Configurer la liste de révocation de certificats (CRL) pour les plug-ins

#### Description de la tâche

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est « `opt/NetApp/snapcenter/scc/etc/crl` ».

#### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `agent.properties` par rapport à la clé `CRL_PATH`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

### Configurez le certificat CA pour le service de plug-ins IBM DB2 SnapCenter sur un hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le

magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier *keystore.jks*, qui se trouve dans *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* à la fois comme magasin de confiance et magasin de clés.

**Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation**

### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé *KEYSTORE\_PASS*.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
```



Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks
```

Procédez de même pour la clé *KEYSTORE\_PASS* dans le fichier *agent.properties*.

4. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

### Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
Keytool -import -trucacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`
2. Localisez le fichier `keystore.jks`.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configurez le nom d'alias à partir du certificat CA dans le fichier `agent.properties`.

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

### Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

#### Description de la tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section ["Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter"](#).

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est 'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'.

## Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier *agent.properties* par rapport à la clé CRL\_PATH.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande run *set-SmCertificateSettings*.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de *get-SmCertificateSettings*.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

# Préparation à la protection des données

## Conditions préalables à l'utilisation du plug-in SnapCenter pour IBM DB2

Avant d'utiliser le plug-in SnapCenter pour IBM DB2, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches requises.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.
- Installez Java 11 sur votre hôte Linux ou Windows.

Vous devez définir le chemin Java dans la variable de chemin d'environnement de la machine hôte.

- Configurer SnapMirror et SnapVault pour la réplication de sauvegarde.

## Utilisation des ressources, des groupes de ressources et des stratégies pour protéger IBM DB2

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des bases de données IBM DB2 que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Les règles spécifient la fréquence des sauvegardes, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

Considérez un groupe de ressources comme définissant ce que vous voulez protéger et quand vous voulez le protéger en termes de jour et d'heure. Considérez une stratégie comme une définition de la façon dont vous voulez la protéger. Si vous sauvegardez toutes les bases de données, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources de manière à

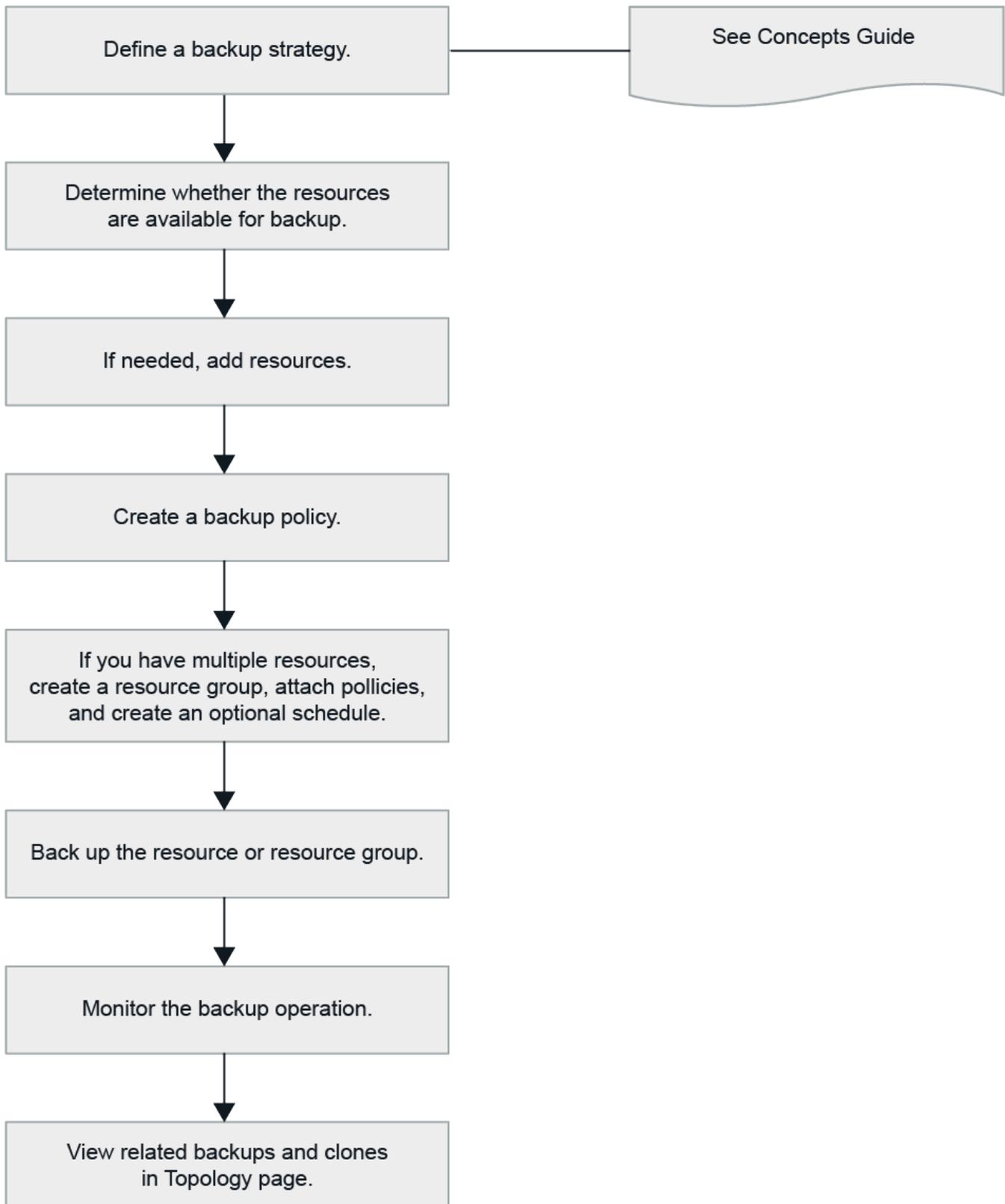
effectuer une sauvegarde complète tous les jours.

## **Sauvegarder les ressources IBM DB2**

### **Sauvegarder les ressources IBM DB2**

Vous pouvez créer une sauvegarde d'une ressource (base de données) ou d'un groupe de ressources. Le workflow de sauvegarde inclut la planification, l'identification des bases de données pour la sauvegarde, la gestion des stratégies de sauvegarde, la création de groupes de ressources et la connexion de stratégies, la création de sauvegardes et le contrôle des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent plus d'informations sur les applets de commande PowerShell. ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Découvrir les bases de données automatiquement

Les ressources sont des bases de données IBM DB2 gérées par SnapCenter sur l'hôte Linux. Vous pouvez ajouter les ressources aux groupes de ressources pour effectuer des opérations de protection des données après avoir découvert les bases de données IBM DB2 disponibles.

### Avant de commencer

- Vous devez avoir déjà effectué des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions du système de stockage.
- Le plug-in SnapCenter pour IBM DB2 ne prend pas en charge la découverte automatique des ressources résidant dans les environnements virtuels RDM/VMDK. Vous devez fournir les informations de stockage pour les environnements virtuels tout en ajoutant les bases de données manuellement.

### Description de la tâche

- Après avoir installé le plug-in, toutes les bases de données de cet hôte Linux sont automatiquement découvertes et affichées sur la page Ressources.
- Seules les bases de données sont découvertes automatiquement.

Les ressources détectées automatiquement ne peuvent pas être modifiées ou supprimées.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in pour IBM DB2 dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste vue.
3. (Facultatif) cliquez sur \* \* , puis sélectionnez le nom d'hôte.

Vous pouvez alors cliquer sur \* \*  pour fermer le volet de filtre.

4. Cliquez sur **Actualiser les ressources** pour découvrir les ressources disponibles sur l'hôte.

Les ressources s'affichent avec des informations telles que le type de ressource, le nom d'hôte, les groupes de ressources associés, le type de sauvegarde, les stratégies et l'état global.

- Si la base de données se trouve sur un système de stockage NetApp et qu'elle n'est pas protégée, elle s'affiche dans la colonne État global.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée, et si aucune opération de sauvegarde n'est effectuée, alors l'option sauvegarde non exécutée s'affiche dans la colonne État global. Dans le cas contraire, l'état passe en échec de la sauvegarde ou la sauvegarde a réussi en fonction de l'état de la dernière sauvegarde.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

## Ajoutez des ressources manuellement au plug-in hôte

La découverte automatique n'est pas prise en charge sur l'hôte Windows. Vous devez ajouter manuellement des instances DB2 et des ressources de base de données.

### Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions du système de stockage.

### Description de la tâche

La découverte manuelle n'est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in SnapCenter pour IBM DB2 dans la liste déroulante.
2. Dans la page Ressources, cliquez sur **Ajouter une ressource IBM DB2**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Spécifiez le nom de la base de données.
Nom d'hôte	Entrez le nom d'hôte.
Type	Sélectionnez une base de données ou une instance.
Fréquence	Spécifiez le nom de l'instance, qui est le parent de la base de données.
Informations d'identification	Sélectionnez les informations d'identification ou ajoutez-les.  Cette option est facultative.

4. Sur la page fournir l'empreinte du stockage, sélectionnez un type de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Enregistrer**.

Facultatif : vous pouvez cliquer sur l'icône \*  pour ajouter d'autres volumes, LUN et qtrees à partir d'autres systèmes de stockage.

5. Facultatif : dans la page Paramètres de ressources, pour les ressources sur l'hôte Windows, entrez des paires clé-valeur personnalisées pour le plug-in IBM DB2
6. Vérifiez le résumé, puis cliquez sur **Terminer**.

Les bases de données sont affichées avec des informations telles que le nom d'hôte, les groupes de ressources et les stratégies associés, ainsi que l'état global

Si vous souhaitez donner aux utilisateurs l'accès aux ressources, vous devez affecter ces ressources aux utilisateurs. Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

["Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources"](#)

Après avoir ajouté les bases de données, vous pouvez modifier les détails de la base de données IBM DB2.

## Créez des stratégies de sauvegarde pour IBM DB2

Avant d'utiliser SnapCenter pour sauvegarder des ressources IBM DB2, vous devez créer une stratégie de sauvegarde pour le groupe de ressources ou de ressources que vous souhaitez sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.

Pour plus de détails, reportez-vous aux informations sur la définition d'une stratégie de protection des données pour les bases de données IBM DB2.

- Vous devez vous préparer à la protection des données en effectuant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout de ressources.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir affecté des SVM aux volumes source et de destination.

En outre, vous pouvez spécifier des paramètres de réplication, de script et d'application dans la stratégie. Ces options vous permettent de gagner du temps lorsque vous souhaitez réutiliser la stratégie d'un autre groupe de ressources.

### Description de la tâche

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un plus grand nombre d'instantanés que le nombre spécifié dans la règle.
  - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez le type de stockage.
  - b. Dans la section **Paramètres de sauvegarde personnalisés**, indiquez tous les paramètres de sauvegarde spécifiques qui doivent être transmis au plug-in au format clé-valeur.

Vous pouvez fournir plusieurs valeurs de clé à transmettre au plug-in.

6. Dans la page instantané et réplication, effectuez les opérations suivantes.

a. Spécifiez la fréquence d'horaire en sélectionnant **sur demande, horaire, quotidien, hebdomadaire** ou **mensuel**.



Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais aussi d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

b. Dans la section Paramètres de l'instantané, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Alors...
Conserver un certain nombre de snapshots	Sélectionnez <b>copies à conserver</b> , puis indiquez le nombre d'instantanés que vous souhaitez conserver.  Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.
Conserver les instantanés pendant un certain nombre de jours	Sélectionnez <b>conserver les copies pour</b> , puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage des copies Snapshot principales	Si vous souhaitez spécifier la période de verrouillage des snapshots pour le stockage primaire, sélectionnez période de verrouillage des copies Snapshot et sélectionnez jours, mois ou années.  La période de conservation SnapLock doit être inférieure à 100 ans.
Période de verrouillage des snapshots secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.



Dans le cas des sauvegardes basées sur des copies Snapshot, vous devez définir le nombre de rétention à 2 ou plus si vous prévoyez d'activer la réplication SnapVault. Si vous définissez le nombre de rétention sur 1, l'opération de rétention risque d'échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.

c. Sélectionnez une étiquette Snapshot.

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

7. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
Mettez à jour SnapMirror après avoir créé une copie Snapshot locale	Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).  Cette option doit être activée pour la synchronisation active SnapMirror.
Mettez à jour SnapVault après avoir créé une copie Snapshot locale	Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).
Deuxième étiquette de police	Sélectionnez une étiquette Snapshot.  Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.   Si vous avez sélectionné <b>mettre à jour SnapMirror après la création d'une copie Snapshot locale</b> , vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné <b>mettre à jour SnapVault après la création d'une copie Snapshot locale</b> , vous devez spécifier l'étiquette de la stratégie secondaire.
Nombre de tentatives d'erreur	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer des groupes de ressources et attacher des stratégies

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.   Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.  Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

Pour ce champ...	Procédez comme ça...
Utilisez un format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.  Par exemple, clienttext_Resource group_policy_hostname ou Resource group_hostname. Par défaut, un horodatage est ajouté au nom du snapshot.

4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.

Cela aide à filtrer les informations affichées à l'écran.

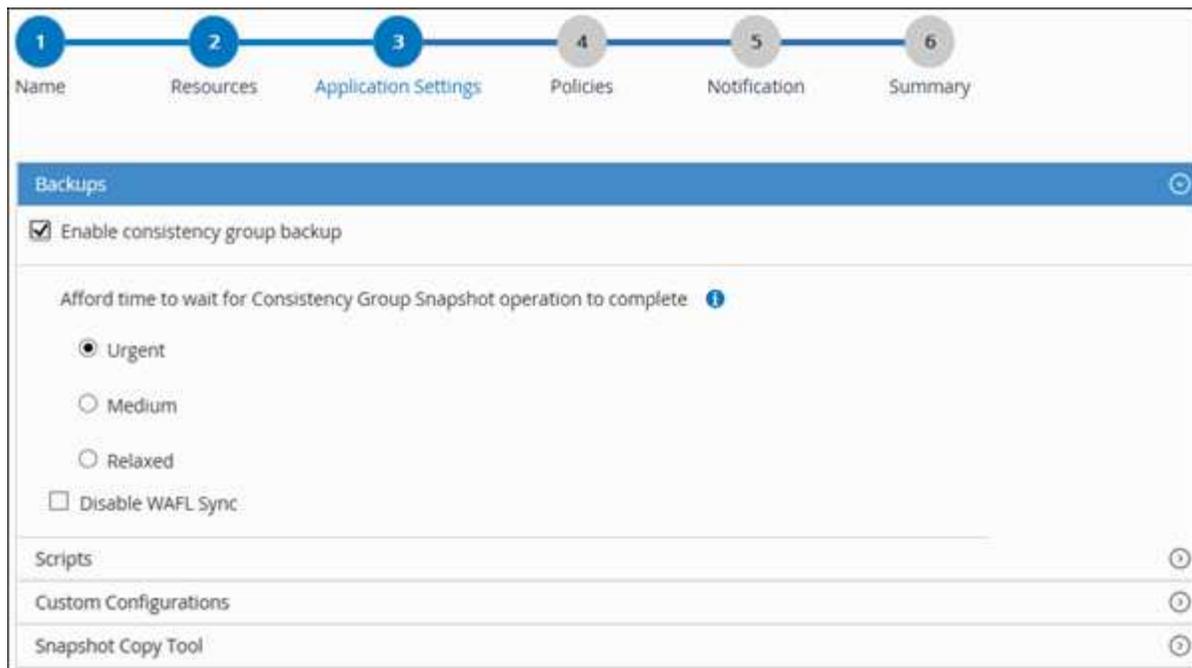
5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page Paramètres de l'application, procédez comme suit :

- a. Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde de groupe de cohérence et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Attendez la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , <b>Moyen</b> ou <b>relâché</b> pour spécifier le temps d'attente pour l'exécution de l'opération de snapshot.  Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

+



- a. Cliquez sur la flèche **scripts** et entrez les commandes pré et post pour les opérations quiesce, snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- b. Cliquez sur la flèche **configurations personnalisées** et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés.  Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.

Paramètre	Réglage	Description
ARCHIVE_LOG_EXT	extension_fichier	Spécifie la longueur d'extension du fichier journal d'archives.  Par exemple, si le journal d'archives est log_backup_0_0_0_0.161518551942 9 et si la valeur file_extension est 5, l'extension du journal conserve 5 chiffres, soit 16151.
ARCHIVE_LOG_RÉCURSIVE_SE ARCH	(O/N)	Permet la gestion des journaux d'archivage dans les sous-répertoires.  Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.



Les paires clé-valeur personnalisées sont prises en charge pour les systèmes de plug-in IBM DB2 Linux et non pour la base de données IBM DB2 enregistrée en tant que plug-in Windows centralisé.

c. Cliquez sur la flèche **Snapshot Copy Tool** pour sélectionner l'outil de création de snapshots :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et mettre le système de fichiers dans un état cohérent avant de créer un snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
SnapCenter pour créer un snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .
Pour saisir la commande à exécuter sur l'hôte afin de créer des copies Snapshot.	Sélectionnez <b>autre</b> , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.

7. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Les stratégies sont répertoriées dans la section Configuration des planifications pour les stratégies sélectionnées.

- b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.

Où, nom\_stratégie est le nom de la règle que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **programmes appliqués**.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Le serveur SMTP doit être configuré dans **Paramètres > Paramètres globaux**.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire des ressources IBM DB2 sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

a. Sélectionnez le type de la règle de réplication.



Règle de réplication synchrone non prise en charge.

b. Indiquez le suffixe du groupe de cohérence à utiliser.

c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.



Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

1. Sur la page Vérification, effectuez les opérations suivantes :

a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.

b.

Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.

c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.

e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell set-SmSmtServer.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour IBM DB2

Vous devez créer une connexion SVM et un identifiant avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner les bases de données IBM DB2.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

### Étapes

1. Cliquez sur **SnapCenterPS** pour lancer PowerShell Core.
2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-SmStorageConnection`.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande `Add-SmCredential`.

Cet exemple montre comment créer un nouvel identifiant nommé `FinanceAdmin` avec les informations d'identification Windows :

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux
-AuthenticationType PasswordBased -Credential db2hostuser
-EnableSudoPrivileges:$true
```

4. Ajoutez l'hôte de communication IBM DB2 au serveur SnapCenter.

Pour Linux :

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

Pour Windows :

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. Installez le package et le plug-in SnapCenter pour IBM DB2 sur l'hôte.

Pour Linux :

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2
```

Pour Windows :

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2, SCW
```

6. Définissez le chemin d'accès à SQLLIB.

Sous Windows, le plug-in DB2 utilise le chemin par défaut du dossier SQLLIB : « C:\Program Files\IBM\SQLLIB\BIN ».

Si vous souhaitez remplacer le chemin par défaut, utilisez la commande suivante.

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
{ "DB2_SQLLIB_CMD" = "<custom_path>\IBM\SQLLIB\BIN" }
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarde des bases de données DB2

La sauvegarde d'une base de données inclut l'établissement d'une connexion avec le serveur SnapCenter, l'ajout de ressources, l'ajout d'une stratégie, la création d'un groupe de ressources de sauvegarde et la sauvegarde.

### Avant de commencer

- Vous devez avoir créé une stratégie de sauvegarde.

- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.
- Pour l'opération de sauvegarde basée sur des copies Snapshot, vérifiez que toutes les bases de données des locataires sont valides et actives.
- Pour les commandes PRE et post pour les opérations quiesce, Snapshot et unquiesce, vous devez vérifier que les commandes existent dans la liste de commandes disponible sur l'hôte plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Sélectionnez , puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Sélectionnez la ressource à sauvegarder.
4. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page Paramètres de l'application, procédez comme suit :
  - Sélectionnez la flèche **backups** pour définir des options de sauvegarde supplémentaires :  
Activez la sauvegarde du groupe de cohérence, si nécessaire, et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Temps d'attente avant la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , ou <b>Moyen</b> , ou <b>détendu</b> pour spécifier le temps d'attente pour la fin de l'opération Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

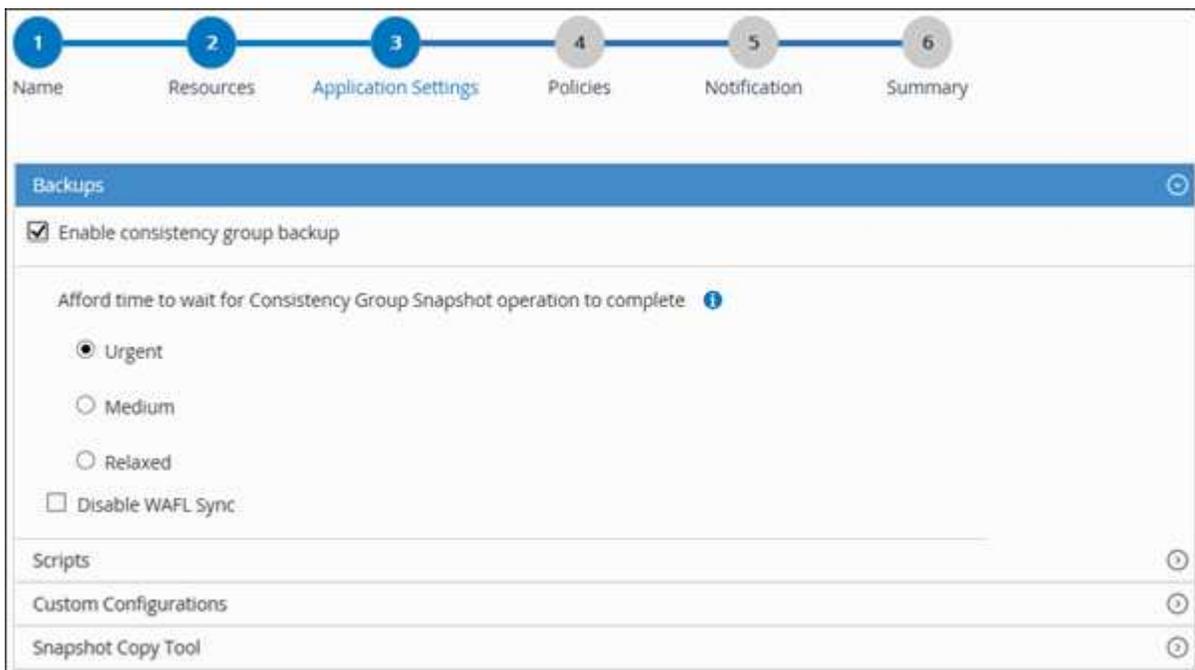
- Sélectionnez la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce.

Vous pouvez également exécuter des pré-commandes avant de quitter l'opération de sauvegarde. Des préscripts et des postscripts sont exécutés sur le serveur SnapCenter.

- Sélectionnez la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- Sélectionner la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows afin de mettre le système de fichiers dans un état cohérent, puis de créer un Snapshot	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
Pour saisir la commande permettant de créer un Snapshot	Sélectionnez <b>autre</b> , puis entrez la commande pour créer un instantané.



6. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Sélectionnez  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres > Paramètres globaux**.

8. Passez en revue le résumé, puis sélectionnez **Terminer**.

La page topologie des ressources s'affiche.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

Pour plus d'informations, voir : ["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)

## Applets de commande PowerShell

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-SmConnection
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Ajoutez des ressources manuelles à l'aide de l'applet de commande Add-SmResources.

Cet exemple montre comment ajouter une instance IBM DB2 :

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

Pour DB2 Database :

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.
4. Protégez la ressource ou ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.
5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet New-SmBackup.

Cet exemple montre comment sauvegarder un groupe de ressources :

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

Cet exemple sauvegarde une instance DB2 :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
db2_policy
```

Cet exemple sauvegarde une base de données DB2 :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCD";"PluginName"="DB2"
} -Policy db2_policy
```

6. Surveillez l'état du travail (en cours d'exécution, terminé ou en échec) à l'aide de l'applet de commande Get-smJobSummaryReport.

```
PS C:\> Get-SmJobSummaryReport -JobId 467
```

```
SmJobId : 467
JobCreatedDateTime :
JobStartDateTime : 27-Jun-24 01:40:09
JobEndDateTime : 27-Jun-24 01:41:15
JobDuration : 00:01:06.7013330
JobName : Backup of Resource Group
 'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
 'snapshot-based-db2'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : Backup
PolicyName : db2_policy
JobResultData :
```

7. Surveillez les détails de la tâche de sauvegarde comme ID de sauvegarde, nom de sauvegarde pour effectuer une opération de restauration ou de clonage à l'aide de l'applet de commande `Get-SmBackupReport`.

```

PS C:\> Get-SmBackupReport -JobId 467

BackedUpObjects : {WINCIR}
FailedObjects : {}
IsScheduled : False
HasMetadata : False
SmBackupId : 84
SmJobId : 467
StartDateTime : 27-Jun-24 01:40:09
EndDateTime : 27-Jun-24 01:41:15
Duration : 00:01:06.7013330
CreatedDateTime : 27-Jun-24 18:39:45
Status : Completed
ProtectionGroupName : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId : 23
PolicyName : db2_policy
SmPolicyId : 13
BackupName : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus : NotApplicable
VerificationStatuses :
SmJobError :
BackupType : SCC_BACKUP
CatalogingStatus : NotApplicable
CatalogingStatuses :
ReportDataCreatedDateTime :
PluginCode : SCC
PluginName : DB2
PluginDisplayName : IBM DB2
JobTypeId :
JobHost : HOSTFQDN

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarder les groupes de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.

- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

### Description de la tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en sélectionnant , puis en  sélectionnant la balise. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.
5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

### Surveillez les opérations de sauvegarde IBM DB2

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Surveillez les opérations de protection des données sur les bases de données IBM DB2 dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

## Annulez les opérations de sauvegarde pour IBM DB2

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

### Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.

- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

## Étapes

1. Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>Sélectionner l'opération.</li> <li>Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Affichez les sauvegardes et clones IBM DB2 dans la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire.

### Description de la tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.



Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la **carte Résumé** pour afficher un résumé du nombre de sauvegardes et de clones disponibles sur le stockage primaire et secondaire.

La section **carte récapitulative** affiche le nombre total de sauvegardes basées sur des copies Snapshot et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Après une sauvegarde à la demande, en cliquant sur le bouton **Refresh**, vous actualisez les détails de la sauvegarde ou du clone.

5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur .

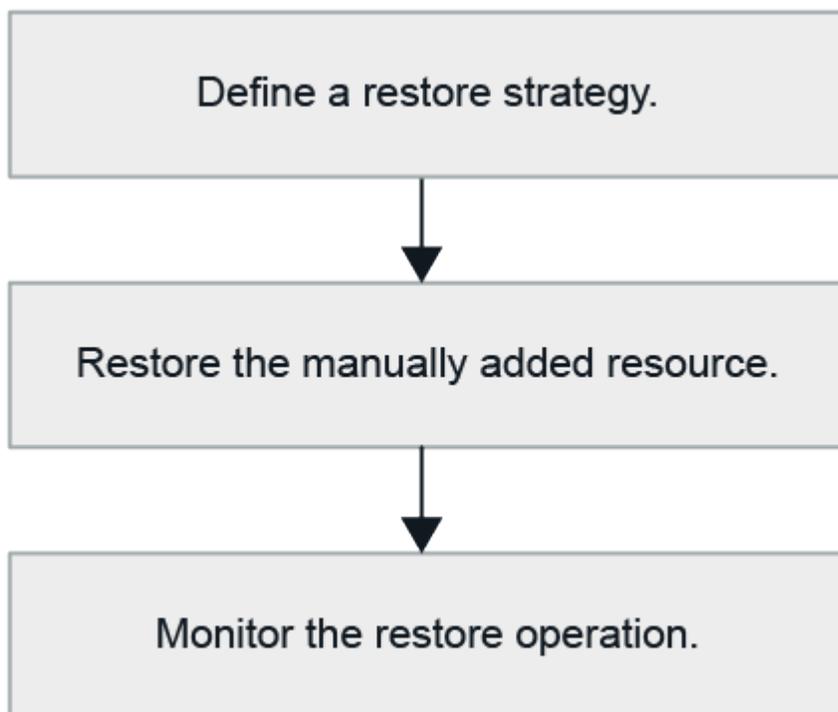
8. Si vous souhaitez diviser un clone, sélectionnez-le dans le tableau, puis cliquez sur .

## Restaurez IBM DB2

### Restaurer le flux de travail

Le workflow de restauration et de reprise comprend la planification, la réalisation des opérations de restauration et la surveillance des opérations.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Restaurer une sauvegarde de ressource ajoutée manuellement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

#### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.

- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

#### **Description de la tâche**

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur



Backup Name	End Date
rg1_scipr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource**.

- a. Si vous sélectionnez **Complete Resource**, tous les volumes de données configurés de la base de données IBM DB2 sont restaurés.

Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

Vous pouvez sélectionner plusieurs LUN.



Si vous sélectionnez **tous**, tous les fichiers des volumes, qtrees ou LUN sont restaurés.

7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.
8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.
9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Une fois que vous avez terminé

La récupération n'est possible que si l'état de récupération aval est à l'état "DB en attente". Cet état s'applique aux bases de données DB2 pour lesquelles la journalisation des archives est activée.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Identifiez la sauvegarde que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple montre que deux sauvegardes sont disponibles pour la restauration :

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library

 BackupId BackupName BackupTime

BackupType

1 Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32
AM Full Backup
2 Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17
AM
```

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

### 3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.



AppObjectId est "hôte\Plugin\UID", où UID = <instance\_name> est pour la ressource d'instance DB2 découverte manuellement et UID = <instance\_name>\<database\_name> est pour la ressource de base de données IBM DB2. Vous pouvez obtenir ResourceID à partir de l'applet de commande Get-smResources.

```
Get-smResources -HostName cn24.sscore.test.com -PluginCode DB2
```

Cet exemple montre comment restaurer la base de données à partir du stockage primaire :

```
Restore-SmBackup -PluginCode DB2 -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

Cet exemple montre comment restaurer la base de données à partir du stockage secondaire :

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @(@{"Primary"="Vserver>:<PrimaryVolume>"; "Secondary"="Vserver>:<SecondaryVolume>"})
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Restaurez et récupérez une sauvegarde de base de données découverte automatiquement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Pour les ressources découvertes automatiquement, la restauration est prise en charge par SFSR.
- La récupération automatique n'est pas prise en charge.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié

dans la liste.

2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).

5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur .



Backup Name	End Date
rg1_scopr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource** pour restaurer les volumes de données configurés de la base de données IBM DB2.
7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas requises pour les ressources découvertes automatiquement.

8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas requises pour les ressources découvertes automatiquement.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Une fois que vous avez terminé

La récupération n'est possible que si l'état de récupération aval est à l'état "DB en attente". Cet état s'applique aux bases de données DB2 pour lesquelles la journalisation des archives est activée.

## Surveillez les opérations de restauration IBM DB2

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Clonage des sauvegardes de ressources IBM DB2

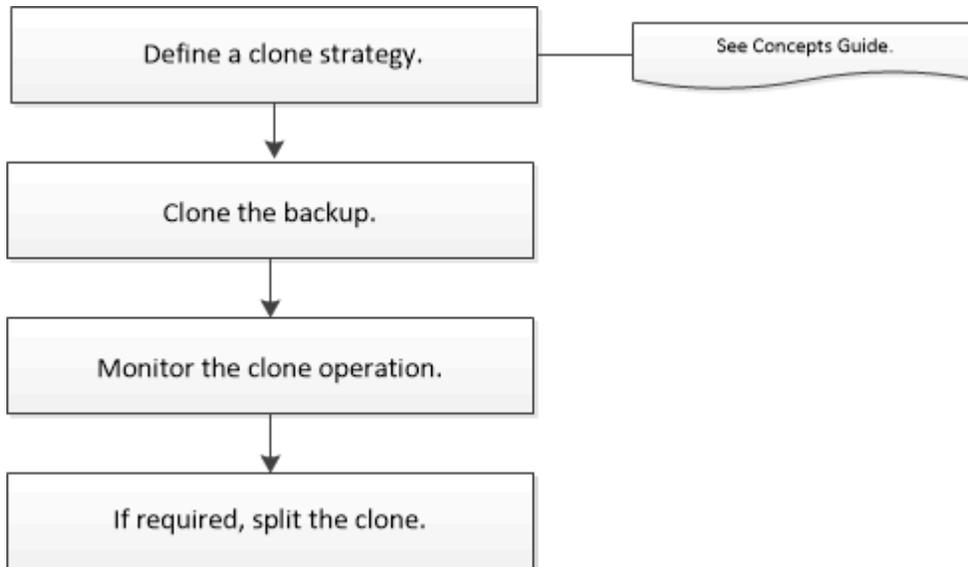
### Workflow de clonage

Le workflow de clonage inclut la réalisation de l'opération de clonage et le contrôle de l'opération.

## Description de la tâche

- Vous pouvez cloner sur le serveur IBM DB2 source.
- Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :
  - Tester les fonctionnalités à implémenter à l'aide de la structure de ressources actuelle et du contenu pendant les cycles de développement d'applications
  - Pour les outils d'extraction et de manipulation de données lors du remplissage d'entrepôts de données
  - Pour récupérer les données qui ont été supprimées ou modifiées par erreur

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

## Une fois que vous avez terminé

Après le clonage des ressources DB2 détectées automatiquement, la ressource clonée est marquée comme ressource manuelle. Cliquez sur **Actualiser les ressources** pour restaurer la ressource DB2 clonée. Lorsque vous supprimez le clone, le stockage et l'hôte sont également nettoyés.

Si vous n'actualisez pas les ressources après l'opération de clonage et que vous tentez de supprimer le clone, le stockage et l'hôte ne seront pas nettoyés. Vous devez supprimer les entrées manuellement dans fstab.

## Cloner une sauvegarde IBM DB2

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde. Vous pouvez cloner à partir d'une sauvegarde principale ou secondaire.

## Avant de commencer

- Vous devriez avoir sauvegardé les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Lors de la création d'un clone pour DB2 sur un autre hôte, vous devez créer une structure de répertoire n-1

pour le chemin de montage du clone identique au chemin de montage d'origine sur l'autre hôte. Le chemin de montage doit avoir une autorisation d'exécution 755.

- Pour les commandes pré-clone ou post-clone, vérifiez si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à "[Séparer un volume FlexClone de son volume parent](#)" la section, .
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources s'affichent avec des informations telles que le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

3. Sélectionnez la ressource ou le groupe de ressources.

Vous devez sélectionner une ressource si vous sélectionnez un groupe de ressources.

La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Serveur clone	Choisissez l'hôte sur lequel le clone doit être créé.
Instance de clone cible	Entrez l'ID d'instance de clone DB2 cible à cloner à partir des sauvegardes existantes.  Cela s'applique uniquement aux ressources de type de stockage ANF.
Nom du clone cible	Indiquez le nom du clone.  Ceci s'applique uniquement à la ressource de base de données DB2.
Adresse IP d'exportation NFS	Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.  Cela s'applique uniquement à la ressource de type de stockage NFS.
Capacité du pool max. Débit (Mio/s)	Entrez le débit maximal d'un pool de capacité.

7. Dans la page scripts, effectuez les opérations suivantes :



Les scripts sont exécutés sur l'hôte du plug-in.

- a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
  - Commande de pré-clonage : permet de supprimer les bases de données existantes portant le même nom
  - Commande post-clone : vérifiez une base de données ou démarrez une base de données.
- b. Entrez la commande mount pour monter un système de fichiers sur un hôte.

Commande mount pour un volume ou un qtree sur une machine Linux :

Exemple pour NFS : `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.
10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Une fois que vous avez terminé

Après le clonage des ressources DB2 détectées automatiquement, la ressource clonée est marquée comme ressource manuelle. Cliquez sur **Actualiser les ressources** pour restaurer la ressource DB2 clonée. Lorsque vous supprimez le clone, le stockage et l'hôte sont également nettoyés.

Si vous n'actualisez pas les ressources après l'opération de clonage et que vous tentez de supprimer le clone, le stockage et l'hôte ne seront pas nettoyés. Vous devez supprimer les entrées manuellement dans fstab.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. Répertoriez les sauvegardes pouvant être clonées à l'aide de l'applet de commande Get-SmBackup ou Get-SmResourceGroup.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

Cet exemple affiche des informations sur un groupe de ressources spécifié, ses ressources et les stratégies associées :

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCOREContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCOREContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
ApplySnapvaultUpdate : False  
ApplyRetention : False  
RetentionCount : 0  
RetentionDays : 0  
ApplySnapMirrorUpdate : False  
SnapVaultLabel :  
MirrorVaultUpdateRetryCount : 7  
AppPolicies : {}  
Description : FinancePolicy  
PreScriptPath :  
PreScriptArguments :  
PostScriptPath :  
PostScriptArguments :  
ScriptTimeOut : 60000  
DateModified : 8/4/2015 3:43:30 PM  
DateCreated : 8/4/2015 3:43:30 PM  
Schedule : SMCoreContracts.SmSchedule  
PolicyType : Backup  
PluginPolicyType : SMSQL  
Name : FinancePolicy  
Type :  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
clab-a13-13.sddev.lab.netapp.com  
DatabaseGUID :  
SQLInstance : clab-a13-13  
DbStatus : AutoClosed  
DbAccess : eUndefined  
IsSystemDb : False  
IsSimpleRecoveryMode : False  
IsSelectable : True  
SqlDbFileGroups : {}  
SqlDbLogFiles : {}

```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. Lancez une opération de clonage à partir d'une sauvegarde existante à l'aide de l'applet de commande `New-SmClone`.

Dans cet exemple, un clone est créé à partir d'une sauvegarde spécifiée avec tous les journaux :

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

Dans cet exemple, un clone est créé dans une instance Microsoft SQL Server spécifiée :

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. Affichez l'état du travail clone à l'aide de l'applet de commande `Get-SmCloneReport`.

Cet exemple affiche un rapport de clonage pour l'ID de tâche spécifié :

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
 Sally_DRAPER}

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveillez les opérations de clonage IBM DB2

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur \* \*  .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

#### Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

## Supprimez ou divisez les clones de base de données IBM DB2 après la mise à niveau de SnapCenter

Après la mise à niveau vers SnapCenter 4.3, vous ne verrez plus les clones. Vous pouvez supprimer le clone ou séparer les clones de la page topologie de la ressource à partir de laquelle les clones ont été créés.

#### Description de la tâche

Si vous souhaitez localiser l'empreinte de stockage des clones masqués, exécutez la commande suivante :  
`Get-SmClone -ListStorageFootprint`

#### Étapes

1. Supprimez les sauvegardes des ressources clonées à l'aide de la cmdlet `remove-smbbackup`.
2. Supprimez le groupe de ressources des ressources clonées à l'aide de la cmdlet `remove-smresregroupement`.
3. Supprimez la protection de la ressource clonée à l'aide de l'applet de commande `remove-smprotectResource`.
4. Sélectionnez la ressource parente dans la page Ressources.

La page topologie de ressources s'affiche.

5. Dans la vue Manage copies (gérer les copies), sélectionnez les clones dans les systèmes de stockage principal ou secondaire (en miroir ou répliqué).
6. Sélectionnez les clones, puis cliquez sur  pour supprimer les clones ou sur  pour les séparer.
7. Cliquez sur **OK**.

# Protéger PostgreSQL

## Plug-in SnapCenter pour PostgreSQL

### Présentation du plug-in SnapCenter pour PostgreSQL

Le plug-in SnapCenter pour le cluster PostgreSQL est un composant côté hôte du logiciel NetApp SnapCenter qui permet la gestion de la protection des données compatible avec les applications des clusters PostgreSQL. Le plug-in pour cluster PostgreSQL automatise la sauvegarde, la restauration et le clonage des clusters PostgreSQL dans votre environnement SnapCenter.

SnapCenter prend en charge les configurations PostgreSQL à un seul cluster et à plusieurs clusters. Vous pouvez utiliser le plug-in pour les clusters PostgreSQL dans les environnements Linux et Windows. Dans les environnements Windows, PostgreSQL sera pris en charge en tant que ressource manuelle.

Une fois le cluster Plug-in pour PostgreSQL installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies miroir des jeux de sauvegarde sur un autre volume. Vous pouvez également utiliser le plug-in doté de la technologie SnapVault de NetApp pour effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes.

Le plug-in SnapCenter pour PostgreSQL prend en charge les protocoles NFS et SAN sur les infrastructures de stockage de fichiers ONTAP et Azure NetApp.

L'organisation du stockage virtuel VMDK, vVol et RDM est prise en charge.

### Ce que vous pouvez faire à l'aide du plug-in SnapCenter pour PostgreSQL

Lorsque vous installez le cluster Plug-in pour PostgreSQL dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner les clusters PostgreSQL et leurs ressources. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Ajouter des clusters.
- Création de sauvegardes.
- Effectuez des restaurations à partir des sauvegardes.
- Sauvegardes clones.
- Planifiez les opérations de sauvegarde.
- Contrôle des opérations de sauvegarde, de restauration et de clonage
- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.

### Plug-in SnapCenter pour les fonctionnalités PostgreSQL

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour utiliser le plug-in pour le cluster PostgreSQL, vous utilisez l'interface utilisateur graphique SnapCenter.

- **Interface utilisateur graphique unifiée**

L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

Vous pouvez planifier des opérations de sauvegarde, configurer la conservation des sauvegardes basée sur des règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie de copie snapshot NetApp non disruptive**

SnapCenter utilise la technologie Snapshot de NetApp avec le plug-in pour le cluster PostgreSQL pour sauvegarder les ressources.

L'utilisation du plug-in pour PostgreSQL offre également les avantages suivants :

- Prise en charge des workflows de sauvegarde, de restauration et de clonage
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Création de copies compactes et ponctuelles de ressources à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonctionnalité de snapshot de groupe de cohérence (CG) de ONTAP dans le cadre de la création des sauvegardes.
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

En une seule opération, les snapshots sont consolidés lorsque les ressources d'un hôte unique partagent le même volume.

- Possibilité de créer des instantanés à l'aide de commandes externes.
- Prise en charge de Linux LVM sur le système de fichiers XFS.

## **Types de stockage pris en charge par le plug-in SnapCenter pour PostgreSQL**

SnapCenter prend en charge de nombreux types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier la prise en charge de votre type de stockage avant d'installer le plug-in SnapCenter pour PostgreSQL.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"> <li>• LUN connectés via FC</li> <li>• LUN connectées à l'iSCSI</li> <li>• Volumes connectés par NFS</li> </ul>
VMware ESXi	<ul style="list-style-type: none"> <li>• L'exécution des LUN RDM connectés par un HBA FC ou iSCSI ESXi peut prendre du temps car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte.</li> </ul> <p data-bbox="862 510 1487 743">Vous pouvez modifier le fichier <b>LinuxConfig.pm</b> situé à  <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> à 1 pour analyser uniquement les HBA répertoriés dans les NOMS de PILOTE HBA.</p> <ul style="list-style-type: none"> <li>• LUN iSCSI connectés directement au système invité par l'initiateur iSCSI</li> <li>• VMDK sur des datastores NFS</li> <li>• VMDK sur VMFS</li> <li>• Volumes NFS connectés directement au système invité</li> <li>• Datastores vVol sur NFS et SAN</li> </ul> <p data-bbox="862 1115 1468 1213">Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>

## Privilèges ONTAP minimum requis pour le plug-in PostgreSQL

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - la création de lun
  - la création de lun
  - suppression de la lun

- lun igroup add
- créez un groupe initiateur lun
- suppression du groupe initiateur lun
- renommer la lun igroup
- renommer la lun igroup
- affichage de la lun igroup
- lun mapping des nœuds supplémentaires
- création d'un mappage de lun
- suppression du mappage de lun
- mappage de lun supprimer-rapports-nœuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- suppression de la réservation persistante de lun
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes

- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- volume snapshot modify-snaplock-expiration-time
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau
  - interface réseau affiche

- un vserver

## Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour PostgreSQL

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Stratégie de sauvegarde pour PostgreSQL

### Définir une stratégie de sauvegarde pour PostgreSQL

Définir une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous aide à disposer des sauvegardes dont vous avez besoin pour restaurer ou cloner vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

#### Description de la tâche

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

#### Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.

2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décidez si vous souhaitez créer une règle basée sur les copies Snapshot pour sauvegarder des copies Snapshot cohérentes au niveau des applications du cluster.
5. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
6. Déterminer la période de conservation des snapshots sur le système de stockage source et la destination SnapMirror.
7. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescripteur ou un PostScript.

### **Découverte automatique des ressources sur l'hôte Linux**

Les ressources sont des clusters et des instances PostgreSQL sur l'hôte Linux qui sont gérés par SnapCenter. Après avoir installé le plug-in SnapCenter pour PostgreSQL, les clusters PostgreSQL de toutes les instances de cet hôte Linux sont automatiquement découverts et affichés dans la page Ressources.

### **Types de sauvegardes pris en charge**

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge les types de sauvegarde basés sur la copie Snapshot pour les clusters PostgreSQL.

### **Sauvegarde basée sur des copies Snapshot**

Les sauvegardes basées sur des copies Snapshot utilisent la technologie NetApp Snapshot pour créer des copies en ligne en lecture seule des volumes sur lesquels résident les clusters PostgreSQL.

### **Comment le plug-in SnapCenter pour PostgreSQL utilise les snapshots de groupes de cohérence**

Vous pouvez utiliser le plug-in pour créer des snapshots de groupes de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes, de sorte que vous puissiez les gérer comme une entité unique. Un groupe de cohérence est une copie instantanée de plusieurs volumes, fournissant ainsi des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente nécessaire au contrôleur de stockage pour regrouper les snapshots de manière cohérente. Les options de temps d'attente disponibles sont **urgent**, **Moyen** et **détendu**. Vous pouvez également activer ou désactiver la synchronisation WAFL (Write Anywhere File Layout) lors d'une opération de snapshot de groupe cohérente. WAFL Sync améliore les performances d'un snapshot de groupe de cohérence.

### **Comment SnapCenter gère la gestion de la gestion des sauvegardes de données**

SnapCenter gère la gestion des sauvegardes de données au niveau du système de stockage et du système de fichiers.

Les snapshots sur le stockage primaire ou secondaire et les entrées correspondantes dans le catalogue

PostgreSQL sont supprimés en fonction des paramètres de conservation.

### **Considérations relatives à la détermination des plannings de sauvegarde pour PostgreSQL**

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes (fréquence des sauvegardes)

La fréquence de sauvegarde, également appelée type de planification pour certains plug-ins, fait partie d'une configuration de règles. Par exemple, vous pouvez configurer la fréquence des sauvegardes sous forme horaire, quotidienne, hebdomadaire ou mensuelle.

- Plannings de sauvegarde (exactement au moment où les sauvegardes doivent être effectuées)

Les planifications de sauvegarde font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour la sauvegarder tous les jeudis à 10 h 00

### **Nombre de tâches de sauvegarde requises pour PostgreSQL**

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

### **Conventions de nommage des sauvegardes pour le plug-in pour les clusters PostgreSQL**

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.
- *03-12-2015\_23.17.26* est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, `clienttext_resourcegroup_policy_hostname` ou `resourcegroup_hostname`. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

## Stratégie de restauration et de récupération pour PostgreSQL

### Définissez une stratégie de restauration et de récupération pour les ressources PostgreSQL

Vous devez définir une stratégie avant de restaurer et de restaurer votre cluster afin de pouvoir effectuer correctement les opérations de restauration et de récupération.



Seule la récupération manuelle du cluster est prise en charge.

#### Étapes

1. Déterminez les stratégies de restauration prises en charge pour les ressources PostgreSQL ajoutées manuellement
2. Déterminez les stratégies de restauration prises en charge pour les clusters PostgreSQL découverts automatiquement
3. Choisissez le type d'opérations de restauration à effectuer.

### Types de stratégies de restauration pris en charge pour les ressources PostgreSQL ajoutées manuellement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter.



Vous ne pouvez pas récupérer les ressources PostgreSQL ajoutées manuellement.

#### Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

REMARQUE : le plug-in pour PostgreSQL crée une étiquette `_sauvegarde` et une table `_map` dans le dossier `<OS_temp_folder>/postgresql_sc_Recovery<Restore_JobId>/_` pour faciliter la restauration manuelle .

### Type de stratégie de restauration pris en charge pour PostgreSQL découvert automatiquement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter.

La restauration complète des ressources est la stratégie de restauration prise en charge pour les clusters PostgreSQL découverts automatiquement. Cette opération restaure tous les volumes, qtree et LUN d'une ressource.

### Types d'opérations de restauration pour PostgreSQL découvert automatiquement

Le plug-in SnapCenter pour PostgreSQL prend en charge les SnapRestore de fichiers uniques et les types de restauration de connexion et de copie pour les clusters PostgreSQL découverts automatiquement.

Single File SnapRestore s'effectue dans des environnements NFS pour les scénarios suivants :

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde sélectionnée provient d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Complete Resource** est sélectionnée

Single File SnapRestore s'effectue dans des environnements SAN pour les scénarios suivants :

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée depuis un emplacement secondaire SnapMirror ou SnapVault et l'option **Complete Resource** est sélectionnée

### Types d'opérations de restauration pris en charge pour les clusters PostgreSQL

SnapCenter vous permet d'effectuer différents types d'opérations de restauration pour les clusters PostgreSQL.

- Restaurez le cluster à l'état le plus récent
- Restaurer le cluster à un point dans le temps spécifique

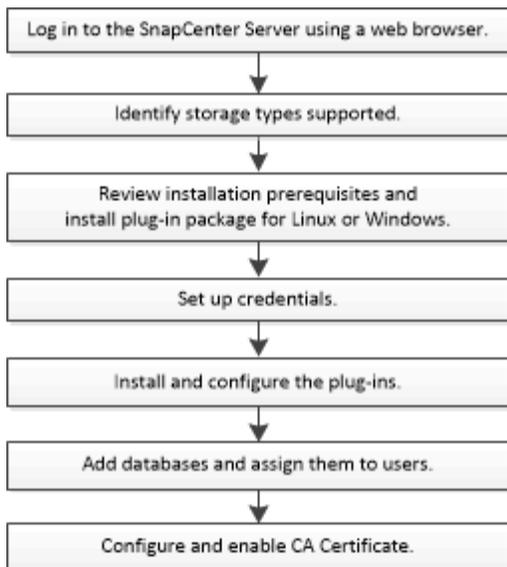
Vous devez indiquer la date et l'heure de la récupération.

SnapCenter propose également l'option aucune restauration pour les clusters PostgreSQL.

## Préparez l'installation du plug-in SnapCenter pour PostgreSQL

### Workflow d'installation du plug-in SnapCenter pour PostgreSQL

Vous devez installer et configurer le plug-in SnapCenter pour PostgreSQL si vous voulez protéger les clusters PostgreSQL.



## Conditions préalables à l'ajout d'hôtes et à l'installation du plug-in SnapCenter pour PostgreSQL

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour PostgreSQL est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 11 sur votre hôte.



IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Pour Windows, le service de création de plug-in doit être exécuté à l'aide de l'utilisateur Windows « LocalSystem », qui est le comportement par défaut lorsque le plug-in pour PostgreSQL est installé en tant qu'administrateur de domaine.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in PostgreSQL sur les hôtes Windows.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte PostgreSQL.

### Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour PostgreSQL sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Windows.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Matrice d'interopérabilité NetApp"](#)

## Hôtes Linux

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Matrice d'interopérabilité NetApp"](#)

- Pour les clusters PostgreSQL qui s'exécutent sur un hôte Linux, lors de l'installation du plug-in pour PostgreSQL, le plug-in SnapCenter pour UNIX est installé automatiquement.
- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

## Commandes supplémentaires

Pour exécuter une commande supplémentaire sur le plug-in SnapCenter pour PostgreSQL, vous devez l'inclure dans le fichier *allowed\_commands.config*.

- Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
- Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*

Pour autoriser des commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier *allowed\_commands.config* dans un éditeur. Entrez chaque commande sur une ligne distincte et les commandes ne sont pas sensibles à la casse. Assurez-vous de spécifier le chemin d'accès complet et de le joindre entre guillemets (") s'il contient des espaces.

Par exemple :

Commande : mount command : commande umount : « C:\Program Files\NetApp\SnapCreator commands\sdcli.exe » commande : myscript.bat

Si le fichier *allowed\_commands.config* n'est pas présent, les commandes ou l'exécution du script seront bloquées et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »

Si la commande ou le script n'est pas présent dans *allowed\_commands.config*, l'exécution de la commande ou du script sera bloquée et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »



Vous ne devez pas utiliser de caractère générique (\*) pour autoriser toutes les commandes.

## Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux

SnapCenter permet à un utilisateur non root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

## Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- `/Home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/Custom_location/NetApp/snapcenter/spl/installation/plugins/désinstaller`
- `/Custom_location/NetApp/snapcenter/spl/bin/spl`

## Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.
2. Ajoutez les lignes suivantes au fichier `/etc/sudoers` à l'aide de l'utilitaire visudo Linux.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

*LINUX\_USER* est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur *checksum\_value* à partir du fichier **sc\_unix\_plugins\_checksum.txt**, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` \_ si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` \_ si le serveur SnapCenter est installé sur un hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	Microsoft Windows  Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a> .

Élément	De formation
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <p> Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section "<a href="#">La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet.</a>"</p>

## Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux

Avant d'installer le module de plug-ins SnapCenter pour Linux, vous devez connaître certains besoins en espace système hôte de base et en dimensionnement.

Élément	De formation
Systèmes d'exploitation	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO

Élément	De formation
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>2 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
Packs logiciels requis	<p>Java 11 Oracle Java et OpenJDK</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p>

## Configurez les informations d'identification du plug-in SnapCenter pour PostgreSQL

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour l'exécution des opérations de protection des données sur les clusters ou les systèmes de fichiers Windows.

### Description de la tâche

- Hôtes Linux

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

**Meilleure pratique:** bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>Administrateur de domaine ou tout membre du groupe d'administrateurs</li> </ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li><i>NetBIOS\username</i></li> <li><i>Domain FQDN\username</i></li> </ul> <ul style="list-style-type: none"> <li>Administrateur local (groupes de travail uniquement)</li> </ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p> <p>N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="margin-right: 10px;"></div> <div>Applicable uniquement aux utilisateurs Linux.</div> </div>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

### Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

### Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediately
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

Par exemple :

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :
  - a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[ ] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gMSA>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gMSA>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Installez le plug-in SnapCenter pour PostgreSQL

### Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter l'hôte et installer des modules d'extension pour un hôte individuel.

#### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.

- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

["Configurez le compte de service géré de groupe sur Windows Server 2016 ou version ultérieure pour PostgreSQL"](#)

### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez le type d'hôte :</p> <ul style="list-style-type: none"> <li>• Répertoires de base</li> <li>• Linux</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL et cet hôte peut se trouver sur un système Windows ou Linux.</p> </div>
Nom d'hôte	<p>Entrez le nom d'hôte de communication. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p>

Pour ce champ...	Procédez comme ça...
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez fourni.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p> </div>

5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

Lorsque vous utilisez l'API REST pour installer le plug-in pour PostgreSQL, vous devez transmettre la version 3.0. Par exemple, PostgreSQL:3.0

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p> </div>

Pour ce champ...	Procédez comme ça...
Chemin d'installation	<p>Le plug-in pour PostgreSQL est installé sur l'hôte client PostgreSQL et cet hôte peut se trouver sur un système Windows ou Linux.</p> <ul style="list-style-type: none"> <li>• Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin.</li> <li>• Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.</li> </ul>
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Ajoutez tous les hôtes du cluster	Cochez cette case pour ajouter tous les nœuds du cluster.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	<p>Pour l'hôte Windows, cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Indiquez le nom GMSA au format suivant : domainname\accountName\$.</p> <p> GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.</p> </div>

## 7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse C:\Program Files\NetApp\SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

9. Surveillez la progression de l'installation.

- Pour le plug-in Windows, les journaux d'installation et de mise à niveau se trouvent à l'adresse suivante : `C:\Windows\SnapCenter plugin\Install<JOBID>\_`
- Pour le plug-in Linux, les journaux d'installation se trouvent à l'adresse suivante : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_` et les journaux de mise à niveau se trouvent à l'adresse : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

## Installez les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer simultanément les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage PowerShell`.

### Avant de commencer

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande `Open-SmConnection`, puis saisissez vos informations d'identification.
3. Installez le plug-in sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Vous pouvez utiliser l'option `-skipreccheck` lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

4. Saisissez vos informations d'identification pour l'installation à distance.

## Installez le plug-in SnapCenter pour PostgreSQL sur les hôtes Linux à l'aide de l'interface de ligne de commande

Vous devez installer le plug-in SnapCenter pour le cluster PostgreSQL en utilisant l'interface utilisateur SnapCenter. Si votre environnement ne permet pas l'installation à

distance du plug-in à partir de l'interface utilisateur SnapCenter, vous pouvez installer le cluster Plug-in pour PostgreSQL en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande.

### Avant de commencer

- Vous devez installer le cluster Plug-in pour PostgreSQL sur chacun des hôtes Linux où réside le client PostgreSQL.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour le cluster PostgreSQL doit répondre à la configuration logicielle, cluster et système d'exploitation requise.

La matrice d'interopérabilité (IMT) contient les dernières informations sur les configurations prises en charge.

#### "Matrice d'interopérabilité NetApp"

- Le cluster SnapCenter Plug-in pour PostgreSQL fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé SnapCenter sur un hôte Windows.

### Étapes

1. Copiez le fichier d'installation du pack de plug-ins SnapCenter pour Linux (snapcenter\_linux\_host\_plugin.bin) depuis C:\ProgramData\NetApp\SnapCenter\Package Repository vers l'hôte sur lequel vous souhaitez installer le plug-in pour PostgreSQL.

Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in :

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server
```

  - -DPORT spécifie le port de communication SMCORE HTTPS.
  - -DSERVER\_IP spécifie l'adresse IP du serveur SnapCenter.
  - -DSERVER\_HTTPS\_PORT spécifie le port HTTPS du serveur SnapCenter.
  - -DUSER\_INSTALL\_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
  - DINSTALL\_LOG\_NAME indique le nom du fichier journal.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Modifiez le fichier /<installation directory>/NetApp/snapcenter/scc/etc/SC\_SMS\_Services.properties, puis ajoutez le paramètre PLUGINS\_ENABLED = PostgreSQL:3.0.
5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres

requis.

Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Surveillez l'état d'installation du plug-in pour PostgreSQL

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

### Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

#### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

### Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

#### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :

- a. Double-cliquez sur le certificat.
- b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
- c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
- d. Copiez les caractères hexadécimaux de la zone.
- e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :

- a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

### Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

#### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCORE 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert iport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert iport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

### Configurez le certificat CA pour le service SnapCenter PostgreSQL Plug-ins sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier « keystore.jks », qui se trouve dans `/opt/NetApp/snapcenter/scc/etc` à la fois comme magasin de confiance et magasin de clés.

**Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation**

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Procédez de même pour la clé KEYSTORE\_PASS dans le fichier `agent.properties`.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in : `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaires pour le plug-in trust-store.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.

7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Si le nom d'alias du certificat de l'autorité de certification est
long et contient de l'espace ou des caractères spéciaux ("*", ",", "),
remplacez le nom d'alias par un nom simple :
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurez le nom d'alias à partir du certificat CA dans le fichier
agent.properties.
```

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in `trust-store`.

### Configurer la liste de révocation de certificats (CRL) pour les plug-ins

#### Description de la tâche

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est « `opt/NetApp/snapcenter/scc/etc/crl` ».

#### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `agent.properties` par rapport à la clé `CRL_PATH`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

### Configurez le certificat CA pour le service SnapCenter PostgreSQL Plug-ins sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier `keystore.jks`, qui se trouve dans `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc` à la fois comme magasin de confiance et magasin de clés.

## Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé `KEYSTORE_PASS`.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
```



Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks
```

Procédez de même pour la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

4. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

### Étapes

1. Accédez au dossier contenant le keystore du plug-in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`

2. Localisez le fichier 'keystore.jks'.

3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
Keytool -import -truacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

### Étapes

1. Accédez au dossier contenant le keystore du plug-in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`

2. Localisez le fichier `keystore.jks`.

3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.

7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configurez le nom d'alias à partir du certificat CA dans le fichier `agent.properties`.

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

## Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

### Description de la tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section ["Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter"](#).
- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est `'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'`.

### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `agent.properties` par rapport à la clé `CRL_PATH`.

2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

### Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

#### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

#### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Préparation à la protection des données

### Conditions préalables à l'utilisation du plug-in SnapCenter pour PostgreSQL

Avant d'utiliser le plug-in SnapCenter pour PostgreSQL, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches requises.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.
- Installez Java 11 sur votre hôte Linux ou Windows.

Vous devez définir le chemin Java dans la variable de chemin d'environnement de la machine hôte.

- Configurer SnapMirror et SnapVault pour la réplication de sauvegarde.

## Utilisation des ressources, des groupes de ressources et des règles pour protéger PostgreSQL

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des clusters PostgreSQL que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Les règles spécifient la fréquence des sauvegardes, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

Considérez un groupe de ressources comme définissant ce que vous voulez protéger et quand vous voulez le protéger en termes de jour et d'heure. Considérez une stratégie comme une définition de la façon dont vous voulez la protéger. Si vous sauvegardez tous les clusters, par exemple, vous pouvez créer un groupe de ressources qui inclut tous les clusters de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources de manière à effectuer une sauvegarde complète tous les jours.

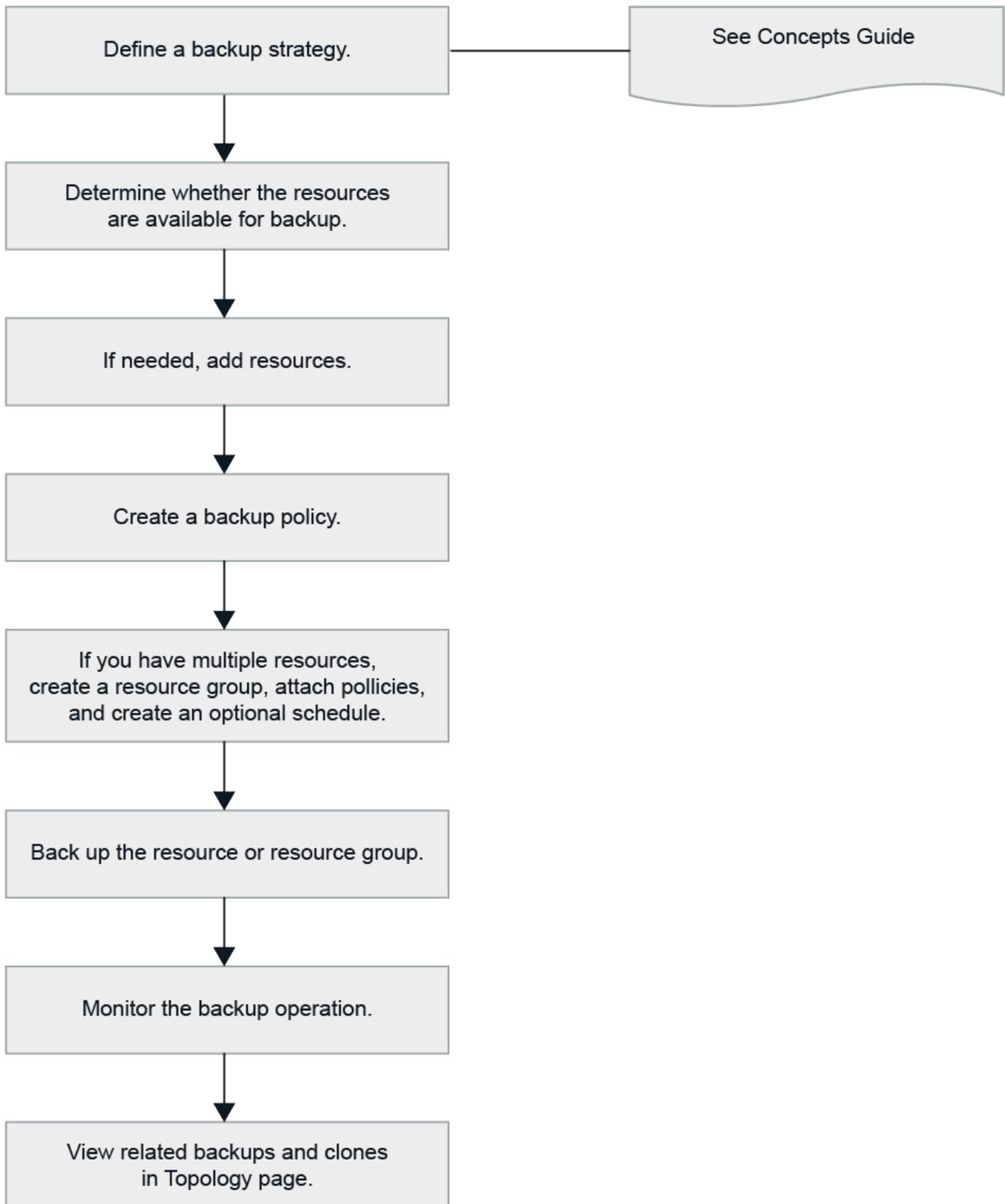
## Sauvegarder les ressources PostgreSQL

### Sauvegarder les ressources PostgreSQL

Vous pouvez créer une sauvegarde d'une ressource (cluster) ou d'un groupe de

ressources. Le workflow de sauvegarde comprend la planification, l'identification des clusters à sauvegarder, la gestion des stratégies de sauvegarde, la création de groupes de ressources et de stratégies de connexion, la création de sauvegardes et la surveillance des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent plus d'informations sur les applets de commande PowerShell. ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Découverte automatique des clusters

Les ressources sont des clusters PostgreSQL sur l'hôte Linux qui sont gérés par SnapCenter. Vous pouvez ajouter des ressources à des groupes de ressources pour exécuter les opérations de protection des données une fois que vous avez découvert les clusters PostgreSQL disponibles.

### Avant de commencer

- Vous devez avoir déjà effectué des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions du système de stockage.
- Le plug-in SnapCenter pour PostgreSQL ne prend pas en charge la découverte automatique des ressources résidant sur les environnements virtuels RDM/VMDK.

### Description de la tâche

- Après l'installation du plug-in, tous les clusters de cet hôte Linux sont automatiquement détectés et affichés sur la page Ressources.
- Seuls les clusters sont découverts automatiquement.

Les ressources détectées automatiquement ne peuvent pas être modifiées ou supprimées.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in pour PostgreSQL dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste vue.
3. (Facultatif) cliquez sur \* \* , puis sélectionnez le nom d'hôte.

Vous pouvez alors cliquer sur \* \*  pour fermer le volet de filtre.

4. Cliquez sur **Actualiser les ressources** pour découvrir les ressources disponibles sur l'hôte.

Les ressources s'affichent avec des informations telles que le type de ressource, le nom d'hôte, les groupes de ressources associés, le type de sauvegarde, les stratégies et l'état global.

- Si le cluster se trouve sur un système de stockage NetApp non protégé, la mention non protégé s'affiche dans la colonne État global.
- Si le cluster se trouve sur un système de stockage NetApp et qu'il est protégé, et si aucune opération de sauvegarde n'est effectuée, la colonne État global affiche sauvegarde non exécutée. Dans le cas contraire, l'état passe en échec de la sauvegarde ou la sauvegarde a réussi en fonction de l'état de la dernière sauvegarde.



Vous devez actualiser les ressources si les clusters sont renommés en dehors de SnapCenter.

## Ajoutez des ressources manuellement au plug-in hôte

La découverte automatique n'est pas prise en charge sur l'hôte Windows. Vous devez ajouter manuellement les ressources de cluster PostgreSQL.

### Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions du système de stockage.

## Description de la tâche

La détection automatique n'est pas prise en charge pour les configurations suivantes :

- Dispositions RDM et VMDK

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez le plug-in SnapCenter pour PostgreSQL dans la liste déroulante, puis cliquez sur **Ressources**.
2. Dans la page Ressources, cliquez sur **Ajouter des ressources PostgreSQL**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Spécifier le nom du cluster
Nom d'hôte	Entrez le nom d'hôte.
Type	Sélectionnez cluster.
Fréquence	Spécifiez le nom de l'instance, qui est le parent du cluster.
Informations d'identification	Sélectionnez les informations d'identification ou ajoutez-les.  Cette option est facultative.

4. Sur la page fournir l'empreinte du stockage, sélectionnez un type de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Enregistrer**.

Facultatif : vous pouvez cliquer sur l'icône \*  pour ajouter d'autres volumes, LUN et qtrees à partir d'autres systèmes de stockage.

5. Facultatif : dans la page Paramètres de ressources, pour les ressources sur l'hôte Windows, entrez des paires clé-valeur personnalisées pour le plug-in PostgreSQL
6. Vérifiez le résumé, puis cliquez sur **Terminer**.

Les clusters s'affichent avec des informations telles que le nom d'hôte, les groupes de ressources et les stratégies associés, ainsi que l'état global

Si vous souhaitez donner aux utilisateurs l'accès aux ressources, vous devez affecter ces ressources aux utilisateurs. Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

["Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources"](#)

## Une fois que vous avez terminé

- Après avoir ajouté les clusters, vous pouvez modifier les détails du cluster PostgreSQL.

- Les ressources migrées (tablespace et clusters) à partir de SnapCenter 5.0 seront marquées comme type de cluster PostgreSQL dans SnapCenter 6.0.
- Lorsque vous modifiez les ressources ajoutées manuellement qui sont migrées depuis SnapCenter 5.0 ou une version antérieure, procédez comme suit dans la page **Paramètres de ressource** pour les paires de valeurs de clé personnalisées :
  - Spécifiez le terme "PORT" dans le champ **Nom**.
  - Spécifiez le numéro de port dans le champ **valeur**.

## Créez des règles de sauvegarde pour PostgreSQL

Avant d'utiliser SnapCenter pour sauvegarder des ressources PostgreSQL, vous devez créer une stratégie de sauvegarde pour le groupe de ressources ou de ressources que vous souhaitez sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.

Pour plus d'informations, reportez-vous aux informations sur la définition d'une stratégie de protection des données pour les clusters PostgreSQL.

- Vous devez vous préparer à la protection des données en effectuant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout de ressources.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir affecté des SVM aux volumes source et de destination.

En outre, vous pouvez spécifier des paramètres de réplication, de script et d'application dans la stratégie. Ces options vous permettent de gagner du temps lorsque vous souhaitez réutiliser la stratégie d'un autre groupe de ressources.

### Description de la tâche

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un plus grand nombre d'instantanés que le nombre spécifié dans la règle.
  - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.

4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez le type de stockage.
  - b. Dans la section **Paramètres de sauvegarde personnalisés**, indiquez tous les paramètres de sauvegarde spécifiques qui doivent être transmis au plug-in au format clé-valeur.

Vous pouvez fournir plusieurs valeurs de clé à transmettre au plug-in.

6. Dans la page sauvegarde et réplication, effectuez les opérations suivantes :
  - a. Spécifiez la fréquence d'horaire en sélectionnant **sur demande, horaire, quotidien, hebdomadaire** ou **mensuel**.



Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais aussi d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

- a. Dans la section Paramètres de l'instantané, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionné dans la page **Type de sauvegarde** :

Les fonctions que vous recherchez...	Alors...
Conserver un certain nombre d'instantanés	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> </div>
Conserver les instantanés pendant un certain nombre de jours	Sélectionnez <b>conserver les copies pour</b> , puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage des copies Snapshot principales	<p>Sélectionnez période de verrouillage des instantanés, puis sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>
Période de verrouillage des copies Snapshot secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.

7. Sélectionnez un libellé de stratégie.

Selon l'étiquette de règle que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à l'étiquette.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

8. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
<p><b>Mettre à jour SnapMirror après avoir créé une copie Snapshot locale</b></p>	<p>Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).</p> <p>Si la relation de protection dans ONTAP est de type miroir et coffre-fort et si vous sélectionnez uniquement cette option, le snapshot créé sur le primaire ne sera pas transféré vers la destination, mais sera répertorié dans la destination. Si cet instantané est sélectionné à partir de la destination pour effectuer une opération de restauration, le message d'erreur suivant s'affiche : l'emplacement secondaire n'est pas disponible pour la sauvegarde en miroir/en coffre-fort sélectionnée.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir "<a href="#">Affichez les sauvegardes et clones liés aux ressources PostgreSQL dans la page topologie</a>".</p>

Pour ce champ...	Procédez comme ça...
<b>Mettre à jour SnapVault après avoir créé une copie Snapshot locale</b>	<p>Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton <b>Actualiser</b> de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, reportez-vous à la section archivage des snapshots en mode WORM sur un coffre-fort destination</p> <p>Voir "<a href="#">Affichez les sauvegardes et clones liés aux ressources PostgreSQL dans la page topologie</a>".</p>
<b>Nombre de tentatives d'erreur</b>	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer des groupes de ressources et attacher des stratégies

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du

SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.   Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.  Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.
Utilisez un format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.  Par exemple, clienttext_Resource group_policy_hostname ou Resource group_hostname. Par défaut, un horodatage est ajouté au nom du snapshot.

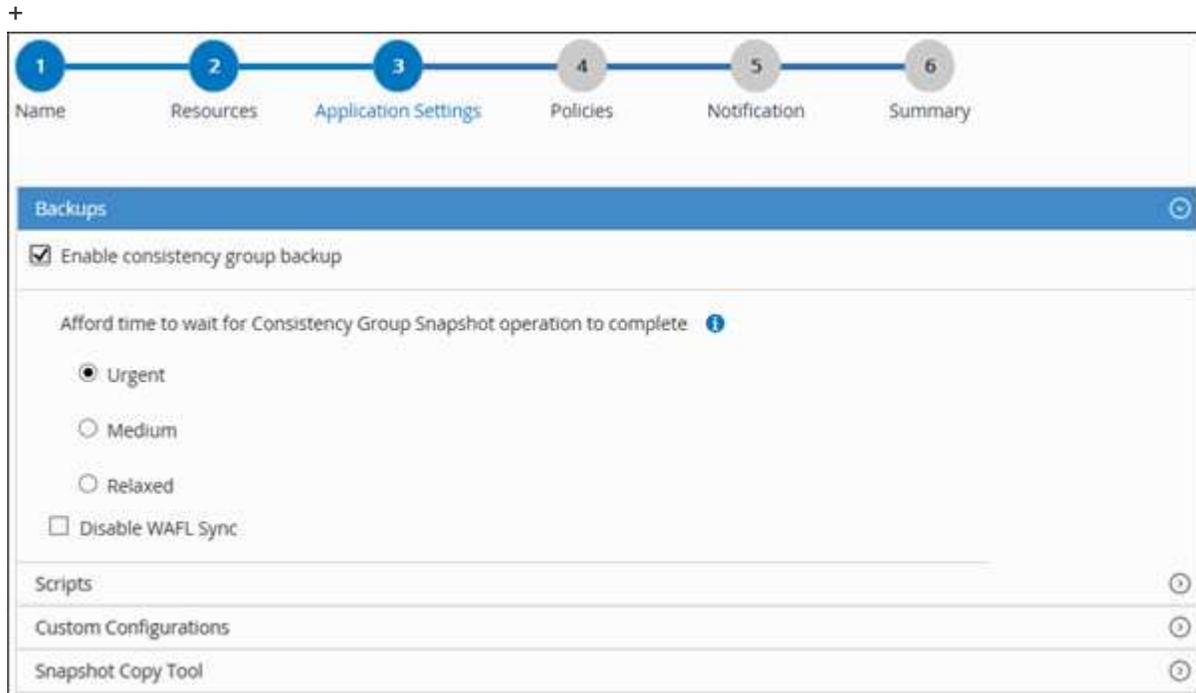
4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.

Cela aide à filtrer les informations affichées à l'écran.

5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page Paramètres de l'application, procédez comme suit :
  - a. Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde de groupe de cohérence et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Attendez la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , <b>Moyen</b> ou <b>relâché</b> pour spécifier le temps d'attente pour l'exécution de l'opération de snapshot.  Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.



- Cliquez sur la flèche **scripts** et entrez les commandes pré et post pour les opérations quiesce, snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- Cliquez sur la flèche **configurations personnalisées** et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.

Paramètre	Réglage	Description
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés.  Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.
ARCHIVE_LOG_EXT	extension_fichier	Spécifie la longueur d'extension du fichier journal d'archives.  Par exemple, si le journal d'archives est log_backup_0_0_0_0.1615185519429 et si la valeur file_extension est 5, l'extension du journal conserve 5 chiffres, soit 16151.
ARCHIVE_LOG_RÉCURSIVE_SE ARCH	(O/N)	Permet la gestion des journaux d'archivage dans les sous-répertoires.  Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.



Les paires clé-valeur personnalisées sont prises en charge pour les systèmes de plug-in PostgreSQL Linux et ne sont pas prises en charge pour les clusters PostgreSQL enregistrés en tant que plug-in Windows centralisé.

c. Cliquez sur la flèche **Snapshot Copy Tool** pour sélectionner l'outil de création de snapshots :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et mettre le système de fichiers dans un état cohérent avant de créer un snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
SnapCenter pour créer un snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
Pour saisir la commande à exécuter sur l'hôte afin de créer des copies Snapshot.	Sélectionnez <b>autre</b> , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.

7. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Les stratégies sont répertoriées dans la section Configuration des planifications pour les stratégies sélectionnées.

- b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.

Où, nom\_stratégie est le nom de la règle que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **programmes appliqués**.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Le serveur SMTP doit être configuré dans **Paramètres > Paramètres globaux**.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire des ressources PostgreSQL sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la

fonction **Secondaryprotection** est activée.

- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

- 8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

- a. Sélectionnez le type de la règle de réplication.

 Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.
- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.

 Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.

 Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

- 1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de

stockage secondaire.

e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtPServer`.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour PostgreSQL

Vous devez créer une connexion SVM (Storage Virtual machine) et des informations d'identification avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner les clusters PostgreSQL.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-in d'hôte ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache d'hôte peut ne pas être mis à jour et l'état des clusters peut être affiché dans l'interface graphique de SnapCenter comme « non disponible pour la sauvegarde » ou « pas sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

### Étapes

1. Lancez une session de connexion PowerShell Core à l'aide de l'applet de commande `Open-SmConnection`.

```
PS C:\> Open-SmConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-`

SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande Add-SmCredential.

Cet exemple montre comment créer un nouvel identifiant nommé FinanceAdmin avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Ajoutez l'hôte de communication PostgreSQL au serveur SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode PostgreSQL
```

5. Installez le package et le plug-in SnapCenter pour PostgreSQL sur l'hôte.

Pour Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL
```

Pour Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FileSystemCode scw -RunAsName FinanceAdmin
```

6. Définissez le chemin d'accès à SQLLIB.

Pour Windows, le plug-in PostgreSQL utilisera le chemin par défaut du dossier SQLLIB : « C:\Program Files\IBM\SQLLIB\BIN »

Si vous souhaitez remplacer le chemin par défaut, utilisez la commande suivante.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{ "PostgreSQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN" }
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de](#)

## Sauvegardez PostgreSQL

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Avant de commencer

- Vous devez avoir créé une stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.
- Pour l'opération de sauvegarde basée sur des copies Snapshot, vérifiez que tous les clusters de locataires sont valides et actifs.
- Pour les commandes PRE et post pour les opérations quiesce, Snapshot et unquiesce, vous devez vérifier que les commandes existent dans la liste de commandes disponible sur l'hôte plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Sélectionnez \* , puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Sélectionnez la ressource à sauvegarder.
4. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page Paramètres de l'application, procédez comme suit :

- Sélectionnez la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde du groupe de cohérence, si nécessaire, et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Temps d'attente avant la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , ou <b>Moyen</b> , ou <b>détendu</b> pour spécifier le temps d'attente pour la fin de l'opération Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

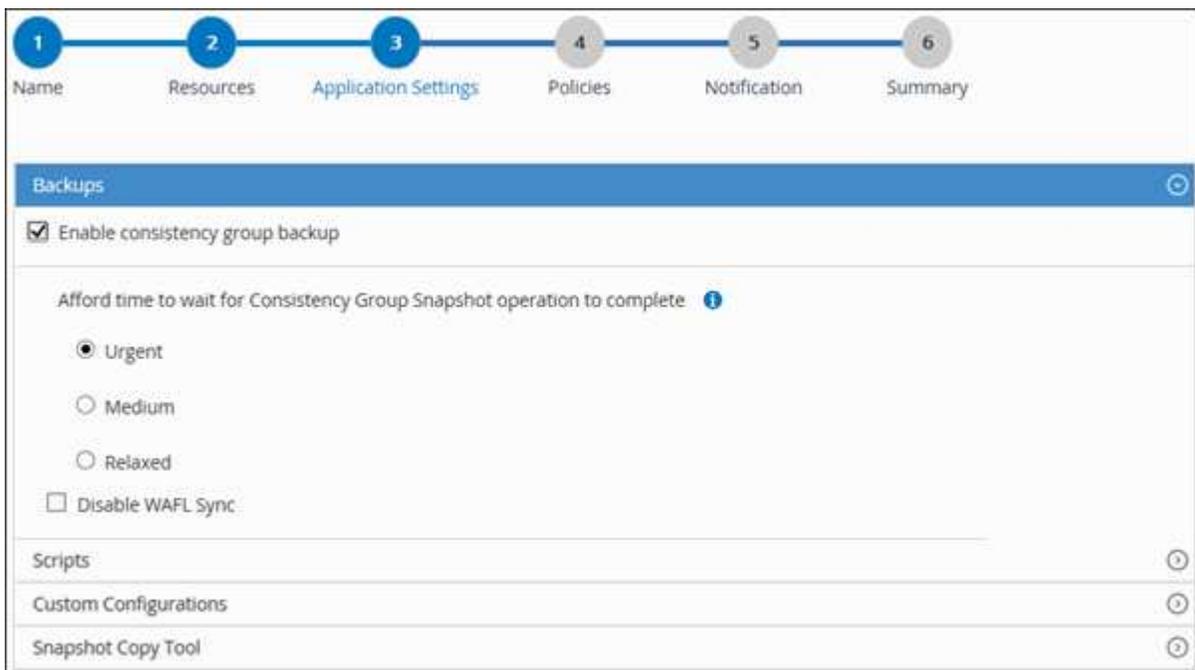
- Sélectionnez la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce.

Vous pouvez également exécuter des pré-commandes avant de quitter l'opération de sauvegarde. Des préscripts et des postscripts sont exécutés sur le serveur SnapCenter.

- Sélectionnez la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- Sélectionner la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows afin de mettre le système de fichiers dans un état cohérent, puis de créer un Snapshot	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
Pour saisir la commande permettant de créer un Snapshot	Sélectionnez <b>autre</b> , puis entrez la commande pour créer un instantané.



6. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Sélectionnez \* \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres > Paramètres globaux**.

8. Passez en revue le résumé, puis sélectionnez **Terminer**.

La page topologie des ressources s'affiche.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

Pour plus d'informations, voir : ["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer.

Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, la commande `do_start method` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante :  
`Java -jar -Xmx8192M -Xms4096M`

## Applets de commande PowerShell

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
PS C:\> Open-SmConnection
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Ajoutez des ressources manuelles à l'aide de l'applet de commande `Add-SmResources`.

Cet exemple montre comment ajouter une instance PostgreSQL :

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.
4. Protégez la ressource ou ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.
5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet New-SmBackup.

Cet exemple montre comment sauvegarder un groupe de ressources :

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
-Policy postgresql_policy1
```

Cet exemple sauvegarde une ressource protégée :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
-Policy postgresql_policy2
```

6. Surveillez l'état du travail (en cours d'exécution, terminé ou en échec) à l'aide de l'applet de commande Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Surveillez les détails de la tâche de sauvegarde comme ID de sauvegarde, nom de sauvegarde pour effectuer une opération de restauration ou de clonage à l'aide de l'applet de commande Get-SmBackupReport.

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects : {DB1}
FailedObjects : {}
IsScheduled : False
HasMetadata : False
SmBackupId : 269
SmJobId : 2361
StartDateTime : 10/4/2016 11:20:45 PM
EndDateTime : 10/4/2016 11:21:32 PM
Duration : 00:00:46.2536470
CreatedDateTime : 10/4/2016 11:21:09 PM
Status : Completed
ProtectionGroupName : Verify_ASUP_Message_windows
SmProtectionGroupId : 211
PolicyName : test2
SmPolicyId : 20
BackupName : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus : NotVerified
VerificationStatuses :
SmJobError :
BackupType : SCC_BACKUP
CatalogingStatus : NotApplicable
CatalogingStatuses :
ReportDataCreatedDateTime :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarder les groupes de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

### Description de la tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une

stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en sélectionnant  , puis en  sélectionnant la balise. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Surveillez les opérations de sauvegarde PostgreSQL

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.

- b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Surveillez les opérations de protection des données sur les clusters PostgreSQL dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

## Annulez les opérations de sauvegarde pour PostgreSQL

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

### Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

### Étapes

1. Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li></ol>
Volet activité	<ol style="list-style-type: none"><li>Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li><li>Sélectionner l'opération.</li><li>Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li></ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Affichez les sauvegardes et clones PostgreSQL dans la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire.

### Description de la tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.



Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la **carte Résumé** pour afficher un résumé du nombre de sauvegardes et de clones disponibles sur le stockage primaire et secondaire.

La section **carte récapitulative** affiche le nombre total de sauvegardes basées sur des copies Snapshot et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Après une sauvegarde à la demande, en cliquant sur le bouton **Refresh**, vous actualisez les détails de la sauvegarde ou du clone.

5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

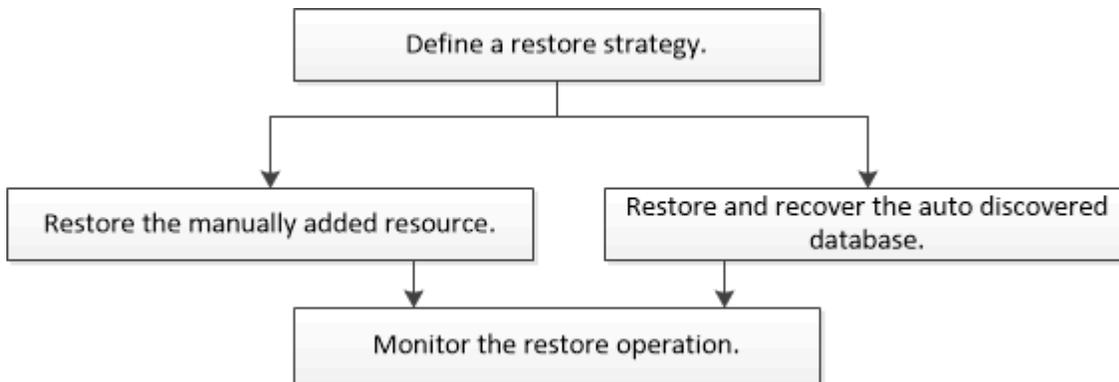
7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur .
8. Si vous souhaitez diviser un clone, sélectionnez-le dans le tableau, puis cliquez sur .

## Restaurer PostgreSQL

## Restaurer le flux de travail

Le workflow de restauration et de reprise comprend la planification, la réalisation des opérations de restauration et la surveillance des opérations.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
  - Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur



Backup Name	End Date
rg1_scipr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource**.

- a. Si vous sélectionnez **Complete Resource**, tous les volumes de données configurés du cluster PostgreSQL sont restaurés.

Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

Vous pouvez sélectionner plusieurs LUN.



Si vous sélectionnez **tous**, tous les fichiers des volumes, qtrees ou LUN sont restaurés.

7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurez et récupérez une sauvegarde de cluster découverte automatiquement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :

- Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
- Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

## Description de la tâche

- Les copies de sauvegarde basées sur des fichiers ne peuvent pas être restaurées depuis SnapCenter.
- Pour les ressources découvertes automatiquement, la restauration est prise en charge par SFSR.
- La récupération automatique n'est pas prise en charge.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).

5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur .

Primary Backup(s)	
Backup Name	End Date
rg1_scapr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource** pour restaurer les volumes de données configurés du cluster PostgreSQL.

7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :

Si...	Procédez comme ça...
Vous souhaitez effectuer une restauration aussi proche que possible de l'heure actuelle	Sélectionnez <b>récupérer à l'état le plus récent</b> . Pour les ressources de conteneur unique, spécifiez un ou plusieurs emplacements de sauvegarde de journaux et de catalogues.
Vous souhaitez effectuer une restauration au point dans le temps spécifié	Sélectionnez <b>récupérer à un point dans le temps</b> .  a. Entrez la date et l'heure. Entrez la date et l'heure. Par exemple, l'hôte Linux PostgreSQL se trouve à Sunnyvale, en Californie, et l'utilisateur de Raleigh, en Caroline du Nord, récupère les journaux dans SnapCenter.  Si l'utilisateur souhaite effectuer une récupération à 5 a.m . Sunnyvale, CA, alors l'utilisateur doit définir le fuseau horaire du navigateur sur le fuseau horaire de l'hôte PostgreSQL Linux, qui est GMT-07:00 et spécifier la date et l'heure à 5:00
Ne pas récupérer	Sélectionnez <b>pas de récupération</b> .



Vous ne pouvez pas récupérer les ressources PostgreSQL ajoutées manuellement.



Le plug-in SnapCenter pour PostgreSQL crée une étiquette `_sauvegarde` et une table `_map` dans le dossier `/<OS_temp_folder>/postgresql_sc_Recovery<Restore_JobId>/_` pour faciliter la restauration manuelle.

1. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

2. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

3. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

4. Vérifiez le résumé, puis cliquez sur **Terminer**.

5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Restaurer des ressources à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de ressources inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande `Get-SmBackup` and `get-SmBackupReport`.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveillez les opérations de restauration PostgreSQL

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours

-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

# Cloner les sauvegardes de ressources PostgreSQL

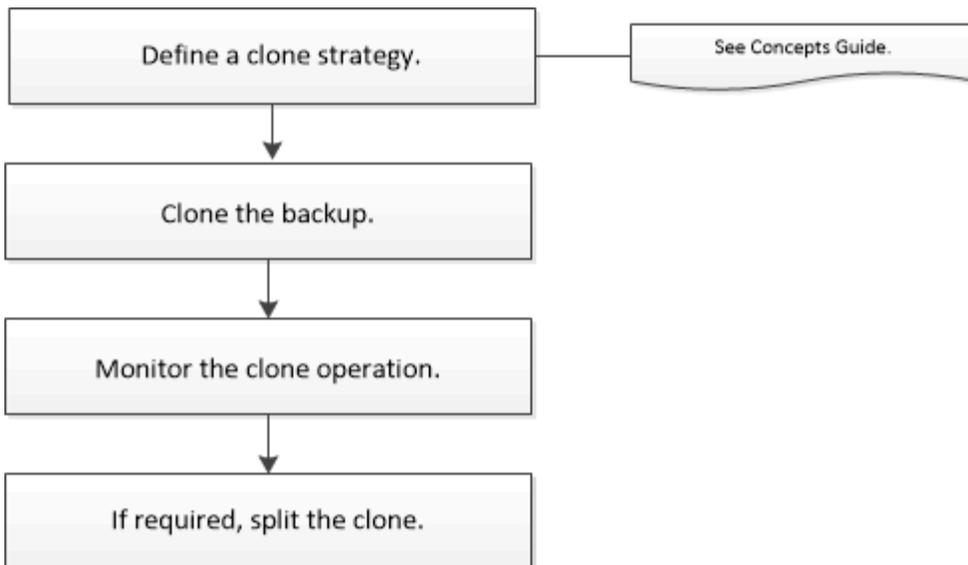
## Workflow de clonage

Le workflow de clonage inclut la réalisation de l'opération de clonage et le contrôle de l'opération.

### Description de la tâche

- Vous pouvez cloner sur le serveur PostgreSQL source.
- Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :
  - Tester les fonctionnalités à implémenter à l'aide de la structure de ressources actuelle et du contenu pendant les cycles de développement d'applications
  - Pour les outils d'extraction et de manipulation de données lors du remplissage d'entrepôts de données
  - Pour récupérer les données qui ont été supprimées ou modifiées par erreur

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

## Cloner une sauvegarde PostgreSQL

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde. Vous pouvez cloner à partir d'une sauvegarde principale ou secondaire.

### Avant de commencer

- Vous devriez avoir sauvegardé les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Pour les commandes pré-clone ou post-clone, vérifiez si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
  - Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à ["Séparer un volume FlexClone de son volume parent"](#) la section, .
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources s'affichent avec des informations telles que le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

3. Sélectionnez la ressource ou le groupe de ressources.

Vous devez sélectionner une ressource si vous sélectionnez un groupe de ressources.

La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Serveur clone	Choisissez l'hôte sur lequel le clone doit être créé.
Port cible	Entrez le port cible PostgreSQL à cloner à partir des sauvegardes existantes.
Adresse IP d'exportation NFS	Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.  Cela s'applique uniquement à la ressource de type de stockage NFS.
Capacité du pool max. Débit (Mio/s)	Entrez le débit maximal d'un pool de capacité.  Cela s'applique uniquement aux ressources de type de stockage ANF.

7. Dans la page scripts, effectuez les opérations suivantes :



Les scripts sont exécutés sur l'hôte du plug-in.

- a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
  - Commande pré-clonage : supprimez les clusters existants portant le même nom
  - Commande post-clonage : vérification d'un cluster ou démarrage d'un cluster

b. Entrez la commande mount pour monter un système de fichiers sur un hôte.

Commande mount pour un volume ou un qtree sur une machine Linux :

Exemple pour NFS : `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Récupérez les sauvegardes pour effectuer l'opération de clonage à l'aide de l'applet de commande Get-SmBackup.

Cet exemple montre que deux sauvegardes sont disponibles pour le clonage :

```
C:\PS> Get-SmBackup

 BackupId BackupName

BackupTime BackupType

1 Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM Full Backup
2 Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM
```

3. Lancez une opération de clonage à partir d'une sauvegarde existante et spécifiez les adresses IP d'exportation NFS sur lesquelles les volumes clonés sont exportés.

Cet exemple montre que la sauvegarde à cloner a une adresse NFSExportalIP de 10.32.212.14 :

Pour le cluster PostgreSQL :

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```



Si NFSExportIPS n'est pas spécifié, la valeur par défaut est exportée vers l'hôte cible du clone.

4. Vérifiez que les sauvegardes ont été correctement clonées à l'aide de l'applet de commande Get-SmCloneReport pour afficher les détails du travail clone.

Vous pouvez afficher des informations telles que l'ID de clone, la date et l'heure de début, la date et l'heure de fin.

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError :
```

## Surveillez les opérations de clonage PostgreSQL

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur \* \* .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCORE redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCORE interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

#### Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

## Supprimez ou répartissez les clones de cluster PostgreSQL après la mise à niveau de SnapCenter

Après la mise à niveau vers SnapCenter 4.3, vous ne verrez plus les clones. Vous pouvez supprimer le clone ou séparer les clones de la page topologie de la ressource à partir de laquelle les clones ont été créés.

#### Description de la tâche

Si vous souhaitez localiser l’empreinte de stockage des clones masqués, exécutez la commande suivante :

```
Get-SmClone -ListStorageFootprint
```

### Étapes

1. Supprimez les sauvegardes des ressources clonées à l’aide de la cmdlet `remove-smbackup`.
2. Supprimez le groupe de ressources des ressources clonées à l’aide de la cmdlet `remove-smresregroupement`.
3. Supprimez la protection de la ressource clonée à l’aide de l’applet de commande `remove-smprotectResource`.
4. Sélectionnez la ressource parente dans la page Ressources.

La page topologie de ressources s’affiche.

5. Dans la vue `Manage copies` (gérer les copies), sélectionnez les clones dans les systèmes de stockage principal ou secondaire (en miroir ou répliqué).
6. Sélectionnez les clones, puis cliquez sur  pour supprimer les clones ou sur  pour les séparer.
7. Cliquez sur **OK**.

# Protéger MySQL

## Plug-in SnapCenter pour MySQL

### Présentation du plug-in SnapCenter pour MySQL

Le plug-in SnapCenter pour la base de données MySQL est un composant côté hôte du logiciel NetApp SnapCenter qui permet la gestion de la protection des données des bases de données MySQL intégrant la cohérence applicative. Le plug-in pour la base de données MySQL automatise la sauvegarde, la restauration et le clonage des bases de données MySQL dans votre environnement SnapCenter.

SnapCenter prend en charge les configurations MySQL à instance unique. Vous pouvez utiliser le plug-in pour la base de données MySQL dans les environnements Linux et Windows. Dans les environnements Windows, MySQL sera pris en charge en tant que ressource manuelle.

Une fois le plug-in pour la base de données MySQL installé, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies miroir des jeux de sauvegarde sur un autre volume. Vous pouvez également utiliser le plug-in doté de la technologie SnapVault de NetApp pour effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes.

Le plug-in SnapCenter pour MySQL prend en charge NFS et SAN sur les infrastructures de stockage de fichiers ONTAP et Azure NetApp.

L'organisation du stockage virtuel VMDK, vVol et RDM est prise en charge.

Les liens symboliques ne sont pas pris en charge.

### Ce que vous pouvez faire en utilisant le plug-in SnapCenter pour MySQL

Lorsque vous installez le plug-in pour la base de données MySQL dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner des instances MySQL. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Ajouter des instances.
- Création de sauvegardes.
- Effectuez des restaurations à partir des sauvegardes.
- Sauvegardes clones.
- Planifiez les opérations de sauvegarde.
- Contrôle des opérations de sauvegarde, de restauration et de clonage
- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.

### Plug-in SnapCenter pour les fonctionnalités MySQL

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour travailler avec le plug-in pour la base de données MySQL,

vous utilisez l'interface utilisateur graphique de SnapCenter.

- **Interface utilisateur graphique unifiée**

L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

Vous pouvez planifier des opérations de sauvegarde, configurer la conservation des sauvegardes basée sur des règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie de copie snapshot NetApp non disruptive**

SnapCenter utilise la technologie Snapshot de NetApp avec le plug-in pour la base de données MySQL pour sauvegarder les ressources.

L'utilisation du plug-in pour MySQL offre également les avantages suivants :

- Prise en charge des workflows de sauvegarde, de restauration et de clonage
- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Création de copies compactes et ponctuelles de ressources à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonctionnalité de snapshot de groupe de cohérence (CG) de ONTAP dans le cadre de la création des sauvegardes.
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

En une seule opération, les snapshots sont consolidés lorsque les ressources d'un hôte unique partagent le même volume.

- Possibilité de créer des instantanés à l'aide de commandes externes.
- Prise en charge de Linux LVM sur le système de fichiers XFS.

## **Types de stockage pris en charge par le plug-in SnapCenter pour MySQL**

SnapCenter prend en charge de nombreux types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier le support de votre type de stockage avant d'installer le plug-in SnapCenter pour MySQL.

Machine	Type de stockage
Serveur physique	<ul style="list-style-type: none"> <li>• LUN connectés via FC</li> <li>• LUN connectées à l'iSCSI</li> <li>• Volumes connectés par NFS</li> </ul>
VMware ESXi	<ul style="list-style-type: none"> <li>• L'exécution des LUN RDM connectés par un HBA FC ou iSCSI ESXi peut prendre du temps car SnapCenter analyse tous les adaptateurs de bus hôte présents dans l'hôte.</li> </ul> <p>Vous pouvez modifier le fichier <b>LinuxConfig.pm</b> situé à  <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> pour définir la valeur du paramètre <b>SCSI_HOSTS_OPTIMIZED_RESCAN</b> à 1 pour analyser uniquement les HBA répertoriés dans les NOMS de PILOTE HBA.</p> <ul style="list-style-type: none"> <li>• LUN iSCSI connectés directement au système invité par l'initiateur iSCSI</li> <li>• VMDK sur des datastores NFS</li> <li>• VMDK sur VMFS créés</li> <li>• Volumes NFS connectés directement au système invité</li> <li>• Datastores vVol sur NFS et SAN</li> </ul> <p>Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>

## Privilèges ONTAP minimum requis pour le plug-in MySQL

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - lun
  - la création de lun
  - la création de lun
  - la création de lun
  - suppression de la lun

- lun igroup add
- créez un groupe initiateur lun
- suppression du groupe initiateur lun
- renommer la lun igroup
- renommer la lun igroup
- affichage de la lun igroup
- lun mapping des nœuds supplémentaires
- création d'un mappage de lun
- suppression du mappage de lun
- mappage de lun supprimer-rapports-nœuds
- les mappages de lun s'affichent
- modification de lun
- déplacement des lun dans le volume
- lun hors ligne
- lun en ligne
- suppression de la réservation persistante de lun
- redimensionner la lun
- série de lun
- affichage de la lun
- ajout de règle snapmirror
- règle de modification de snapmirror
- règle de suppression de snapmirror
- affichage des règles snapmirror
- restauration snapmirror
- montrer snapmirror
- historique des données du mode snapmirror
- mise à jour snapmirror
- snapmirror update-ls-set
- destinations des listes snapmirror
- version
- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes

- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- volume snapshot modify-snaplock-expiration-time
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- iscsi vserver
- vserver iscsi connection show
- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau
  - interface réseau affiche

- un vserver

## Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour MySQL

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Stratégie de sauvegarde pour MySQL

### Définir une stratégie de sauvegarde pour MySQL

Définir une stratégie de sauvegarde avant de créer vos tâches de sauvegarde vous aide à disposer des sauvegardes dont vous avez besoin pour restaurer ou cloner vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

#### Description de la tâche

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

#### Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.

2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décidez si vous souhaitez créer une règle basée sur les copies Snapshot pour sauvegarder des copies Snapshot cohérentes au niveau des applications de la base de données.
5. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
6. Déterminer la période de conservation des snapshots sur le système de stockage source et la destination SnapMirror.
7. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescripteur ou un PostScript.

### **Découverte automatique des ressources sur l'hôte Linux**

Les ressources sont des instances MySQL sur l'hôte Linux qui sont gérées par SnapCenter. Après avoir installé le plug-in SnapCenter pour MySQL, les instances MySQL sur cet hôte Linux sont automatiquement découvertes et affichées dans la page Ressources.

### **Types de sauvegardes pris en charge**

Le type de sauvegarde spécifie le type de sauvegarde que vous souhaitez créer. SnapCenter prend en charge le type de sauvegarde basée sur la copie Snapshot pour les bases de données MySQL.

### **Sauvegarde basée sur des copies Snapshot**

Les sauvegardes basées sur des copies Snapshot utilisent la technologie Snapshot de NetApp pour créer des copies en ligne en lecture seule des volumes sur lesquels résident les bases de données MySQL.

### **Comment le plug-in SnapCenter pour MySQL utilise les snapshots de groupes de cohérence**

Vous pouvez utiliser le plug-in pour créer des snapshots de groupes de ressources. Un groupe de cohérence est un conteneur qui peut héberger plusieurs volumes, de sorte que vous puissiez les gérer comme une entité unique. Un groupe de cohérence est une copie instantanée de plusieurs volumes, fournissant ainsi des copies cohérentes d'un groupe de volumes.

Vous pouvez également spécifier le temps d'attente nécessaire au contrôleur de stockage pour regrouper les snapshots de manière cohérente. Les options de temps d'attente disponibles sont **urgent**, **Moyen** et **détendu**. Vous pouvez également activer ou désactiver la synchronisation WAFL (Write Anywhere File Layout) lors d'une opération de snapshot de groupe cohérente. WAFL Sync améliore les performances d'un snapshot de groupe de cohérence.

### **Comment SnapCenter gère la gestion des sauvegardes de journaux**

SnapCenter gère la gestion des sauvegardes de données au niveau du système de stockage et du système de fichiers.

## Considérations pour déterminer les plannings de sauvegarde pour MySQL

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes (fréquence des sauvegardes)

La fréquence de sauvegarde, également appelée type de planification pour certains plug-ins, fait partie d'une configuration de règles. Par exemple, vous pouvez configurer la fréquence des sauvegardes sous forme horaire, quotidienne, hebdomadaire ou mensuelle.

- Plannings de sauvegarde (exactement au moment où les sauvegardes doivent être effectuées)

Les planifications de sauvegarde font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour la sauvegarder tous les jeudis à 10 h 00

## Nombre de tâches de sauvegarde nécessaires pour MySQL

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

## Conventions de dénomination des sauvegardes pour le plug-in pour les bases de données MySQL

Vous pouvez utiliser la nomenclature établie par défaut des snapshots ou une nomenclature établie personnalisée. La convention de dénomination des sauvegardes par défaut ajoute un horodatage aux noms des snapshots pour vous aider à identifier la date de création des copies.

Le Snapshot utilise la nomenclature établie par défaut suivante :

```
resourcegroupname_hostname_timestamp
```

Vous devez nommer vos groupes de ressources de sauvegarde de manière logique, comme dans l'exemple suivant :

```
dts1_mach1x88_03-12-2015_23.17.26
```

Dans cet exemple, les éléments de syntaxe ont la signification suivante :

- *dts1* est le nom du groupe de ressources.
- *mach1x88* est le nom d'hôte.

- 03-12-2015\_23.17.26 est la date et l'horodatage.

Vous pouvez également spécifier le format du nom de l'instantané tout en protégeant les ressources ou les groupes de ressources en sélectionnant **utiliser le format de nom personnalisé pour la copie Snapshot**. Par exemple, clienttext\_resourcegroup\_policy\_hostname ou resourcegroup\_hostname. Par défaut, le suffixe de l'horodatage est ajouté au nom du Snapshot.

## Stratégie de restauration et de récupération pour MySQL

### Définir une stratégie de restauration et de récupération pour les ressources MySQL

Vous devez définir une stratégie avant de restaurer et de récupérer votre base de données pour que vous puissiez effectuer correctement les opérations de restauration et de récupération.



Seule la récupération manuelle de la base de données est prise en charge.

#### Étapes

1. Déterminez les stratégies de restauration prises en charge pour les ressources MySQL ajoutées manuellement
2. Déterminez les stratégies de restauration prises en charge pour les bases de données MySQL découvertes automatiquement
3. Choisissez le type d'opérations de restauration à effectuer.

### Types de stratégies de restauration prises en charge pour les ressources MySQL ajoutées manuellement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les ressources MySQL ajoutées manuellement.



Vous ne pouvez pas récupérer les ressources MySQL ajoutées manuellement.

#### Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

### Type de stratégie de restauration pris en charge pour MySQL découvert automatiquement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter.

La restauration complète des ressources est la stratégie de restauration prise en charge pour les bases de données MySQL découvertes automatiquement. Cette opération restaure tous les volumes, qtrees et LUN d'une ressource.

## Types d'opérations de restauration pour MySQL découvert automatiquement

Le plug-in SnapCenter pour MySQL prend en charge les types de restauration Single File SnapRestore et Connect-and-copy pour les bases de données MySQL découvertes automatiquement.

Single File SnapRestore s'effectue dans des environnements NFS pour les scénarios suivants :

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde sélectionnée provient d'un emplacement secondaire SnapMirror ou SnapVault et que l'option **Complete Resource** est sélectionnée

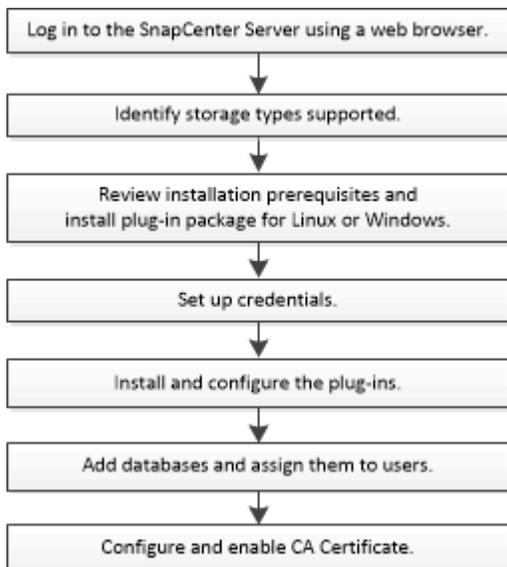
Single File SnapRestore s'effectue dans des environnements SAN pour les scénarios suivants :

- Si seule l'option **ressource complète** est sélectionnée
- Lorsque la sauvegarde est sélectionnée depuis un emplacement secondaire SnapMirror ou SnapVault et l'option **Complete Resource** est sélectionnée

## Préparez-vous à installer le plug-in SnapCenter pour MySQL

### Workflow d'installation du plug-in SnapCenter pour MySQL

Vous devez installer et configurer le plug-in SnapCenter pour MySQL si vous voulez protéger les bases de données MySQL.



### Conditions préalables pour ajouter des hôtes et installer le plug-in SnapCenter pour MySQL

Avant d'ajouter un hôte et d'installer les modules d'extension, vous devez remplir toutes les conditions requises. Le plug-in SnapCenter pour MySQL est disponible dans les environnements Windows et Linux.

- Vous devez avoir installé Java 11 sur votre hôte.



IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Pour Windows, le service de création de plug-in doit être exécuté à l'aide de l'utilisateur Windows « LocalSystem », qui est le comportement par défaut lorsque Plug-in pour MySQL est installé en tant qu'administrateur de domaine.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte. Le plug-in SnapCenter pour Microsoft Windows sera déployé par défaut avec le plug-in MySQL sur les hôtes Windows.
- Le serveur SnapCenter doit avoir accès au port 8145 ou personnalisé du plug-in pour l'hôte MySQL.
- Pour MySQL 5.7, binlog doit être spécifié dans le fichier mysql config (my.cnf ou mysql-Server.cnf).

## Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Lors de l'installation du plug-in pour MySQL sur un hôte Windows, le plug-in SnapCenter pour Microsoft Windows est installé automatiquement.
- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Windows.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Matrice d'interopérabilité NetApp"](#)

## Hôtes Linux

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

["Télécharger JAVA pour tous les systèmes d'exploitation"](#)

["Matrice d'interopérabilité NetApp"](#)

- Pour les bases de données MySQL qui s'exécutent sur un hôte Linux, lors de l'installation de Plug-in pour MySQL, SnapCenter Plug-in pour UNIX est installé automatiquement.
- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

## Commandes supplémentaires

Pour exécuter une commande supplémentaire sur le plug-in SnapCenter pour MySQL, vous devez l'inclure dans le fichier *allowed\_commands.config*.

- Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
- Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*

Pour autoriser des commandes supplémentaires sur l'hôte du plug-in, ouvrez le fichier

*allowed\_commands.config* dans un éditeur. Entrez chaque commande sur une ligne distincte et les commandes ne sont pas sensibles à la casse. Assurez-vous de spécifier le chemin d'accès complet et de le joindre entre guillemets (") s'il contient des espaces.

Par exemple :

Commande : mount command : commande umount : « C:\Program Files\NetApp\SnapCreator  
commands\sdcli.exe » commande : myscript.bat

Si le fichier *allowed\_commands.config* n'est pas présent, les commandes ou l'exécution du script seront bloquées et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »

Si la commande ou le script n'est pas présent dans *allowed\_commands.config*, l'exécution de la commande ou du script sera bloquée et le flux de travail échouera avec l'erreur suivante :

"[/mnt/mount -a] exécution non autorisée. Autoriser en ajoutant la commande dans le fichier %s sur l'hôte du plug-in. »



Vous ne devez pas utiliser de caractère générique (\*) pour autoriser toutes les commandes.

## Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte Linux

SnapCenter permet à un utilisateur non root d'installer le package de plug-ins SnapCenter pour Linux et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Si umask est 0027, assurez-vous que le dossier Java et tous les fichiers à l'intérieur doivent avoir la permission de 555. Sinon, l'installation du plug-in risque d'échouer.
- Pour l'utilisateur non root, assurez-vous que le nom de l'utilisateur non root et le groupe de l'utilisateur doivent être identiques.
- Modifiez le fichier */etc/ssh/sshd\_config* pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

## À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- /Home/*LINUX\_USER*/.sc\_netapp/snapcenter\_linux\_host\_plugin.bin
- /Custom\_location/NetApp/snapcenter/spl/installation/plugins/désinstaller
- /Custom\_location/NetApp/snapcenter/spl/bin/spl

## Étapes

1. Connectez-vous à l'hôte Linux sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour Linux.
2. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`LINUX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` \_ si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` \_ si le serveur SnapCenter est installé sur un hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

## Configuration requise pour l'installation du module de plug-ins SnapCenter pour Linux

Avant d'installer le module de plug-ins SnapCenter pour Linux, vous devez connaître certains besoins en espace système hôte de base et en dimensionnement.

Élément	De formation
<p>Systemes d'exploitation</p>	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>
<p>RAM minimale pour le plug-in SnapCenter sur l'hôte</p>	<p>1 GO</p>
<p>Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte</p>	<p>2 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
<p>Packs logiciels requis</p>	<p>Java 11 Oracle Java et OpenJDK</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le "<a href="#">Matrice d'interopérabilité NetApp</a>".</p>

## Configurez les informations d'identification pour le plug-in SnapCenter pour MySQL

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

### Description de la tâche

- Hôtes Linux

Vous devez configurer les informations d'identification pour l'installation des plug-ins sur les hôtes Linux.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

**Meilleure pratique:** bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>Administrateur de domaine ou tout membre du groupe d'administrateurs</li> </ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li><i>NetBIOS\username</i></li> <li><i>Domain FQDN\username</i></li> </ul> <ul style="list-style-type: none"> <li>Administrateur local (groupes de travail uniquement)</li> </ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p> <p>N'utilisez pas de guillemets (") ou de contre-coches (") dans les mots de passe. Vous ne devez pas utiliser moins de (&lt;) et un point d'exclamation (!) symboles ensemble dans les mots de passe. Par exemple, moins&lt;!10, moins dix&lt;!, contre-recul 12.</p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Mode d'authentification	Sélectionnez le mode d'authentification que vous souhaitez utiliser.
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p> <div style="display: flex; align-items: center; margin-top: 10px;"> <div style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin-right: 10px;"> <span style="font-size: 18px; font-weight: bold;">i</span> </div> <div> <p>Applicable uniquement aux utilisateurs Linux.</p> </div> </div>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs de la page utilisateur et accès.

## Installez le plug-in SnapCenter pour MySQL

### Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter l'hôte et installer des modules d'extension pour un hôte individuel.

#### Avant de commencer

- Si le système d'exploitation de l'hôte du serveur SnapCenter est Windows 2019 et que le système d'exploitation de l'hôte du plug-in est Windows 2022, effectuez les opérations suivantes :
  - Mise à niveau vers Windows Server 2019 (se Build 17763.5936) ou version ultérieure
  - Mise à niveau vers Windows Server 2022 (se Build 20348.2402) ou version ultérieure
- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- La documentation d'administration contient des informations sur la gestion des hôtes.

#### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	Sélectionnez le type d'hôte : <ul style="list-style-type: none"><li>• Répertoires de base</li><li>• Linux</li></ul> <div style="display: flex; align-items: center;"><p>Le plug-in pour MySQL doit être installé sur le serveur de base de données MySQL.</p></div>

Pour ce champ...	Procédez comme ça...
Nom d'hôte	Entrez le nom d'hôte de communication. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte. SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification. Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez fourni.</p> <div data-bbox="873 884 927 940" style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;">  </div> <p style="margin-left: 20px;">Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p>

- Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.

Lorsque vous utilisez l'API REST pour installer Plug-in pour MySQL, vous devez passer la version 3.0. Par exemple, MySQL:3.0

- (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port. Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div data-bbox="873 1646 927 1703" style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;">  </div> <p style="margin-left: 20px;">Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p>

Pour ce champ...	Procédez comme ça...
Chemin d'installation	<p>Le plug-in pour MySQL est installé sur l'hôte client MySQL, et cet hôte peut se trouver sur un système Windows ou Linux.</p> <ul style="list-style-type: none"> <li>• Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter. Vous pouvez également personnaliser le chemin.</li> <li>• Pour le package de plug-ins SnapCenter pour Linux, le chemin par défaut est /opt/NetApp/snapcenter. Vous pouvez également personnaliser le chemin.</li> </ul>
Ignorer les vérifications de préinstallation	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.
Ajoutez tous les hôtes du cluster	Sans objet.
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	Sans objet.

## 7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse C:\Program Files\NetApp\SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

## 8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

## 9. Surveillez la progression de l'installation.

- Pour le plug-in Windows, les journaux d'installation et de mise à niveau se trouvent à l'adresse suivante : C:\Windows\SnapCenter plugin\Install<JOBID>\\_

- Pour le plug-in Linux, les journaux d'installation se trouvent à l'adresse suivante : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_` et les journaux de mise à niveau se trouvent à l'adresse : `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

### Une fois que vous avez terminé

Si vous souhaitez effectuer une mise à niveau vers la version SnapCenter 6.0, le plug-in PERL existant pour MySQL sera désinstallé du serveur de plug-in distant.

### Installez les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer simultanément les modules SnapCenter Plug-in pour Linux ou Windows sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage` PowerShell.

#### Avant de commencer

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez installer le module externe.

#### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande `Open-SmConnection`, puis saisissez vos informations d'identification.
3. Installez le plug-in sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

Vous pouvez utiliser l'option `-skipreccheck` lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

4. Saisissez vos informations d'identification pour l'installation à distance.

### Installez le plug-in SnapCenter pour MySQL sur les hôtes Linux à l'aide de l'interface de ligne de commande

Vous devez installer le plug-in SnapCenter pour la base de données MySQL à l'aide de l'interface utilisateur SnapCenter. Si votre environnement ne permet pas l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter, vous pouvez installer le plug-in pour la base de données MySQL en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande (CLI).

#### Avant de commencer

- Vous devez installer le plug-in pour la base de données MySQL sur chacun des hôtes Linux sur lesquels l'instance MySQL doit être protégée.
- L'hôte Linux sur lequel vous installez le plug-in SnapCenter pour la base de données MySQL doit répondre aux exigences du logiciel, de la base de données et du système d'exploitation.

La matrice d'interopérabilité (IMT) contient les dernières informations sur les configurations prises en charge.

### "Matrice d'interopérabilité NetApp"

- Le plug-in SnapCenter pour la base de données MySQL fait partie du package de plug-ins SnapCenter pour Linux. Avant d'installer SnapCenter Plug-ins Package pour Linux, vous devez avoir déjà installé SnapCenter sur un hôte Windows.

### Étapes

1. Copiez le fichier d'installation du pack de plug-ins SnapCenter pour Linux (snapcenter\_linux\_host\_plugin.bin) depuis C:\ProgramData\NetApp\SnapCenter\Package Repository vers l'hôte sur lequel vous souhaitez installer le plug-in pour MySQL.

Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in : `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
  - -DPORT spécifie le port de communication SMCore HTTPS.
  - -DSERVER\_IP spécifie l'adresse IP du serveur SnapCenter.
  - -DSERVER\_HTTPS\_PORT spécifie le port HTTPS du serveur SnapCenter.
  - -DUSER\_INSTALL\_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
  - DINSTALL\_LOG\_NAME indique le nom du fichier journal.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Editez le fichier `<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties`, puis ajoutez le paramètre `PLUGINS_ENABLED = MySQL:3.0`.
5. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande `Add-Smhost` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Surveillez l'état d'installation du plug-in pour MySQL

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

## Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section ["Comment générer un fichier CSR de certificat CA"](#).



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être

mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

## Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

### Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.
2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

## Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :

- a. Double-cliquez sur le certificat.
- b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
- c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
- d. Copiez les caractères hexadécimaux de la zone.
- e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

## 2. Effectuer les opérations suivantes à partir de PowerShell :

- a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

## Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Configurez le certificat CA pour le service SnapCenter MySQL Plug-ins sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier « keystore.jks », qui se trouve dans `/opt/NetApp/snapcenter/scc/etc` à la fois comme magasin de confiance et magasin de clés.

### Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Procédez de même pour la clé KEYSTORE\_PASS dans le fichier `agent.properties`.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

## Étapes

1. Accédez au dossier contenant le keystore du plug-in : `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaires pour le plug-in trust-store.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

## Étapes

1. Accédez au dossier contenant le keystore du plug-in `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
```

. Si le nom d'alias du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("\*", ",", "), remplacez le nom d'alias par un nom simple :

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
```

. Configurez le nom d'alias à partir du certificat CA dans le fichier `agent.properties`.

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in `trust-store`.

### Configurer la liste de révocation de certificats (CRL) pour les plug-ins

#### Description de la tâche

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est « `opt/NetApp/snapcenter/scc/etc/crl` ».

#### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `agent.properties` par rapport à la clé `CRL_PATH`.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

### Configurez le certificat d'autorité de certification pour le service de plug-ins MySQL SnapCenter sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier `keystore.jks`, qui se trouve dans `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc` à la fois comme magasin de confiance et magasin de clés.

### Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé `KEYSTORE_PASS`.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
```



Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks
```

Procédez de même pour la clé `KEYSTORE_PASS` dans le fichier `agent.properties`.

4. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

#### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
Keytool -import -trcaccts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

#### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du

plug-in.

## Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier *keystore.jks*.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore.jks -desstoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé `KEYSTORE_PASS` dans le fichier *agent.properties*.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configurez le nom d'alias à partir du certificat CA dans le fichier *agent.properties*.

Mettez cette valeur à jour par rapport à la clé `SCC_CERTIFICATE_ALIAS`.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in *trust-store*.

## Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

### Description de la tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section ["Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter"](#).
- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est *'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl'*.

### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier *agent.properties* par rapport à la clé `CRL_PATH`.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Préparation à la protection des données

### Conditions préalables à l'utilisation du plug-in SnapCenter pour MySQL

Avant d'utiliser le plug-in SnapCenter pour MySQL, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches requises.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.

- Installez Java 11 sur votre hôte Linux ou Windows.

Vous devez définir le chemin Java dans la variable de chemin d'environnement de la machine hôte.

- Configurer SnapMirror et SnapVault pour la réplication de sauvegarde.

## Utilisation des ressources, des groupes de ressources et des stratégies pour protéger MySQL

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des instances MySQL que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Les règles spécifient la fréquence des sauvegardes, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

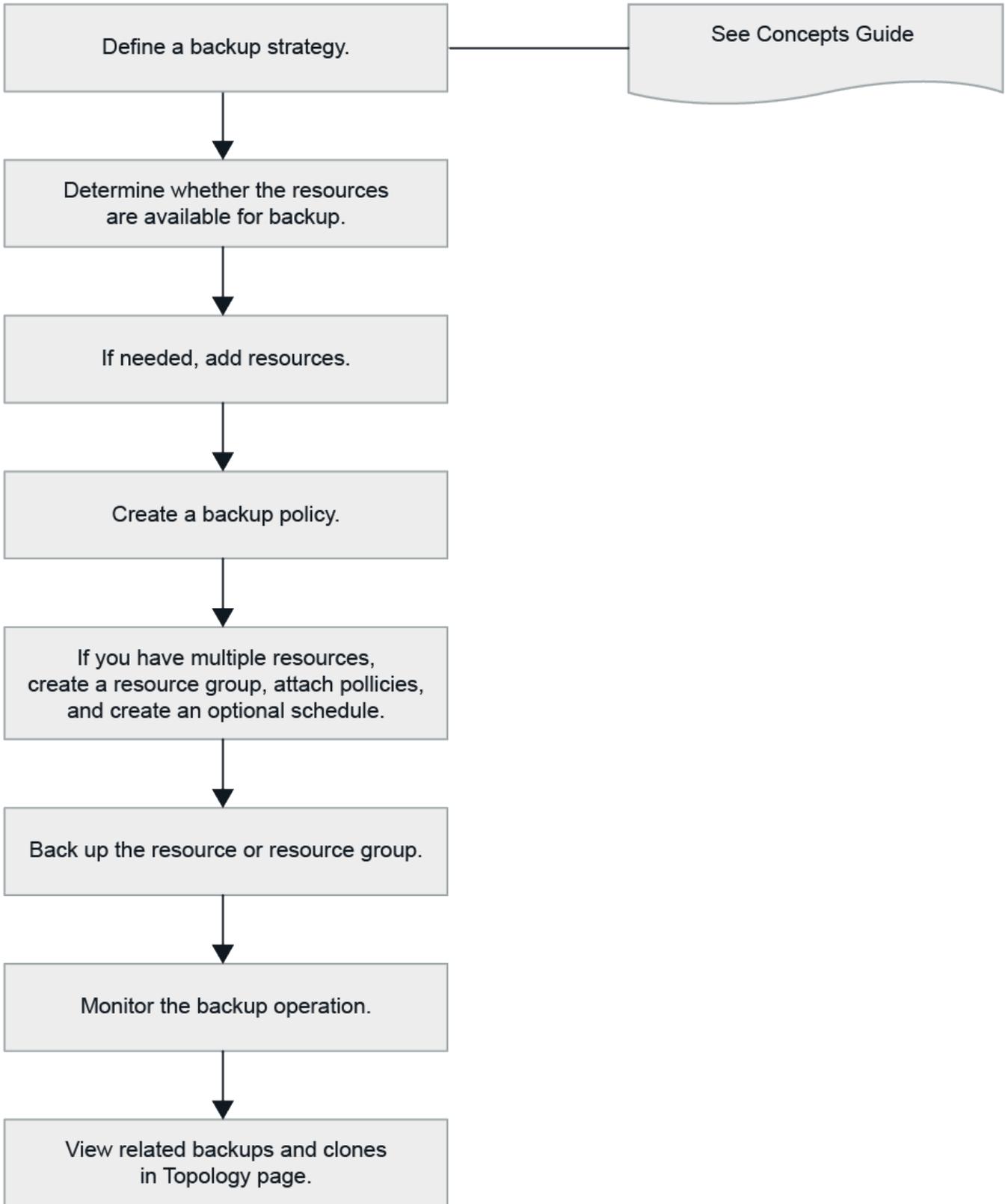
Considérez un groupe de ressources comme définissant ce que vous voulez protéger et quand vous voulez le protéger en termes de jour et d'heure. Considérez une stratégie comme une définition de la façon dont vous voulez la protéger. Si vous sauvegardez toutes les bases de données, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources de manière à effectuer une sauvegarde complète tous les jours.

## Sauvegarder les ressources MySQL

### Sauvegarder les ressources MySQL

Vous pouvez créer une sauvegarde d'une ressource (base de données) ou d'un groupe de ressources. Le workflow de sauvegarde inclut la planification, l'identification des bases de données pour la sauvegarde, la gestion des stratégies de sauvegarde, la création de groupes de ressources et la connexion de stratégies, la création de sauvegardes et le contrôle des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent plus d'informations sur les applets de commande

## Découvrir les bases de données automatiquement

Les ressources sont des bases de données MySQL gérées par SnapCenter sur l'hôte Linux. Vous pouvez ajouter les ressources aux groupes de ressources pour effectuer des opérations de protection des données après avoir découvert les bases de données MySQL disponibles.

### Avant de commencer

- Vous devez avoir déjà effectué des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions du système de stockage.
- Le plug-in SnapCenter pour MySQL ne prend pas en charge la découverte automatique des ressources résidant dans les environnements virtuels RDM/VMDK. Vous devez fournir les informations de stockage pour les environnements virtuels tout en ajoutant les bases de données manuellement.

### Description de la tâche

- Après avoir installé le plug-in, toutes les bases de données de cet hôte Linux sont automatiquement découvertes et affichées sur la page Ressources.
- Seules les bases de données sont découvertes automatiquement.

Les ressources détectées automatiquement ne peuvent pas être modifiées ou supprimées.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in pour MySQL dans la liste.
2. Dans la page Ressources, sélectionnez le type de ressource dans la liste vue.
3. (Facultatif) cliquez sur \* , puis sélectionnez le nom d'hôte.

Vous pouvez alors cliquer sur \*  pour fermer le volet de filtre.

4. Cliquez sur **Actualiser les ressources** pour découvrir les ressources disponibles sur l'hôte.

Les ressources s'affichent avec des informations telles que le type de ressource, le nom d'hôte, les groupes de ressources associés, le type de sauvegarde, les stratégies et l'état global.

- Si la base de données se trouve sur un système de stockage NetApp et qu'elle n'est pas protégée, elle s'affiche dans la colonne État global.
- Si la base de données se trouve sur un système de stockage NetApp et est protégée, et si aucune opération de sauvegarde n'est effectuée, alors l'option sauvegarde non exécutée s'affiche dans la colonne État global. Dans le cas contraire, l'état passe en échec de la sauvegarde ou la sauvegarde a réussi en fonction de l'état de la dernière sauvegarde.



Vous devez actualiser les ressources si les instances sont renommées en dehors de SnapCenter.

## Ajoutez des ressources manuellement au plug-in hôte

La découverte automatique n'est pas prise en charge sur l'hôte Windows. Vous devez ajouter des instances MySQL et des ressources de base de données manuellement.

## Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la configuration des connexions du système de stockage.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez le plug-in SnapCenter pour MySQL dans la liste déroulante, puis cliquez sur **Ressources**.
2. Dans la page Ressources, cliquez sur **Ajouter des ressources MySQL**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Spécifiez le nom de la base de données.
Nom d'hôte	Entrez le nom d'hôte.
Type	Sélectionnez une instance.
Fréquence	Sans objet
Informations d'identification	Sélectionnez les informations d'identification ou ajoutez-les.  Cette option est facultative.

4. Sur la page fournir l'empreinte du stockage, sélectionnez un type de stockage et choisissez un ou plusieurs volumes, LUN et qtrees, puis cliquez sur **Enregistrer**.

Facultatif : vous pouvez cliquer sur l'icône \*  pour ajouter d'autres volumes, LUN et qtrees à partir d'autres systèmes de stockage.

5. Facultatif : dans la page Paramètres de ressource, entrez des paires clé-valeur personnalisées pour le plug-in MySQL.
6. Vérifiez le résumé, puis cliquez sur **Terminer**.

Les bases de données sont affichées avec des informations telles que le nom d'hôte, les groupes de ressources et les stratégies associés, ainsi que l'état global

Si vous souhaitez donner aux utilisateurs l'accès aux ressources, vous devez affecter ces ressources aux utilisateurs. Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

["Ajoutez un utilisateur ou un groupe et attribuez un rôle et des ressources"](#)

Après avoir ajouté les bases de données, vous pouvez modifier les détails de la base de données MySQL.

## Créez des stratégies de sauvegarde pour MySQL

Avant d'utiliser SnapCenter pour sauvegarder des ressources MySQL, vous devez créer

une stratégie de sauvegarde pour le groupe de ressources ou de ressources que vous souhaitez sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes.

### Avant de commencer

- Vous devez avoir défini votre stratégie de sauvegarde.

Pour plus de détails, reportez-vous aux informations sur la définition d'une stratégie de protection des données pour les bases de données MySQL.

- Vous devez vous préparer à la protection des données en effectuant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la configuration des connexions du système de stockage et l'ajout de ressources.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir affecté des SVM aux volumes source et de destination.

En outre, vous pouvez spécifier des paramètres de réplication, de script et d'application dans la stratégie. Ces options vous permettent de gagner du temps lorsque vous souhaitez réutiliser la stratégie d'un autre groupe de ressources.

### Description de la tâche

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un plus grand nombre d'instantanés que le nombre spécifié dans la règle.
  - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez le type de stockage.
  - b. Dans la section Paramètres de sauvegarde personnalisés, indiquez tous les paramètres de sauvegarde spécifiques qui doivent être transmis au plug-in au format clé-valeur.

Vous pouvez fournir plusieurs valeurs de clé à transmettre au plug-in.

6. Dans la page instantané et réplication, effectuez les opérations suivantes :
  - a. Spécifiez le type d'horaire en sélectionnant **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.



Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais vous permet d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

- b. Dans la section Paramètres de l'instantané, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionné dans la page **Type de sauvegarde** :

Les fonctions que vous recherchez...	Alors...
Conserver un certain nombre d'instantanés	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> </div>
Conserver les instantanés pendant un certain nombre de jours	Sélectionnez <b>conserver les copies pour</b> , puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage des copies Snapshot principales	<p>Sélectionnez période de verrouillage des instantanés, puis sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>

Les fonctions que vous recherchez...	Alors...
Période de verrouillage des copies Snapshot secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.

c. Sélectionnez un libellé de stratégie.

Selon l'étiquette de règle que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à l'étiquette.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

7. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
<b>Mettre à jour SnapMirror après avoir créé une copie Snapshot locale</b>	<p>Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).</p> <p>Si la relation de protection dans ONTAP est de type miroir et coffre-fort et si vous sélectionnez uniquement cette option, le snapshot créé sur le primaire ne sera pas transféré vers la destination, mais sera répertorié dans la destination. Si cet instantané est sélectionné à partir de la destination pour effectuer une opération de restauration, le message d'erreur suivant s'affiche : l'emplacement secondaire n'est pas disponible pour la sauvegarde en miroir/en coffre-fort sélectionnée.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir <a href="#">"Afficher les sauvegardes et clones liés aux ressources MySQL dans la page topologie"</a>.</p>

Pour ce champ...	Procédez comme ça...
<b>Mettre à jour SnapVault après avoir créé une copie Snapshot locale</b>	<p>Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton <b>Actualiser</b> de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, reportez-vous à la section archivage des snapshots en mode WORM sur un coffre-fort destination</p> <p>Voir "<a href="#">Afficher les sauvegardes et clones liés aux ressources MySQL dans la page topologie</a>".</p>
<b>Nombre de tentatives d'erreur</b>	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer des groupes de ressources et attacher des stratégies

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du

SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.   Le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.  Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.
Utilisez un format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.  Par exemple, clienttext_Resource group_policy_hostname ou Resource group_hostname. Par défaut, un horodatage est ajouté au nom du snapshot.

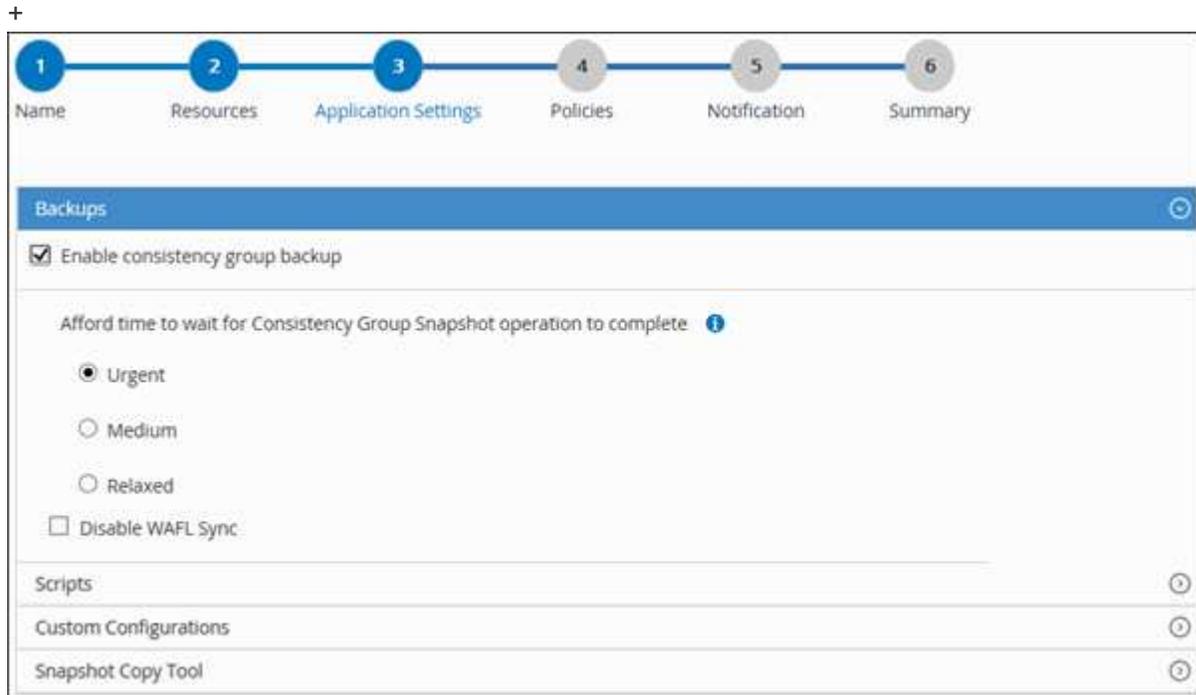
4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.

Cela aide à filtrer les informations affichées à l'écran.

5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page Paramètres de l'application, procédez comme suit :
  - a. Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde de groupe de cohérence et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Attendez la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , <b>Moyen</b> ou <b>relâché</b> pour spécifier le temps d'attente pour l'exécution de l'opération de snapshot.  Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.



- Cliquez sur la flèche **scripts** et entrez les commandes pré et post pour les opérations quiesce, snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- Cliquez sur la flèche **configurations personnalisées** et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.

Paramètre	Réglage	Description
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés.  Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.
ARCHIVE_LOG_EXT	extension_fichier	Spécifie la longueur d'extension du fichier journal d'archives.  Par exemple, si le journal d'archives est log_backup_0_0_0_0.1615185519429 et si la valeur file_extension est 5, l'extension du journal conserve 5 chiffres, soit 16151.
ARCHIVE_LOG_RÉCURSIVE_SE ARCH	(O/N)	Permet la gestion des journaux d'archivage dans les sous-répertoires.  Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.



Les paires clé-valeur personnalisées sont prises en charge pour les systèmes plug-in MySQL Linux et ne sont pas prises en charge pour la base de données MySQL enregistrée en tant que plug-in Windows centralisé.

c. Cliquez sur la flèche **Snapshot Copy Tool** pour sélectionner l'outil de création de snapshots :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et mettre le système de fichiers dans un état cohérent avant de créer un snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
SnapCenter pour créer un snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
Pour saisir la commande à exécuter sur l'hôte afin de créer des copies Snapshot.	Sélectionnez <b>autre</b> , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.

7. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Les stratégies sont répertoriées dans la section Configuration des planifications pour les stratégies sélectionnées.

- b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.

Où, nom\_stratégie est le nom de la règle que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne **programmes appliqués**.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Le serveur SMTP doit être configuré dans **Paramètres > Paramètres globaux**.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire des ressources MySQL sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la

fonction **Secondaryprotection** est activée.

- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

- 8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

- a. Sélectionnez le type de la règle de réplication.

 Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.
- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.

 Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.

 Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

- 1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de

stockage secondaire.

e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez une connexion au système de stockage et des informations d'identification à l'aide des applets de commande PowerShell pour MySQL

Vous devez créer une connexion de machine virtuelle de stockage (SVM) et un identifiant avant d'utiliser les applets de commande PowerShell pour sauvegarder, restaurer ou cloner les bases de données MySQL.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de données unique.

### Étapes

1. Lancez une session de connexion PowerShell Core à l'aide de l'applet de commande `Open-SmConnection`.

```
PS C:\> Open-SmConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-`

SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande Add-SmCredential.

Cet exemple montre comment créer un nouvel identifiant nommé FinanceAdmin avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Ajoutez l'hôte de communication MySQL au serveur SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode mysql
```

5. Installez le paquet et le plug-in SnapCenter pour MySQL sur l'hôte.

Pour Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
mysql
```

Pour Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. Définissez le chemin d'accès à SQLLIB.

Sous Windows, le plug-in MySQL utilise le chemin par défaut du dossier SQLLIB : « C:\Program Files\IBM\SQLLIB\BIN ».

Si vous souhaitez remplacer le chemin par défaut, utilisez la commande suivante.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{ "MySQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN" }
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de](#)

[référence de l'applet de commande du logiciel SnapCenter](#)".

## Sauvegardez MySQL

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Avant de commencer

- Vous devez avoir créé une stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.
- Pour l'opération de sauvegarde basée sur des copies Snapshot, vérifiez que toutes les bases de données des locataires sont valides et actives.
- Pour les commandes PRE et post pour les opérations quiesce, Snapshot et unquiesce, vous devez vérifier que les commandes existent dans la liste de commandes disponible sur l'hôte plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Sélectionnez \* , puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Sélectionnez la ressource à sauvegarder.
4. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

5. Dans la page Paramètres de l'application, procédez comme suit :

- Sélectionnez la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde du groupe de cohérence, si nécessaire, et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Temps d'attente avant la fin de l'opération de snapshot de groupe de cohérence	Sélectionnez <b>urgent</b> , ou <b>Moyen</b> , ou <b>détendu</b> pour spécifier le temps d'attente pour la fin de l'opération Snapshot. Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

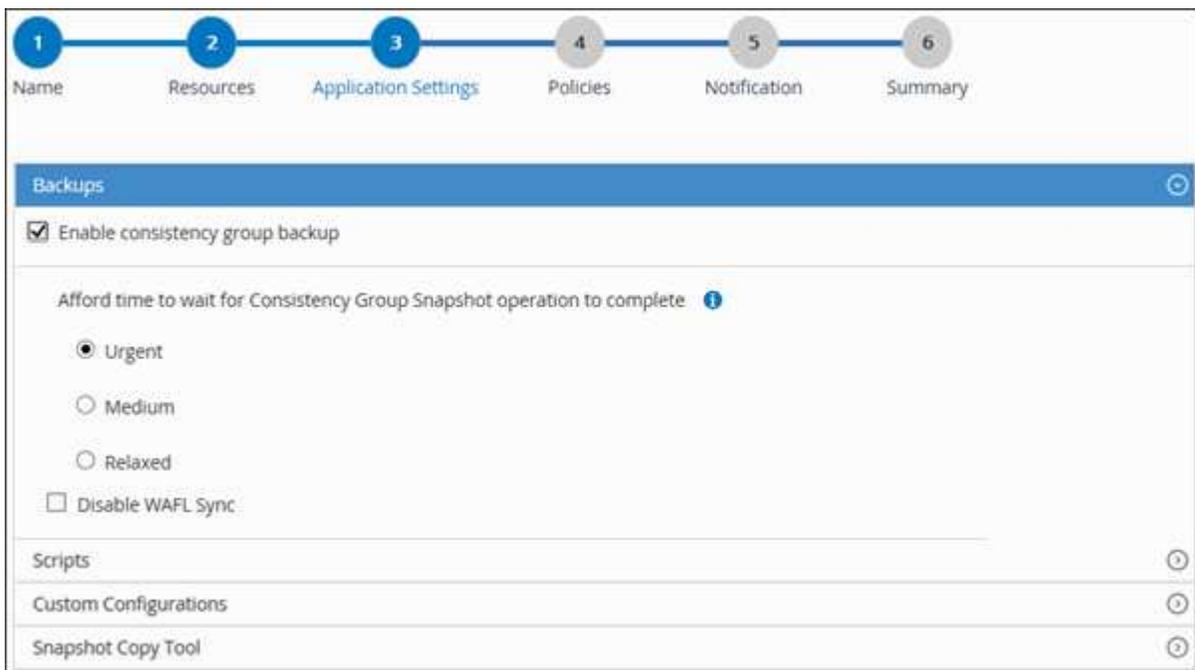
- Sélectionnez la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce.

Vous pouvez également exécuter des pré-commandes avant de quitter l'opération de sauvegarde. Des préscripts et des postscripts sont exécutés sur le serveur SnapCenter.

- Sélectionnez la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- Sélectionner la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows afin de mettre le système de fichiers dans un état cohérent, puis de créer un Snapshot	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
Pour saisir la commande permettant de créer un Snapshot	Sélectionnez <b>autre</b> , puis entrez la commande pour créer un instantané.



6. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une police en cliquant sur \*\*  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Sélectionnez \* \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres > Paramètres globaux**.

8. Passez en revue le résumé, puis sélectionnez **Terminer**.

La page topologie des ressources s'affiche.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

Pour plus d'informations, voir : ["Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"](#)

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer.

Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, la commande `do_start method` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante :  
`Java -jar -Xmx8192M -Xms4096M`

## Applets de commande PowerShell

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Ajoutez des ressources manuelles à l'aide de l'applet de commande `Add-SmResources`.

Cet exemple montre comment ajouter une instance MySQL :

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.
4. Protégez la ressource ou ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.
5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet New-SmBackup.

Cet exemple montre comment sauvegarder un groupe de ressources :

```
C:\PS> New-SmBackup -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
luginName"="MySQL"} -Policy "MySQL_snapshotbased"
```

Cet exemple sauvegarde une ressource protégée :

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy mysql_policy2
```

6. Surveillez l'état du travail (en cours d'exécution, terminé ou en échec) à l'aide de l'applet de commande Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Surveillez les détails de la tâche de sauvegarde comme ID de sauvegarde, nom de sauvegarde pour effectuer une opération de restauration ou de clonage à l'aide de l'applet de commande Get-SmBackupReport.

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects : {DB1}
FailedObjects : {}
IsScheduled : False
HasMetadata : False
SmBackupId : 269
SmJobId : 2361
StartDateTime : 10/4/2016 11:20:45 PM
EndDateTime : 10/4/2016 11:21:32 PM
Duration : 00:00:46.2536470
CreatedDateTime : 10/4/2016 11:21:09 PM
Status : Completed
ProtectionGroupName : Verify_ASUP_Message_windows
SmProtectionGroupId : 211
PolicyName : test2
SmPolicyId : 20
BackupName : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus : NotVerified
VerificationStatuses :
SmJobError :
BackupType : SCC_BACKUP
CatalogingStatus : NotApplicable
CatalogingStatuses :
ReportDataCreatedDateTime :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarder les groupes de ressources

Un groupe de ressources est un ensemble de ressources sur un hôte. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « *napmirror All* ». Toutefois, si vous utilisez le rôle « *vsadmin* », le privilège « *napmirror all* » n'est pas requis.

### Description de la tâche

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une

stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en sélectionnant  , puis en  sélectionnant la balise. Vous pouvez ensuite choisir de  fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Sélectionnez **Backup**.

5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Surveillez les opérations de sauvegarde MySQL

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.

- b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Surveillez les opérations de protection des données sur les instances MySQL dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

## Annuler les opérations de sauvegarde pour MySQL

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

### Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

### Étapes

1. Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"><li>Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li><li>Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li></ol>
Volet activité	<ol style="list-style-type: none"><li>Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li><li>Sélectionner l'opération.</li><li>Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li></ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Afficher les sauvegardes et clones MySQL dans la page topologie

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire.

### Description de la tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

-  affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
-  Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
-  Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.



Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la **carte Résumé** pour afficher un résumé du nombre de sauvegardes et de clones disponibles sur le stockage primaire et secondaire.

La section **carte récapitulative** affiche le nombre total de sauvegardes basées sur des copies Snapshot et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Après une sauvegarde à la demande, en cliquant sur le bouton **Refresh**, vous actualisez les détails de la sauvegarde ou du clone.

5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

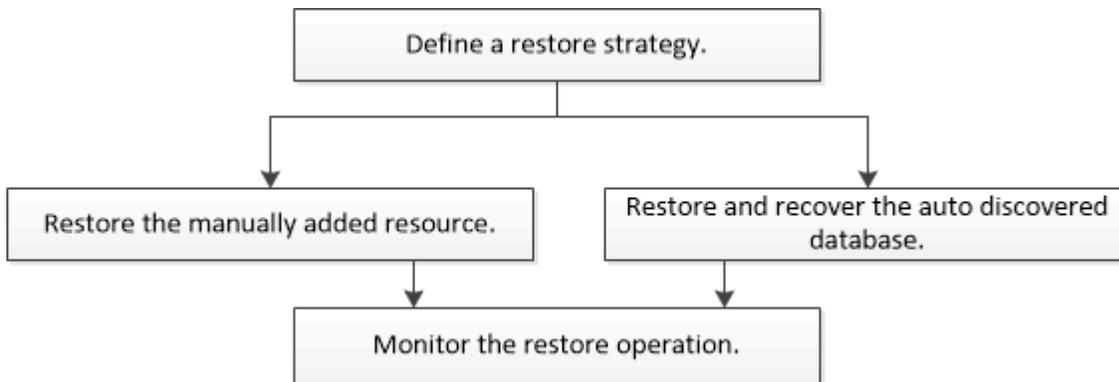
7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur .
8. Si vous souhaitez diviser un clone, sélectionnez-le dans le tableau, puis cliquez sur .

## Restaurer MySQL

## Restaurer le flux de travail

Le workflow de restauration et de reprise comprend la planification, la réalisation des opérations de restauration et la surveillance des opérations.

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurez et restaurez une sauvegarde de ressources ajoutée manuellement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
  - Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

### Description de la tâche

- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur



Backup Name	End Date
rg1_scipr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource**.

- a. Si vous sélectionnez **Complete Resource**, tous les volumes de données configurés de la base de données MySQL sont restaurés.

Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

Vous pouvez sélectionner plusieurs LUN.



Si vous sélectionnez **tous**, tous les fichiers des volumes, qtrees ou LUN sont restaurés.

7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet `Restore-SmBackup`.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurez et récupérez une sauvegarde de base de données découverte automatiquement

Vous pouvez utiliser SnapCenter pour restaurer et récupérer des données à partir d'une ou plusieurs sauvegardes.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources que vous souhaitez restaurer.
- Pour les commandes de pré-restauration, post-restauration, montage et démontage, vous devez vérifier si

les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in depuis les chemins suivants :

- Emplacement par défaut sur l'hôte Windows : `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed_commands.config`
- Emplacement par défaut sur l'hôte Linux : `/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config`



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue.

## Description de la tâche

- Pour les ressources découvertes automatiquement, la restauration est prise en charge par SFSR.
- La restauration automatique à un point dans le temps et à une minute n'est pas prise en charge.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources sont affichées avec le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

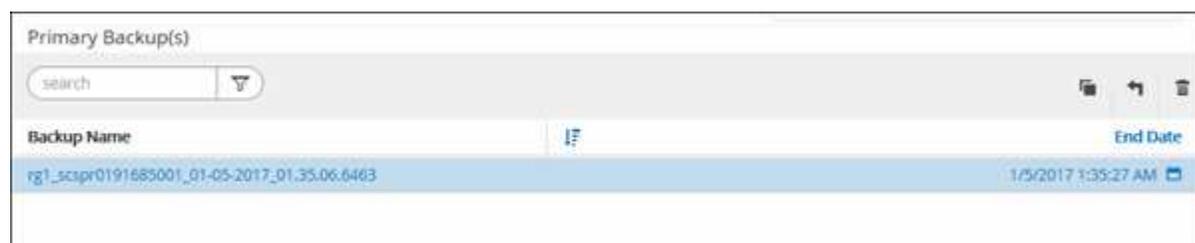
Si la ressource n'est pas protégée, « non protégée » s'affiche dans la colonne État global. Cela peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).

5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur .



Backup Name	End Date
rg1_scspr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page Restore Scope, sélectionnez **Complete Resource** pour restaurer les volumes de données

configurés de la base de données MySQL.

7. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.

Les commandes de démontage ne sont pas disponibles pour les ressources détectées automatiquement.

8. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.

Les commandes de montage ne sont pas disponibles pour les ressources détectées automatiquement.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Restaurer des ressources à l'aide des applets de commande PowerShell

La restauration d'une sauvegarde de ressources inclut le lancement d'une session de connexion avec le serveur SnapCenter, la liste des sauvegardes, la récupération des informations de sauvegarde et la restauration d'une sauvegarde.

Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.

### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
-----		
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Surveiller les opérations de restauration MySQL

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours

-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Cloner les sauvegardes de ressources MySQL

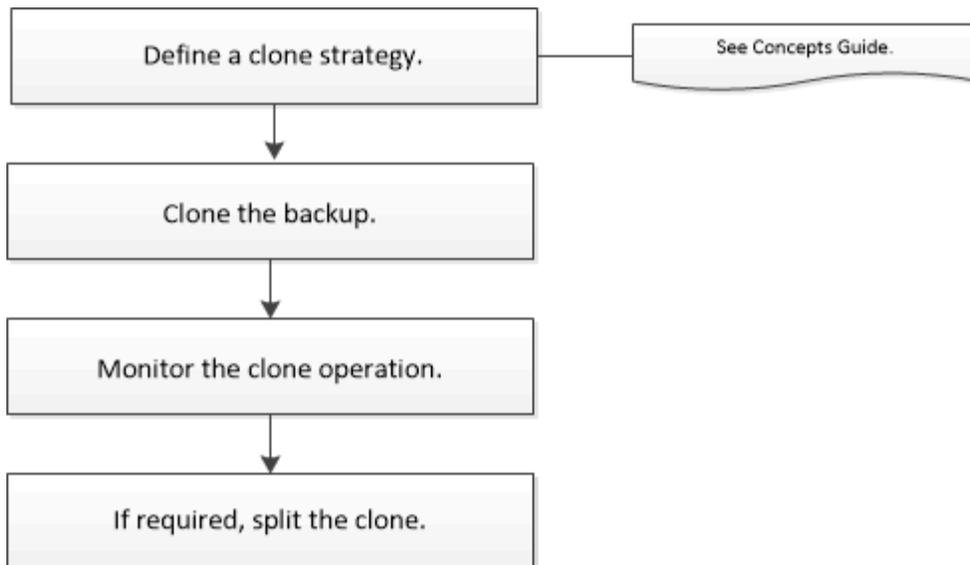
### Workflow de clonage

Le workflow de clonage inclut la réalisation de l'opération de clonage et le contrôle de l'opération.

#### Description de la tâche

- Vous pouvez cloner sur le serveur MySQL source.
- Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :
  - Tester les fonctionnalités à implémenter à l'aide de la structure de ressources actuelle et du contenu pendant les cycles de développement d'applications
  - Pour les outils d'extraction et de manipulation de données lors du remplissage d'entrepôts de données
  - Pour récupérer les données qui ont été supprimées ou modifiées par erreur

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent des informations détaillées sur les applets de commande PowerShell.

## Cloner une sauvegarde MySQL

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde. Vous pouvez cloner à partir d'une sauvegarde principale ou secondaire.

### Avant de commencer

- Vous devriez avoir sauvegardé les ressources ou le groupe de ressources.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).
- Pour les commandes pré-clone ou post-clone, vérifiez si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir des chemins suivants :
  - Emplacement par défaut sur l'hôte Windows : *C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in Creator\etc\allowed\_commands.config*
  - Emplacement par défaut sur l'hôte Linux : */opt/NetApp/SnapCenter/scc/etc/allowed\_commands.config*



Si les commandes n'existent pas dans la liste de commandes, l'opération échoue. \* Pour MySQL version 5.7, vous devez définir `IGNORE_MYSQLX_PORT = TRUE` (par défaut `FALSE`) dans MySQL. fichier de propriétés.

### Description de la tâche

- Vous ne pouvez pas protéger les instances MySQL clonées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à "[Séparer un volume FlexClone de son volume parent](#)" la section, .
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots du coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources s'affichent avec des informations telles que le type, l'hôte, les groupes de ressources et les stratégies associés et l'état.

3. Sélectionnez la ressource ou le groupe de ressources.

Vous devez sélectionner une ressource si vous sélectionnez un groupe de ressources.

La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Serveur clone	Choisissez l'hôte sur lequel le clone doit être créé.
Port	Indiquez le port sur lequel l'instance MySQL clonée doit être démarrée.
Adresse IP d'exportation NFS	Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.

7. Dans la page scripts, effectuez les opérations suivantes :



Les scripts sont exécutés sur l'hôte du plug-in.

- a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
  - Commande de pré-clonage : permet de supprimer les bases de données existantes portant le même nom
  - Commande post-clone : vérifiez une base de données ou démarrez une base de données.
- b. Entrez la commande mount pour monter un système de fichiers sur un hôte.

Commande mount pour un volume ou un qtree sur une machine Linux :

Exemple pour NFS : `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.
10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Récupérez les sauvegardes pour effectuer l'opération de clonage à l'aide de l'applet de commande Get-SmBackup.

Cet exemple montre que deux sauvegardes sont disponibles pour le clonage :

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. Lancez une opération de clonage à partir d'une sauvegarde existante et spécifiez les adresses IP d'exportation NFS sur lesquelles les volumes clonés sont exportés.

Cet exemple montre que la sauvegarde à cloner a une adresse NFSExportalIP de 10.32.212.14 :

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName
"scs000211748_gdl_englab_netapp_com_MySQL_mysqlid_3306_scs000211748_0
6-26-2024_06.08.35.4307" -Resources
{ "Host"="scs000211748.gdl.englab.netapp.com"; "Uid"="mysqlid_3306"}
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```



Si NFSExportIPS n'est pas spécifié, la valeur par défaut est exportée vers l'hôte cible du clone.

4. Vérifiez que les sauvegardes ont été correctement clonées à l'aide de l'applet de commande Get-SmCloneReport pour afficher les détails du travail clone.

Vous pouvez afficher des informations telles que l'ID de clone, la date et l'heure de début, la date et l'heure de fin.

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError :
```

## Surveillez les opérations de clonage MySQL

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
- 



Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements

- En file d'attente
- Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

## Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur \* \* .

5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.

6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

#### Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

## Supprimez ou divisez les clones de base de données MySQL après la mise à niveau de SnapCenter

Après la mise à niveau vers SnapCenter 4.3, vous ne verrez plus les clones. Vous pouvez supprimer le clone ou séparer les clones de la page topologie de la ressource à partir de laquelle les clones ont été créés.

#### Description de la tâche

Si vous souhaitez localiser l'empreinte de stockage des clones masqués, exécutez la commande suivante :

```
Get-SmClone -ListStorageFootprint
```

#### Étapes

1. Supprimez les sauvegardes des ressources clonées à l'aide de la cmdlet remove-smbbackup.
2. Supprimez le groupe de ressources des ressources clonées à l'aide de la cmdlet remove-smresregroupement.
3. Supprimez la protection de la ressource clonée à l'aide de l'applet de commande remove-smprotectResource.
4. Sélectionnez la ressource parente dans la page Ressources.

La page topologie de ressources s'affiche.

5. Dans la vue Manage copies (gérer les copies), sélectionnez les clones dans les systèmes de stockage principal ou secondaire (en miroir ou répliqué).
6. Sélectionnez les clones, puis cliquez sur  pour supprimer les clones ou sur  pour les séparer.
7. Cliquez sur **OK**.

# Protégez les applications à l'aide des plug-ins pris en charge par NetApp

## Plug-ins pris en charge par NetApp

### Présentation des plug-ins pris en charge par NetApp

Vous pouvez utiliser les plug-ins pris en charge par NetApp tels que MongoDB, ORASCPM (applications Oracle), SAP ASE, SAP MaxDB et Storage Plug-in pour les applications que vous utilisez, puis utiliser SnapCenter pour sauvegarder, restaurer ou cloner ces applications. Vos plug-ins pris en charge par NetApp font office de composants côté hôte du logiciel NetApp SnapCenter, ce qui permet une protection des données compatible avec les applications et une gestion des ressources.

Une fois les plug-ins pris en charge par NetApp installés, vous pouvez utiliser SnapCenter avec la technologie NetApp SnapMirror pour créer des copies miroir de jeux de sauvegarde sur un autre volume et utiliser la technologie NetApp SnapVault pour effectuer la réplication de sauvegarde disque à disque. Les plug-ins pris en charge par NetApp peuvent être utilisés dans les environnements Windows et Linux.



SnapCenter CLI ne prend pas en charge les commandes des plug-ins pris en charge par NetApp.

NetApp fournit le plug-in de stockage pour effectuer des opérations de protection des données du volume de données sur le stockage ONTAP à l'aide de l'infrastructure de plug-in intégrée à SnapCenter.

Vous pouvez installer les plug-ins pris en charge par NetApp à partir de la page [Ajouter un hôte](#).

["Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants."](#)



La politique de support de SnapCenter couvre le framework de plug-ins, le moteur principal et les API associées. Le support ne couvre pas le code source du plug-in ni les scripts associés basés sur le framework.

### Avantages des plug-ins pris en charge par NetApp

Vous pouvez utiliser les plug-ins pris en charge par NetApp comme MongoDB, ORASCPM, les applications Oracle, SAP ASE, SAP MaxDB et le plug-in de stockage pour les opérations de protection des données.

- Ajoutez des ressources telles que les bases de données, les instances, les documents ou les espaces de stockage.
- Création de sauvegardes.
- Effectuez des restaurations à partir des sauvegardes.
- Sauvegardes clones.
- Planifiez les opérations de sauvegarde.
- Contrôle des opérations de sauvegarde, de restauration et de clonage

- Afficher les rapports relatifs aux opérations de sauvegarde, de restauration et de clonage.

Vous pouvez utiliser les plug-ins pris en charge par NetApp pour vos opérations de protection des données.

- Prenez des copies Snapshot de groupes de cohérence des volumes de stockage sur les clusters ONTAP.
- Sauvegardez des applications personnalisées à l'aide de l'infrastructure intégrée de pré et post-script

La sauvegarde d'un volume ONTAP, d'une LUN ou d'un qtree peut être effectuée.

- Mettre à jour les copies Snapshot du stockage primaire vers un système secondaire ONTAP, en exploitant la relation de réplication existante (SnapVault/SnapMirror/réplication unifiée) à l'aide de règles SnapCenter

Le système principal et le système secondaire ONTAP peuvent être ONTAP FAS, AFF, ASA, ONTAP Select ou Cloud Volumes ONTAP.

- Restaurez l'intégralité de votre volume ONTAP, LUN ou fichiers.

Vous devez fournir manuellement le chemin de fichier correspondant, car les fonctions de navigation ou d'indexation ne sont pas intégrées au produit.

La restauration des qtrees ou des répertoires n'est pas prise en charge, mais vous pouvez cloner et exporter uniquement le qtree si l'étendue de la sauvegarde est définie au niveau qtree.

## Fonctionnalités des plug-ins pris en charge par NetApp

SnapCenter s'intègre avec l'application de plug-in et avec les technologies NetApp sur le système de stockage. Pour utiliser les plug-ins pris en charge par NetApp, tels que MongoDB, ORASCPM (applications Oracle), SAP ASE, SAP MaxDB et Storage Plug-in, vous utilisez l'interface utilisateur graphique de SnapCenter.

- **Interface utilisateur graphique unifiée**

L'interface SnapCenter assure la standardisation et la cohérence dans l'ensemble des plug-ins et des environnements. L'interface SnapCenter vous permet d'effectuer toutes les opérations de sauvegarde, de restauration et de clonage cohérentes sur l'ensemble des plug-ins, d'utiliser le reporting centralisé, d'utiliser des vues de tableau de bord d'un coup d'œil, de configurer le contrôle d'accès basé sur des rôles (RBAC) et de surveiller les tâches dans l'ensemble des plug-ins.

- **Administration centrale automatisée**

Vous pouvez planifier des opérations de sauvegarde, configurer la conservation des sauvegardes basée sur des règles et effectuer des opérations de restauration. Vous pouvez également surveiller votre environnement de manière proactive en configurant SnapCenter pour envoyer des alertes par e-mail.

- **Technologie snapshot NetApp non disruptive**

SnapCenter utilise la technologie Snapshot de NetApp avec les plug-ins NetApp pris en charge pour sauvegarder les ressources. Les copies Snapshot consomment un espace de stockage minimal.

Les plug-ins NetApp pris en charge offrent également les avantages suivants :

- Prise en charge des workflows de sauvegarde, de restauration et de clonage

- Sécurité prise en charge par le RBAC et délégation centralisée des rôles

Vous pouvez également définir les informations d'identification de sorte que les utilisateurs SnapCenter autorisés disposent de droits d'accès au niveau de l'application.

- Création de copies compactes et ponctuelles de ressources à des fins de test ou d'extraction de données grâce à la technologie NetApp FlexClone

Une licence FlexClone est requise sur le système de stockage dans lequel vous souhaitez créer le clone.

- Prise en charge de la fonctionnalité Snapshot de groupe de cohérence (CG) de ONTAP dans le cadre de la création des sauvegardes.
- Possibilité d'exécuter plusieurs sauvegardes simultanément sur plusieurs hôtes de ressources

En une seule opération, les snapshots sont consolidés lorsque les ressources d'un hôte unique partagent le même volume.

- Possibilité de créer un instantané à l'aide de commandes externes.
- Fonctionnalité de création de copies Snapshot cohérentes avec le système de fichiers dans les environnements Windows.

## Types de stockage pris en charge par les plug-ins NetApp pris en charge

SnapCenter prend en charge un large éventail de types de stockage sur les serveurs physiques et virtuels. Vous devez vérifier la prise en charge de votre type de stockage avant d'installer les plug-ins NetApp pris en charge.

Machine	Type de stockage
Montages physiques et directs NFS sur les hôtes de machine virtuelle (les VMDK et les LUN RDM ne sont pas pris en charge).	LUN connectés via FC
Montages physiques et directs NFS sur les hôtes de machine virtuelle (les VMDK et les LUN RDM ne sont pas pris en charge).	LUN connectées à l'iSCSI
Montages physiques et directs NFS sur les hôtes de machine virtuelle (les VMDK et les LUN RDM ne sont pas pris en charge).	Volumes connectés par NFS
VMware ESXi	Datastores vVol sur NFS et SAN  Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.

## Privilèges ONTAP minimum requis pour le plug-in pris en charge par NetApp

Les privilèges minimum ONTAP requis varient en fonction des plug-ins SnapCenter utilisés pour la protection des données.

- Commandes All-Access : privilèges minimum requis pour ONTAP 9.12.1 et versions ultérieures
  - event generate-autosupport-log
  - l'historique des tâches s'affiche
  - fin de la tâche
  - l'attribut de lun affiche
  - la création de lun
  - suppression de la lun
  - géométrie de lun
  - lun igroup add
  - créez un groupe initiateur lun
  - suppression du groupe initiateur lun
  - renommer la lun igroup
  - affichage de la lun igroup
  - lun mapping des nœuds supplémentaires
  - création d'un mappage de lun
  - suppression du mappage de lun
  - mappage de lun supprimer-rapports-nœuds
  - les mappages de lun s'affichent
  - modification de lun
  - déplacement des lun dans le volume
  - lun hors ligne
  - lun en ligne
  - redimensionner la lun
  - série de lun
  - affichage de la lun
  - interface réseau
  - ajout de règle snapmirror
  - règle de modification de snapmirror
  - règle de suppression de snapmirror
  - affichage des règles snapmirror
  - restauration snapmirror
  - montrer snapmirror
  - historique des données du mode snapmirror
  - mise à jour snapmirror
  - snapmirror update-ls-set
  - destinations des listes snapmirror
  - version

- création de clones de volumes
- clone de volume affiche
- démarrage du fractionnement du clone de volume
- arrêt du fractionnement du clone de volume
- création de volumes
- destruction des volumes
- création d'un clone de fichiers de volumes
- volume fichier show-disk-usage
- volume hors ligne
- volume en ligne
- modification de volume
- création de qtree volume
- suppression qtree du volume
- modification de qtree volume
- volume qtree show
- restrictions de volume
- volume affiché
- création de copies snapshot de volume
- suppression du snapshot de volume
- modification de snapshot de volume
- renommage snapshot de volume
- restauration snapshot du volume
- fichier de restauration de snapshot de volume
- snapshot de volume apparaît
- démontage de volume
- cifs vserver
- création d'un partage cifs vserver
- suppression du partage cifs vserver
- vserver cifs shadowcopy show
- vserver cifs share show
- cifs montrer un vserver
- vserver export-policy créé
- vserver export-policy delete
- vserver export-policy create
- vserver export-policy règle show
- vserver export-policy show
- vserver iscsi connection show

- vserver show
- Commandes en lecture seule : privilèges minimum requis pour ONTAP 8.3.0 et versions ultérieures
  - interface réseau

## Préparez les systèmes de stockage pour SnapMirror et la réplication SnapVault pour les plug-ins pris en charge par NetApp

Vous pouvez utiliser un plug-in SnapCenter avec la technologie ONTAP SnapMirror pour créer des copies en miroir des jeux de sauvegarde sur un autre volume. Avec la technologie ONTAP SnapVault, vous pouvez effectuer une réplication de sauvegarde disque à disque afin d'assurer la conformité aux normes et d'autres objectifs de gouvernance. Avant d'effectuer ces tâches, vous devez configurer une relation de protection des données entre les volumes source et destination, et initialiser la relation.

SnapCenter effectue les mises à jour vers SnapMirror et SnapVault une fois l'opération Snapshot terminée. Les mises à jour SnapMirror et SnapVault sont effectuées dans le cadre de la tâche SnapCenter ; ne créez pas de planification ONTAP distincte.



Si vous pensez arriver à SnapCenter d'un produit NetApp SnapManager et que vous êtes satisfait des relations de protection des données que vous avez configurées, vous pouvez ignorer cette section.

Une relation de protection des données réplique les données du système de stockage primaire (volume source) vers le stockage secondaire (volume de destination). Lorsque vous initialisez la relation, ONTAP transfère ainsi les blocs de données référencés sur le volume source vers le volume de destination.



SnapCenter ne prend pas en charge les relations en cascade entre SnapMirror et les volumes SnapVault (**primaire** > **miroir** > **coffre-fort**). Vous devez utiliser des relations de fanout.

SnapCenter prend en charge la gestion des relations SnapMirror flexibles de version. Pour plus d'informations sur les relations SnapMirror flexibles de la version et sur la configuration de ces relations, consultez le "[Documentation ONTAP](#)".

## Définir une stratégie de sauvegarde

La définition d'une stratégie de sauvegarde avant de créer vos tâches de sauvegarde permet de s'assurer que vous disposez des sauvegardes dont vous avez besoin pour restaurer ou cloner vos ressources. Votre contrat de niveau de service (SLA), votre objectif de délai de restauration (RTO) et votre objectif de point de restauration (RPO) déterminent largement votre stratégie de sauvegarde.

### Description de la tâche

Un SLA définit le niveau de service attendu et traite de nombreux problèmes liés à la prestation, notamment la disponibilité et les performances du service. Le RTO est le moment par lequel un processus métier doit être restauré suite à une interruption de service. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service, RTO et RPO contribuent à la stratégie de protection des données.

### Étapes

1. Déterminez à quel moment il est nécessaire de sauvegarder vos ressources.
2. Déterminer le nombre de tâches de sauvegarde dont vous avez besoin
3. Choisissez le nom de vos sauvegardes.
4. Décidez si vous souhaitez obtenir des snapshots de groupe de cohérence et décidez des options appropriées pour supprimer les snapshots de groupe de cohérence.
5. Choisissez si vous souhaitez utiliser la technologie NetApp SnapMirror pour la réplication ou la technologie NetApp SnapVault pour la conservation à long terme.
6. Déterminez la période de conservation des snapshots sur le système de stockage source et la destination SnapMirror.
7. Déterminez si vous souhaitez exécuter des commandes avant ou après l'opération de sauvegarde et fournissez un prescripteur ou un PostScript.

## Stratégie de sauvegarde pour les plug-ins pris en charge par NetApp

### Plannings de sauvegarde des ressources de plug-in NetApp prises en charge

Le facteur le plus important dans la détermination d'un planning de sauvegarde est le taux de modification de la ressource. Le nombre de journaux d'archivage que SnapCenter doit utiliser pour la restauration, donc le plus souvent pour les sauvegardes, accélère les opérations de restauration.

Vous pouvez sauvegarder chaque heure une ressource largement utilisée et il vous est possible de sauvegarder une ressource peu utilisée une fois par jour. D'autres facteurs entrent en ligne de compte l'importance des ressources pour votre entreprise, votre contrat de niveau de service et votre objectif de point de récupération (RPO).

Le SLA définit le niveau de service attendu et traite de nombreux problèmes liés aux services, notamment la disponibilité et les performances de celui-ci. L'objectif RPO définit la stratégie selon laquelle les fichiers doivent être récupérés depuis le stockage de sauvegarde afin que les opérations régulières puissent reprendre après une défaillance. Les niveaux de service et le RPO contribuent à la stratégie de protection des données.

Les planifications de sauvegarde ont deux parties, comme suit :

- Fréquence des sauvegardes

La fréquence des sauvegardes (fréquence d'exécution des sauvegardes), également appelée type de planification pour certains plug-ins, fait partie d'une configuration de règles. Par exemple, vous pouvez configurer la fréquence des sauvegardes sous la forme horaire, quotidien, hebdomadaire ou mensuel. Vous pouvez accéder aux stratégies dans l'interface utilisateur graphique de SnapCenter en cliquant sur **Paramètres > stratégies**.

- Planifications de sauvegarde

Les planifications de sauvegarde (exactement quand les sauvegardes doivent être effectuées) font partie d'une configuration de ressource ou de groupe de ressources. Par exemple, si un groupe de ressources dispose d'une stratégie configurée pour les sauvegardes hebdomadaires, vous pouvez configurer la planification pour la sauvegarder tous les jeudis à 10 h 00. Vous pouvez accéder aux planifications de groupes de ressources dans l'interface utilisateur graphique SnapCenter en cliquant sur **Ressources**, puis en sélectionnant le plug-in approprié et en cliquant sur **Affichage > Groupe de ressources**.

## Nombre de tâches de sauvegarde nécessaires

Les facteurs qui déterminent le nombre de tâches de sauvegarde dont vous avez besoin incluent la taille de la ressource, le nombre de volumes utilisés, le taux de changement de la ressource et votre contrat de niveau de service.

Le nombre de tâches de sauvegarde que vous choisissez dépend généralement du nombre de volumes sur lesquels vous avez placé vos ressources. Par exemple, si vous placez un groupe de petites ressources sur un volume et une grande ressource sur un autre volume, vous pouvez créer une tâche de sauvegarde pour les petites ressources et une tâche de sauvegarde pour la grande ressource.

## Types de stratégies de restauration prises en charge pour les ressources de plug-in prises en charge par NetApp ajoutées manuellement

Vous devez définir une stratégie pour pouvoir effectuer les opérations de restauration à l'aide de SnapCenter. Il existe deux types de stratégies de restauration pour les ressources de plug-in prises en charge par NetApp ajoutées manuellement.



Vous ne pouvez pas restaurer les ressources de plug-in NetApp ajoutées manuellement.

### Restauration des ressources terminée

- Restauration de tous les volumes, qtrees et LUN d'une ressource



Si la ressource contient des volumes ou des qtrees, les snapshots pris après le Snapshot sélectionné pour la restauration sur ces volumes ou ces qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

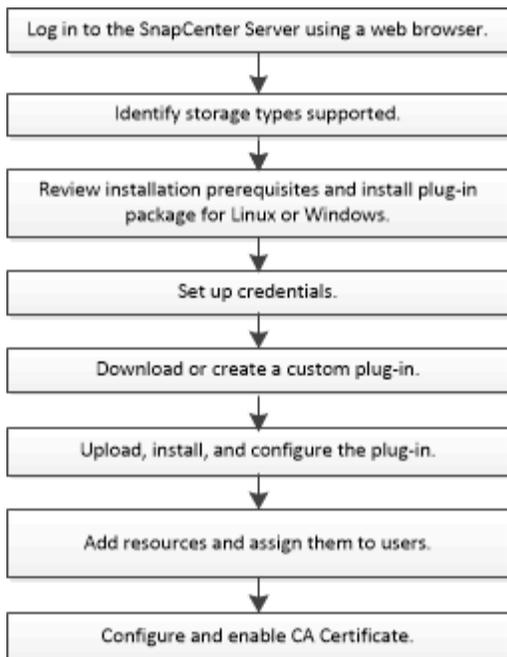
### Restauration au niveau des fichiers

- Restaure les fichiers à partir de volumes, de qtrees ou de répertoires
- Restaure uniquement les LUN sélectionnées

## Préparez l'installation des plug-ins pris en charge par NetApp

### Workflow d'installation des plug-ins pris en charge par SnapCenter NetApp

Vous devez installer et configurer les plug-ins pris en charge par SnapCenter NetApp si vous souhaitez protéger les ressources des plug-ins pris en charge par NetApp.



## Conditions préalables à l'ajout d'hôtes et à l'installation du module Plug-ins pour Windows, Linux ou AIX

Avant d'ajouter un hôte et d'installer les packages de plug-ins, vous devez respecter toutes les exigences. Les plug-ins pris en charge par NetApp sont pris en charge dans les environnements Windows, Linux et AIX.



Les applications de stockage et Oracle sont prises en charge sous AIX.

- Vous devez avoir installé Java 11 sur votre hôte Linux, Windows ou AIX.



IBM Java n'est pas pris en charge sur les hôtes Windows et Linux.

- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Les plug-ins pris en charge par NetApp comme MongoDB, ORASCPM, les applications Oracle, SAP ASE, SAP MaxDB et le plug-in de stockage doivent être disponibles sur l'hôte client à partir duquel l'opération d'ajout d'hôte est effectuée.

### Généralités

Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.

### Hôtes Windows

- Vous devez disposer d'un utilisateur de domaine disposant de privilèges d'administrateur local avec des autorisations de connexion locales sur l'hôte distant.
- Si vous gérez des nœuds de cluster dans SnapCenter, vous devez disposer d'un utilisateur disposant de privilèges d'administration sur tous les nœuds du cluster.

- Vous devez sélectionner manuellement le plug-in SnapCenter pour Microsoft Windows.

["Télécharger JAVA pour Windows"](#)

## Hôtes Linux et AIX



Les applications de stockage et Oracle sont prises en charge sous AIX.

- Vous devez avoir activé la connexion SSH par mot de passe pour l'utilisateur root ou non-root.
- Vous devez avoir installé Java 11 sur votre hôte Linux.

Si vous utilisez Windows Server 2019 ou Windows Server 2016 pour l'hôte SnapCenter Server, vous devez installer Java 11. La matrice d'interopérabilité (IMT) contient les dernières informations sur les conditions requises.

["Télécharger JAVA pour Linux"](#)

["Télécharger JAVA pour AIX"](#)

["Matrice d'interopérabilité NetApp"](#)

- Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins. Ajoutez les lignes suivantes au fichier /etc/sudoers à l'aide de l'utilitaire visudo Linux.



Assurez-vous que vous utilisez la version 1.8.7 ou ultérieure de sudo.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

*LINUX\_USER* est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur *checksum\_value* à partir du fichier **sc\_unix\_plugins\_checksum.txt**, situé à l'adresse suivante :

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc\_unix\_plugins\_checksum.txt* si le serveur SnapCenter est installé sur l'hôte Windows.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc\_unix\_plugins\_checksum.txt* si le serveur SnapCenter est installé sur l'hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configuration requise pour l'hôte AIX

Vous devez vous assurer que l'hôte répond aux exigences requises avant d'installer le module de plug-ins SnapCenter pour AIX.



Les applications de stockage et Oracle sont prises en charge sous AIX.



Le plug-in SnapCenter pour UNIX qui fait partie du package de plug-ins SnapCenter pour AIX ne prend pas en charge les groupes de volumes simultanés.

Élément	De formation
Systèmes d'exploitation	AIX 7.1 ou version ultérieure
RAM minimale pour le plug-in SnapCenter sur l'hôte	4 Go
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	2 GO   Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.
Packs logiciels requis	Java 11 IBM Java  Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option <code>JAVA_HOME</code> située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.

Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice](#)"

d'interopérabilité NetApp".

### Configurez les privilèges sudo pour les utilisateurs non-root pour l'hôte AIX

SnapCenter 4.4 et version ultérieure permet à un utilisateur non-root d'installer le module de plug-ins SnapCenter pour AIX et de démarrer le processus de plug-in. Les processus de plug-in s'exécutent en tant qu'utilisateur non racine efficace. Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder à plusieurs chemins.

#### Ce dont vous aurez besoin

- Sudo version 1.8.7 ou ultérieure.
- Modifiez le fichier `/etc/ssh/sshd_config` pour configurer les algorithmes de code d'authentification de message : Mac hmac-sha2-256 et MAC hmac-sha2-512.

Redémarrez le service sshd après la mise à jour du fichier de configuration.

Exemple :

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

#### À propos de cette tâche

Vous devez configurer les privilèges sudo pour que l'utilisateur non-root puisse accéder aux chemins suivants :

- `/Home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/Custom_location/NetApp/snapcenter/spl/installation/plugins/désinstaller`
- `/Custom_location/NetApp/snapcenter/spl/bin/spl`

#### Étapes

1. Connectez-vous à l'hôte AIX sur lequel vous souhaitez installer SnapCenter Plug-ins Package pour AIX.
2. Ajoutez les lignes suivantes au fichier `/etc/sudoers` à l'aide de l'utilitaire visudo Linux.

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



Si vous avez une configuration RAC, avec les autres commandes autorisées, vous devez ajouter ce qui suit au fichier `/etc/sudoers` : `'/<crs_home>/bin/olsnodes'`

Vous pouvez obtenir la valeur de `crs_Home` à partir du fichier `/etc/oracle/olr.loc`.

`AIX_USER` est le nom de l'utilisateur non-root que vous avez créé.

Vous pouvez obtenir la valeur `checksum_value` à partir du fichier `sc_unix_plugins_checksum.txt`, situé à l'adresse suivante :

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Windows.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` si le serveur SnapCenter est installé sur l'hôte Linux.



Cet exemple ne doit être utilisé que comme référence pour la création de vos propres données.

## Configuration requise pour l'hôte pour installer le module de plug-ins SnapCenter pour Windows

Avant d'installer le package de plug-ins SnapCenter pour Windows, vous devez connaître les exigences en matière d'espace système hôte de base et de dimensionnement.

Élément	De formation
Systèmes d'exploitation	<p>Microsoft Windows</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	<p>5 GO</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>
Packs logiciels requis	<ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x suivants) Hosting Bundle</li> <li>• PowerShell Core 7.4.2</li> <li>• Java 11 Oracle Java et OpenJDK</li> </ul> <p>Java 11 Oracle Java et OpenJDK sont requis uniquement pour SAP HANA, IBM DB2, PostgreSQL, MySQL, les plug-ins pris en charge par NetApp et d'autres applications personnalisées qui peuvent être installées sur l'hôte Windows.</p> <p>Pour obtenir les dernières informations sur les versions prises en charge, consultez le <a href="#">"Matrice d'interopérabilité NetApp"</a>.</p> <p>Pour obtenir des informations de dépannage spécifiques à .NET, reportez-vous à la section <a href="#">"La mise à niveau ou l'installation de SnapCenter échoue pour les systèmes existants qui ne disposent pas de connexion Internet."</a></p>

## Configuration requise pour l'hôte pour l'installation du pack de plug-ins SnapCenter pour Linux et AIX

Vous devez vous assurer que l'hôte répond aux exigences requises avant d'installer le

## module de plug-ins SnapCenter pour Linux ou AIX.



Les applications de stockage et Oracle sont prises en charge sous AIX.

Élément	De formation
Systemes d'exploitation	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• SUSE Linux Enterprise Server (SLES)</li></ul>
RAM minimale pour le plug-in SnapCenter sur l'hôte	1 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	2 GO   <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p>
Packs logiciels requis	Java 11 Oracle Java ou OpenJDK  Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans /var/opt/snapcenter/spl/etc/spl.properties est définie sur la version JAVA correcte et le chemin correct.

Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp](#)"

## Configurez les informations d'identification des plug-ins pris en charge par NetApp

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter. Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour exécuter des opérations de protection des données sur des bases de données ou des systèmes de fichiers Windows.

### Avant de commencer

- Hôtes Linux ou AIX

Vous devez configurer des informations d'identification pour l'installation de plug-ins sur des hôtes Linux ou AIX.

Vous devez configurer les informations d'identification pour l'utilisateur root ou pour un utilisateur non-root disposant de privilèges sudo pour installer et démarrer le processus de plug-in.

**Meilleure pratique:** bien que vous soyez autorisé à créer des informations d'identification pour Linux après le déploiement des hôtes et l'installation des plug-ins, la meilleure pratique consiste à créer des informations d'identification après l'ajout de SVM, avant de déployer des hôtes et d'installer des plug-ins.

- Hôtes Windows

Vous devez configurer les informations d'identification Windows avant d'installer les plug-ins.

Vous devez configurer les informations d'identification avec les privilèges d'administrateur, y compris les droits d'administrateur sur l'hôte distant.

- Plug-ins d'applications pris en charge par NetApp

Le plug-in utilise les informations d'identification sélectionnées ou créées lors de l'ajout d'une ressource. Si une ressource ne nécessite pas d'informations d'identification pendant les opérations de protection des données, vous pouvez définir les informations d'identification comme **aucun**.

### Description de la tâche

Si vous configurez des informations d'identification pour des groupes de ressources individuels et que le nom d'utilisateur ne dispose pas de privilèges d'administrateur complets, vous devez affecter au moins le groupe de ressources et les privilèges de sauvegarde au nom d'utilisateur.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page **Credential**, spécifiez les informations requises pour la configuration des informations d'identification :

Pour ce champ...	Procédez comme ça...
Nom d'identification	Saisissez un nom pour les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom d'utilisateur	<p>Entrez le nom d'utilisateur et le mot de passe à utiliser pour l'authentification.</p> <ul style="list-style-type: none"> <li>Administrateur de domaine ou tout membre du groupe d'administrateurs</li> </ul> <p>Spécifiez l'administrateur de domaine ou tout membre du groupe d'administrateurs sur le système sur lequel vous installez le plug-in SnapCenter. Les formats valides pour le champ Nom d'utilisateur sont les suivants :</p> <ul style="list-style-type: none"> <li><i>NetBIOS\username</i></li> <li><i>Domain FQDN\username</i></li> </ul> <ul style="list-style-type: none"> <li>Administrateur local (groupes de travail uniquement)</li> </ul> <p>Pour les systèmes appartenant à un groupe de travail, spécifiez l'administrateur local intégré sur le système sur lequel vous installez le plug-in SnapCenter. Vous pouvez spécifier un compte d'utilisateur local appartenant au groupe d'administrateurs locaux si le compte d'utilisateur dispose de privilèges élevés ou si la fonction de contrôle d'accès utilisateur est désactivée sur le système hôte. Le format valide du champ Nom d'utilisateur est : <i>username</i></p>
Mot de passe	Entrez le mot de passe utilisé pour l'authentification.
Type d'authentification	Sélectionnez le type d'authentification que vous souhaitez utiliser.
Utilisez les privilèges sudo	<p>Cochez la case <b>utiliser privilèges sudo</b> si vous créez des informations d'identification pour un utilisateur non-root.</p> <div style="display: flex; align-items: center;">  <p>Applicable aux utilisateurs Linux et AIX uniquement.</p> </div>

5. Cliquez sur **OK**.

Une fois les informations d'identification terminées, vous pouvez affecter la maintenance des informations d'identification à un utilisateur ou à un groupe d'utilisateurs sur la page utilisateur et accès.

## Configurez GMSA sur Windows Server 2016 ou version ultérieure

Windows Server 2016 ou version ultérieure vous permet de créer un compte de service

géré de groupe (GMSA) qui fournit une gestion automatisée des mots de passe de compte de service à partir d'un compte de domaine géré.

#### Avant de commencer

- Vous devez disposer d'un contrôleur de domaine Windows Server 2016 ou version ultérieure.
- Vous devez disposer d'un hôte Windows Server 2016 ou version ultérieure, qui est membre du domaine.

#### Étapes

1. Créez une clé racine KDS pour générer des mots de passe uniques pour chaque objet de votre GMSA.
2. Pour chaque domaine, exécutez la commande suivante à partir du contrôleur de domaine Windows : Add-KDSRootKey -EffectiveImmediately
3. Créez et configurez votre GMSA :
  - a. Créez un compte de groupe d'utilisateurs au format suivant :

```
domainName\accountName$
.. Ajouter des objets d'ordinateur au groupe.
.. Utilisez le groupe d'utilisateurs que vous venez de créer pour
créer le GMSA.
```

Par exemple :

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. Courez `Get-ADServiceAccount` pour vérifier le compte de service.
```

4. Configurez le GMSA sur vos hôtes :
  - a. Activez le module Active Directory pour Windows PowerShell sur l'hôte sur lequel vous souhaitez utiliser le compte GMSA.

Pour ce faire lancer la commande suivante depuis PowerShell :

```

PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name Name Install State

[] Active Directory Domain Services AD-Domain-Services Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code Feature Result

True No Success {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.

```

- a. Redémarrez votre hôte.
  - b. Installez GMSA sur votre hôte en exécutant la commande suivante à partir de l'invite de commande PowerShell : `Install-AdServiceAccount <gmsa>`
  - c. Vérifiez votre compte GMSA en exécutant la commande suivante : `Test-AdServiceAccount <gmsa>`
5. Attribuez les privilèges d'administration au GMSA configuré sur l'hôte.
  6. Ajoutez l'hôte Windows en spécifiant le compte GMSA configuré dans le serveur SnapCenter.

Le serveur SnapCenter installe les plug-ins sélectionnés sur l'hôte et le GMSA spécifié sera utilisé comme compte de journal de service lors de l'installation du plug-in.

## Installez les plug-ins pris en charge par NetApp

### Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants

Vous devez utiliser la page Ajouter hôte de SnapCenter pour ajouter des hôtes, puis installer les modules de plug-in. Les plug-ins sont automatiquement installés sur les hôtes distants. Vous pouvez ajouter un hôte et installer les modules d'extension pour un hôte individuel ou pour un cluster.

#### Avant de commencer

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Assurez-vous que le service de mise en file d'attente des messages est en cours d'exécution.
- Si vous utilisez le compte de service géré de groupe (GMSA), vous devez configurer GMSA avec des privilèges d'administration.

["Configurez le compte de service géré par groupe sur Windows Server 2016 ou version ultérieure pour des](#)

- Pour l'hôte Windows, vous devez vous assurer de sélectionner le plug-in SnapCenter pour Windows.

### Description de la tâche

- Vous ne pouvez pas ajouter un serveur SnapCenter en tant qu'hôte de plug-in à un autre serveur SnapCenter.
- Si vous installez des plug-ins sur un cluster (WSFC), les plug-ins sont installés sur tous les nœuds du cluster.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Sélectionnez **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	<p>Sélectionnez le type d'hôte :</p> <ul style="list-style-type: none"><li>• Répertoires de base</li><li>• Linux</li><li>• AIX</li></ul> <p> Les plug-ins pris en charge par NetApp peuvent être utilisés dans les environnements Windows, Linux et AIX.</p> <p> Les applications de stockage et Oracle sont prises en charge sous AIX.</p>

Pour ce champ...	Procédez comme ça...
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p> <p>Pour les environnements Windows, l'adresse IP n'est prise en charge que pour les hôtes de domaine non fiables s'il résout le FQDN.</p> <p>Vous pouvez entrer les adresses IP ou FQDN d'un hôte autonome.</p> <p>Si vous ajoutez un hôte à l'aide de SnapCenter et que l'hôte fait partie d'un sous-domaine, vous devez fournir le FQDN.</p>
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification.</p> <p>Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom d'identification que vous avez spécifié.</p> <div data-bbox="873 1318 927 1373" style="border: 1px solid #ccc; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span style="font-size: 18px; font-weight: bold;">i</span> </div> <p style="margin-left: 20px;">Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p>

5. Dans la section **Select Plug-ins to Install**, sélectionnez les plug-ins à installer.

Vous pouvez installer les plug-ins suivants à partir de la liste :

- MongoDB
- ORASCPM (affiché comme applications Oracle)
- ASE SAP
- SAP MaxDB
- Stockage

6. (Facultatif) sélectionnez **plus d'options** pour installer les autres modules externes.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port.</p> <p>Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue. </div>
Chemin d'installation	<p>Les plug-ins pris en charge par NetApp peuvent être installés sur un système Windows ou Linux.</p> <ul style="list-style-type: none"> <li>• Pour le package de plug-ins SnapCenter pour Windows, le chemin par défaut est C:\Program Files\NetApp\SnapCenter.</li> </ul> <p>Vous pouvez également personnaliser le chemin.</p> <ul style="list-style-type: none"> <li>• Pour le module de plug-ins SnapCenter pour Linux et le module de plug-ins SnapCenter pour AIX, le chemin par défaut est /opt/NetApp/snapcenter.</li> </ul> <p>Vous pouvez également personnaliser le chemin.</p>
Ignorer les vérifications de préinstallation	<p>Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.</p>

Pour ce champ...	Procédez comme ça...
Utilisez le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in	<p>Pour l'hôte Windows, cochez cette case si vous souhaitez utiliser le compte de service géré de groupe (GMSA) pour exécuter les services du plug-in.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> Indiquez le nom GMSA au format suivant : domainname\accountName\$.</p> <p> GMSA sera utilisé comme compte de service de connexion uniquement pour le plug-in SnapCenter pour Windows.</p> </div>

7. Sélectionnez **soumettre**.

Si vous n'avez pas coché la case **Skip précontrôles**, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in. L'espace disque, la RAM, la version PowerShell, la version .NET, l'emplacement (pour les plug-ins Windows) et la version Java (pour les plug-ins Linux) sont validés par rapport à la configuration minimale requise. Si la configuration minimale requise n'est pas respectée, des messages d'erreur ou d'avertissement appropriés s'affichent.

Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l' C:\Program Files\NetApp\SnapCenter WebApp pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration haute disponibilité, si vous mettez à jour SnapManager.Web.UI.dll.config, vous devez mettre à jour le fichier sur les deux nœuds et redémarrer le pool d'applications SnapCenter.

Le chemin d'accès par défaut de Windows est C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

Le chemin d'accès par défaut de Linux est /opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. Si le type d'hôte est Linux, vérifiez l'empreinte, puis sélectionnez **confirmer et soumettre**.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

9. Surveillez la progression de l'installation.

Les fichiers journaux spécifiques à l'installation se trouvent à l'adresse /custom\_location/snapcenter/ journaux.

## Installez les modules de plug-in SnapCenter pour Linux, Windows ou AIX sur plusieurs hôtes distants à l'aide d'applets de commande

Vous pouvez installer simultanément les modules de plug-in SnapCenter pour Linux, Windows ou AIX sur plusieurs hôtes à l'aide de l'applet de commande PowerShell `Install-SmHostPackage`.

### Avant de commencer

L'utilisateur qui ajoute un hôte doit disposer des droits d'administration sur l'hôte.



Les applications de stockage et Oracle sont prises en charge sous AIX.

### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande `Open-SmConnection`, puis saisissez vos informations d'identification.
3. Installez le plug-in sur plusieurs hôtes à l'aide de l'applet de commande `Install-SmHostPackage` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

Vous pouvez utiliser l'option `-skipreccheck` lorsque vous avez installé les plug-ins manuellement et ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

4. Saisissez vos informations d'identification pour l'installation à distance.

## Installez les plug-ins pris en charge par NetApp sur les hôtes Linux à l'aide de l'interface de ligne de commande

Vous devez installer les plug-ins pris en charge par NetApp à l'aide de l'interface utilisateur SnapCenter. Si votre environnement n'autorise pas l'installation à distance du plug-in à partir de l'interface utilisateur SnapCenter, vous pouvez installer les plug-ins pris en charge par NetApp en mode console ou en mode silencieux à l'aide de l'interface de ligne de commande.

### Étapes

1. Copiez le fichier d'installation du pack de plug-ins SnapCenter pour Linux (`snapcenter_linux_host_plugin.bin`) depuis `C:\ProgramData\NetApp\SnapCenter\Package Repository` vers l'hôte sur lequel vous souhaitez installer les plug-ins pris en charge par NetApp.

Vous pouvez accéder à ce chemin à partir de l'hôte sur lequel le serveur SnapCenter est installé.

2. À partir de l'invite de commande, accédez au répertoire dans lequel vous avez copié le fichier d'installation.
3. Installez le plug-in : `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin`  
`-i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address`  
`-DSERVER_HTTPS_PORT=port_number_for_server`

- -DPORT spécifie le port de communication SMCore HTTPS.
- -DSERVER\_IP spécifie l'adresse IP du serveur SnapCenter.
- -DSERVER\_HTTPS\_PORT spécifie le port HTTPS du serveur SnapCenter.
- -DUSER\_INSTALL\_DIR indique le répertoire dans lequel vous souhaitez installer le module de plug-ins SnapCenter pour Linux.
- \_DINSTALL\_LOG\_NAME indique le nom du fichier journal.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Ajoutez l'hôte au serveur SnapCenter à l'aide de l'applet de commande Add-Smhost et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

5. Connectez-vous à SnapCenter et téléchargez le plug-in pris en charge par NetApp depuis l'interface utilisateur ou à l'aide des applets de commande PowerShell.

Vous pouvez télécharger le plug-in pris en charge par NetApp à partir de l'interface utilisateur en vous reportant "[Ajoutez des hôtes et installez des modules plug-ins sur des hôtes distants](#)" à la section.

L'aide de la cmdlet de SnapCenter et les informations de référence de la cmdlet contiennent plus d'informations sur les applets de commande PowerShell.

"[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

### Surveillez l'état d'installation des plug-ins pris en charge par NetApp

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

#### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le certificat CA

### Générer le fichier CSR de certificat CA

Vous pouvez générer une requête de signature de certificat (CSR) et importer le certificat qui peut être obtenu auprès d'une autorité de certification (CA) à l'aide de la RSC générée. Une clé privée sera associée au certificat.

CSR est un bloc de texte codé donné à un fournisseur de certificats autorisé pour obtenir le certificat d'autorité de certification signé.



La longueur de la clé RSA du certificat CA doit être d'au moins 3072 bits.

Pour plus d'informations sur la génération d'une RSC, reportez-vous à la section "[Comment générer un fichier CSR de certificat CA](#)".



Si vous possédez le certificat de l'autorité de certification pour votre domaine (\*.domain.company.com) ou votre système (machine1.domain.company.com), vous pouvez ignorer la génération du fichier CSR du certificat de l'autorité de certification. Vous pouvez déployer le certificat d'autorité de certification existant avec SnapCenter.

Pour les configurations de cluster, le nom de cluster (FQDN du cluster virtuel) et les noms d'hôte correspondants doivent être mentionnés dans le certificat de l'autorité de certification. Le certificat peut être mis à jour en remplissant le champ Nom alternatif du sujet (SAN) avant d'obtenir le certificat. Pour un certificat de type Wild card (\*.domain.company.com), le certificat contiendra implicitement tous les noms d'hôte du domaine.

### Importer des certificats CA

Vous devez importer les certificats d'autorité de certification sur le serveur SnapCenter et les plug-ins hôtes Windows à l'aide de la console de gestion Microsoft (MMC).

## Étapes

1. Accédez à la console de gestion Microsoft (MMC), puis cliquez sur **fichier > Ajouter/Supprimer Snapin**.

2. Dans la fenêtre Ajouter ou supprimer des Snap-ins, sélectionnez **certificats**, puis cliquez sur **Ajouter**.
3. Dans la fenêtre du composant logiciel enfichable certificats, sélectionnez l'option **compte ordinateur**, puis cliquez sur **Terminer**.
4. Cliquez sur **Console Root > certificats – ordinateur local > autorités de certification racines de confiance > certificats**.
5. Cliquez avec le bouton droit de la souris sur le dossier "autorités de certification racine de confiance", puis sélectionnez **toutes les tâches > Importer** pour lancer l'assistant d'importation.
6. Complétez l'assistant comme suit :

Dans cette fenêtre de l'assistant...	Procédez comme suit...
Importer une clé privée	Sélectionnez l'option <b>Oui</b> , importez la clé privée, puis cliquez sur <b>Suivant</b> .
Importer le format de fichier	N'apportez aucune modification ; cliquez sur <b>Suivant</b> .
Sécurité	Spécifiez le nouveau mot de passe à utiliser pour le certificat exporté, puis cliquez sur <b>Suivant</b> .
Exécution de l'assistant d'importation de certificat	Vérifiez le résumé, puis cliquez sur <b>Terminer</b> pour lancer l'importation.



Le certificat d'importation doit être fourni avec la clé privée (les formats pris en charge sont : \*.pfx, \*.p12 et \*.p7b).

7. Répétez l'étape 5 pour le dossier « personnel ».

### Obtenez le certificat CA imprimé

Une empreinte de certificat est une chaîne hexadécimale qui identifie un certificat. Une empreinte est calculée à partir du contenu du certificat à l'aide d'un algorithme d'empreinte.

#### Étapes

1. Effectuez les opérations suivantes sur l'interface graphique :
  - a. Double-cliquez sur le certificat.
  - b. Dans la boîte de dialogue certificat, cliquez sur l'onglet **Détails**.
  - c. Faites défiler la liste des champs et cliquez sur **Thumbprint**.
  - d. Copiez les caractères hexadécimaux de la zone.
  - e. Supprimez les espaces entre les nombres hexadécimaux.

Par exemple, si l'empreinte est : "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", après avoir retiré les espaces, il sera : "a909502dd82a41433e6f83886b00d4277a32a7b".

2. Effectuer les opérations suivantes à partir de PowerShell :

- a. Exécutez la commande suivante pour lister l'empreinte du certificat installé et identifier le certificat récemment installé par le nom de l'objet.

```
Get-ChildItem -Path Cert:\Localmachine\My
```

- b. Copiez l'empreinte.

### Configurez le certificat d'autorité de certification avec les services de plug-in d'hôte Windows

Vous devez configurer le certificat d'autorité de certification avec les services de plug-in d'hôte Windows pour activer le certificat numérique installé.

Effectuez les étapes suivantes sur le serveur SnapCenter et sur tous les hôtes du plug-in où les certificats CA sont déjà déployés.

#### Étapes

1. Supprimez la liaison du certificat existant avec le port par défaut SMCore 8145 en exécutant la commande suivante :

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

Par exemple :

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. Associez le certificat récemment installé aux services du plug-in hôte
Windows, en exécutant les commandes suivantes :
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Par exemple :

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

### Configurez le certificat CA pour le service de plug-ins pris en charge par NetApp sur l'hôte Linux

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le

## certificat numérique installé.

Les plug-ins utilisent le fichier « keystore.jks », qui se trouve dans `/opt/NetApp/snapcenter/scc/etc` à la fois comme magasin de confiance et magasin de clés.

### Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé 'KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Procédez de même pour la clé KEYSTORE\_PASS dans le fichier *agent.properties*.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in : `/opt/NetApp/snapcenter/scc/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaires pour le plug-in trust-store.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in /opt/NetApp/snapcenter/scc/etc.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Répertoriez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé KEYSTORE\_PASS dans le fichier agent.properties.

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Si le nom d'alias du certificat de l'autorité de certification est
long et contient de l'espace ou des caractères spéciaux ("*", ",", "),
remplacez le nom d'alias par un nom simple :
```

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurez le nom d'alias à partir du certificat CA dans le fichier
agent.properties.
```

Mettez cette valeur à jour par rapport à la clé SCC\_CERTIFICATE\_ALIAS.

8. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

### Configurer la liste de révocation de certificats (CRL) pour les plug-ins

#### Description de la tâche

- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est « opt/NetApp/snapcenter/scc/etc/crl ».

#### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier agent.properties par rapport à la clé CRL\_PATH.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

### Configurez le certificat CA pour le service de plug-ins pris en charge par NetApp sur l'hôte Windows

Vous devez gérer le mot de passe du magasin de clés des plug-ins et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaires dans le magasin de confiance des plug-ins et configurer la paire de clés signée CA dans le magasin de confiance des plug-ins avec le service de plug-ins SnapCenter pour activer le certificat numérique installé.

Les plug-ins utilisent le fichier *keystore.jks*, qui se trouve dans *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* à la fois comme magasin de confiance et magasin de clés.

#### Gérer le mot de passe du magasin de clés du plug-in et l'alias de la paire de clés signée par l'autorité de certification en cours d'utilisation

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés du plug-in à partir du fichier de propriétés de l'agent du plug-in.

C'est la valeur correspondant à la clé *KEYSTORE\_PASS*.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
```



Si la commande "keytool" n'est pas reconnue sur l'invite de commande Windows, remplacez la commande keytool par son chemin complet.

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe » -storepasswd -keystore.jks
```

3. Remplacez le mot de passe de tous les alias des entrées de clé privée du magasin de clés par le même mot de passe que celui utilisé pour le magasin de clés :

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore.jks
```

Procédez de même pour la clé KEYSTORE\_PASS dans le fichier *agent.properties*.

4. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés du plug-in et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

### Configurer les certificats racine ou intermédiaires pour le plug-in trust-store

Vous devez configurer les certificats racine ou intermédiaires sans la clé privée pour connecter le magasin de confiance.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajouter un certificat racine ou intermédiaire :

```
Keytool -import -truacts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore.jks
```

5. Redémarrez le service après avoir configuré les certificats racine ou intermédiaires pour le plug-in trust-store.



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

### Configurer la paire de clés signée par l'autorité de certification pour le plug-in trust-store

Vous devez configurer la paire de clés signée par l'autorité de certification dans le magasin de confiance du plug-in.

#### Étapes

1. Accédez au dossier contenant le keystore du plug-in *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localisez le fichier *keystore.jks*.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
```

4. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.

```
Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12
-destkeystore.jks -desstoretype JKS
```

5. Répertoirez les certificats ajoutés dans le magasin de clés.

```
keytool -list -v -keystore keystore.jks
```

6. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
7. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.

Le mot de passe du magasin de clés du plug-in par défaut est la valeur de la clé KEYSTORE\_PASS dans le fichier agent.properties.

```
Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore.jks
```

8. Configurez le nom d'alias à partir du certificat CA dans le fichier *agent.properties*.

Mettez cette valeur à jour par rapport à la clé SCC\_CERTIFICATE\_ALIAS.

9. Redémarrez le service après avoir configuré la paire de clés signée par l'autorité de certification pour le plug-in trust-store.

## Configurer la liste de révocation des certificats (CRL) pour les plug-ins SnapCenter

### Description de la tâche

- Pour télécharger le fichier CRL le plus récent pour le certificat d'autorité de certification associé, reportez-vous à la section ["Comment mettre à jour le fichier de liste de révocation de certificats dans le certificat d'autorité de certification SnapCenter"](#).
- Les plug-ins SnapCenter rechercheront les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour les plug-ins SnapCenter est 'C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'.

### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier *agent.properties* par rapport à la clé CRL\_PATH.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

## Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

## Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.
-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

# Préparation à la protection des données

## Conditions préalables à l'utilisation des plug-ins pris en charge par NetApp

Avant d'utiliser les plug-ins pris en charge par SnapCenter NetApp, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches requises.

- Installer et configurer SnapCenter Server.
- Connectez-vous au serveur SnapCenter.
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage et en créant des identifiants, le cas échéant.
- Ajoutez des hôtes, et installez et téléchargez les plug-ins.
- Le cas échéant, installez Java 11 sur l'hôte du plug-in.
- Si vous disposez de plusieurs chemins d'accès aux données (LIF) ou d'une configuration dNFS, vous pouvez effectuer les opérations suivantes à l'aide de l'interface de ligne de commandes SnapCenter sur l'hôte de base de données :

- Par défaut toutes les adresses IP de l'hôte de base de données sont ajoutées à la règle d'exportation du stockage NFS dans la machine virtuelle de stockage (SVM) pour les volumes clonés. Si vous souhaitez avoir une adresse IP spécifique ou restreindre à un sous-ensemble d'adresses IP, exécutez l'interface de ligne de commande `set-PreferredHostIPsInStorageExportPolicy`.
- Si plusieurs chemins de données (LIF) sont disponibles dans des SVM, SnapCenter choisit le chemin d'accès aux données (LIF) approprié pour le montage du volume cloné NFS. Toutefois, si vous souhaitez spécifier un chemin de données spécifique (LIF), vous devez exécuter l'interface de ligne de commande `set-SvmPreferredDataPath`. Les informations relatives aux paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence sur les commandes du logiciel SnapCenter](#)".
- Configurer SnapMirror et SnapVault pour la réplication de sauvegarde.
- Assurez-vous que le port 9090 n'est pas utilisé par une autre application de l'hôte.

Le port 9090 doit être réservé aux plug-ins pris en charge par NetApp en plus des autres ports requis par SnapCenter.

## Utilisation des ressources, des groupes de ressources et des règles pour protéger les ressources des plug-ins pris en charge par NetApp

Avant d'utiliser SnapCenter, il est utile de maîtriser les concepts de base associés aux opérations de sauvegarde, de clonage et de restauration que vous souhaitez effectuer. Vous interagissez avec les ressources, les groupes de ressources et les stratégies pour différentes opérations.

- Les ressources sont généralement des bases de données, des systèmes de fichiers Windows ou des machines virtuelles que vous sauvegardez ou clonez avec SnapCenter.
- Un groupe de ressources SnapCenter est un ensemble de ressources sur un hôte ou un cluster.

Lorsque vous effectuez une opération sur un groupe de ressources, vous effectuez cette opération sur les ressources définies dans le groupe de ressources en fonction du planning que vous spécifiez pour le groupe de ressources.

Vous pouvez sauvegarder à la demande une seule ressource ou un groupe de ressources. Vous pouvez également effectuer des sauvegardes planifiées pour des ressources et des groupes de ressources uniques.

- Ces règles précisent la fréquence des sauvegardes, la conservation des copies, la réplication, les scripts et d'autres caractéristiques des opérations de protection des données.

Lorsque vous créez un groupe de ressources, vous sélectionnez une ou plusieurs stratégies pour ce groupe. Vous pouvez également sélectionner une stratégie lorsque vous effectuez une sauvegarde à la demande pour une seule ressource.

Pensez à un groupe de ressources comme définissant *quoi* vous voulez protéger et quand vous voulez le protéger en termes de jour et de temps. Pensez à une stratégie comme définir *comment* vous voulez la protéger. Si vous sauvegardez toutes les bases de données ou que vous sauvegardez tous les systèmes de fichiers d'un hôte, par exemple, vous pouvez créer un groupe de ressources qui inclut toutes les bases de données ou tous les systèmes de fichiers de l'hôte. Vous pouvez ensuite associer deux stratégies au groupe de ressources : une stratégie quotidienne et une stratégie horaire. Lorsque vous créez le groupe de ressources et joignez les stratégies, vous pouvez configurer le groupe de ressources de manière à effectuer

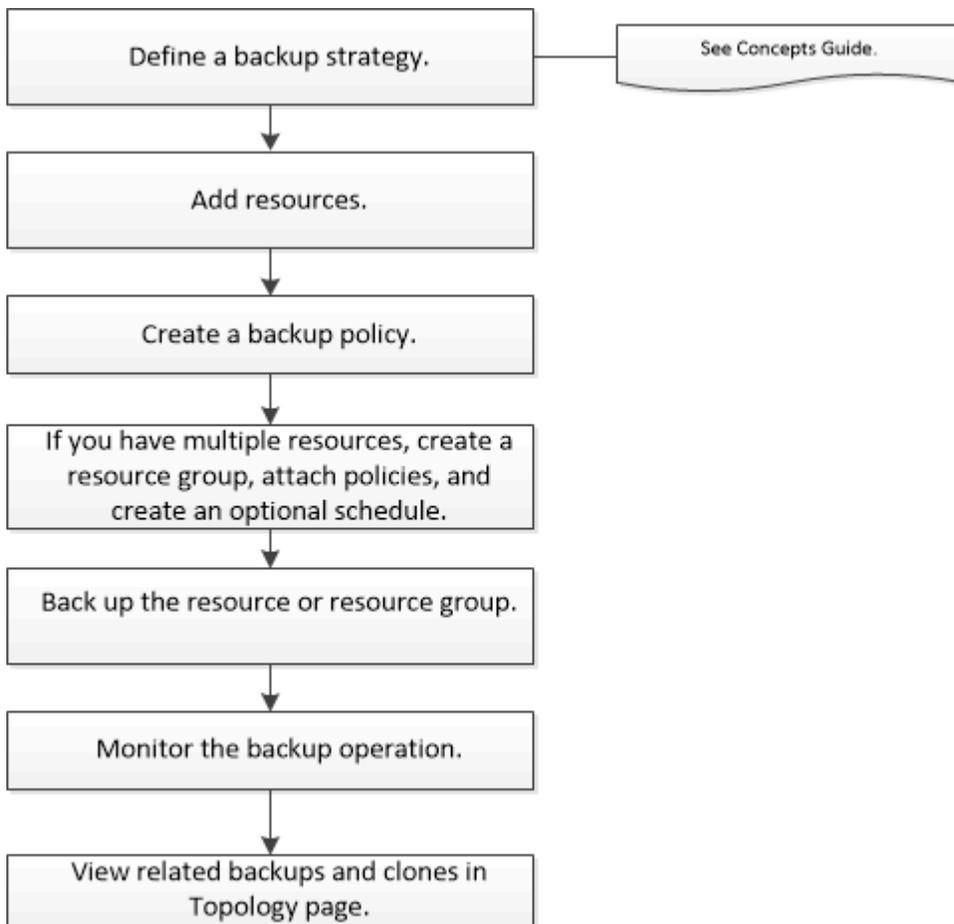
une sauvegarde quotidienne basée sur les fichiers et un autre programme qui effectue une sauvegarde horaire basée sur les copies Snapshot.

## Sauvegarde des ressources des plug-ins pris en charge par NetApp

### Sauvegarde des ressources des plug-ins pris en charge par NetApp

Le workflow de sauvegarde comprend la planification, l'identification des ressources de sauvegarde, la gestion des stratégies de sauvegarde, la création de groupes de ressources et la connexion de stratégies, la création de sauvegardes et le contrôle des opérations.

Le workflow suivant montre la séquence dans laquelle vous devez effectuer l'opération de sauvegarde :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. Pour plus d'informations sur les applets de commande PowerShell, utilisez l'aide du cmdlet SnapCenter ou consultez le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#)

### Ajoutez des ressources aux plug-ins NetApp pris en charge

Vous devez ajouter les ressources à sauvegarder ou à cloner. Selon votre environnement, les ressources peuvent être des instances de base de données ou des

collections que vous souhaitez sauvegarder ou cloner.

### Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes, la création de connexions au système de stockage et l'ajout d'informations d'identification.
- Vous devez avoir chargé les plug-ins sur SnapCenter Server.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Ajouter une ressource**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez le nom de la ressource.
Nom d'hôte	Sélectionnez l'hôte.
Type	Sélectionnez le type. Le type est défini par l'utilisateur conformément au fichier de description du plug-in. Par exemple, base de données et instance.  Si le type sélectionné a un parent, entrez les détails du parent. Par exemple, si le type est base de données et que le parent est instance, entrez les détails de l'instance.
Nom d'identification	Sélectionnez Credential ou créez une nouvelle information d'identification.
Chemins de montage	Entrez les chemins de montage sur lesquels la ressource est montée. Cette option est applicable uniquement à un hôte Windows.

4. Sur la page fournir l'empreinte du stockage, sélectionnez un système de stockage, choisissez un ou plusieurs volumes, LUN et qtrees, puis sélectionnez **Enregistrer**.

Facultatif : sélectionnez le  Icône pour ajouter d'autres volumes, LUN et qtrees à partir d'autres systèmes de stockage.



Les plug-ins pris en charge par NetApp ne prennent pas en charge la détection automatique des ressources. De plus, les détails du stockage des environnements physiques et virtuels ne sont pas découverts automatiquement. Vous devez fournir les informations de stockage pour les environnements physiques et virtuels tout en créant les ressources.

5. Dans la page Resource Settings, fournissez des paires clé-valeur personnalisées pour la ressource.



Assurez-vous que le nom des clés personnalisées est en majuscules.

#### Resource settings

Name	Value
HOST	localhost
PORT	3306
MASTER_SLAVE	NO

Pour connaître les paramètres de plug-in respectifs, reportez-vous à la section "[Paramètres de configuration de la ressource](#)"

6. Passez en revue le résumé, puis sélectionnez **Terminer**.

#### Résultat

Les ressources s'affichent avec des informations telles que le type, le nom de l'hôte ou du cluster, les groupes de ressources et les stratégies associés et l'état global.



Vous devez actualiser les ressources si les bases de données sont renommées en dehors de SnapCenter.

#### Une fois que vous avez terminé

Si vous souhaitez donner accès aux ressources à d'autres utilisateurs, l'administrateur SnapCenter doit attribuer des ressources à ces utilisateurs. Cela permet aux utilisateurs d'effectuer les actions pour lesquelles ils ont des autorisations sur les ressources qui leur sont assignées.

Après avoir ajouté les ressources, vous pouvez modifier les détails de la ressource. Si des sauvegardes sont associées à une ressource plug-ins prise en charge par NetApp, les champs suivants ne peuvent pas être modifiés : nom de ressource, type de ressource et nom d'hôte.

## Paramètres de configuration de la ressource

Si vous ajoutez les plug-ins manuellement, vous pouvez utiliser les paramètres suivants pour configurer la ressource dans la page Paramètres de ressource.

### Plug-in pour MongoDB

Paramètres de ressource :

- MONGODB\_APP\_SERVER=(pour le type de ressource en tant que cluster partagé) ou MONGODB\_REPLIASET\_SERVER=(pour le type de ressource en tant que Repliaset)
- OPLOG\_PATH=(paramètre facultatif s'il est fourni à partir de MongoDB.propertiesfile)
- MONGODB\_AUTHENTICATION\_TYPE= (ORDINAIRE pour l'authentification LDAP et aucun pour les autres)

Vous devez fournir les paramètres suivants dans le fichier n MongoDB.properties :

- DISABLE\_STARTING\_SERVICES=
  - N si les services de démarrage/arrêt sont effectués par le plug-in.
  - Y si start/\*\*stop les services sont exécutés par l'utilisateur.
  - Le paramètre facultatif comme valeur par défaut est défini sur N.
- OPLOG\_PATH\_= (paramètre facultatif s'il est déjà fourni en tant que paire clé-valeur personnalisée dans SnapCenter).

### Plug-in pour MaxDB

Paramètres de ressource :

- XUSER\_ENABLE (y|N) active ou désactive l'utilisation d'un xuser pour MaxDB de sorte qu'un mot de passe ne soit pas requis pour l'utilisateur de la base de données.
- HANDLE\_LOGWRITER (y|N) exécute les opérations suspendre l'enregistreur de journal (N) ou reprendre l'enregistreur de journal (y).
- DBMCLICMD (PATH\_to\_dbmcli\_cmd) indique le chemin d'accès à la commande MaxDB dbmcli. Si ce n'est pas le cas, dbmcli sur le chemin de recherche est utilisé.



Dans un environnement Windows, le chemin doit être entre guillemets ("...").

- SQLCLICMD (chemin\_vers\_sqlcli\_cmd) indique le chemin d'accès à la commande MaxDB sqlcli. Si le chemin n'est pas défini, sqlcli est utilisé sur le chemin de recherche.
- MAXDB\_UPDATE\_HIST\_LOG (y|N) indique au programme de sauvegarde MaxDB s'il doit mettre à jour le journal historique MaxDB.
- MAXDB\_CHECK\_SNAPSHOT\_DIR : exemple, SID1:Directory[,Directory...]; [SID2:directory[,Directory...]] Vérifie qu'une opération de copie Snapshot Snap Creator a réussi et s'assure que le snapshot est créé.

Cela s'applique uniquement à NFS. Le répertoire doit pointer vers l'emplacement qui contient le répertoire .snapshot. Plusieurs répertoires peuvent être inclus dans une liste séparée par des virgules.

Dans MaxDB 7.8 et versions ultérieures, la demande de sauvegarde de la base de données est marquée comme ayant échoué dans l'historique des sauvegardes.

- MAXDB\_BACKUP\_TEMPLATES : spécifie un modèle de sauvegarde pour chaque base de données.

Le modèle doit exister et être un type externe de modèle de sauvegarde. Pour activer l'intégration d'instantanés pour MaxDB 7.8 et versions ultérieures, vous devez disposer de la fonctionnalité de serveur d'arrière-plan MaxDB et d'un modèle de sauvegarde MaxDB de type EXTERNE déjà configuré.

- MAXDB\_BG\_SERVER\_PREFIX : indique le préfixe du nom du serveur d'arrière-plan.

Si LE paramètre MAXDB\_BACKUP\_TEMPLATES est défini, vous devez également définir LE paramètre MAXDB\_BG\_SERVER\_PREFIX. Si vous ne définissez pas le préfixe, la valeur par défaut na\_bg\_ est utilisée.

### Plug-in pour SAP ASE

Paramètres de ressource :

- SYBASE\_SERVER (nom\_serveur\_données) spécifie le nom du serveur de données Sybase (option-S sur la commande isql). Par exemple, p\_test.
- SYBASE\_DATABASES\_EXCLUDE (db\_name) permet d'exclure les bases de données si la construction "ALL" est utilisée.

Vous pouvez spécifier plusieurs bases de données à l'aide d'une liste séparée par des points-virgules. Par exemple : pubs2;test\_db1.

- SYBASE\_USER : nom\_utilisateur indique l'utilisateur du système d'exploitation qui peut exécuter la commande isql.

Requis pour UNIX. Ce paramètre est requis si l'utilisateur exécutant les commandes de démarrage et d'arrêt de Snap Creator Agent (généralement l'utilisateur root) et l'utilisateur exécutant la commande isql sont différents.

- SYBASE\_TRAN\_DUMP nom\_bdd:chemin\_répertoire vous permet d'effectuer un vidage de transaction Sybase après la création d'un instantané. Par exemple, pubs2:/sybasedumps/ pubs2

Vous devez spécifier chaque base de données nécessitant un vidage de transaction.

- SYBASE\_TRAN\_DUMP\_COMPRESS (y|N ) active ou désactive la compression de vidage de transaction Sybase native.
- SYBASE\_ISQL\_CMD (par exemple, /opt/sybase/OCS-15\_0/bin/isql) définit le chemin d'accès à la commande isql.
- SYBASE\_EXCLUDE\_TEMPDB (y|N) vous permet d'exclure automatiquement les bases de données temporaires créées par l'utilisateur.

### Plug-in pour applications Oracle (ORASCPM)

Paramètres de ressource :

- SQLPLUS\_CMD spécifie le chemin vers sqlplus.
- ORACLE\_DATABASES répertorie les bases de données Oracle à sauvegarder et l'utilisateur correspondant (database:user).
- CNTL\_FILE\_BACKUP\_DIR spécifie le répertoire de sauvegarde du fichier de contrôle.
- ORA\_TEMP spécifie le répertoire des fichiers temporaires.

- ORACLE\_HOME spécifie le répertoire dans lequel le logiciel Oracle est installé.
- ARCHIVE\_LOG\_ONLY indique si les journaux d'archive doivent être sauvegardés ou non.
- ORACLE\_BACKUPMODE spécifie s'il faut effectuer une sauvegarde en ligne ou hors ligne.
- ORACLE\_EXPORT\_PARAMETERS spécifie si les variables d'environnement définies ci-dessus doivent être réexportées lors de l'exécution de `/bin/su <utilisateur exécutant sqlplus> -c sqlplus /nolog <cmd>`. C'est généralement le cas lorsque l'utilisateur exécutant sqlplus n'a pas défini toutes les variables d'environnement nécessaires à la connexion à la base de données via `connect / as sysdba`.

## Créez des règles pour les ressources des plug-ins pris en charge par NetApp

Avant d'utiliser SnapCenter pour sauvegarder des ressources spécifiques au plug-in pris en charge par NetApp, vous devez créer une stratégie de sauvegarde pour le groupe de ressources ou de ressources que vous souhaitez sauvegarder.

### Avant de commencer

- Vous devriez avoir défini votre stratégie de sauvegarde.

Pour en savoir plus, consultez les informations sur la définition d'une stratégie de protection des données pour les plug-ins pris en charge par NetApp.

- Vous devriez avoir préparé pour la protection des données.

La préparation à la protection des données comprend des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la création de connexions au système de stockage et l'ajout de ressources.

- Les serveurs virtuels de stockage (SVM) doivent vous être affectés pour les opérations de mise en miroir ou de copie sécurisée.

Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir affecté des SVM aux volumes source et de destination.

- Vous devez avoir ajouté manuellement les ressources que vous voulez protéger.

### Description de la tâche

- Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes. En outre, vous pouvez spécifier les paramètres de réplication, de script et d'application.
- La définition d'options dans une stratégie permet de gagner du temps lorsque vous souhaitez réutiliser la stratégie pour un autre groupe de ressources.
- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.
  - La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.
  - Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.



Les paramètres SnapLock principaux sont gérés dans la stratégie de sauvegarde SnapCenter et les paramètres SnapLock secondaires sont gérés par ONTAP.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et les détails de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez le type de stockage.
  - b. Dans la section Paramètres de sauvegarde personnalisés, indiquez tous les paramètres de sauvegarde spécifiques qui doivent être transmis au plug-in au format clé-valeur.

Vous pouvez fournir plusieurs valeurs de clé à transmettre au plug-in.

6. Dans la page instantané et réplication, effectuez les opérations suivantes :
  - a. Spécifiez le type d'horaire en sélectionnant **On Demand, Hourly, Daily, Weekly** ou **Monthly**.



Vous pouvez spécifier la planification (date de début, date de fin et fréquence) de l'opération de sauvegarde lors de la création d'un groupe de ressources. Cela vous permet de créer des groupes de ressources partageant la même stratégie et la même fréquence de sauvegarde, mais vous permet d'affecter des programmes de sauvegarde différents à chaque stratégie.



Si vous avez prévu 2 h 00, l'horaire ne sera pas déclenché pendant l'heure d'été (DST).

- b. Dans la section Paramètres de l'instantané, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionné dans la page **Type de sauvegarde** :

Les fonctions que vous recherchez...	Alors...
Conserver un certain nombre d'instantanés	<p>Sélectionnez <b>copies à conserver</b>, puis indiquez le nombre d'instantanés que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> </div> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> </div>
Conserver les instantanés pendant un certain nombre de jours	Sélectionnez <b>conserver les copies pour</b> , puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les instantanés avant de les supprimer.
Période de verrouillage des copies Snapshot principales	<p>Sélectionnez période de verrouillage des instantanés, puis sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>
Période de verrouillage des copies Snapshot secondaires	Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b> , puis sélectionnez jours, mois ou années.

c. Sélectionnez un libellé de stratégie.

Selon l'étiquette de règle que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à l'étiquette.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

7. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif.

Pour ce champ...	Procédez comme ça...
<p><b>Mettre à jour SnapMirror après avoir créé une copie Snapshot locale</b></p>	<p>Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).</p> <p>Si la relation de protection dans ONTAP est de type miroir et coffre-fort et si vous sélectionnez uniquement cette option, le snapshot créé sur le primaire ne sera pas transféré vers la destination, mais sera répertorié dans la destination. Si cet instantané est sélectionné à partir de la destination pour effectuer une opération de restauration, le message d'erreur suivant s'affiche : l'emplacement secondaire n'est pas disponible pour la sauvegarde en miroir/en coffre-fort sélectionnée.</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal.</p> <p>Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Voir "<a href="#">Consultez la page topologie des plug-ins pris en charge par NetApp, ainsi que les sauvegardes et clones liés aux ressources</a>".</p>

Pour ce champ...	Procédez comme ça...
<b>Mettre à jour SnapVault après avoir créé une copie Snapshot locale</b>	<p>Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).</p> <p>Lors de la réplication secondaire, le délai d'expiration SnapLock charge le délai d'expiration du SnapLock principal. Si vous cliquez sur le bouton <b>Rafraîchir</b> de la page topologie, l'heure d'expiration SnapLock secondaire et primaire est actualisée à partir de ONTAP.</p> <p>Lorsque SnapLock est configuré uniquement sur le serveur secondaire à partir de ONTAP appelé coffre-fort SnapLock, cliquez sur le bouton <b>Actualiser</b> de la page topologie pour actualiser la période de verrouillage sur le serveur secondaire extrait de ONTAP.</p> <p>Pour plus d'informations sur le coffre-fort SnapLock, reportez-vous à la section archivage des snapshots en mode WORM sur une destination de coffre-fort.</p> <p>Voir "<a href="#">Consultez la page topologie des plug-ins pris en charge par NetApp, ainsi que les sauvegardes et clones liés aux ressources</a>".</p>
<b>Nombre de tentatives d'erreur</b>	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer des groupes de ressources et attacher des stratégies

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger. Il vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez Nouveau groupe de ressources.

3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.  Remarque : le nom du groupe de ressources ne doit pas dépasser 250 caractères.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.  Par exemple, si vous ajoutez HR comme balise à plusieurs groupes de ressources, vous trouverez plus tard tous les groupes de ressources associés à la balise HR.
Utilisez le format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.  Par exemple, <i>customtext_Resource group_policy_hostname</i> ou <i>Resource group_hostname</i> . Par défaut, un horodatage est ajouté au nom du Snapshot.

4. Facultatif : dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.

Cela aide à filtrer les informations affichées à l'écran.

5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis sélectionnez la flèche droite pour les déplacer vers la section **Ressources sélectionnées**.

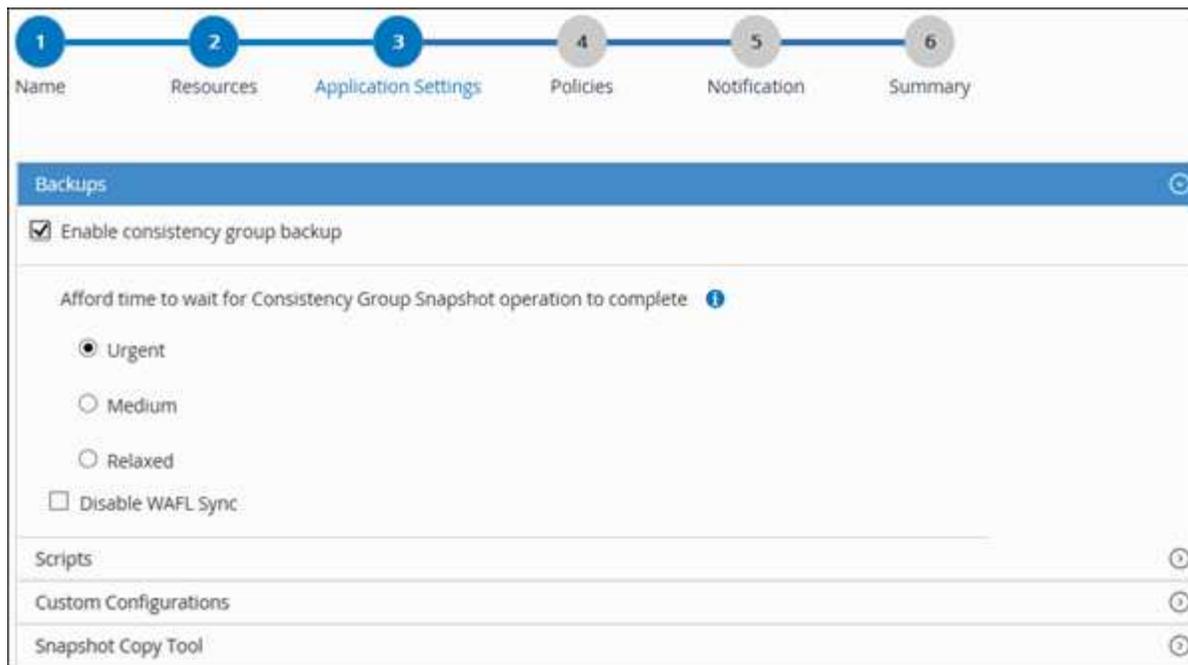
6. Facultatif : dans la page **Paramètres de l'application**, procédez comme suit :

a. Sélectionnez la flèche sauvegardes pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde de groupe de cohérence et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Permet d'attendre la fin de l'opération Snapshot du groupe de cohérence	Sélectionnez urgent, Moyen ou détendu pour spécifier le temps d'attente pour l'exécution de l'opération Snapshot.  Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

+



- a. Sélectionnez la flèche scripts et entrez les commandes pré et post pour les opérations quiesce, Snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- b. Sélectionnez la flèche configurations personnalisées et entrez les paires clé-valeur personnalisées requises pour toutes les opérations de protection des données utilisant cette ressource.

Paramètre	Réglage	Description
ARCHIVE_LOG_ENABLE	(O/N)	Permet à la gestion des journaux d'archive de supprimer les journaux d'archive.
ARCHIVAGE_LOG_RÉTENTION	nombre_de_jours	Indique le nombre de jours pendant lesquels les journaux d'archive sont conservés.  Ce paramètre doit être supérieur ou égal à NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_répertoire/logs	Indique le chemin d'accès au répertoire contenant les journaux d'archive.

Paramètre	Réglage	Description
ARCHIVE_LOG_EXT	extension_fichier	Spécifie la longueur d'extension du fichier journal d'archives.  Par exemple, si le journal d'archives est log_backup_0_0_0_0.161518551942 9 et si la valeur file_extension est 5, l'extension du journal conserve 5 chiffres, soit 16151.
ARCHIVE_LOG_RÉCURSIVE_SE ARCH	(O/N)	Permet la gestion des journaux d'archivage dans les sous-répertoires.  Vous devez utiliser ce paramètre si les journaux d'archivage sont situés sous des sous-répertoires.

c. Sélectionner la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour utiliser le plug-in pour Windows et placer le système de fichiers dans un état cohérent avant de créer un Snapshot. Pour les ressources Linux, cette option n'est pas applicable.	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .  Cette option ne s'applique pas au plug-in SnapCenter pour base de données SAP HANA.
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .
Pour saisir la commande à exécuter sur l'hôte pour créer des snapshots.	Sélectionnez <b>autre</b> , puis entrez la commande à exécuter sur l'hôte pour créer un instantané.

7. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en sélectionnant  .

Les stratégies sont répertoriées dans la section **configurer les plannings pour les stratégies sélectionnées**.

b. Dans la colonne **configurer les plannings**, sélectionnez  pour la stratégie que vous souhaitez configurer.

- c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification et sélectionnez OK.

Où *nom\_règle* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués. Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la liste déroulante **préférence de messagerie** de la page **notification**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Le serveur SMTP doit être configuré dans **Paramètres > Paramètres globaux**.

9. Passez en revue le résumé, puis sélectionnez **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire des ressources sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.
- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :
  - a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous

pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.

6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.

7. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

a. Sélectionnez le type de la règle de réplication.



Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.
- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.



Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.
- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.
- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.
- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell set-SmSmtServer.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créer une connexion au système de stockage et une autorisation d'accès à l'aide des applets de commande PowerShell

Vous devez créer une connexion SVM (Storage Virtual machine) et une identifiant avant d'utiliser les applets de commande PowerShell pour réaliser les opérations de protection des données.

### Avant de commencer

- Vous devez avoir préparé l'environnement PowerShell pour exécuter les applets de commande PowerShell.
- Pour créer des connexions de stockage, vous devez disposer des autorisations requises dans le rôle d'administrateur d'infrastructure.
- Vous devez vous assurer que les installations du plug-in ne sont pas en cours.

Les installations de plug-ins hôtes ne doivent pas être en cours d'ajout d'une connexion au système de stockage, car le cache hôte n'est pas nécessairement mis à jour et l'état des bases de données peut être affiché dans l'interface utilisateur graphique de SnapCenter sous la forme « non disponible pour la sauvegarde » ou « non sur le stockage NetApp ».

- Les noms des systèmes de stockage doivent être uniques.

SnapCenter ne prend pas en charge plusieurs systèmes de stockage portant le même nom sur des clusters différents. Chaque système de stockage pris en charge par SnapCenter doit disposer d'un nom unique et d'une adresse IP de LIF de gestion unique.

### Étapes

1. Lancez une session de connexion PowerShell Core à l'aide de l'applet de commande `Open-SmConnection`.

Cet exemple ouvre une session PowerShell :

```
PS C:\> Open-SmConnection
```

2. Créez une nouvelle connexion au système de stockage à l'aide de l'applet de commande `Add-SmStorageConnection`.

Dans cet exemple, une nouvelle connexion au système de stockage est créée :

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Créez une nouvelle information d'identification à l'aide de l'applet de commande `Add-SmCredential`.

Cet exemple crée un nouvel identifiant nommé `FinancieAdmin` avec les informations d'identification Windows :

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Sauvegarde de ressources individuelles des plug-ins pris en charge par NetApp

Si une ressource individuelle de plug-ins pris en charge par NetApp ne fait partie d'aucun groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources. Vous pouvez sauvegarder la ressource à la demande ou, si une stratégie est associée à la ressource et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Avant de commencer

- Vous devez avoir créé une stratégie de sauvegarde.
- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror avec un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Cliquez sur , puis sélectionnez le nom d'hôte et le type de ressource pour filtrer les ressources. Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

3. Cliquez sur la ressource à sauvegarder.
4. Dans la page ressource, si vous souhaitez utiliser un nom personnalisé, cochez la case **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé pour le nom de l'instantané.

Par exemple, *customtext\_policy\_hostname* ou *Resource\_hostname*. Par défaut, un horodatage est ajouté au nom du Snapshot.

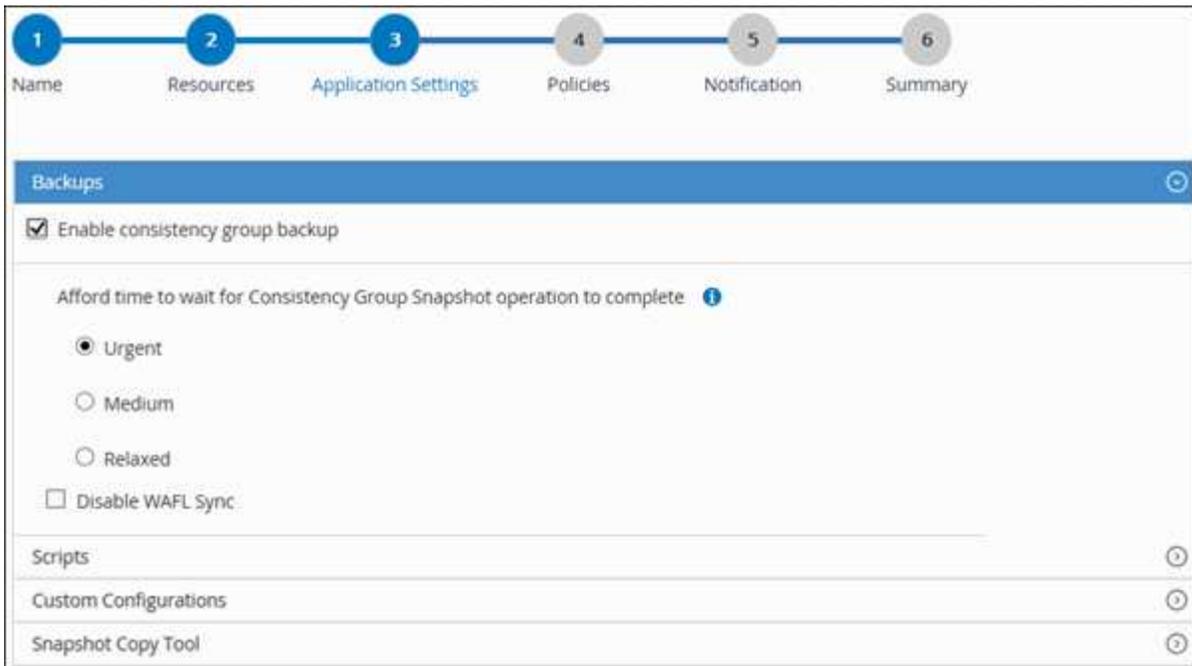
5. Dans la page Paramètres de l'application, procédez comme suit :

- a. Cliquez sur la flèche **backups** pour définir des options de sauvegarde supplémentaires :

Activez la sauvegarde du groupe de cohérence, si nécessaire, et effectuez les tâches suivantes :

Pour ce champ...	Procédez comme ça...
Permet d'attendre la fin de l'opération Snapshot du groupe de cohérence	Sélectionnez urgent, Moyen ou détendu pour spécifier le temps d'attente pour l'exécution de l'opération Snapshot.  Urgent = 5 secondes, Moyen = 7 secondes et détendu = 20 secondes.
Désactivez la synchronisation WAFL	Sélectionnez cette option pour éviter de forcer un point de cohérence WAFL.

+



- a. Cliquez sur la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce. Vous pouvez également exécuter des pré-commandes avant de quitter l'opération de sauvegarde.

Des préscripits et des postscripts sont exécutés sur le serveur SnapCenter.

- b. Cliquez sur la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
- c. Cliquez sur la flèche **outil de copie d'instantanés** pour sélectionner l'outil de création d'instantanés :

Les fonctions que vous recherchez...	Alors...
SnapCenter pour créer une copie Snapshot au niveau du stockage	Sélectionnez <b>SnapCenter sans cohérence du système de fichiers</b> .
SnapCenter pour utiliser le plug-in pour Windows afin de mettre le système de fichiers dans un état cohérent, puis de créer une copie Snapshot	Sélectionnez <b>SnapCenter avec cohérence du système de fichiers</b> .
Pour saisir la commande permettant de créer un Snapshot	Sélectionnez <b>autre</b> , puis entrez la commande pour créer un instantané.

6. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies

sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres > Paramètres globaux**.

8. Vérifiez le résumé, puis cliquez sur **Terminer**.

La page topologie des ressources s'affiche.

9. Cliquez sur **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
Open-smconnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

L'invite du nom d'utilisateur et du mot de passe s'affiche.

2. Ajoutez des ressources à l'aide de l'applet de commande Add-SmResources.

Cet exemple ajoute des ressources :

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_voll_scc55_sscore_test_com";"QREENAME"="qtree
Voll";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Créez une stratégie de sauvegarde à l'aide de l'applet de commande Add-SmPolicy.

Cet exemple crée une nouvelle stratégie de sauvegarde :

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Ajoutez un nouveau groupe de ressources à SnapCenter à l'aide de l'applet de commande Add-SmResourceGroup.

Cet exemple crée un nouveau groupe de ressources avec la stratégie et les ressources spécifiées :

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dum
myPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Lancez une nouvelle tâche de sauvegarde à l'aide de la cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Affichez l'état de la tâche de sauvegarde à l'aide de l'applet de commande Get-SmBackupReport.

Cet exemple affiche un rapport récapitulatif de tous les travaux exécutés à la date spécifiée :

```
Get-SmBackupReport -JobId 149
```

```
BackedUpObjects : {QTREE2, QTREE}
FailedObjects : {}
IsScheduled : False
HasMetadata : False
SmBackupId : 1
SmJobId : 149
StartDateTime : 1/15/2024 1:35:17 AM
EndDateTime : 1/15/2024 1:36:19 AM
Duration : 00:01:02.4265750
CreatedDateTime : 1/15/2024 1:35:51 AM
Status : Completed
ProtectionGroupName :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId : 1
PolicyName : test2
SmPolicyId : 4
BackupName :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus : NotApplicable
VerificationStatuses :
SmJobError :
BackupType : SCC_BACKUP
CatalogingStatus : NotApplicable
CatalogingStatuses :
ReportDataCreatedDateTime :
PluginCode : SCC
PluginName : DummyPlugin
PluginDisplayName : DummyPlugin
JobTypeId :
JobHost : scc55.sscore.test.com
```

## Sauvegarder les groupes de ressources des plug-ins pris en charge par NetApp

Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont automatiquement effectuées en fonction de la planification.

### Avant de commencer

- Vous devez avoir créé un groupe de ressources associé à une stratégie.

- Si vous souhaitez sauvegarder une ressource avec une relation SnapMirror sur un système de stockage secondaire, le rôle ONTAP attribué à l'utilisateur de stockage doit inclure le privilège « napmirror All ». Toutefois, si vous utilisez le rôle « vsadmin », le privilège « napmirror all » n'est pas requis.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

Vous pouvez effectuer une recherche dans le groupe de ressources en entrant le nom du groupe de ressources dans la zone de recherche ou en cliquant sur et en  sélectionnant la balise. Vous pouvez ensuite cliquer sur  pour fermer le volet de filtre.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis cliquez sur **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si vous avez associé plusieurs stratégies au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

5. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

- Dans les configurations MetroCluster, il est possible que SnapCenter ne détecte pas une relation de protection après un basculement.

"Impossible de détecter la relation SnapMirror ou SnapVault après le basculement de MetroCluster"

- Si vous sauvegardez des données d'application sur des disques VMDK et que la taille du segment de mémoire Java du plug-in SnapCenter pour VMware vSphere n'est pas suffisamment importante, la sauvegarde risque d'échouer. Pour augmenter la taille du segment de mémoire Java, localisez le fichier de script `/opt/netapp/init_scripts/scvservice`. Dans ce script, le `do_start method Command` démarre le service du plug-in SnapCenter VMware. Mettez à jour cette commande à l'adresse suivante : `Java -jar -Xmx8192M -Xms4096M`.

## Surveillez les opérations de sauvegarde des ressources prises en charge par les plug-ins NetApp

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès

-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Annulez les opérations de sauvegarde pour les plug-ins NetApp pris en charge

Vous pouvez annuler les opérations de sauvegarde mises en file d'attente.

### Ce dont vous aurez besoin

- Pour annuler des opérations, vous devez être connecté en tant qu'administrateur SnapCenter ou propriétaire du travail.
- Vous pouvez annuler une opération de sauvegarde à partir de la page **Monitor** ou du volet **Activity**.
- Vous ne pouvez pas annuler une opération de sauvegarde en cours d'exécution.
- Vous pouvez utiliser l'interface graphique SnapCenter, les applets de commande PowerShell ou les commandes CLI pour annuler les opérations de sauvegarde.
- Le bouton **Annuler tâche** est désactivé pour les opérations qui ne peuvent pas être annulées.
- Si vous avez sélectionné **tous les membres de ce rôle peuvent voir et fonctionner sur d'autres objets membres** dans la page utilisateurs\groupes lors de la création d'un rôle, vous pouvez annuler les opérations de sauvegarde en file d'attente d'autres membres tout en utilisant ce rôle.

## Étapes

1. Effectuez l'une des opérations suivantes :

Du...	Action
Page moniteur	<ol style="list-style-type: none"> <li>Dans le volet de navigation de gauche, cliquez sur <b>moniteur &gt; travaux</b>.</li> <li>Sélectionnez l'opération, puis cliquez sur <b>Annuler le travail</b>.</li> </ol>
Volet activité	<ol style="list-style-type: none"> <li>Après avoir lancé l'opération de sauvegarde, cliquez sur * *  dans le volet activité pour afficher les cinq opérations les plus récentes.</li> <li>Sélectionner l'opération.</li> <li>Dans la page Détails du travail, cliquez sur <b>Annuler le travail</b>.</li> </ol>

L'opération est annulée et la ressource est rétablie à l'état précédent.

## Consultez la page topologie des plug-ins pris en charge par NetApp, ainsi que les sauvegardes et clones liés aux ressources

Lorsque vous préparez une sauvegarde ou le clonage d'une ressource, vous trouverez peut-être utile d'afficher une représentation graphique de toutes les sauvegardes et clones sur le stockage primaire et secondaire. Sur la page topologie, vous pouvez voir toutes les sauvegardes et clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes et clones, puis les sélectionner pour effectuer des opérations de protection des données.

### Description de la tâche

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).

- 
 affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.
- 
 Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.
- 
 Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes du miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.
- 
 Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.

Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par

exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie pour ne conserver que 4 sauvegardes, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes du miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologique de la ressource sélectionnée s'affiche.

4. Consultez la fiche récapitulative pour connaître le nombre de sauvegardes et de clones disponibles sur les stockages primaire et secondaire.

La section carte récapitulative affiche le nombre total de sauvegardes et de clones.

Cliquez sur le bouton Actualiser pour afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque la ressource d'application est répartie sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Après une sauvegarde à la demande, en cliquant sur le bouton **Refresh**, vous actualisez les détails de la sauvegarde ou du clone.

5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage, de renommage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le système de stockage secondaire.



Vous ne pouvez pas renommer les sauvegardes qui se trouvent sur le système de stockage principal.

7. Pour supprimer un clone, sélectionnez-le dans le tableau, puis cliquez sur  pour supprimer le clone.

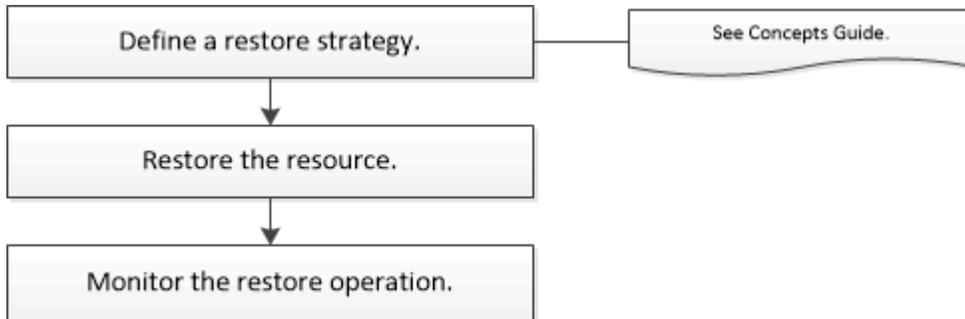
# Restaurez les ressources des plug-ins pris en charge par NetApp

## Restaurez les ressources de plug-in prises en charge par NetApp

Le workflow de restauration et de reprise comprend la planification, la réalisation des opérations de restauration et la surveillance des opérations.

### Description de la tâche

Le flux de travail suivant montre l'ordre dans lequel vous devez effectuer l'opération de restauration :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. Pour plus d'informations sur les applets de commande PowerShell, utilisez l'aide de la cmdlet SnapCenter ou consultez le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Restaurer une sauvegarde de ressource

Vous pouvez utiliser SnapCenter pour restaurer des ressources. Les fonctionnalités des opérations de restauration dépendent du plug-in utilisé.

### Avant de commencer

- Vous devez avoir sauvegardé la ressource ou les groupes de ressources.
- Si vous répliquez des snapshots sur un miroir ou un coffre-fort, l'administrateur SnapCenter doit vous avoir attribué les machines virtuelles de stockage (SVM) des volumes source et de destination.
- Vous devez avoir annulé toute opération de sauvegarde en cours pour la ressource ou le groupe de ressources à restaurer.

### Description de la tâche

- L'opération de restauration par défaut restaure uniquement les objets de stockage. Les opérations de restauration au niveau de l'application ne peuvent être effectuées que si le plug-in NetApp pris en charge offre cette fonctionnalité.
- Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources s'affichent avec des informations telles que le type, le nom de l'hôte ou du cluster, les groupes de ressources et les stratégies associés et l'état.



Bien qu'une sauvegarde soit possible pour un groupe de ressources, lors de la restauration, vous devez sélectionner les ressources individuelles que vous souhaitez restaurer.

Si la ressource n'est pas protégée, *non protégé* s'affiche dans la colonne **Etat général**.

L'état *Not Protected* dans la colonne **Overall Status** peut signifier que la ressource n'est pas protégée ou que la ressource a été sauvegardée par un autre utilisateur.

3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur



Backup Name	End Date
rg1_scipr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. Dans la page objectif de restauration, sélectionnez **ressource complète** ou **niveau de fichier**.
  - a. Si vous avez sélectionné **Complete Resource**, la sauvegarde de la ressource est restaurée.

Si la ressource contient des volumes ou des qtrees comme empreinte du stockage, les snapshots les plus récents sur ces volumes ou qtrees sont supprimés et ne peuvent pas être restaurés. De même, si une autre ressource est hébergée sur les mêmes volumes ou qtrees, cette ressource est également supprimée.

- b. Si vous avez sélectionné **File Level**, vous pouvez sélectionner **All**, ou sélectionner des volumes ou des qtrees, puis entrer le chemin d'accès relatif aux volumes ou aux qtrees sélectionnés séparés par des virgules.
  - Vous pouvez sélectionner plusieurs volumes et qtrees.
  - Si le type de ressource est LUN, la LUN entière est restaurée. Vous pouvez sélectionner

plusieurs LUN. + REMARQUE : si vous sélectionnez **tous**, tous les fichiers des volumes, qtree ou LUN sont restaurés.

7. Dans la page **Pre ops**, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.
8. Dans la page **Post OPS**, entrez les commandes mount et post-restauration à exécuter après l'exécution d'une tâche de restauration.
9. Dans la page **notification**, dans la liste déroulante **préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans la page **Paramètres > Paramètres globaux**.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

1. Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Récupérez les informations sur une ou plusieurs sauvegardes que vous souhaitez restaurer à l'aide des applets de commande Get-SmBackup and get-SmBackupReport.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple contient des informations détaillées sur la sauvegarde du 29 janvier 2015 au 3 février 2015 :

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId : 113
SmJobId : 2032
StartDateTime : 2/2/2015 6:57:03 AM
EndDateTime : 2/2/2015 6:57:11 AM
Duration : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId : 114
SmJobId : 2183
StartDateTime : 2/2/2015 1:02:41 PM
EndDateTime : 2/2/2015 1:02:38 PM
Duration : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName : Vault
SmPolicyId : 18
BackupName : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restaurez les données de la sauvegarde à l'aide de la cmdlet Restore-SmBackup.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : {}
ParentJobID : 0
EventId : 0
JobTypeId :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Monitor NetApp prend en charge les opérations de restauration des ressources du plug-in

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

# Cloner les sauvegardes de ressources de plug-ins pris en charge par NetApp

## Cloner les sauvegardes de ressources de plug-ins pris en charge par NetApp

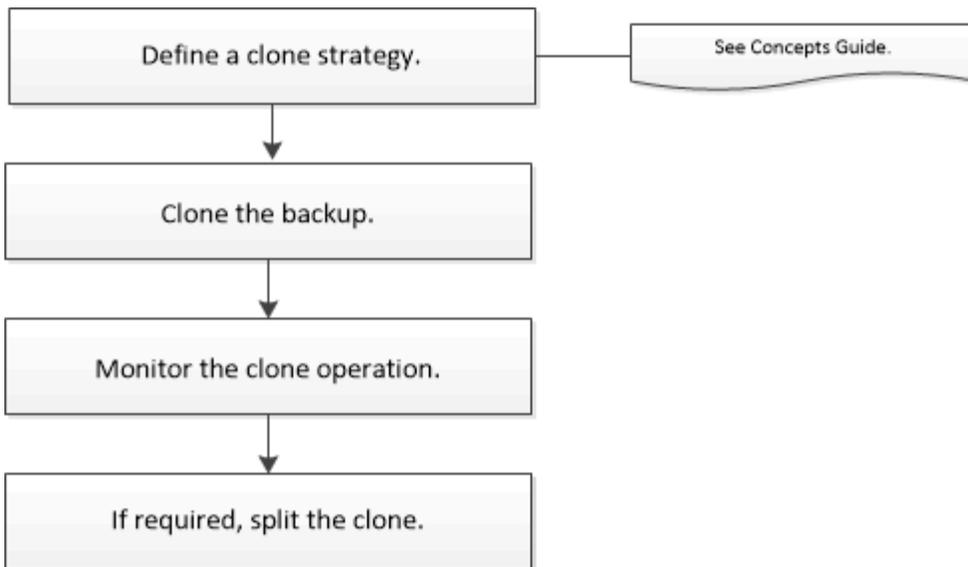
Le workflow de clonage inclut la réalisation de l'opération de clonage et le contrôle de l'opération.

### Description de la tâche

Vous pouvez cloner des sauvegardes de ressources pour les raisons suivantes :

- Tester les fonctionnalités à implémenter à l'aide de la structure de ressources actuelle et du contenu pendant les cycles de développement d'applications
- Pour les outils d'extraction et de manipulation de données lors du remplissage d'entrepôts de données
- Pour récupérer les données qui ont été supprimées ou modifiées par erreur

Le workflow suivant affiche la séquence dans laquelle vous devez effectuer l'opération de clonage :



Vous pouvez également utiliser les applets de commande PowerShell manuellement ou dans des scripts pour réaliser des opérations de sauvegarde, de restauration et de clonage. Pour plus d'informations sur les applets de commande PowerShell, utilisez l'aide de la cmdlet SnapCenter ou consultez le ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Cloner à partir d'une sauvegarde

Vous pouvez utiliser SnapCenter pour cloner une sauvegarde. Vous pouvez cloner à partir d'une sauvegarde principale ou secondaire. Les fonctionnalités des opérations de clonage dépendent du plug-in que vous utilisez.

### Avant de commencer

- Vous devez avoir sauvegardé les ressources ou le groupe de ressources.
- L'opération de clonage par défaut ne clone que les objets de stockage. Les opérations de clonage au niveau de l'application ne peuvent être effectuées que si le plug-in NetApp pris en charge offre cette fonctionnalité.
- Vous devez vous assurer que les agrégats hébergeant les volumes doivent se trouver dans la liste des agrégats attribués de la machine virtuelle de stockage (SVM).

### Description de la tâche

Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

## UI SnapCenter

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.

Les ressources s'affichent avec des informations telles que le type, le nom de l'hôte ou du cluster, les groupes de ressources et les stratégies associés et l'état.

3. Sélectionnez la ressource ou le groupe de ressources.

Vous devez sélectionner une ressource si vous sélectionnez un groupe de ressources.

La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacements, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Serveur clone	Par défaut, l'hôte source est renseigné.  Si vous souhaitez spécifier un autre hôte, sélectionnez l'hôte sur lequel le clone doit être monté et le plug-in est installé.
Suffixe du clone	Cette opération est obligatoire lorsque la destination du clone est la même que la source.  Indiquez un suffixe à ajouter au nom du nouveau clone. Le suffixe garantit que la ressource clonée est unique sur l'hôte.  Par exemple, rs1_clone. Si vous effectuez le clonage sur le même hôte que la ressource d'origine, vous devez fournir un suffixe permettant de différencier la ressource clonée de la ressource d'origine. Dans le cas contraire, l'opération échoue.

Si la ressource sélectionnée est une LUN et si vous effectuez un clonage à partir d'une sauvegarde secondaire, les volumes de destination sont répertoriés. Une seule source peut avoir plusieurs volumes de destination.

7. Dans la page **Paramètres**, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom de l'initiateur	Entrez le nom de l'initiateur hôte, qui est soit un IQDN, soit un WWPN.
Protocole d'iGroup	Sélectionnez le protocole iGroup.



La page des paramètres s'affiche uniquement si le type de stockage est LUN.

- Dans la page **scripts**, entrez les commandes de pré-clonage ou post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement. Entrez la commande **mount** pour monter un système de fichiers sur un hôte.

Par exemple :

- Commande de pré-clonage : permet de supprimer les bases de données existantes portant le même nom
- Commande post-clone : vérifiez une base de données ou démarrez une base de données.

Commande **mount** pour un volume ou un qtrees sur une machine Linux :  
`mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>`

- Dans la page **notification**, dans la liste déroulante **préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail.

- Vérifiez le résumé et cliquez sur **Terminer**.
- Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

### Applets de commande PowerShell

#### Étapes

- Lancez une session de connexion avec le serveur SnapCenter pour un utilisateur spécifié à l'aide de l'applet de commande `Open-SmConnection`.

```
Open-SmConnection -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

- Répertoriez les sauvegardes pouvant être clonées à l'aide de l'applet de commande `Get-SmBackup` ou `Get-SmResourceGroup`.

Cet exemple affiche des informations sur toutes les sauvegardes disponibles :

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

Cet exemple affiche des informations sur un groupe de ressources spécifié :

```
PS C:\> Get-SmResourceGroup
```

```
Description :
CreationTime : 10/10/2016 4:45:53 PM
ModificationTime : 10/10/2016 4:45:53 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {}
HostResourceMapping : {}
Configuration :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus : Completed
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Tag :
IsInternal : False
```

```

EnableEmailAttachment : False
VerificationSettings : {}
Name : NFS_DB
Type : Group
Id : 2
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
Hosts :
StorageName :
ResourceGroupNames :
PolicyNames :

Description :
CreationTime : 10/10/2016 4:51:36 PM
ModificationTime : 10/10/2016 5:27:57 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {}
HostResourceMapping : {}
Configuration :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus : Failed
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassRunAs : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Tag :

```

```

IsInternal : False
EnableEmailAttachment : False
VerificationSettings : {}
Name : Test
Type : Group
Id : 3
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
Hosts :
StorageName :
ResourceGroupNames :
PolicyNames :

```

3. Lancez une opération de clonage à partir d'un groupe de ressources clone ou d'une sauvegarde existante à l'aide de l'applet de commande `New-SmClone`.

Dans cet exemple, un clone est créé à partir d'une sauvegarde spécifiée avec tous les journaux :

```

New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sscore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sscore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sscore.test.com' -igroupprotocol 'mixed'

```

4. Affichez l'état du travail clone à l'aide de l'applet de commande `Get-SmCloneReport`.

Cet exemple affiche un rapport de clonage pour l'ID de tâche spécifié :

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError :

```

## Monitor NetApp prend en charge les opérations de clonage de ressources du plug-in

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.

2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

# Protégez les systèmes de fichiers Unix

## Ce que vous pouvez faire avec le plug-in SnapCenter pour les systèmes de fichiers Unix

Lorsque le plug-in pour systèmes de fichiers Unix est installé dans votre environnement, vous pouvez utiliser SnapCenter pour sauvegarder, restaurer et cloner des systèmes de fichiers Unix. Vous pouvez également effectuer des tâches prenant en charge ces opérations.

- Découvrir les ressources
- Sauvegardez les systèmes de fichiers Unix
- Planifiez les opérations de sauvegarde
- Restaurer les sauvegardes du système de fichiers
- Cloner les sauvegardes du système de fichiers
- Contrôle des opérations de sauvegarde, de restauration et de clonage

### Configurations compatibles

Élément	Configuration prise en charge
Des environnements	<ul style="list-style-type: none"><li>• Serveur physique</li><li>• Serveur virtuel</li></ul> <p>Datstores vVol sur NFS et SAN. Le datastore vVol peut uniquement être provisionné avec les outils ONTAP pour VMware vSphere.</p>
Systèmes d'exploitation	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• SUSE Linux Enterprise Server (SLES)</li></ul>
Systèmes de fichiers	<ul style="list-style-type: none"><li>• SAN :<ul style="list-style-type: none"><li>◦ Systèmes de fichiers basés sur LVM et non LVM</li><li>◦ LVM sur VMDK ext3, ext4 et xfs</li></ul></li><li>• NFS : NFS v3, NFS v4.x</li></ul>
Protocoles	<ul style="list-style-type: none"><li>• FC</li><li>• FCoE</li><li>• iSCSI</li><li>• NFS</li></ul>

Élément	Configuration prise en charge
Chemins d'accès multiples	oui

## Limites

- La combinaison de RDM et de disques virtuels dans un groupe de volumes n'est pas prise en charge.
- La restauration au niveau des fichiers n'est pas prise en charge.

Toutefois, vous pouvez effectuer manuellement une restauration au niveau des fichiers en clonant la sauvegarde, puis en copiant les fichiers manuellement.

- La combinaison de systèmes de fichiers répartis sur des VMDK provenant à la fois des datastores NFS et VMFS n'est pas prise en charge.
- NVMe n'est pas pris en charge.
- Le provisionnement n'est pas pris en charge.

## Caractéristiques

- Permet au plug-in pour Oracle Database d'effectuer des opérations de protection des données sur les bases de données Oracle en gérant la pile de stockage hôte sous-jacente sur les systèmes Linux ou AIX
- Prend en charge les protocoles NFS (Network File System) et SAN (Storage Area Network) sur un système de stockage exécutant ONTAP.
- Pour les systèmes Linux, les bases de données Oracle sur des LUN VMDK et RDM sont prises en charge lorsque vous déployez le plug-in SnapCenter pour VMware vSphere et que vous enregistrez le plug-in avec SnapCenter.
- Prend en charge Mount Guard pour AIX sur les systèmes de fichiers SAN et la disposition LVM.
- Prise en charge du système JFS2 (Enhanced journalised File System) avec consignation en ligne sur les systèmes de fichiers SAN et disposition LVM pour les systèmes AIX uniquement.

Les périphériques SAN natifs, les systèmes de fichiers et les dispositions LVM basées sur des périphériques SAN sont pris en charge.

- Automatise les opérations de sauvegarde, de restauration et de clonage respectueuses des applications pour les systèmes de fichiers UNIX de votre environnement SnapCenter

## Installez le plug-in SnapCenter pour les systèmes de fichiers Unix

### Conditions préalables à l'ajout d'hôtes et à l'installation de Plug-ins Package pour Linux

Avant d'ajouter un hôte et d'installer le package de plug-ins pour Linux, vous devez remplir toutes les conditions requises.

- Si vous utilisez iSCSI, le service iSCSI doit être en cours d'exécution.
- Vous pouvez utiliser l'authentification basée sur un mot de passe pour l'utilisateur root ou non root ou l'authentification basée sur une clé SSH.

Le plug-in SnapCenter pour systèmes de fichiers Unix peut être installé par un utilisateur non root. Cependant, vous devez configurer les privilèges sudo pour que l'utilisateur non-root installe et démarre le processus de plug-in. Après l'installation du plug-in, les processus s'exécutent en tant qu'utilisateur non-racine efficace.

- Créez des informations d'identification avec le mode d'authentification Linux pour l'utilisateur d'installation.
- Vous devez avoir installé Java 11 sur votre hôte Linux.



Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux.

Pour plus d'informations sur le téléchargement DE JAVA, voir : "[Téléchargements Java pour tous les systèmes d'exploitation](#)"

- Vous devez avoir **bash** comme shell par défaut pour l'installation du plug-in.

### Configuration requise pour l'hôte Linux

Vous devez vous assurer que l'hôte répond à la configuration requise avant d'installer le module de plug-ins SnapCenter pour Linux.

Élément	De formation
Systèmes d'exploitation	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• Oracle Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul>
RAM minimale pour le plug-in SnapCenter sur l'hôte	2 GO
Espace minimal d'installation et de journalisation pour le plug-in SnapCenter sur l'hôte	2 GO <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Vous devez allouer suffisamment d'espace disque et surveiller la consommation de stockage par le dossier des journaux. L'espace de journalisation requis varie en fonction du nombre d'entités à protéger et de la fréquence des opérations de protection des données. S'il n'y a pas suffisamment d'espace disque, les journaux ne seront pas créés pour les opérations récentes.</p> </div>

Élément	De formation
Packs logiciels requis	<p>Java 11 Oracle Java et OpenJDK</p> <p> Assurez-vous que vous avez installé uniquement l'édition certifiée DE JAVA 11 sur l'hôte Linux.</p> <p>Si vous avez mis à niveau JAVA vers la dernière version, vous devez vous assurer que l'option JAVA_HOME située dans <code>/var/opt/snapcenter/spl/etc/spl.properties</code> est définie sur la version JAVA correcte et le chemin correct.</p>

Pour obtenir les dernières informations sur les versions prises en charge, consultez le "[Matrice d'interopérabilité NetApp](#)".

## Ajoutez des hôtes et installez Plug-ins Package pour Linux à l'aide de l'interface graphique

Vous pouvez utiliser la page Ajouter un hôte pour ajouter des hôtes, puis installer le module de plug-ins SnapCenter pour Linux. Les plug-ins sont automatiquement installés sur les hôtes distants.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Type d'hôte	Sélectionnez <b>Linux</b> comme type d'hôte.
Nom d'hôte	<p>Saisissez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.</p> <p>SnapCenter dépend de la configuration appropriée du DNS. Par conséquent, la meilleure pratique consiste à saisir le FQDN.</p> <p>Si vous ajoutez un hôte à l'aide de SnapCenter et que l'hôte fait partie d'un sous-domaine, vous devez fournir le FQDN.</p>

Pour ce champ...	Procédez comme ça...
Informations d'identification	<p>Sélectionnez le nom d'identification que vous avez créé ou créez de nouvelles informations d'identification.</p> <p>Les informations d'identification doivent disposer de droits d'administration sur l'hôte distant. Pour plus de détails, reportez-vous aux informations sur la création des informations d'identification.</p> <p>Vous pouvez afficher des détails sur les informations d'identification en positionnant le curseur sur le nom des informations d'identification que vous avez spécifié.</p> <div data-bbox="873 699 927 751" style="border: 1px solid #ccc; padding: 5px; display: inline-block;">  </div> <p>Le mode d'authentification des informations d'identification est déterminé par le type d'hôte que vous spécifiez dans l'assistant Ajout d'hôte.</p>

5. Dans la section Select Plug-ins to Install, sélectionnez **Unix File Systems**.

6. (Facultatif) cliquez sur **plus d'options**.

Pour ce champ...	Procédez comme ça...
Port	<p>Conservez le numéro de port par défaut ou spécifiez le numéro de port.</p> <p>Le numéro de port par défaut est 8145. Si le serveur SnapCenter a été installé sur un port personnalisé, ce numéro de port est affiché comme port par défaut.</p> <div data-bbox="873 1413 927 1465" style="border: 1px solid #ccc; padding: 5px; display: inline-block;">  </div> <p>Si vous avez installé manuellement les plug-ins et spécifié un port personnalisé, vous devez spécifier le même port. Dans le cas contraire, l'opération échoue.</p>
Chemin d'installation	<p>Le chemin par défaut est <i>/opt/NetApp/snapcenter</i>.</p> <p>Vous pouvez éventuellement personnaliser le chemin. Si vous utilisez le chemin personnalisé, assurez-vous que le contenu par défaut des sudoers est mis à jour avec le chemin personnalisé.</p>

Pour ce champ...	Procédez comme ça...
Ignorer les vérifications de préinstallation facultatives	Cochez cette case si vous avez déjà installé les plug-ins manuellement et que vous ne souhaitez pas vérifier si l'hôte répond aux exigences d'installation du plug-in.

7. Cliquez sur **soumettre**.

Si vous n'avez pas coché la case Ignorer les contrôles préalables, l'hôte est validé pour vérifier si l'hôte répond aux exigences d'installation du plug-in.



Le script de vérification préalable ne valide pas l'état du pare-feu du port du plug-in s'il est spécifié dans les règles de rejet du pare-feu.

Les messages d'erreur ou d'avertissement appropriés s'affichent si les exigences minimales ne sont pas respectées. Si l'erreur est liée à l'espace disque ou à la RAM, vous pouvez mettre à jour le fichier web.config situé à l'adresse *C:\Program Files\NetApp\SnapCenter WebApp* pour modifier les valeurs par défaut. Si l'erreur est liée à d'autres paramètres, vous devez corriger le problème.



Dans une configuration HA, si vous mettez à jour le fichier web.config, vous devez le mettre à jour sur les deux nœuds.

8. Vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.



SnapCenter ne prend pas en charge l'algorithme ECDSA.



La vérification des empreintes est obligatoire même si le même hôte a été ajouté précédemment à SnapCenter et que l'empreinte a été confirmée.

9. Surveillez la progression de l'installation.

Les fichiers journaux spécifiques à l'installation se trouvent à l'adresse */Custom\_location/snapcenter/logs*.

## Résultat

Tous les systèmes de fichiers montés sur l'hôte sont automatiquement découverts et affichés sous la page Ressources. Si rien ne s'affiche, cliquez sur **Actualiser les ressources**.

## Surveiller l'état de l'installation

Vous pouvez contrôler la progression de l'installation du module d'extension SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression de l'installation pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès

-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **Jobs**, pour filtrer la liste de manière à ce que seules les opérations d'installation des plug-ins soient répertoriées, procédez comme suit :
  - a. Cliquez sur **Filtrer**.
  - b. Facultatif : spécifiez les dates de début et de fin.
  - c. Dans le menu déroulant Type, sélectionnez **installation du plug-in**.
  - d. Dans le menu déroulant État, sélectionnez l'état de l'installation.
  - e. Cliquez sur **appliquer**.
4. Sélectionnez le travail d'installation et cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

## Configurer le service du chargeur enfichable SnapCenter

Le service chargeur de plug-in SnapCenter charge le package de plug-in pour Linux afin qu'il interagisse avec le serveur SnapCenter. Le service chargeur de plug-in SnapCenter est installé lorsque vous installez le module de plug-ins SnapCenter pour Linux.

### À propos de cette tâche

Après avoir installé le pack de plug-ins SnapCenter pour Linux, le service de chargeur de plug-in SnapCenter démarre automatiquement. Si le service du chargeur enfichable SnapCenter ne démarre pas automatiquement, vous devez :

- Assurez-vous que le répertoire dans lequel le plug-in fonctionne n'est pas supprimé
- Augmentez l'espace mémoire alloué à la machine virtuelle Java

Le fichier `spl.properties`, qui se trouve à `/Custom_location/NetApp/snapcenter/spl/etc/`, contient les paramètres suivants. Les valeurs par défaut sont attribuées à ces paramètres.

Nom du paramètre	Description
NIVEAU_JOURNAL	Affiche les niveaux de journaux pris en charge.  Les valeurs possibles sont TRACE, DEBUG, INFO, WARN, ERROR, ET FATAL.

Nom du paramètre	Description
SPL_PROTOCOL	<p>Affiche le protocole pris en charge par le chargeur SnapCenter Plug-in.</p> <p>Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.</p>
SNAPCENTER_SERVER_PROTOCOL	<p>Affiche le protocole pris en charge par le serveur SnapCenter.</p> <p>Seul le protocole HTTPS est pris en charge. Vous pouvez ajouter la valeur si la valeur par défaut est manquante.</p>
SKIP_JAVAHOME_UPDATE	<p>Par défaut, le service SPL détecte le chemin Java et met à jour LE paramètre JAVA_HOME.</p> <p>Par conséquent, la valeur par défaut est DÉFINIE sur FALSE. Vous pouvez définir LA valeur TRUE si vous souhaitez désactiver le comportement par défaut et corriger manuellement le chemin Java.</p>
SPL_KEYSTORE_PASS	<p>Affiche le mot de passe du fichier keystore.</p> <p>Vous ne pouvez modifier cette valeur que si vous modifiez le mot de passe ou si vous créez un nouveau fichier de magasin de clés.</p>
SPL_PORT	<p>Affiche le numéro de port sur lequel le service du chargeur enfichable SnapCenter est exécuté.</p> <p>Vous pouvez ajouter la valeur si la valeur par défaut est manquante.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Vous ne devez pas modifier la valeur après l'installation des modules externes. </div>
SNAPCENTER_SERVER_HOST	<p>Affiche l'adresse IP ou le nom d'hôte du serveur SnapCenter.</p>
CHEMIN_DU_MAGASIN_DE_CLÉS SPL	<p>Affiche le chemin absolu du fichier de magasin de clés.</p>
SNAPCENTER_SERVER_PORT	<p>Affiche le numéro de port sur lequel le serveur SnapCenter s'exécute.</p>

Nom du paramètre	Description
LOGS_MAX_COUNT	<p>Affiche le nombre de fichiers journaux du chargeur de plug-in SnapCenter qui sont conservés dans le dossier <code>/Custom_location/snapcenter/spl/logs</code>.</p> <p>La valeur par défaut est 5000. Si le nombre est supérieur à la valeur spécifiée, les 5000 derniers fichiers modifiés sont conservés. La vérification du nombre de fichiers est effectuée automatiquement toutes les 24 heures à partir du démarrage du service du chargeur de plug-in SnapCenter.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Si vous supprimez manuellement le fichier <code>spl.properties</code>, le nombre de fichiers à conserver est défini sur 9999. </div>
JAVA_HOME	<p>Affiche le chemin absolu du répertoire <code>Java_HOME</code> utilisé pour démarrer le service SPL.</p> <p>Ce chemin est déterminé lors de l'installation et dans le cadre du démarrage de SPL.</p>
LOG_MAX_SIZE	<p>Affiche la taille maximale du fichier journal des travaux.</p> <p>Une fois la taille maximale atteinte, le fichier journal est compressé et les journaux sont écrits dans le nouveau fichier de ce travail.</p>
RETAIN_LOGS_OF_LAST_DAYS	<p>Affiche le nombre de jours jusqu'à lesquels les journaux sont conservés.</p>
ACTIVER_CERTIFICAT_VALIDATION	<p>Affiche <code>TRUE</code> lorsque la validation du certificat CA est activée pour l'hôte.</p> <p>Vous pouvez activer ou désactiver ce paramètre en modifiant le fichier <code>spl.properties</code> ou en utilisant l'interface graphique ou l'applet de commande SnapCenter.</p>

Si l'un de ces paramètres n'est pas affecté à la valeur par défaut ou si vous souhaitez attribuer ou modifier la valeur, vous pouvez modifier le fichier `spl.properties`. Vous pouvez également vérifier le fichier `spl.properties` et le modifier pour résoudre tous les problèmes liés aux valeurs qui sont affectées aux paramètres. Après avoir modifié le fichier `spl.properties`, vous devez redémarrer le service de chargeur de plug-in SnapCenter.

## Étapes

1. Effectuez l'une des opérations suivantes, si nécessaire :
  - Démarrez le service du chargeur de plug-in SnapCenter :
    - En tant qu'utilisateur `root`, exécutez :

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```

- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl start
```

- Arrêtez le service du chargeur enfichable SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl stop
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop
```



Vous pouvez utiliser l'option `-force` avec la commande `stop` pour arrêter le service SnapCenter Plug-in Loader avec force. Cependant, vous devez faire preuve de prudence avant de le faire car il met également fin aux opérations existantes.

- Redémarrez le service du chargeur Plug-in SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl restart
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart
```

- Rechercher l'état du service du chargeur enfichable SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl status
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl status
```

- Trouver le changement dans le service du chargeur Plug-in SnapCenter :

- En tant qu'utilisateur root, exécutez :  

```
/custom_location/NetApp/snapcenter/spl/bin/spl change
```
- En tant qu'utilisateur non root, exécutez :  

```
sudo /custom_location/NetApp/snapcenter/spl/bin/spl change
```

## Configurez le certificat CA avec le service SnapCenter Plug-in Loader (SPL) sur un hôte Linux

Vous devez gérer le mot de passe du magasin de clés SPL et son certificat, configurer le certificat CA, configurer les certificats racine ou intermédiaire pour le magasin de confiance SPL et configurer la paire de clés signée CA pour le magasin de confiance SPL avec le service de chargeur de plug-in SnapCenter pour activer le certificat numérique installé.



SPL utilise le fichier « `keystore.jks` », qui se trouve dans `'/var/opt/snapcenter/spl/etc.'` en tant que magasin de confiance et clé.

### Gérer le mot de passe pour le magasin de clés SPL et l'alias de la paire de clés signée CA utilisée

#### Étapes

1. Vous pouvez récupérer le mot de passe par défaut du magasin de clés SPL dans le fichier de propriétés SPL.

C'est la valeur correspondant à la clé 'PL\_KEYSTORE\_PASS'.

2. Modifiez le mot de passe du magasin de clés :

```
keytool -storepasswd -keystore keystore.jks
. Remplacez le mot de passe de tous les alias des entrées de clé privée
du magasin de clés par le même mot de passe que celui utilisé pour le
magasin de clés :
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Mettez à jour la même chose pour la clé SPL\_KEYSTORE\_PASS dans le fichier spl.properties.

3. Redémarrez le service après avoir modifié le mot de passe.



Le mot de passe du magasin de clés SPL et de tous les mots de passe d'alias associés à la clé privée doivent être identiques.

## Configurez les certificats racine ou intermédiaire sur le magasin de confiance SPL

Vous devez configurer les certificats racine ou intermédiaire sans la clé privée dans le stockage de confiance SPL.

### Étapes

1. Accédez au dossier contenant le magasin de clés SPL : `/var/opt/snapcenter/spl/etc`.
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
. Ajouter un certificat racine ou intermédiaire :
```

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Redémarrez le service après avoir configuré les certificats racine ou
intermédiaire sur le stockage de confiance SPL.
```



Vous devez ajouter le certificat de l'autorité de certification racine, puis les certificats de l'autorité de certification intermédiaire.

## Configurez la paire de clés signée CA sur le magasin de confiance SPL

Vous devez configurer la paire de clés signée CA dans le magasin de confiance SPL.

### Étapes

1. Accédez au dossier contenant le magasin de clés de la SPL `/var/opt/snapcenter/spl/etc`
2. Localisez le fichier 'keystore.jks'.
3. Répertoriez les certificats ajoutés dans le magasin de clés :

```
keytool -list -v -keystore keystore.jks
. Ajoutez le certificat de l'autorité de certification ayant une clé privée et une clé publique.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Répertoriez les certificats ajoutés dans le magasin de clés.
```

```
keytool -list -v -keystore keystore.jks
. Vérifiez que le magasin de clés contient l'alias correspondant au nouveau certificat de l'autorité de certification, qui a été ajouté au magasin de clés.
. Remplacez le mot de passe de la clé privée ajoutée pour le certificat CA par le mot de passe du magasin de clés.
```

Le mot de passe du magasin de clés SPL par défaut est la valeur de la clé `SPL_KEYSTORE_PASS` dans le fichier `spl.properties`.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks
. Si le nom d'alias du certificat de l'autorité de certification est long et contient de l'espace ou des caractères spéciaux ("*", ",", "), remplacez le nom d'alias par un nom simple :
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks
. Configurez le nom d'alias à partir du magasin de clés situé dans le fichier spl.properties.
```

Mettez à jour cette valeur par rapport à la clé `SPL_CERTIFICATE_ALIAS`.

4. Redémarrez le service après avoir configuré la paire de clés signée CA dans la boutique de confiance

SPL.

## Configurer la liste de révocation de certificats (CRL) pour SPL

Vous devez configurer la CRL pour SPL

### À propos de cette tâche

- SPL recherche les fichiers CRL dans un répertoire préconfiguré.
- Le répertoire par défaut des fichiers CRL pour SPL est `/var/opt/snapcenter/spl/etc/crl`.

### Étapes

1. Vous pouvez modifier et mettre à jour le répertoire par défaut du fichier `spl.properties` par rapport à la clé `SPL_CRL_PATH`.
2. Vous pouvez placer plusieurs fichiers CRL dans ce répertoire.

Les certificats entrants seront vérifiés pour chaque CRL.

## Activez les certificats CA pour les plug-ins

Vous devez configurer les certificats d'autorité de certification et déployer les certificats d'autorité de certification dans le serveur SnapCenter et les hôtes de plug-in correspondants. Vous devez activer la validation du certificat de l'autorité de certification pour les plug-ins.

### Avant de commencer

- Vous pouvez activer ou désactiver les certificats CA à l'aide de l'applet de commande `run set-SmCertificateSettings`.
- Vous pouvez afficher l'état du certificat pour les plug-ins à l'aide de `get-SmCertificateSettings`.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Sélectionnez des hôtes à un ou plusieurs plug-ins.
4. Cliquez sur **plus d'options**.
5. Sélectionnez **Activer la validation de certificat**.

### Une fois que vous avez terminé

L'hôte de l'onglet hôtes gérés affiche un cadenas et la couleur du cadenas indique l'état de la connexion entre le serveur SnapCenter et l'hôte du plug-in.

-  Indique que le certificat CA n'est ni activé ni affecté à l'hôte du plug-in.
-  Indique que le certificat CA a été validé avec succès.

-  Indique que le certificat CA n'a pas pu être validé.
-  indique que les informations de connexion n'ont pas pu être récupérées.



Lorsque l'état est jaune ou vert, les opérations de protection des données s'achève correctement.

## Installation du plug-in SnapCenter pour VMware vSphere

Si votre base de données ou votre système de fichiers est stocké sur des machines virtuelles (VM) ou si vous souhaitez protéger des VM et des datastores, vous devez déployer l'appliance virtuelle du plug-in SnapCenter pour VMware vSphere.

Pour plus d'informations sur le déploiement, reportez-vous à la section "[Présentation du déploiement](#)".

### Déployer le certificat d'autorité de certification

Pour configurer le certificat d'autorité de certification avec le plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Créez ou importez un certificat SSL](#)".

### Configurez le fichier CRL

Le plug-in SnapCenter pour VMware vSphere recherche les fichiers CRL dans un répertoire préconfiguré. Le répertoire par défaut des fichiers CRL pour le plug-in SnapCenter pour VMware vSphere est */opt/netapp/config/crl*.

Vous pouvez placer plusieurs fichiers CRL dans ce répertoire. Les certificats entrants seront vérifiés pour chaque CRL.

## Préparez-vous à protéger les systèmes de fichiers Unix

Avant d'effectuer toute opération de protection des données, telle que des opérations de sauvegarde, de clonage ou de restauration, vous devez configurer votre environnement. Vous pouvez également configurer le serveur SnapCenter pour qu'il utilise la technologie SnapMirror et SnapVault.

Pour profiter des avantages de SnapVault et de la technologie SnapMirror, vous devez configurer et initialiser une relation de protection des données entre les volumes source et destination sur le périphérique de stockage. Vous pouvez utiliser NetAppSystem Manager ou utiliser la ligne de commandes de la console de stockage pour effectuer ces tâches.

Avant d'utiliser le plug-in pour les systèmes de fichiers Unix, l'administrateur SnapCenter doit installer et configurer le serveur SnapCenter et effectuer les tâches requises.

- Installer et configurer SnapCenter Server. "[En savoir plus >>](#)"
- Configurez l'environnement SnapCenter en ajoutant des connexions au système de stockage. "[En savoir plus >>](#)"



SnapCenter ne prend pas en charge plusieurs SVM de même nom sur différents clusters. Chaque SVM enregistré avec SnapCenter via l'enregistrement de SVM ou de cluster doit être unique.

- Ajoutez des hôtes, installez les plug-ins et découvrez les ressources.
- Si vous utilisez SnapCenter Server pour protéger les systèmes de fichiers Unix qui résident sur des LUN RDM ou VMDK VMware, vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter.
- Installez Java sur votre hôte Linux.
- Configurez SnapMirror et SnapVault sur ONTAP si vous souhaitez la réplication de sauvegarde.

## Sauvegardez les systèmes de fichiers Unix

### Découvrez les systèmes de fichiers UNIX disponibles pour la sauvegarde

Après l'installation du plug-in, tous les systèmes de fichiers de cet hôte sont automatiquement détectés et affichés dans la page Ressources. Vous pouvez ajouter ces systèmes de fichiers à des groupes de ressources pour effectuer des opérations de protection des données.

#### Avant de commencer

- Vous devez avoir terminé des tâches telles que l'installation du serveur SnapCenter, l'ajout d'hôtes et la création de connexions au système de stockage.
- Si les systèmes de fichiers résident sur un disque VMDK (Virtual machine Disk) ou un RDM (Raw Device Mapping), vous devez déployer le plug-in SnapCenter pour VMware vSphere et enregistrer le plug-in avec SnapCenter.

Pour plus d'informations, voir "[Déployez le plug-in SnapCenter pour VMware vSphere](#)".

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **chemin** dans la liste Affichage.
3. Cliquez sur **Actualiser les ressources**.

Les systèmes de fichiers s'affichent avec des informations telles que le type, le nom d'hôte, les groupes de ressources et les stratégies associés, ainsi que l'état.

### Créez des règles de sauvegarde pour les systèmes de fichiers Unix

Avant d'utiliser SnapCenter pour sauvegarder des systèmes de fichiers Unix, vous devez créer une stratégie de sauvegarde pour la ressource ou le groupe de ressources que vous souhaitez sauvegarder. Une stratégie de sauvegarde est un ensemble de règles qui régit la gestion, la planification et la conservation des sauvegardes. Vous pouvez également spécifier les paramètres de réplication, de script et de type de sauvegarde. La création d'une stratégie permet de gagner du temps lorsque vous souhaitez réutiliser la

stratégie sur une autre ressource ou un autre groupe de ressources.

### Avant de commencer

- Vous devez vous préparer à la protection des données en réalisant des tâches telles que l'installation de SnapCenter, l'ajout d'hôtes, la découverte des systèmes de fichiers et la création de connexions au système de stockage.
- Si vous répliquez des snapshots sur un stockage secondaire de copie miroir ou d'archivage sécurisé, l'administrateur SnapCenter doit vous avoir assigné les SVM pour les volumes source et de destination.
- Vérifiez les prérequis et les limites spécifiques de la synchronisation active SnapMirror. Pour plus d'informations, reportez-vous à "[Limites d'objet pour la synchronisation active SnapMirror](#)".

### Description de la tâche

- SnapLock
  - Si l'option « conserver les copies de sauvegarde pendant un nombre de jours spécifique » est sélectionnée, la période de conservation SnapLock doit être inférieure ou égale aux jours de conservation mentionnés.

La spécification d'une période de verrouillage de snapshot empêche la suppression des snapshots jusqu'à l'expiration de la période de conservation. Cela peut entraîner la conservation d'un nombre plus important de snapshots que le nombre spécifié dans la règle.

Pour ONTAP 9.12.1 et les versions antérieures, les clones créés à partir des snapshots de coffre-fort SnapLock dans le cadre de la restauration hériteront de l'heure d'expiration du coffre-fort SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Sélectionnez **Unix File Systems** dans la liste déroulante.
4. Cliquez sur **Nouveau**.
5. Dans la page Nom, entrez le nom et les détails de la stratégie.
6. Dans la page sauvegarde et réplication, effectuez les opérations suivantes :
  - a. Spécifiez les paramètres de sauvegarde.
  - b. Spécifiez la fréquence d'horaire en sélectionnant **sur demande, horaire, quotidien, hebdomadaire** ou **mensuel**.
  - c. Sélectionnez une étiquette Snapshot.

Selon le libellé de snapshot que vous sélectionnez, ONTAP applique la règle de conservation des snapshots secondaires qui correspond à celui-ci.



Si vous avez sélectionné **mettre à jour SnapMirror après la création d'une copie Snapshot locale**, vous pouvez éventuellement spécifier l'étiquette de règle secondaire. Toutefois, si vous avez sélectionné **mettre à jour SnapVault après la création d'une copie Snapshot locale**, vous devez spécifier l'étiquette de la stratégie secondaire.

- d. Dans la section Sélectionner les options de réplication secondaire, sélectionnez l'une des options de

réplication secondaires suivantes ou les deux :



Vous devez sélectionner les options de réplication secondaires pour **période de verrouillage de copie d'instantané secondaire** pour être effectif. L'option **période de verrouillage de copie d'instantané secondaire** est disponible sur la page Retention.

Pour ce champ...	Procédez comme ça...
Mettez à jour SnapMirror après avoir créé une copie Snapshot locale	Sélectionnez ce champ pour créer des copies en miroir des jeux de sauvegarde sur un autre volume (réplication SnapMirror).  Cette option doit être activée pour la synchronisation active SnapMirror.
Mettez à jour SnapVault après avoir créé une copie Snapshot locale	Sélectionnez cette option pour effectuer la réplication de sauvegarde disque à disque (sauvegardes SnapVault).
Nombre de tentatives d'erreur	Saisissez le nombre maximal de tentatives de réplication pouvant être autorisées avant l'arrêt de l'opération.

+



Vous devez configurer la règle de conservation SnapMirror dans ONTAP pour le stockage secondaire afin d'éviter d'atteindre la limite maximale des snapshots sur le stockage secondaire.

7. Dans la page Retention, spécifiez les paramètres de rétention pour le type de sauvegarde et le type de planification sélectionnés dans la page sauvegarde et réplication :

Les fonctions que vous recherchez...	Alors...
--------------------------------------	----------

<p>Conserver un certain nombre d'instantanés</p>	<p>Sélectionnez <b>nombre total de copies Snapshot à conserver</b>, puis indiquez le nombre de snapshots que vous souhaitez conserver.</p> <p>Si le nombre d'instantanés dépasse le nombre spécifié, les instantanés sont supprimés avec les plus anciennes copies supprimées en premier.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> La valeur de rétention maximale est 1018. Les sauvegardes échouent si la conservation est définie sur une valeur supérieure à celle prise en charge par la version ONTAP sous-jacente.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Si vous prévoyez d'activer la réplication SnapVault, vous devez définir le nombre de rétention sur 2 ou plus. Si vous définissez le nombre de rétention sur 1, l'opération de conservation peut échouer, car le premier snapshot est l'instantané de référence de la relation SnapVault jusqu'à ce qu'un nouvel instantané soit répliqué sur la cible.</p> </div>
<p>Conserver les instantanés pendant un certain nombre de jours</p>	<p>Sélectionnez <b>conserver les copies Snapshot pour</b>, puis indiquez le nombre de jours pendant lesquels vous souhaitez conserver les snapshots avant de les supprimer.</p>
<p>Période de verrouillage des copies Snapshot principales</p>	<p>Si vous souhaitez spécifier la période de verrouillage des snapshots pour le stockage primaire, sélectionnez <b>période de verrouillage des copies d'instantanés primaires</b>, puis sélectionnez jours, mois ou années.</p> <p>La période de conservation SnapLock doit être inférieure à 100 ans.</p>
<p>Période de verrouillage des snapshots secondaires</p>	<p>Sélectionnez <b>période de verrouillage de copie d'instantané secondaire</b>, puis sélectionnez jours, mois ou années.</p>



Vous ne pouvez conserver les sauvegardes du journal d'archivage que si vous avez sélectionné les fichiers journaux d'archive dans le cadre de votre sauvegarde.

- Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript que vous souhaitez exécuter avant ou après l'opération de sauvegarde, respectivement.



Vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir de `_ /opt/NetApp/SnapCenter/scc/etc/allowed_commands.config_path`.

Vous pouvez également spécifier la valeur du délai d'expiration du script. La valeur par défaut est 60 secondes.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et associez des stratégies pour les systèmes de fichiers Unix

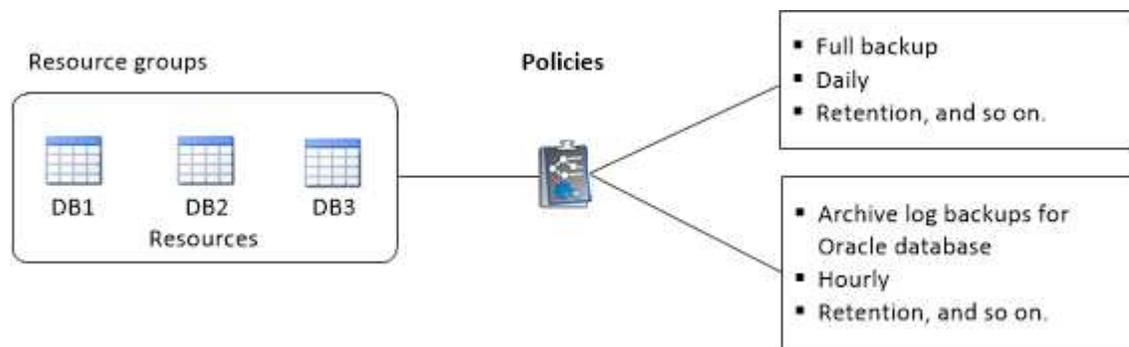
Un groupe de ressources est un conteneur dans lequel vous ajoutez des ressources que vous souhaitez sauvegarder et protéger. Un groupe de ressources vous permet de sauvegarder toutes les données associées aux systèmes de fichiers.

### Description de la tâche

- Une base de données contenant des fichiers dans des groupes de disques ASM doit être à l'état "MOUNT" ou "OPEN" pour vérifier ses sauvegardes à l'aide de l'utilitaire Oracle DBVERIFY.

Associez une ou plusieurs règles au groupe de ressources pour définir le type de tâche de protection des données à exécuter.

L'image suivante illustre la relation entre les ressources, les groupes de ressources et les politiques des bases de données :



- Pour les règles activées par SnapLock, pour ONTAP 9.12.1 et versions antérieures, si vous spécifiez une période de verrouillage de snapshot, les clones créés à partir des snapshots inviolables dans le cadre de la restauration hériteront de l'heure d'expiration de SnapLock. L'administrateur du stockage doit nettoyer manuellement les clones après l'heure d'expiration du SnapLock.
- L'ajout de nouveaux systèmes de fichiers sans synchronisation active SnapMirror à un groupe de ressources existant contenant des ressources avec la synchronisation active SnapMirror n'est pas pris en charge.
- L'ajout de nouveaux systèmes de fichiers à un groupe de ressources existant en mode de basculement de la synchronisation active SnapMirror n'est pas pris en charge. Vous pouvez ajouter des ressources au groupe de ressources uniquement à l'état normal ou de retour arrière.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.

3. Dans la page Nom, effectuez les opérations suivantes :

a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

c. Cochez la case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

4. Dans la page Ressources, sélectionnez un nom d'hôte de systèmes de fichiers Unix dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources de la section Ressources disponibles et déplacez-les vers la section Ressources sélectionnées.

6. Dans la page Paramètres de l'application, effectuez les opérations suivantes :

- Sélectionnez la flèche scripts et entrez les commandes pré et post pour les opérations quiesce, Snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
- Sélectionnez l'une des options de cohérence des sauvegardes :
  - Sélectionnez **cohérence système de fichiers** si vous voulez vous assurer que les données mises en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde et qu'aucune opération d'entrée ou de sortie n'est autorisée sur le système de fichiers lors de la création de la sauvegarde.



Pour une cohérence avec le système de fichiers, des snapshots de groupes de cohérence seront créés pour les LUN impliqués dans le groupe de volumes.

- Sélectionnez **cohérence de panne** si vous souhaitez vous assurer que les données en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde.



Si vous avez ajouté des systèmes de fichiers différents dans le groupe de ressources, tous les volumes provenant de systèmes de fichiers différents du groupe de ressources seront placés dans un groupe de cohérence.

7. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.
- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des groupes de ressources et activez la protection secondaire pour les systèmes de fichiers Unix sur les systèmes ASA r2

Vous devez créer le groupe de ressources pour ajouter les ressources qui se trouvent sur les systèmes ASA r2. Vous pouvez également provisionner la protection secondaire lors de la création du groupe de ressources.

### Avant de commencer

- Vous devez vous assurer que vous n'ajoutez pas les ressources ONTAP 9.x et ASA r2 au même groupe de ressources.
- Vous devez vous assurer que vous ne disposez pas d'une base de données contenant à la fois des ressources ONTAP 9.x et ASA r2.

### Description de la tâche

- La protection secondaire n'est disponible que si l'utilisateur connecté est affecté au rôle pour lequel la fonction **Secondaryprotection** est activée.
- Si vous avez activé la protection secondaire, le groupe de ressources passe en mode maintenance lors de la création des groupes de cohérence principal et secondaire. Une fois les groupes de cohérence primaire et secondaire créés, le groupe de ressources est mis hors mode de maintenance.

- SnapCenter ne prend pas en charge la protection secondaire pour une ressource clone.

## Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

- a. Entrez un nom pour le groupe de ressources dans le champ Nom.



Le nom du groupe de ressources ne doit pas dépasser 250 caractères.

- b. Saisissez une ou plusieurs étiquettes dans le champ balise pour vous aider à rechercher le groupe de ressources ultérieurement.

Par exemple, si vous ajoutez des RH comme étiquette à plusieurs groupes de ressources, vous pourrez rechercher par la suite tous les groupes de ressources associés à la balise RH.

- c. Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple, clienttext\_Resource group\_policy\_hostname ou Resource group\_hostname. Par défaut, un horodatage est ajouté au nom du Snapshot.

- d. Spécifiez les destinations des fichiers journaux d'archive que vous ne souhaitez pas sauvegarder.



Si nécessaire, vous devez utiliser la même destination que celle définie dans l'application, y compris le préfixe.

4. Dans la page Ressources, sélectionnez le nom d'hôte de la base de données dans la liste déroulante **hôte**.



Les ressources sont répertoriées dans la section Ressources disponibles uniquement si la ressource a été découverte avec succès. Si vous avez récemment ajouté des ressources, elles apparaissent dans la liste des ressources disponibles uniquement après avoir actualisé votre liste de ressources.

5. Sélectionnez les ressources ASA r2 dans la section Ressources disponibles et déplacez-les dans la section Ressources sélectionnées.
6. Dans la page Paramètres de l'application, sélectionnez l'option de sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :

- a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez également créer une stratégie en cliquant sur .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont répertoriées.

- b. Cliquez sur  Dans la colonne configurer les programmes de la stratégie pour laquelle vous souhaitez configurer un planning.

- c. Dans la fenêtre Ajouter des planifications pour la stratégie *policy\_name*, configurez le planning, puis cliquez sur **OK**.

Où, *policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

Les planifications de sauvegardes tierces ne sont pas prises en charge lorsqu'elles se chevauchent avec les planifications de sauvegarde SnapCenter.

- 8. Si la protection secondaire est activée pour la stratégie que vous avez sélectionnée, la page protection secondaire s'affiche et vous devez effectuer les étapes suivantes :

- a. Sélectionnez le type de la règle de réplication.



Règle de réplication synchrone non prise en charge.

- b. Indiquez le suffixe du groupe de cohérence à utiliser.

- c. Dans les menus déroulants cluster de destination et SVM de destination, sélectionnez le cluster peering et le SVM que vous souhaitez utiliser.



Le cluster et le peering de SVM ne sont pas pris en charge par SnapCenter. Vous devez utiliser les interfaces de ligne de commande System Manager ou ONTAP pour effectuer le peering de cluster et de SVM.



Si les ressources sont déjà protégées en dehors de SnapCenter, elles s'affichent dans la section Ressources protégées secondaires.

- 1. Sur la page Vérification, effectuez les opérations suivantes :

- a. Cliquez sur **Charger les localisateurs** pour charger les volumes SnapMirror ou SnapVault afin d'effectuer une vérification sur le stockage secondaire.

- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer le planning de vérification pour tous les types de planning de la stratégie.

- c. Dans la boîte de dialogue Ajouter des programmes de vérification nom\_stratégie, effectuez les opérations suivantes :

Les fonctions que vous recherchez...	Procédez comme ça...
Exécutez la vérification après la sauvegarde	Sélectionnez <b>Exécuter la vérification après la sauvegarde</b> .
Planifier une vérification	Sélectionnez <b>Exécuter la vérification programmée</b> , puis sélectionnez le type de planification dans la liste déroulante.

- d. Sélectionnez **vérifier sur l'emplacement secondaire** pour vérifier vos sauvegardes sur le système de stockage secondaire.

- e. Cliquez sur **OK**.

Les planifications de vérification configurées sont répertoriées dans la colonne programmes appliqués.

2. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération effectuée sur le groupe de ressources, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

3. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Sauvegardez les systèmes de fichiers Unix

Si une ressource ne fait pas partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **chemin** dans la liste Affichage.
3. Cliquez sur , puis sélectionnez le nom d'hôte et les systèmes de fichiers Unix pour filtrer les ressources.
4. Sélectionnez le système de fichiers à sauvegarder.
5. Dans la page Ressources, vous pouvez effectuer les opérations suivantes :
  - a. Cochez la case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

Par exemple : `customtext_policy_hostname` ou `resource_hostname`. Par défaut, un horodatage est ajouté au nom du Snapshot.

6. Dans la page Paramètres de l'application, effectuez les opérations suivantes :
  - Sélectionnez la flèche scripts et entrez les commandes pré et post pour les opérations quiesce, Snapshot et unquiesce. Vous pouvez également saisir les pré-commandes à exécuter avant de quitter en cas de défaillance.
  - Sélectionnez l'une des options de cohérence des sauvegardes :
    - Sélectionnez **File System cohérente** si vous voulez vous assurer que les données en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde et qu'aucune opération n'est effectuée sur le système de fichiers lors de la création de la sauvegarde.
    - Sélectionnez **cohérence de panne** si vous souhaitez vous assurer que les données en cache des systèmes de fichiers sont vidées avant de créer la sauvegarde.
7. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.



Vous pouvez créer une stratégie en cliquant sur  .

Dans la section configurer les plannings des stratégies sélectionnées, les stratégies sélectionnées sont

répertoriées.

- b. Cliquez sur  Dans la colonne configurer les plannings pour configurer un planning pour la stratégie souhaitée.
- c. Dans la fenêtre Ajouter des plannings pour la règle *nom\_règle*, configurez la planification, puis sélectionnez OK.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

Les planifications configurées sont répertoriées dans la colonne programmes appliqués.

8. Dans la page notification, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails dans la liste déroulante **préférence de messagerie**.

Vous devez spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de sauvegarde effectuée sur la ressource, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `Set-SmSmtServer`.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

La page topologie s'affiche.

10. Cliquez sur **Sauvegarder maintenant**.

11. Dans la page sauvegarde, effectuez les opérations suivantes :

- a. Si vous avez appliqué plusieurs stratégies à la ressource, dans la liste déroulante Stratégie, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

- b. Cliquez sur **Backup**.

12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Sauvegardez les groupes de ressources des systèmes de fichiers Unix

Vous pouvez sauvegarder les systèmes de fichiers Unix définis dans le groupe de ressources. Vous pouvez sauvegarder un groupe de ressources à la demande à partir de la page Ressources. Si une stratégie est associée à un groupe de ressources et qu'une planification est configurée, les sauvegardes sont créées en fonction de la planification.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Entrez le nom du groupe de ressources dans la zone de recherche ou cliquez sur , puis sélectionnez la balise.

Cliquez sur  pour fermer le volet de filtre.

4. Dans la page Groupe de ressources, sélectionnez le groupe de ressources à sauvegarder.
5. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si plusieurs stratégies sont associées au groupe de ressources, sélectionnez la stratégie de sauvegarde que vous souhaitez utiliser dans la liste déroulante **Stratégie**.  
  
Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.
  - b. Sélectionnez **Backup**.
6. Surveillez la progression en sélectionnant **Monitor > Jobs**.

## Surveiller la sauvegarde des systèmes de fichiers Unix

Découvrez comment surveiller la progression des opérations de sauvegarde et de protection des données.

### Surveillez les opérations de sauvegarde des systèmes de fichiers Unix

Vous pouvez surveiller la progression des différentes opérations de sauvegarde à l'aide de la page SnapCenterJobs. Vous pouvez vérifier la progression pour déterminer quand elle est terminée ou s'il y a un problème.

#### Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état correspondant des opérations :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **travaux**.
3. Dans la page travaux, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de sauvegarde soient répertoriées.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Backup**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de la sauvegarde.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.

4. Sélectionnez une tâche de sauvegarde, puis cliquez sur **Détails** pour afficher les détails de la tâche.



Bien que l'état de la tâche  de sauvegarde s'affiche, lorsque vous cliquez sur les détails de la tâche, vous pouvez constater que certaines des tâches enfants de l'opération de sauvegarde sont toujours en cours ou marquées d'un avertissement.

5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

### Surveiller les opérations de protection des données dans le volet activité

Le volet activité affiche les cinq opérations les plus récentes effectuées. Le volet activité s'affiche également lorsque l'opération a été lancée et que l'état de l'opération a été défini.

Le volet activité affiche des informations concernant les opérations de sauvegarde, de restauration, de clonage et de sauvegarde planifiée.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Cliquez sur  le volet activité pour afficher les cinq opérations les plus récentes.

Lorsque vous cliquez sur l'une des opérations, les détails de l'opération sont répertoriés dans la page **Détails du travail**.

### Afficher les systèmes de fichiers Unix protégés dans la page topologie

Lorsque vous préparez la sauvegarde, la restauration ou le clonage d'une ressource, il peut être utile d'afficher une représentation graphique de toutes les sauvegardes, systèmes de fichiers restaurés et clones sur le stockage primaire et secondaire.

#### À propos de cette tâche

Dans la page topologie, vous pouvez voir toutes les sauvegardes, les systèmes de fichiers restaurés et les clones disponibles pour la ressource ou le groupe de ressources sélectionné. Vous pouvez afficher les détails de ces sauvegardes, systèmes de fichiers restaurés et clones, puis les sélectionner pour exécuter des opérations de protection des données.

Vous pouvez consulter les icônes suivantes dans la vue gérer les copies pour déterminer si les sauvegardes et les clones sont disponibles sur le stockage principal ou secondaire (copies en miroir ou copies du coffre-fort).



affiche le nombre de sauvegardes et de clones disponibles sur le stockage principal.



Affiche le nombre de sauvegardes et de clones mis en miroir sur le système de stockage secondaire à l'aide de la technologie SnapMirror.





Affiche le nombre de sauvegardes et de clones répliqués sur le système de stockage secondaire à l'aide de la technologie SnapVault.

Le nombre de sauvegardes affichées inclut les sauvegardes supprimées du stockage secondaire. Par exemple, si vous avez créé 6 sauvegardes à l'aide d'une stratégie de conservation de 4 sauvegardes seulement, le nombre de sauvegardes affichées est 6.



Les clones d'une sauvegarde d'un miroir flexible de version sur un volume de type miroir-coffre-fort sont affichés dans la vue topologique, mais le nombre de sauvegardes en miroir dans la vue topologique n'inclut pas la sauvegarde flexible de version.

Si vous utilisez une relation secondaire comme SnapMirror actif Sync (initialement commercialisé sous la forme SnapMirror Business Continuity [SM-BC]), les icônes supplémentaires suivantes s'affichent :

-  Le site de réplica est en cours.
-  Le site de réplica est en panne.
-  La relation miroir ou coffre-fort secondaire n'a pas été rétablie.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource dans la vue Détails de la ressource ou dans la vue Détails du groupe de ressources.

Si la ressource est protégée, la page topologie de la ressource sélectionnée s'affiche.

4. Consultez la fiche récapitulative pour connaître le nombre de sauvegardes et de clones disponibles sur les stockages primaire et secondaire.

La section carte récapitulative affiche le nombre total de sauvegardes et de clones.

Cliquez sur le bouton **Actualiser** pour lancer une requête sur le stockage afin d'afficher un décompte précis.

Si une sauvegarde SnapLock est activée, cliquez sur le bouton **Refresh** pour actualiser l'heure d'expiration SnapLock principale et secondaire récupérée depuis ONTAP. Un planning hebdomadaire actualise également les temps d'expiration SnapLock primaire et secondaire extraits de ONTAP.

Lorsque le système de fichiers est réparti sur plusieurs volumes, le délai d'expiration SnapLock de la sauvegarde correspond au temps d'expiration SnapLock le plus long défini pour un instantané d'un volume. Le temps d'expiration SnapLock le plus long est extrait de ONTAP.

Pour la synchronisation active SnapMirror, cliquez sur le bouton **Refresh** pour actualiser l'inventaire des sauvegardes SnapCenter en interrogeant ONTAP sur les sites principaux et de réplica. Une planification hebdomadaire effectue également cette activité pour toutes les bases de données contenant une relation

de synchronisation active SnapMirror.

- Pour la synchronisation active SnapMirror et uniquement pour ONTAP 9.14.1, les relations SnapMirror miroir asynchrone ou MirrorVault asynchrone vers la nouvelle destination principale doivent être configurées manuellement après le basculement. À partir de ONTAP 9.15.1, Async Mirror ou Async MirrorVault est automatiquement configuré sur la nouvelle destination principale.
  - Après le basculement, une sauvegarde doit être créée afin que SnapCenter puisse prendre connaissance du basculement. Vous ne pouvez cliquer sur **Rafraîchir** qu'après la création d'une sauvegarde.
5. Dans la vue gérer les copies, cliquez sur **sauvegardes** ou **clones** à partir du stockage primaire ou secondaire pour afficher les détails d'une sauvegarde ou d'un clone.

Le détail des sauvegardes et des clones est affiché sous forme de tableau.

6. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur les icônes de protection des données pour effectuer des opérations de restauration, de clonage et de suppression.



Vous ne pouvez ni renommer, ni supprimer les sauvegardes qui se trouvent sur le stockage secondaire.

7. Si vous souhaitez supprimer un clone, sélectionnez-le dans la table, puis cliquez sur .

### Exemple de sauvegardes et de clones sur le stockage primaire

Manage Copies



Summary Card	
2 Backups	
1 Clone	
0 Snapshots Locked	

# Restaurez et restaurez les systèmes de fichiers Unix

## Restaurer les systèmes de fichiers Unix

En cas de perte de données, vous pouvez utiliser SnapCenter pour restaurer les systèmes de fichiers Unix.

### À propos de cette tâche

- Vous devez exécuter les commandes suivantes pour établir la connexion avec le serveur SnapCenter, répertorier les sauvegardes et récupérer ses informations, et restaurer la sauvegarde.

Les informations concernant les paramètres pouvant être utilisés avec la commande et leurs descriptions peuvent être obtenues en exécutant `Get-Help command_name`. Vous pouvez également vous reporter à la ["Guide de référence sur les commandes du logiciel SnapCenter"](#).

- Pour une opération de restauration de synchronisation active SnapMirror, vous devez sélectionner la sauvegarde à partir de l'emplacement principal.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **chemin** ou **Groupe de ressources** dans la liste **Afficher**.
3. Sélectionnez le système de fichiers dans la vue détaillée ou dans la vue détaillée du groupe de ressources.

La page topologie s'affiche.

4. Dans la vue gestion des copies, sélectionnez **backups** dans les systèmes de stockage principal ou secondaire (mis en miroir ou répliqué).
5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur .
6. Dans la page étendue de la restauration :
  - Pour les systèmes de fichiers NFS, la fonction **Connect and Copy** restore est sélectionnée par défaut. Vous pouvez également sélectionner **Volume Revert** ou **Fast Restore**.
  - Pour les systèmes de fichiers non NFS, le périmètre de restauration est sélectionné en fonction de la disposition.

Les nouveaux fichiers créés après la sauvegarde peuvent ne pas être disponibles après la restauration, selon le type et la disposition du système de fichiers.

7. Sur la page PreOps, entrez les commandes de pré-restauration à exécuter avant d'exécuter une tâche de restauration.
8. Sur la page PostOps, entrez les commandes post-restauration à exécuter après l'exécution d'une tâche de restauration.



Vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à l'emplacement `_/opt/NetApp/SnapCenter/scc/etc/allowed_commands.config_path`.

9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les notifications par e-mail.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de restauration effectuée, vous devez sélectionner **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface utilisateur graphique ou de la commande PowerShell `set-SmtpServer`.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.



Si l'opération de restauration échoue, la restauration n'est pas prise en charge.



En cas de restauration d'un système de fichiers résidant sur un groupe de volumes, l'ancien contenu du système de fichiers n'est pas supprimé. Seul le contenu du système de fichiers cloné sera copié dans le système de fichiers source. Ceci s'applique lorsqu'il y a plusieurs systèmes de fichiers sur le groupe de volumes et lors des restaurations par défaut du système de fichiers NFS.

11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Surveiller les opérations de restauration des systèmes de fichiers Unix

Vous pouvez contrôler la progression des différentes opérations de restauration SnapCenter à l'aide de la page travaux. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

### Description de la tâche

Les États post-restauration décrivent les conditions de la ressource après une opération de restauration et toutes les autres actions de restauration que vous pouvez effectuer.

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin que seules les opérations de restauration soient répertoriées.

- b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Restaurer**.
  - d. Dans la liste déroulante **Status**, sélectionnez l'état de restauration.
  - e. Cliquez sur **appliquer** pour afficher les opérations qui ont été effectuées avec succès.
4. Sélectionnez le travail de restauration, puis cliquez sur **Détails** pour afficher les détails du travail.
  5. Dans la page **Détails du travail**, cliquez sur **Afficher les journaux**.

Le bouton **Afficher les journaux** affiche les journaux détaillés de l'opération sélectionnée.

## Cloner des systèmes de fichiers Unix

### Cloner la sauvegarde du système de fichiers Unix

Vous pouvez utiliser SnapCenter pour cloner un système de fichiers Unix à l'aide de la sauvegarde du système de fichiers.

#### Avant de commencer

- Vous pouvez ignorer la mise à jour du fichier FSTAB en définissant la valeur de `SKIP_FSTAB_UPDATE` sur **true** dans le fichier `agent.properties` situé à l'adresse `/opt/NetApp/snapcenter/scc/etc`.
- Vous pouvez avoir un nom de volume de clone statique et un chemin de jonction en définissant la valeur de `USE_CUSTOM_CLONE_NAME_FORMAT` sur **true** dans le fichier `agent.properties` situé à `/opt/NetApp/snapcenter/scc/etc`. Après avoir mis à jour le fichier, vous devez redémarrer le service de création du plug-in SnapCenter en exécutant la commande : `/opt/NetApp/snapcenter/scc/bin/scc restart`.

Exemple : sans cette propriété, le nom du volume clone et le chemin de jonction seront comme `<Source_volume_name>_Clone_<Timestamp>`, mais il s'agit maintenant de `<Source_volume_name>_Clone_<Clone_Name>`

Ceci garde le nom constant pour que vous puissiez garder manuellement le fichier `fstab` mis à jour si vous ne préférez pas mettre à jour le `fstab` par SnapCenter.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **chemin** ou **Groupe de ressources** dans la liste **Afficher**.
3. Sélectionnez le système de fichiers dans la vue détaillée ou dans la vue détaillée du groupe de ressources.

La page topologie s'affiche.

4. Dans la vue gérer les copies, sélectionnez les sauvegardes depuis les copies locales (primaires), les copies miroir (secondaires) ou les copies de coffre-fort (secondaires).
5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Serveur clone	Par défaut, l'hôte source est renseigné.
Cloner le point de montage	Spécifiez le chemin où le système de fichiers sera monté.

7. Dans la page scripts, effectuez les opérations suivantes :

- a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.



Vous devez vérifier si les commandes existent dans la liste de commandes disponible sur l'hôte du plug-in à partir du chemin `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. Si vous souhaitez joindre le rapport de l'opération de clonage effectuée, sélectionnez **attacher un rapport de travail**.



Pour la notification par e-mail, vous devez avoir spécifié les détails du serveur SMTP à l'aide de l'interface graphique ou de la commande PowerShell `set-SmSmtServer`.

9. Vérifiez le résumé, puis cliquez sur **Terminer**.

10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Séparer un clone

Vous pouvez utiliser SnapCenter pour séparer une ressource clonée de la ressource parent. Le clone divisé devient indépendant de la ressource parent.

### Description de la tâche

- Vous ne pouvez pas effectuer l'opération de fractionnement de clone sur un clone intermédiaire.

Par exemple, après avoir créé clone1 à partir d'une sauvegarde de base de données, vous pouvez créer une sauvegarde de clone1, puis cloner cette sauvegarde (clone2). Après avoir créé clone2, clone1 est un clone intermédiaire et vous ne pouvez pas effectuer l'opération de séparation de clone sur clone1. Toutefois, vous pouvez réaliser l'opération de séparation des clones sur clone2.

Après avoir divisé le clone2, vous pouvez effectuer l'opération de fractionnement de clone sur clone1 car clone1 n'est plus le clone intermédiaire.

- Lorsque vous fractionnez un clone, les copies de sauvegarde et les tâches de clonage du clone sont supprimées.
- Pour plus d'informations sur les opérations de fractionnement de volume FlexClone, reportez-vous à la section, "[Séparer un volume FlexClone de son volume parent](#)".
- Assurez-vous que le volume ou l'agrégat du système de stockage est en ligne.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page **Ressources**, sélectionnez l'option appropriée dans la liste Affichage :

Option	Description
Des applications de base de données	Sélectionnez <b>Database</b> dans la liste Affichage.
Pour les systèmes de fichiers	Sélectionnez <b>Path</b> dans la liste vue.

3. Sélectionnez la ressource appropriée dans la liste.

La page topologie de ressources s'affiche.

4. Dans la vue **gérer les copies**, sélectionnez la ressource clonée (par exemple, la base de données ou la LUN), puis cliquez sur **\*\*** .
5. Vérifiez la taille estimée du clone à diviser et l'espace requis disponible sur l'agrégat, puis cliquez sur **Start**.
6. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

L'opération de fractionnement du clone cesse de répondre si le service SMCore redémarre. Vous devez exécuter la cmdlet Stop-SmJob pour arrêter l'opération de fractionnement du clone, puis recommencer l'opération de fractionnement du clone.

Si vous voulez un temps d'interrogation plus long ou plus court pour vérifier si le clone est divisé ou non, vous pouvez modifier la valeur du paramètre *CloneSplitStatusCheckPollTime* dans le fichier *SMCoreServiceHost.exe.config* pour définir l'intervalle de temps pour que SMCore interroge l'état de l'opération de fractionnement du clone. La valeur est exprimée en millisecondes et la valeur par défaut est 5 minutes.

Par exemple :

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'opération de démarrage du fractionnement du clone échoue si la sauvegarde, la restauration ou un autre clone est en cours d'exécution. Redémarrez l'opération de fractionnement de clone uniquement une fois les opérations en cours d'exécution terminées.

## Informations associées

["Le clone SnapCenter ou une vérification échoue avec un agrégat"](#)

## Surveillez les opérations de clonage des systèmes de fichiers Unix

Vous pouvez contrôler la progression des opérations de clonage SnapCenter à l'aide de la page tâches. Vous pouvez vérifier la progression d'une opération pour déterminer quand elle est terminée ou s'il y a un problème.

## Description de la tâche

Les icônes suivantes apparaissent sur la page travaux et indiquent l'état de l'opération :

-  En cours
-  Terminé avec succès
-  Échec
-  Terminé avec des avertissements ou impossible de démarrer en raison d'avertissements
-  En file d'attente
-  Annulée

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page **moniteur**, cliquez sur **travaux**.
3. Dans la page **travaux**, effectuez les opérations suivantes :
  - a. Cliquez sur  pour filtrer la liste afin de répertorier uniquement les opérations de clonage.
  - b. Spécifiez les dates de début et de fin.
  - c. Dans la liste déroulante **Type**, sélectionnez **Clone**.
  - d. Dans la liste déroulante **Statut**, sélectionnez l'état du clone.
  - e. Cliquez sur **appliquer** pour afficher les opérations effectuées avec succès.
4. Sélectionnez le travail clone, puis cliquez sur **Détails** pour afficher les détails du travail.
5. Dans la page Détails du travail, cliquez sur **Afficher les journaux**.

# Protégez les applications exécutées sur Azure NetApp Files

## Protégez les applications exécutées sur Azure NetApp Files

SnapCenter prend en charge la protection de vos applications telles qu'Oracle, SQL et SAP HANA résidant sur Azure NetApp Files. Depuis la version 6.0.1, SnapCenter prend en charge la fonction de sauvegarde Azure NetApp Files qui étend les fonctionnalités de protection des données d'Azure NetApp Files en fournissant une solution de sauvegarde entièrement gérée pour la restauration, l'archivage et la conformité à long terme.

Azure NetApp Files est une solution de stockage premium qui peut s'avérer coûteuse pour la conservation à long terme des sauvegardes. Pour optimiser les coûts, vous pouvez déplacer les sauvegardes du stockage Azure NetApp Files vers un magasin d'objets Azure. Depuis la version SnapCenter 6.0.1, vous pouvez sauvegarder et cloner les applications résidant sur Azure NetApp Files vers Azure Blob Storage (magasin d'objets). Vous pouvez conserver deux copies de vos données, des copies Snapshot de volume sur un système de stockage Azure NetApp Files pour une restauration à court terme et une autre copie sur Azure Blob Storage pour une restauration à long terme.

Lorsqu'une règle avec sauvegarde Azure NetApp Files est activée et associée à une ressource, SnapCenter gère la création de snapshots de volume et la sauvegarde dans Azure Blob Storage. SnapCenter crée le coffre-fort de sauvegarde et active la sauvegarde pour le volume. Si vous avez activé la sauvegarde pour le volume, SnapCenter utilise le coffre-fort existant.

### Limites

- Les fonctionnalités de stockage objet pour les systèmes de stockage FAS, ASA ou AFF ONTAP et Amazon FSX pour NetApp ONTAP ne sont pas prises en charge.
- Les workflows de montage et de catalogue Oracle et SAP HANA ne sont pas pris en charge pour les sauvegardes de stockage objet, mais pour les copies Snapshot.
- Les clones PDB Oracle ne sont pas pris en charge pour les sauvegardes de stockage objet, mais pour les snapshots.
- La vérification des sauvegardes à partir du stockage objet, la prise en charge de l'API REST, la gestion du cycle de vie des clones à partir du stockage objet et les fonctionnalités de reporting pour les sauvegardes de stockage objet ne sont pas prises en charge.
- La restauration à partir de sauvegardes du stockage Azure Blob Storage vers Azure NetApp Files n'est pas prise en charge. Vous pouvez également utiliser l'option de clonage.
- La répartition des clones n'est pas prise en charge.

## Installez SnapCenter et créez des informations d'identification

### Installez SnapCenter sur la machine virtuelle Azure

Vous pouvez télécharger le logiciel SnapCenter depuis le site du support NetApp et l'installer sur la machine virtuelle Azure.

## Avant de commencer

- Assurez-vous que la machine virtuelle Azure Windows est conforme aux conditions requises pour l'installation de SnapCenter Server. Pour plus d'informations, voir "[Configuration requise pour installer le serveur SnapCenter](#)".
- Si vous êtes nouveau sur Azure NetApp Files et que vous ne possédez pas de compte NetApp, assurez-vous que vous vous êtes inscrit pour pouvoir accéder au logiciel SnapCenter. Pour plus d'informations, voir "[Inscrivez-vous pour accéder au logiciel SnapCenter](#)".

## Étapes

1. Téléchargez le package d'installation du serveur SnapCenter à partir de "[Site de support NetApp](#)".
2. Lancez l'installation du serveur SnapCenter en double-cliquant sur le fichier .exe téléchargé.

Après le lancement de l'installation, tous les pré-contrôles sont effectués et si les exigences minimales ne sont pas satisfaites, des messages d'erreur ou d'avertissement appropriés s'affichent. Vous pouvez ignorer les messages d'avertissement et poursuivre l'installation ; cependant, les erreurs doivent être résolues.

3. Vérifiez les valeurs pré-remplies requises pour l'installation du serveur SnapCenter et modifiez-les si nécessaire.

Vous n'avez pas besoin de spécifier le mot de passe pour la base de données du référentiel MySQL Server. Lors de l'installation du serveur SnapCenter, le mot de passe est généré automatiquement.



Le caractère spécial "%" n'est pas pris en charge dans le chemin personnalisé de la base de données du référentiel. Si vous incluez " %" dans le chemin, l'installation échoue.

4. Cliquez sur **installer maintenant**.

Si vous avez spécifié des valeurs non valides, des messages d'erreur appropriés s'affichent. Entrez à nouveau les valeurs, puis lancez l'installation.



Si vous cliquez sur le bouton **Annuler**, l'étape en cours d'exécution est terminée, puis démarrez l'opération de restauration. Le serveur SnapCenter sera complètement supprimé de l'hôte.

Toutefois, si vous cliquez sur **Annuler** lorsque vous exécutez des opérations "redémarrage du site du serveur SnapCenter" ou "attente du démarrage du serveur SnapCenter", l'installation se poursuit sans annuler l'opération.

## Enregistrez le produit pour activer le support

Si vous découvrez NetApp et ne possédez pas de compte NetApp, enregistrez le produit pour activer le support.

## Étapes

1. Après avoir installé SnapCenter, accédez à **aide > à propos de**.
2. Dans la boîte de dialogue *a propos de SnapCenter*, notez l'instance SnapCenter, un nombre à 20 chiffres commençant par 971.
3. Cliquez sur <https://register.netapp.com>.
4. Cliquez sur **Je ne suis pas un client NetApp enregistré**.
5. Indiquez vos coordonnées pour vous inscrire.

6. Laissez le champ NetApp Reference SN vide.
7. Sélectionnez **SnapCenter** dans la liste déroulante gamme de produits.
8. Sélectionnez le fournisseur de facturation.
9. Entrez l'ID d'instance SnapCenter à 20 chiffres.
10. Cliquez sur **soumettre**.

## Créez les informations d'identification Azure dans SnapCenter

Vous devez créer les identifiants Azure dans SnapCenter pour accéder au compte Azure NetApp.

### Avant de commencer

- Vérifiez que vous avez créé le principal de service dans Azure.
- Assurez-vous que vous disposez de l'ID locataire, de l'ID client et de la clé secrète associés à l'entité de service.
  - L'ID de locataire est disponible sur le portail Azure sur la page de présentation de l'identifiant Entra.
  - L'ID client est également connu sous le nom d'ID de l'application pour le principal d'application/de service d'entreprise. Vous trouverez ces informations sur le portail Azure sur la page de présentation de l'application d'entreprise que vous avez créée pour agir en tant que responsable de service pour SnapCenter.
  - La clé secrète du client est également appelée valeur secrète. Vous pouvez créer ce secret de client dans le portail Azure en accédant à **enregistrements d'applications** sous Entra ID. Après avoir sélectionné l'application Enterprise que vous avez créée, accédez à **certificats et secrets**, puis à **Nouveau secret client**.



La valeur secrète est uniquement accessible lors de sa création. Vous ne pouvez pas y accéder ultérieurement.

- Le responsable de service doit obtenir des autorisations. Le rôle de Contributor permettra au principal de service d'effectuer les actions requises dans Azure. Ceci peut être accordé à partir de la page contrôle d'accès (IAM) de la page abonnement.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations suivantes requises pour créer les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom des informations d'identification	Entrez un nom pour l'identifiant.
Mode d'authentification	Sélectionnez <b>Azure Credential</b> dans la liste déroulante.

Pour ce champ...	Procédez comme ça...
ID locataire	Entrez l'ID du locataire.
ID client	Entrez l'ID client.
Clé secrète du client	Entrez la clé secrète du client.

5. Cliquez sur **OK**.

## Configuration du compte de stockage Azure

Vous devez configurer le compte de stockage Azure dans SnapCenter.

Le compte de stockage Azure contient des informations sur l'ID d'abonnement, les informations d'identification Azure et le compte Azure NetApp.



Les licences standard et basées sur la capacité ne sont pas requises pour Azure NetApp Files.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Systems**.
2. Sur la page systèmes de stockage, sélectionnez **Azure NetApp Files** et cliquez sur **Nouveau**.
3. Sélectionnez les informations d'identification, l'ID d'abonnement et le compte NetApp dans les listes déroulantes correspondantes.
4. Cliquez sur **soumettre**.

## Créez les informations d'identification pour ajouter l'hôte du plug-in

SnapCenter utilise des identifiants pour authentifier les utilisateurs pour les opérations SnapCenter.

Vous devez créer des informations d'identification pour l'installation des plug-ins SnapCenter et des informations d'identification supplémentaires pour les opérations de protection des données.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Credential**.
3. Cliquez sur **Nouveau**.
4. Dans la page informations d'identification, spécifiez les informations suivantes requises pour créer les informations d'identification.

Pour ce champ...	Procédez comme ça...
Nom des informations d'identification	Entrez un nom pour l'identifiant.
Mode d'authentification	Sélectionnez le mode d'authentification dans la liste déroulante.

Pour ce champ...	Procédez comme ça...
Type d'authentification	Sélectionnez <b>Mot de passe</b> ou <b>clé SSH</b> (uniquement pour l'hôte Linux).
Nom d'utilisateur	Spécifiez le nom d'utilisateur.
Mot de passe	Si vous avez sélectionné authentification par mot de passe, spécifiez le mot de passe.
Clé privée SSH	Si vous avez sélectionné l'authentification basée sur une clé SSH, spécifiez la clé privée.
Utilisez les privilèges sudo	<p>Cochez la case utiliser les privilèges sudo si vous créez des informations d'identification pour un utilisateur non root.</p> <div style="display: flex; align-items: center;">  <p>Ceci s'applique uniquement aux utilisateurs de Linux.</p> </div>

5. Cliquez sur **OK**.

## Protection des bases de données SAP HANA

### Ajoutez des hôtes et installez le plug-in SnapCenter pour la base de données SAP HANA

Vous devez utiliser la page SnapCenter Ajouter un hôte pour ajouter des hôtes, puis installer les modules de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants.

#### Avant de commencer

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.
- Si vous effectuez l'installation sur l'hôte centralisé, assurez-vous que le logiciel client SAP HANA est installé sur cet hôte et ouvrez les ports requis sur l'hôte de base de données SAP HANA pour exécuter les requêtes SQL HDB à distance.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :

- a. Dans le champ Type d'hôte, sélectionnez le type d'hôte.
  - b. Dans le champ Nom d'hôte, entrez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.
  - c. Dans le champ informations d'identification, entrez les informations d'identification que vous avez créées.
5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.
  6. (Facultatif) cliquez sur **plus d'options** et spécifiez les détails.
  7. Cliquez sur **soumettre**.
  8. Si le type d'hôte est Linux, vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.

9. Surveillez la progression de l'installation.

## Ajoutez la base de données SAP HANA

Vous devez ajouter la base de données SAP HANA manuellement.

### Description de la tâche

Les ressources doivent être ajoutées manuellement si le plug-in est installé sur un serveur centralisé. Si le plug-in SAP HANA est installé sur l'hôte de base de données HANA, le système HANA est automatiquement détecté.



La découverte automatique n'est pas prise en charge pour la configuration multi-hôtes HANA, mais elle doit être ajoutée via un plug-in centralisé uniquement.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez le plug-in SnapCenter pour base de données SAP HANA dans la liste déroulante, puis cliquez sur **Ressources**.
2. Dans la page Ressources, cliquez sur **Ajouter une base de données SAP HANA**.
3. Dans la page Détails de la ressource, effectuez les opérations suivantes :
  - a. Entrez le type de ressource en tant que conteneur unique, conteneur de base de données multilocataire ou Volume non-données.
  - b. Entrez le nom du système SAP HANA.
  - c. Saisissez l'ID système (SID).
  - d. Sélectionnez l'hôte du plug-in.
  - e. Entrez la clé pour vous connecter au système SAP HANA.
    - f. Entrez le nom d'utilisateur pour lequel la clé de stockage utilisateur sécurisé HDB est configurée.
4. Dans la page fournir l'empreinte du stockage, sélectionnez **Azure NetApp Files** comme type de stockage.
  - a. Sélectionnez le compte Azure NetApp.
  - b. Sélectionnez le pool de capacité et les volumes associés.
  - c. Cliquez sur **Enregistrer**.
5. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Créez des règles de sauvegarde pour les bases de données SAP HANA

Avant d'utiliser SnapCenter pour sauvegarder les ressources de base de données SAP HANA, vous devez créer une règle de sauvegarde pour la ressource ou le groupe de ressources à sauvegarder.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et la description de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez **Azure NetApp Files** comme type de stockage.
  - b. Sélectionnez **basé sur un fichier** si vous souhaitez effectuer un contrôle d'intégrité de la base de données.
  - c. Sélectionnez **snapshot based** si vous souhaitez créer une sauvegarde à l'aide de la technologie Snapshot.
6. Dans la page instantané et sauvegarde, effectuez les opérations suivantes :
  - a. Sélectionnez la fréquence de la sauvegarde planifiée.
  - b. Spécifiez les paramètres de rétention.
  - c. Si vous souhaitez activer la sauvegarde Azure NetApp Files, sélectionnez **Activer la sauvegarde** et spécifiez les paramètres de rétention.
7. Vérifiez le résumé et cliquez sur **Terminer**.

## Créez des groupes de ressources et associez des politiques de sauvegarde SAP HANA

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger.

Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.

Pour ce champ...	Procédez comme ça...
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.
Utilisez le format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.
5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.
  - b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
  - c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.
7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
8. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Sauvegardez les bases de données SAP HANA s'exécutant sur Azure NetApp Files

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.
3. Sélectionnez la ressource à sauvegarder.
4. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.
5. Dans la page Paramètres de l'application, procédez comme suit :
  - a. Sélectionnez la flèche **backups** pour définir des options de sauvegarde supplémentaires.
  - b. Sélectionnez la flèche **scripts** pour exécuter des commandes pré et post pour les opérations quiesce, Snapshot et unquiesce.
  - c. Sélectionnez la flèche **configurations personnalisées**, puis entrez les paires de valeurs personnalisées requises pour tous les travaux utilisant cette ressource.
  - d. Sélectionnez l'outil **Snapshot Copy Tool > SnapCenter without File System Consistency** pour créer des snapshots.

L'option **File System Consistency** ne s'applique qu'aux applications exécutées sur des hôtes

Windows.

6. Dans la page stratégies, effectuez les opérations suivantes :

a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.

b. Sélectionnez \* \* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

7. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également spécifier les adresses e-mail de l'expéditeur et du destinataire, ainsi que l'objet de l'e-mail. SMTP doit également être configuré dans **Paramètres > Paramètres globaux**.

8. Passez en revue le résumé, puis sélectionnez **Terminer**.

9. Sélectionnez **Sauvegarder maintenant**.

10. Dans la page sauvegarde, effectuez les opérations suivantes :

a. Si plusieurs stratégies sont associées à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de conservation spécifiés pour le type de programme.

11. Sélectionnez **Backup**.

12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Sauvegardez les groupes de ressources SAP HANA

Un groupe de ressources est un ensemble de ressources sur un hôte. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.

2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.

3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.

4. Dans la page sauvegarde, effectuez les opérations suivantes :

a. Si plusieurs stratégies sont associées au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.

Si la stratégie sélectionnée pour la sauvegarde à la demande est associée à un planning de sauvegarde, les sauvegardes à la demande seront conservées en fonction des paramètres de

conservation spécifiés pour le type de programme.

b. Sélectionnez **Backup**.

5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Restaurez et restaurez les bases de données SAP HANA

Vous pouvez restaurer et récupérer les données à partir des sauvegardes.

### Description de la tâche

Pour les systèmes HANA découverts automatiquement, si l'option **Complete Resource** est sélectionnée, la restauration s'effectue à l'aide de la technologie de restauration de snapshot de fichier unique. Si la case **Fast Restore** est cochée, la technologie Volume Revert est utilisée.

Pour les ressources ajoutées manuellement, la technologie Volume Revert est toujours utilisée.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.
3. Sélectionnez la ressource ou sélectionnez un groupe de ressources, puis sélectionnez une ressource dans ce groupe.
4. Dans la vue gestion des copies, sélectionnez **sauvegardes** dans les systèmes de stockage primaire ou secondaire (en miroir ou en stockage).
5. Dans le tableau sauvegarde(s) principale(s), sélectionnez la sauvegarde à restaurer, puis cliquez sur .
6. Dans la page Restore Scope, sélectionnez **Complete Resource**.

Tous les volumes de données configurés de la base de données SAP HANA sont restaurés.

7. Pour les systèmes HANA découverts automatiquement, sur la page étendue de la récupération, effectuez les opérations suivantes :
  - a. Sélectionnez **rétablir à l'état le plus récent** si vous voulez récupérer le plus près possible de l'heure actuelle.
  - b. Sélectionnez **Recover to point in Time** si vous souhaitez restaurer le point dans le temps spécifié.
  - c. Sélectionnez **Recover to specified data backup** si vous souhaitez effectuer une restauration vers une sauvegarde de données spécifique.
  - d. Sélectionnez **pas de récupération** si vous ne voulez pas récupérer maintenant.
  - e. Spécifiez les emplacements de sauvegarde des journaux.
  - f. Spécifiez l'emplacement du catalogue de sauvegardes.
8. Dans la page pré-opérations, entrez les commandes de pré-restauration et de démontage à exécuter avant d'effectuer une tâche de restauration.
9. Dans la page Post OPS, entrez les commandes de montage et de post-restauration à exécuter après l'exécution d'une tâche de restauration.
10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

Vous devez également indiquer les adresses e-mail de l'expéditeur et du destinataire ainsi que l'objet de l'e-mail. SMTP doit également être configuré sur la page **Paramètres > Paramètres globaux**.

11. Vérifiez le résumé, puis cliquez sur **Terminer**.
12. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Clonez la sauvegarde de la base de données SAP HANA

Vous pouvez utiliser SnapCenter pour cloner une base de données SAP HANA à l'aide de la sauvegarde de la base de données. Les clones créés sont des clones épais et sont créés dans le pool de capacité parent.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, filtrez les ressources de la liste déroulante **View** en fonction du type de ressource.
3. Sélectionnez la ressource ou le groupe de ressources.
4. Dans la vue gérer les copies, sélectionnez **backups** dans le système de stockage principal.
5. Sélectionnez la sauvegarde des données dans le tableau, puis cliquez sur .
6. Dans la page emplacement, effectuez les opérations suivantes :
  - a. Sélectionnez l'hôte sur lequel le plug-in SAP HANA est installé pour gérer le système HANA cloné.

Il peut s'agir d'un hôte de plug-in centralisé ou d'un hôte système HANA.



Si le plug-in HANA est installé sur un hôte centralisé qui gère les bases de données HANA sur d'autres hôtes lors de la création ou de la suppression de clones, SnapCenter ignore intentionnellement les opérations côté hôte (montage ou démontage du système de fichiers) car le serveur cible est un hôte centralisé. Vous devez utiliser des scripts personnalisés pré ou post-clonage pour effectuer des opérations de montage et de démontage.

- a. Entrez le SID SAP HANA à cloner à partir des sauvegardes existantes.
- b. Entrez les adresses IP ou les noms d'hôte sur lesquels les volumes clonés seront exportés.
- c. Si les volumes ANF de la base de données SAP HANA sont configurés dans un pool de capacité QoS manuelle, spécifiez la QoS pour les volumes clonés.

Si la QoS des volumes clonés n'est pas spécifiée, la QoS du volume source sera utilisée. Si le pool de capacité de QoS automatique est utilisé, la valeur de QoS spécifiée sera ignorée.

7. Dans la page scripts, effectuez les opérations suivantes :
  - a. Entrez les commandes du pré-clonage ou du post-clonage qui doivent être exécutées avant ou après l'opération de clonage, respectivement.
  - b. Entrez la commande mount pour monter un système de fichiers sur un hôte.

Si le système HANA source est détecté automatiquement et que le plug-in hôte cible clone est installé sur l'hôte SAP HANA, SnapCenter démonte automatiquement les volumes de données HANA existants sur l'hôte cible clone et monte les volumes de données HANA nouvellement clonés.

8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
9. Vérifiez le résumé, puis cliquez sur **Terminer**.
10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.



La répartition des clones est désactivée pour les clones ANF, car le clone ANF est déjà un volume indépendant créé à partir du Snapshot sélectionné.

## Protection des bases de données Microsoft SQL Server

### Ajoutez des hôtes et installez le plug-in SnapCenter pour la base de données SQL Server

SnapCenter prend en charge la protection des données des instances SQL sur des partages SMB sur Azure NetApp Files. Les configurations autonome et de groupe de disponibilité (AG) sont prises en charge.

Vous devez utiliser la page Ajout d'hôte de SnapCenter pour ajouter des hôtes, puis installer le package de plug-ins. Les plug-ins sont automatiquement installés sur les hôtes distants.

#### Avant de commencer

- Vous devez être un utilisateur affecté à un rôle disposant des autorisations d'installation et de désinstallation du plug-in, comme le rôle d'administrateur SnapCenter.
- Lors de l'installation d'un plug-in sur un hôte Windows, si vous spécifiez un identifiant qui n'est pas intégré ou si l'utilisateur appartient à un utilisateur de groupe de travail local, vous devez désactiver l'UAC sur l'hôte.

#### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné en haut.
3. Sélectionnez **Ajouter**.
4. Dans la page hôtes, procédez comme suit :
  - a. Dans le champ Type d'hôte, sélectionnez le type d'hôte.
  - b. Dans le champ Nom d'hôte, entrez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.
  - c. Dans le champ informations d'identification, entrez les informations d'identification que vous avez créées.
5. Dans la section **Select Plug-ins to Install**, sélectionnez les plug-ins à installer.
6. (Facultatif) cliquez sur **plus d'options** et spécifiez les détails.
7. Sélectionnez **soumettre**.
8. Sélectionnez **Configure log Directory** et dans la page Configure host log Directory, entrez le chemin SMB du répertoire log hôte, puis cliquez sur **Save**.
9. Cliquez sur **Submit** et surveillez la progression de l'installation.

## Créer des stratégies de sauvegarde pour les bases de données SQL Server

Vous pouvez créer une stratégie de sauvegarde pour la ressource ou le groupe de ressources avant d'utiliser SnapCenter pour sauvegarder les ressources SQL Server, ou vous pouvez créer une stratégie de sauvegarde au moment où vous créez un groupe de ressources ou sauvegardez une seule ressource.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Cliquez sur **Nouveau**.
4. Dans la page Nom, entrez le nom et la description de la stratégie.
5. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez **Azure NetApp Files** comme type de stockage.
  - b. Sélectionnez le type de sauvegarde.
    - i. Sélectionnez **sauvegarde complète et sauvegarde du journal** si vous souhaitez sauvegarder les fichiers de base de données et les journaux de transactions.
    - ii. Sélectionnez **sauvegarde complète** si vous souhaitez sauvegarder uniquement les fichiers de base de données.
    - iii. Sélectionnez **Log Backup** si vous souhaitez sauvegarder uniquement les journaux de transactions.
    - iv. Sélectionnez **Copier uniquement la sauvegarde** si vous souhaitez sauvegarder vos ressources à l'aide d'une autre application.
  - c. Dans la section Paramètres du groupe de disponibilité, effectuez les opérations suivantes :
    - i. Sélectionnez Sauvegarder sur la réplique de sauvegarde préférée si vous souhaitez sauvegarder uniquement sur la réplique.
    - ii. Sélectionnez le réplica GA principal ou le réplica GA secondaire pour la sauvegarde.
    - iii. Sélectionnez la priorité de sauvegarde.
6. Dans la page instantané et sauvegarde, effectuez les opérations suivantes :
  - a. Sélectionnez la fréquence de la sauvegarde planifiée.
  - b. Spécifiez les paramètres de rétention en fonction du type de sauvegarde sélectionné.
  - c. Si vous souhaitez activer la sauvegarde Azure NetApp Files, sélectionnez **Activer la sauvegarde** et spécifiez les paramètres de rétention.
7. Dans la page Vérification, effectuez les opérations suivantes :
  - a. Dans la section Exécuter la vérification pour les programmes de sauvegarde suivants, sélectionnez la fréquence de planification.
  - b. Dans la section Options de vérification de cohérence de la base de données, effectuez les opérations suivantes :
    - i. Sélectionnez **Limit the Integrity structure to Physical structure of the database (PHYSICAL\_ONLY)** (limiter la vérification de l'intégrité à la structure physique de la base de données) et pour détecter les pages déchirées, les échecs de somme de contrôle et les défaillances matérielles courantes qui affectent la base de données.

- ii. Sélectionnez **Supprimer tous les messages d'information (NO\_INFOMSGS)** pour supprimer tous les messages d'information.

Sélectionné par défaut.

- iii. Sélectionnez **Afficher tous les messages d'erreur signalés par objet (ALL\_ERRORMSGs)** pour afficher toutes les erreurs signalées par objet.
- iv. Sélectionnez **ne pas cocher les index non clusterisés (REGROUPÉS EN CLUSTERS)** si vous ne souhaitez pas vérifier les index non clusterisés.

La base de données SQL Server utilise le vérificateur de cohérence de base de données Microsoft SQL Server (DBCC) pour vérifier l'intégrité logique et physique des objets de la base de données.

- v. Sélectionnez **limiter les vérifications et obtenir les verrous au lieu d'utiliser une copie Snapshot de base de données interne (TABLOCK)** pour limiter les vérifications et obtenir des verrous au lieu d'utiliser un instantané de base de données interne.
- c. Dans la section **Log Backup**, sélectionnez **Verify log backup upon terminés** pour vérifier la sauvegarde du journal à la fin de l'opération.
  - d. Dans la section **Paramètres du script de vérification**, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript qui doivent être exécutés avant ou après l'opération de vérification, respectivement.

8. Vérifiez le résumé et cliquez sur **Terminer**.

## Créez des groupes de ressources et associez des stratégies de sauvegarde SQL

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger.

Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.
Utilisez le format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.

4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.
5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.
  - b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
  - c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.
  - d. Sélectionnez le planificateur Microsoft SQL Server.
7. Dans la page Vérification, effectuez les opérations suivantes :
  - a. Sélectionnez le serveur de vérification.
  - b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer votre planning de vérification, puis cliquez sur \*\*  .
  - c. Sélectionnez **Exécuter la vérification après la sauvegarde** ou **Exécuter la vérification planifiée**.
  - d. Cliquez sur **OK**.
8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Sauvegardez les bases de données SQL Server exécutées sur Azure NetApp Files

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Avant de commencer

Vous devez créer un équilibreur de charge si aucune IP de cluster n'est attribuée au cluster de basculement Windows Azure ou s'il n'est pas accessible depuis SnapCenter. L'adresse IP de l'équilibreur de charge doit être configurée et accessible depuis le serveur SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, sélectionnez **base de données**, **instance** ou **Groupe de disponibilité** dans la liste déroulante Affichage.
3. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.
4. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.
  - b. Sélectionnez \*\* \*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous souhaitez configurer un planning.

- c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.

*policy\_name* est le nom de la stratégie que vous avez sélectionnée.

- d. Sélectionnez **utiliser le planificateur Microsoft SQL Server**, puis sélectionnez l'instance du planificateur dans la liste déroulante **instance du planificateur** associée à la stratégie de planification.
5. Dans la page Vérification, effectuez les opérations suivantes :
    - a. Sélectionnez le serveur de vérification.
    - b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer votre planning de vérification, puis cliquez sur \* \*  .
    - c. Sélectionnez **Exécuter la vérification après la sauvegarde** ou **Exécuter la vérification planifiée**.
    - d. Cliquez sur OK.
  6. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
  7. Vérifiez le résumé, puis cliquez sur **Terminer**.
  8. Sélectionnez **Sauvegarder maintenant**.
  9. Dans la page sauvegarde, effectuez les opérations suivantes :
    - a. Si plusieurs stratégies sont associées à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.
    - b. Sélectionnez **vérifier après la sauvegarde**.
    - c. Sélectionnez **Backup**.
  10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Sauvegardez les groupes de ressources SQL Server

Vous pouvez sauvegarder les groupes de ressources composés de plusieurs ressources. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si plusieurs stratégies sont associées au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.
  - b. Après la sauvegarde, sélectionnez **Verify** pour vérifier la sauvegarde à la demande.
  - c. Sélectionnez **Backup**.
5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Restaurer et restaurer des bases de données SQL Server

Vous pouvez utiliser SnapCenter pour restaurer des bases de données SQL Server sauvegardées. La restauration de la base de données est un processus en plusieurs phases qui copie toutes les pages de données et de journaux d'une sauvegarde SQL Server spécifiée vers une base de données spécifiée.

### Description de la tâche

Vous devez vous assurer que l'instance cible de restauration est configurée avec un utilisateur Active Directory qui appartient au domaine SMB ADactive Directory et dispose des autorisations nécessaires pour définir les autorisations de fichier de manière appropriée. Vous devez configurer les informations d'identification dans SnapCenter au niveau de l'instance.

L'authentification SQL pour l'instance cible ne sera pas prise en charge pour les configurations SMB. L'instance cible doit être configurée dans SnapCenter avec l'utilisateur Active Directory disposant des autorisations requises.

Si le compte de service de services de plug-in SnapCenter n'est pas un utilisateur Active Directory, alors lors de la restauration sur un autre hôte, l'utilisateur qui a le contrôle total sur les volumes source est requis pour qu'il puisse être usurpé et effectuer l'opération requise.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **base de données** ou **Groupe de ressources** dans la liste Affichage.
3. Sélectionnez la base de données ou le groupe de ressources dans la liste.
4. Dans la vue gérer les copies, sélectionnez **backups** à partir du système de stockage.
5. Sélectionnez la sauvegarde dans la table, puis cliquez sur  icône.
6. Dans la page objectif de restauration, sélectionnez l'une des options suivantes :
  - a. Sélectionnez **Restaurer la base de données sur le même hôte que celui sur lequel la sauvegarde a été créée** si vous souhaitez restaurer la base de données sur le même serveur SQL sur lequel les sauvegardes sont effectuées.
  - b. Sélectionnez **Restaurer la base de données sur un autre hôte** si vous souhaitez que la base de données soit restaurée sur un autre serveur SQL sur le même hôte ou sur un autre hôte sur lequel les sauvegardes sont effectuées.
7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :
  - a. Sélectionnez **aucun** si vous devez restaurer uniquement la sauvegarde complète sans journaux.
  - b. Sélectionnez **toutes les sauvegardes de journaux** opération de restauration de sauvegarde à la minute pour restaurer toutes les sauvegardes de journaux disponibles après la sauvegarde complète.
  - c. Sélectionnez **par sauvegardes de journaux** pour effectuer une opération de restauration ponctuelle, qui restaure la base de données en fonction des journaux de sauvegarde jusqu'à ce que le journal de sauvegarde avec la date sélectionnée.
  - d. Sélectionnez **par date spécifique jusqu'à** pour spécifier la date et l'heure après lesquelles les journaux de transactions ne sont pas appliqués à la base de données restaurée.
  - e. Si vous avez sélectionné **toutes les sauvegardes de journaux, par sauvegarde de journaux** ou **par**

**date spécifique jusqu'à** et que les journaux se trouvent à un emplacement personnalisé, sélectionnez **utiliser le répertoire de journaux personnalisé**, puis spécifiez l'emplacement du journal.

8. Dans la page pré-opérations et post-opérations, spécifiez les détails requis.
9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez le processus de restauration à l'aide de la page **Monitor > Jobs**.

## Cloner la sauvegarde de la base de données SQL Server

Vous pouvez utiliser SnapCenter pour cloner une base de données SQL à l'aide de la sauvegarde de la base de données. Les clones créés sont des clones épais et sont créés dans le pool de capacité parent.

### Description de la tâche

Vous devez vous assurer que l'instance cible du clone est configurée avec un utilisateur Active Directory qui appartient au domaine SMB ADactive Directory et dispose des autorisations nécessaires pour définir les autorisations de fichier de manière appropriée. Vous devez configurer les informations d'identification dans SnapCenter au niveau de l'instance.

L'authentification SQL pour l'instance cible ne sera pas prise en charge pour les configurations SMB. L'instance cible doit être configurée dans SnapCenter avec l'utilisateur Active Directory disposant des autorisations requises.

Si le compte de service de services de plug-in SnapCenter n'est pas un utilisateur Active Directory, alors lors de l'exécution du clonage, l'utilisateur qui a le contrôle total sur les volumes source est requis pour qu'il puisse être usurpé et effectuer l'opération requise.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données ou le groupe de ressources.
4. Dans la page d'affichage **gérer les copies**, sélectionnez la sauvegarde à partir du système de stockage principal.
5. Sélectionnez la sauvegarde, puis sélectionnez .
6. Dans la page **Clone Options**, fournissez tous les détails requis.
7. Dans la page emplacement, sélectionnez un emplacement de stockage pour créer un clone.

Si les volumes ANF de la base de données SQL Server sont configurés dans un pool de capacité QoS manuel, spécifiez la QoS pour les volumes clonés.

Si la QoS des volumes clonés n'est pas spécifiée, la QoS du volume source sera utilisée. Si le pool de capacité de QoS automatique est utilisé, la valeur de QoS spécifiée sera ignorée.

8. Dans la page journaux, sélectionnez l'une des options suivantes :
  - a. Sélectionnez **aucun** si vous souhaitez cloner uniquement la sauvegarde complète sans journal.

- b. Sélectionnez **toutes les sauvegardes de journaux** si vous souhaitez cloner toutes les sauvegardes de journaux disponibles datées après la sauvegarde complète.
  - c. Sélectionnez **par sauvegardes de journal jusqu'à** si vous souhaitez cloner la base de données en fonction des journaux de sauvegarde créés jusqu'au journal de sauvegarde avec la date sélectionnée.
  - d. Sélectionnez **par date spécifique jusqu'à** si vous ne souhaitez pas appliquer les journaux de transactions après la date et l'heure spécifiées.
9. Sur la page **script**, entrez le délai d'expiration du script, le chemin et les arguments du prescripteur ou du postscript qui doivent être exécutés avant ou après l'opération de clonage, respectivement.
  10. Dans la page **notification**, dans la liste déroulante **préférence de courrier électronique**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
  11. Passez en revue le résumé, puis sélectionnez **Terminer**.
  12. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

### Réaliser le cycle de vie des clones

SnapCenter permet de créer des clones à partir d'un groupe de ressources ou d'une base de données. Vous pouvez cloner à la demande ou planifier des opérations de clonage récurrentes d'un groupe de ressources ou d'une base de données. Si vous clonez régulièrement une sauvegarde, vous pouvez utiliser le clone pour développer des applications, remplir des données ou restaurer des données.

#### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Database** ou **Resource Group** dans la liste **View**.
3. Sélectionnez la base de données ou le groupe de ressources.
4. Dans la page d'affichage **gérer les copies**, sélectionnez la sauvegarde à partir du système de stockage principal.
5. Sélectionnez la sauvegarde, puis sélectionnez .
6. Dans la page **Clone Options**, fournissez tous les détails requis.
7. Dans la page emplacement, sélectionnez un emplacement de stockage pour créer un clone.

Si les volumes ANF de la base de données SQL Server sont configurés dans un pool de capacité QoS manuel, spécifiez la QoS pour les volumes clonés.

Si la QoS des volumes clonés n'est pas spécifiée, la QoS du volume source sera utilisée. Si le pool de capacité de QoS automatique est utilisé, la valeur de QoS spécifiée sera ignorée.

8. Sur la page **script**, entrez le délai d'expiration du script, le chemin et les arguments du prescripteur ou du postscript qui doivent être exécutés avant ou après l'opération de clonage, respectivement.
9. Dans la page planification, effectuez l'une des opérations suivantes :
  - Sélectionnez **Exécuter maintenant** si vous souhaitez exécuter le travail de clonage immédiatement.
  - Sélectionnez **Configure schedule** pour déterminer la fréquence à laquelle l'opération de clonage doit se produire, le moment où la planification de clonage doit démarrer, le jour où l'opération de clonage doit se produire, le moment où la planification doit expirer et si les clones doivent être supprimés après l'expiration de la planification.
10. Dans la page **notification**, dans la liste déroulante **préférence de courrier électronique**, sélectionnez les

scénarios dans lesquels vous souhaitez envoyer les e-mails.

11. Passez en revue le résumé, puis sélectionnez **Terminer**.
12. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Protection des bases de données Oracle

### Ajoutez des hôtes et installez le plug-in SnapCenter pour la base de données Oracle

Vous pouvez utiliser la page Ajouter un hôte pour ajouter des hôtes, puis installer le package de plug-ins SnapCenter pour Linux ou le package de plug-ins SnapCenter pour AIX. Les plug-ins sont automatiquement installés sur les hôtes distants.

Vous pouvez ajouter un hôte et installer des modules de plug-in pour un hôte individuel ou pour un cluster. Si vous installez le plug-in sur un cluster (Oracle RAC), il est installé sur tous les nœuds du cluster. Pour Oracle RAC One Node, vous devez installer le plug-in sur les nœuds actif et passif.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que l'onglet **Managed Hosts** est sélectionné.
3. Cliquez sur **Ajouter**.
4. Dans la page hôtes, effectuez les opérations suivantes :
  - a. Dans le champ Type d'hôte, sélectionnez le type d'hôte.
  - b. Dans le champ Nom d'hôte, entrez le nom de domaine complet (FQDN) ou l'adresse IP de l'hôte.
  - c. Dans le champ informations d'identification, entrez les informations d'identification que vous avez créées.
5. Dans la section Sélectionner les plug-ins à installer, sélectionnez les plug-ins à installer.
6. (Facultatif) cliquez sur **plus d'options** et spécifiez les détails.
7. Cliquez sur **soumettre**.
8. Vérifiez l'empreinte digitale, puis cliquez sur **confirmer et soumettre**.

Dans une configuration de cluster, vous devez vérifier l'empreinte de chacun des nœuds du cluster.

9. Surveillez la progression de l'installation.

### Créez des règles de sauvegarde pour les bases de données Oracle

Avant d'utiliser SnapCenter pour sauvegarder les ressources de la base de données Oracle, vous devez créer une stratégie de sauvegarde pour la ressource ou le groupe de ressources à sauvegarder.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Sélectionnez Oracle Database dans la liste déroulante.

4. Cliquez sur **Nouveau**.
5. Dans la page Nom, entrez le nom et la description de la stratégie.
6. Dans la page Type de stratégie, effectuez les opérations suivantes :
  - a. Sélectionnez **Azure NetApp Files** comme type de stockage.
  - b. Sélectionnez le type de sauvegarde en tant que sauvegarde en ligne ou hors ligne.
  - c. Si vous souhaitez cataloguer la sauvegarde à l'aide d'Oracle Recovery Manager (RMAN), sélectionnez **sauvegarde de catalogue avec Oracle Recovery Manager (RMAN)**.
  - d. Si vous souhaitez élaguer les journaux d'archive après la sauvegarde, sélectionnez **Prune archive logs après la sauvegarde**.
  - e. Spécifiez les paramètres de suppression du journal d'archivage.
7. Dans la page instantané et sauvegarde, effectuez les opérations suivantes :
  - a. Sélectionnez la fréquence de la sauvegarde planifiée.
  - b. Spécifiez les paramètres de rétention.
  - c. Si vous souhaitez activer la sauvegarde Azure NetApp Files, sélectionnez **Activer la sauvegarde** et spécifiez les paramètres de rétention.
8. Dans la page script, entrez le chemin d'accès et les arguments du prescripteur ou du PostScript que vous souhaitez exécuter avant ou après l'opération de sauvegarde, respectivement.
9. Dans la page Vérification, sélectionnez le planning de sauvegarde pour lequel vous souhaitez effectuer l'opération de vérification et entrez respectivement le chemin et les arguments du prescripteur ou du postscript que vous souhaitez exécuter avant ou après l'opération de vérification.
10. Vérifiez le résumé et cliquez sur **Terminer**.

## Créez des groupes de ressources et associez des stratégies de sauvegarde Oracle

Un groupe de ressources est le conteneur dans lequel vous devez ajouter des ressources que vous souhaitez sauvegarder et protéger.

Un groupe de ressources vous permet de sauvegarder simultanément toutes les données associées à une application donnée. Un groupe de ressources est requis pour toute tâche de protection des données. Vous devez également associer une ou plusieurs stratégies au groupe de ressources pour définir le type de travail de protection des données que vous souhaitez exécuter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, cliquez sur **Nouveau groupe de ressources**.
3. Dans la page Nom, effectuez les opérations suivantes :

Pour ce champ...	Procédez comme ça...
Nom	Entrez un nom pour le groupe de ressources.
Étiquettes	Entrez un ou plusieurs libellés qui vous aideront à rechercher ultérieurement le groupe de ressources.

Pour ce champ...	Procédez comme ça...
Utilisez le format de nom personnalisé pour la copie Snapshot	Cochez cette case et entrez un format de nom personnalisé à utiliser pour le nom du snapshot.
Destination du fichier journal d'archivage	Spécifiez les destinations des fichiers journaux d'archive.

4. Dans la page Ressources, sélectionnez un nom d'hôte dans la liste déroulante **hôte** et le type de ressource dans la liste déroulante **Type de ressource**.
5. Sélectionnez les ressources dans la section **Ressources disponibles**, puis cliquez sur la flèche vers la droite pour les déplacer dans la section **Ressources sélectionnées**.
6. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.
  - b. Dans la colonne configurer les plannings, cliquez sur \*\*  pour la stratégie que vous souhaitez configurer.
  - c. Dans la boîte de dialogue Ajouter des planifications pour la stratégie *policy\_name*, configurez le programme, puis cliquez sur **OK**.
7. Dans la page Vérification, effectuez les opérations suivantes :
  - a. Sélectionnez le serveur de vérification.
  - b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer votre planification de vérification, puis cliquez sur \* .
  - c. Sélectionnez **Exécuter la vérification après la sauvegarde** ou **Exécuter la vérification planifiée**.
  - d. Cliquez sur **OK**.
8. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
9. Vérifiez le résumé, puis cliquez sur **Terminer**.

## Sauvegarde des bases de données Oracle exécutées sur Azure NetApp Files

Si une ressource ne fait pas encore partie d'un groupe de ressources, vous pouvez sauvegarder la ressource à partir de la page Ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page ressource, sélectionnez **base de données** dans la liste déroulante Affichage.
3. Dans la page ressource, sélectionnez **utiliser le format de nom personnalisé pour la copie Snapshot**, puis entrez un format de nom personnalisé que vous souhaitez utiliser pour le nom de l'instantané.
4. Dans la page stratégies, effectuez les opérations suivantes :
  - a. Sélectionnez une ou plusieurs stratégies dans la liste déroulante.
  - b. Sélectionnez \*\*\*  dans la colonne configurer les plannings pour la stratégie pour laquelle vous

souhaitez configurer un planning.

- c. Dans la boîte de dialogue Ajouter des plannings pour la stratégie *nom\_règle*, configurez la planification, puis sélectionnez **OK**.
5. Dans la page Vérification, effectuez les opérations suivantes :
  - a. Sélectionnez le serveur de vérification.
  - b. Sélectionnez la stratégie pour laquelle vous souhaitez configurer votre planning de vérification, puis cliquez sur \* \*  .
  - c. Sélectionnez **Exécuter la vérification après la sauvegarde** ou **Exécuter la vérification planifiée**.
  - d. Cliquez sur OK.
6. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
7. Vérifiez le résumé, puis cliquez sur **Terminer**.
8. Sélectionnez **Sauvegarder maintenant**.
9. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si plusieurs stratégies sont associées à la ressource, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.
  - b. Cliquez sur **Backup**.
10. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Sauvegarder les groupes de ressources Oracle

Vous pouvez sauvegarder les groupes de ressources composés de plusieurs ressources. Une opération de sauvegarde sur le groupe de ressources est effectuée sur toutes les ressources définies dans le groupe de ressources.

### Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Dans la page groupes de ressources, sélectionnez le groupe de ressources à sauvegarder, puis sélectionnez **Sauvegarder maintenant**.
4. Dans la page sauvegarde, effectuez les opérations suivantes :
  - a. Si plusieurs stratégies sont associées au groupe de ressources, dans la liste déroulante **Stratégie**, sélectionnez la stratégie que vous souhaitez utiliser pour la sauvegarde.
  - b. Sélectionnez **Backup**.
5. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

## Restaurez et récupérez les bases de données Oracle

En cas de perte de données, vous pouvez utiliser SnapCenter pour restaurer les données d'une ou plusieurs sauvegardes sur votre système de fichiers actif, puis restaurer la base de données.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **base de données** ou **Groupe de ressources** dans la liste Affichage.
3. Sélectionnez la base de données ou le groupe de ressources dans la liste.
4. Dans la vue gérer les copies, sélectionnez **backups** dans le système de stockage principal.
5. Sélectionnez la sauvegarde dans le tableau, puis cliquez sur .
6. Dans la page objectif de restauration, effectuez les tâches suivantes :
  - a. Sélectionnez RAC si vous avez sélectionné une sauvegarde d'une base de données dans un environnement RAC.
  - b. Effectuez les opérations suivantes :
    - i. Sélectionnez **tous les fichiers de données** si vous souhaitez restaurer uniquement les fichiers de base de données.
    - ii. Sélectionnez **tablespaces** si vous souhaitez restaurer uniquement les tablespaces.
    - iii. Sélectionnez **Redo log files** si vous souhaitez restaurer les fichiers redo log des bases de données de secours Data Guard ou Active Data Guard.
    - iv. Sélectionnez **bases de données enfichables** et spécifiez les PDB à restaurer.
    - v. Sélectionnez **Pluggable database (PDB) tablespaces**, puis spécifiez le PDB et les espaces de stockage de ce PDB que vous souhaitez restaurer.
    - vi. Sélectionnez **Restaurer la base de données sur le même hôte que celui sur lequel la sauvegarde a été créée** si vous souhaitez restaurer la base de données sur le même serveur SQL sur lequel les sauvegardes sont effectuées.
    - vii. Sélectionnez **Restaurer la base de données sur un autre hôte** si vous souhaitez que la base de données soit restaurée sur un autre serveur SQL sur le même hôte ou sur un autre hôte sur lequel les sauvegardes sont effectuées.
    - viii. Sélectionnez **changer l'état de la base de données si nécessaire pour restaurer et restaurer** pour changer l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de reprise.
    - ix. Sélectionnez **forcer la restauration sur place** si vous souhaitez effectuer une restauration sur place dans les scénarios où de nouveaux fichiers de données sont ajoutés après la sauvegarde ou lorsque des LUN sont ajoutées, supprimés ou recrées à un groupe de disques LVM.
7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :
  - a. Sélectionnez **tous les journaux** si vous souhaitez récupérer la dernière transaction.
  - b. Sélectionnez **jusqu'à ce que SCN (Numéro de changement de système)** si vous souhaitez restaurer un SCN spécifique.
  - c. Sélectionnez **Date et heure** si vous souhaitez récupérer une date et une heure spécifiques.
  - d. Sélectionnez **pas de récupération** si vous ne voulez pas récupérer.
  - e. Sélectionnez **spécifier les emplacements des journaux d'archives externes** si vous souhaitez spécifier l'emplacement des fichiers journaux d'archives externes.
8. Dans la page pré-opérations et post-opérations, spécifiez les détails requis.
9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans

lesquels vous souhaitez envoyer les e-mails.

10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez la progression de l'opération en cliquant sur **moniteur > travaux**.

## Restauration et restauration d'espaces de stockage à partir d'une restauration instantanée

Vous pouvez restaurer un sous-ensemble d'espaces de stockage qui ont été corrompus ou supprimés sans affecter les autres espaces de stockage de la base de données. SnapCenter utilise RMAN pour effectuer une restauration instantanée (PITR) des tablespaces.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **base de données** ou **Groupe de ressources** dans la liste Affichage.
3. Sélectionnez la base de données de type instance unique (multitenant).
4. Dans la vue gérer les copies, sélectionnez **sauvegardes** dans le système de stockage.

Si la sauvegarde n'est pas cataloguée, sélectionnez la sauvegarde et cliquez sur **Catalogue**.

5. Sélectionnez la sauvegarde cataloguée, puis cliquez sur  .
6. Dans la page objectif de restauration, effectuez les tâches suivantes :
  - a. Sélectionnez **RAC** si vous avez sélectionné une sauvegarde d'une base de données dans un environnement RAC.
  - b. Sélectionnez **tablespaces** si vous souhaitez restaurer uniquement les tablespaces.
  - c. Sélectionnez **changer l'état de la base de données si nécessaire pour restaurer et restaurer** pour changer l'état de la base de données à l'état requis pour effectuer les opérations de restauration et de reprise.
7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :
  - a. Sélectionnez **jusqu'à ce que SCN (Numéro de changement de système)** si vous souhaitez restaurer un SCN spécifique.
  - b. Sélectionnez **Date et heure** si vous souhaitez récupérer une date et une heure spécifiques.
8. Dans la page pré-opérations et post-opérations, spécifiez les détails requis.
9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez le processus de restauration à l'aide de la page **Monitor > Jobs**.

## Restaurez et récupérez une base de données enfichable à l'aide d'une récupération ponctuelle

Vous pouvez restaurer et récupérer une base de données enfichable (PDB) qui a été corrompue ou supprimée sans affecter les autres PDB dans la base de données du conteneur (CDB). SnapCenter utilise RMAN pour effectuer une récupération ponctuelle (PITI) du PDB.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié

dans la liste.

2. Dans la page Ressources, sélectionnez **base de données** ou **Groupe de ressources** dans la liste Affichage.
3. Sélectionnez la base de données de type instance unique (multitenant).
4. Dans la vue gérer les copies, sélectionnez **sauvegardes** dans le système de stockage.

Si la sauvegarde n'est pas cataloguée, sélectionnez la sauvegarde et cliquez sur **Catalogue**.

5. Sélectionnez la sauvegarde cataloguée, puis cliquez sur .
6. Dans la page objectif de restauration, effectuez les tâches suivantes :
  - a. Sélectionnez **RAC** si vous avez sélectionné une sauvegarde d'une base de données dans un environnement RAC.
  - b. Selon que vous souhaitez restaurer le PDB ou les espaces de stockage dans un PDB, effectuez l'une des opérations suivantes :
    - Sélectionnez **bases de données enfichables (PDB)** si vous souhaitez restaurer un PDB.
    - Sélectionnez **tablespaces de base de données enfichables (PDB)** si vous souhaitez restaurer des tablespaces dans un PDB.
7. Dans la page étendue de la récupération, sélectionnez l'une des options suivantes :
  - a. Sélectionnez **jusqu'à ce que SCN (Numéro de changement de système)** si vous souhaitez restaurer un SCN spécifique.
  - b. Sélectionnez **Date et heure** si vous souhaitez récupérer une date et une heure spécifiques.
8. Dans la page pré-opérations et post-opérations, spécifiez les détails requis.
9. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
10. Vérifiez le résumé, puis cliquez sur **Terminer**.
11. Surveillez le processus de restauration à l'aide de la page **Monitor > Jobs**.

## Cloner la sauvegarde de la base de données Oracle

Vous pouvez utiliser SnapCenter pour cloner une base de données Oracle à l'aide de la sauvegarde de la base de données. Les clones créés sont des clones épais et sont créés dans le pool de capacité parent.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **base de données** ou **Groupe de ressources** dans la liste Affichage.
3. Sélectionnez la base de données.
4. Dans la page d'affichage gérer les copies, sélectionnez la sauvegarde à partir du système de stockage principal.
5. Sélectionnez la sauvegarde des données, puis cliquez sur .

6. Dans la page Nom, indiquez si vous souhaitez cloner une base de données (CDB ou non CDB) ou cloner une base de données enfichable (PDB).
7. Dans la page emplacements, spécifiez les détails requis.

Si les volumes ANF de la base de données Oracle sont configurés dans un pool de capacité QoS manuelle, spécifiez la QoS pour les volumes clonés.

Si la QoS des volumes clonés n'est pas spécifiée, la QoS du volume source sera utilisée. Si le pool de capacité de QoS automatique est utilisé, la valeur de QoS spécifiée sera ignorée.

8. Dans la page informations d'identification, effectuez l'une des opérations suivantes :
  - a. Pour Nom d'identification de l'utilisateur sys, sélectionnez les informations d'identification à utiliser pour définir le mot de passe utilisateur sys de la base de données clone.
  - b. Pour le nom d'informations d'identification de l'instance ASM, sélectionnez **None** si l'authentification du système d'exploitation est activée pour la connexion à l'instance ASM sur l'hôte clone.

Sinon, sélectionnez les informations d'identification Oracle ASM configurées avec l'utilisateur « sys » ou un utilisateur disposant du privilège « sysasm » applicable à l'hôte clone.

9. Dans la page opérations préalables, spécifiez le chemin et les arguments des prescripteurs et, dans la section Paramètres des paramètres de base de données, modifiez les valeurs des paramètres de base de données préremplis utilisés pour initialiser la base de données.
10. Dans la page Post-Ops, **recover database** et **until Cancel** sont sélectionnés par défaut pour effectuer la récupération de la base de données clonée.
  - a. Si vous sélectionnez **jusqu'à ce que Annuler**, SnapCenter effectue la récupération en montant la dernière sauvegarde de journal ayant la séquence ininterrompue des journaux d'archive après la sauvegarde de données sélectionnée pour le clonage.
  - b. Si vous sélectionnez **Date et heure**, SnapCenter restaure la base de données jusqu'à une date et une heure spécifiées.
  - c. Si vous sélectionnez **jusqu'à SCN**, SnapCenter restaure la base de données jusqu'à un SCN spécifié.
  - d. Si vous sélectionnez **spécifier les emplacements des journaux d'archives externes**, SnapCenter identifie et monte le nombre optimal de sauvegardes de journaux en fonction du SCN spécifié ou de la date et de l'heure sélectionnées.
  - e. Par défaut, la case **Create New DBID** (Créer un nouvel ID de base de données) est cochée pour générer un numéro unique (DBID) pour la base de données clonée qui la différencie de la base de données source.

Décochez la case si vous souhaitez affecter le DBID de la base de données source à la base de données clonée. Dans ce scénario, si vous souhaitez enregistrer la base de données clonée avec le catalogue RMAN externe où la base de données source est déjà enregistrée, l'opération échoue.
  - f. Cochez la case **Créer un fichier temporaire pour l'espace table temporaire** si vous souhaitez créer un fichier temporaire pour l'espace table temporaire par défaut de la base de données clonée.
  - g. Dans **Entrez les entrées sql à appliquer lorsque le clone est créé**, ajoutez les entrées sql que vous souhaitez appliquer lors de la création du clone.
  - h. Dans **Entrez les scripts à exécuter après l'opération de clonage**, spécifiez le chemin et les arguments du script PostScript que vous souhaitez exécuter après l'opération de clonage.

11. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.

12. Passez en revue le résumé, puis sélectionnez **Terminer**.
13. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

### Cloner une base de données enfichable

Vous pouvez cloner une base de données enfichable (PDB) sur un CDB cible différent ou identique sur le même hôte ou un autre hôte. Vous pouvez également récupérer le PDB cloné sur un SCN ou une date et une heure souhaités.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **base de données** ou **Groupe de ressources** dans la liste Affichage.
3. Sélectionnez la base de données de type instance unique (multitenant).
4. Dans la page d'affichage gérer les copies, sélectionnez la sauvegarde à partir du système de stockage principal.
5. Sélectionnez la sauvegarde, puis cliquez sur .
6. Dans la page Nom, sélectionnez **PDB Clone** et spécifiez les autres détails.
7. Dans la page emplacements, spécifiez les détails requis.
8. Dans la page opérations préalables, spécifiez le chemin et les arguments des prescripteurs et, dans la section Paramètres des paramètres de base de données, modifiez les valeurs des paramètres de base de données préremplis utilisés pour initialiser la base de données.
9. Dans la page Post-Ops, **jusqu'à ce que Annuler** soit sélectionné par défaut pour effectuer la récupération de la base de données clonée.
  - a. Si vous sélectionnez **jusqu'à ce que Annuler**, SnapCenter effectue la récupération en montant la dernière sauvegarde de journal ayant la séquence ininterrompue des journaux d'archive après la sauvegarde de données sélectionnée pour le clonage.
  - b. Si vous sélectionnez **Date et heure**, SnapCenter restaure la base de données jusqu'à une date et une heure spécifiées.
  - c. Si vous sélectionnez **spécifier les emplacements des journaux d'archives externes**, SnapCenter identifie et monte le nombre optimal de sauvegardes de journaux en fonction du SCN spécifié ou de la date et de l'heure sélectionnées.
  - d. Par défaut, la case **Create New DBID** (Créer un nouvel ID de base de données) est cochée pour générer un numéro unique (DBID) pour la base de données clonée qui la différencie de la base de données source.

Décochez la case si vous souhaitez affecter le DBID de la base de données source à la base de données clonée. Dans ce scénario, si vous souhaitez enregistrer la base de données clonée avec le catalogue RMAN externe où la base de données source est déjà enregistrée, l'opération échoue.
  - e. Cochez la case **Créer un fichier temporaire pour l'espace table temporaire** si vous souhaitez créer un fichier temporaire pour l'espace table temporaire par défaut de la base de données clonée.
  - f. Dans **Entrez les entrées sql à appliquer lorsque le clone est créé**, ajoutez les entrées sql que vous souhaitez appliquer lors de la création du clone.
  - g. Dans **Entrez les scripts à exécuter après l'opération de clonage**, spécifiez le chemin et les arguments du script PostScript que vous souhaitez exécuter après l'opération de clonage.

10. Dans la page notification, dans la liste déroulante Préférences de **E-mail**, sélectionnez les scénarios dans lesquels vous souhaitez envoyer les e-mails.
11. Passez en revue le résumé, puis sélectionnez **Terminer**.
12. Surveillez la progression de l'opération en sélectionnant **Monitor > Jobs**.

# Gestion de SnapCenter Server et des plug-ins

## Voir le tableau de bord

### Présentation du tableau de bord

Dans le volet de navigation de SnapCenter à gauche, le tableau de bord vous présente un premier aperçu de l'état de santé de votre système, y compris l'activité récente des tâches, les alertes, le récapitulatif de la protection, l'efficacité et l'utilisation du stockage, l'état des tâches SnapCenter (sauvegarde, clonage, restauration), l'état de la configuration pour les hôtes de cluster Windows et autonomes, Nombre de SVM (Storage Virtual machines) gérés par SnapCenter et capacité des licences.

Les informations affichées dans la vue Tableau de bord dépendent du rôle attribué à l'utilisateur actuellement connecté à SnapCenter. Il est possible que certains contenus ne s'affichent pas si l'utilisateur n'est pas autorisé à afficher ces informations.

Dans de nombreux cas, vous pouvez afficher plus d'informations sur un affichage en positionnant le pointeur de la souris sur **i**. Dans certains cas, les informations affichées dans le tableau de bord sont liées à des informations sources détaillées dans les pages de l'interface graphique de SnapCenter, telles que Ressources, moniteur et Rapports.

### Activités récentes du poste

La mosaïque activités de travail récentes affiche l'activité de tâche la plus récente à partir de toutes les tâches de sauvegarde, de restauration et de clonage auxquelles vous avez accès. Les travaux de cet écran ont l'un des États suivants : terminé, Avertissement, échec, exécution, en file d'attente, Et annulée.

Passez la souris sur un travail pour plus d'informations. Vous pouvez afficher des informations supplémentaires sur les tâches en cliquant sur un numéro de travail spécifique, qui vous redirige vers la page moniteur. À partir de là, vous pouvez obtenir les détails du travail ou les informations du journal et générer un rapport spécifique à ce travail.

Cliquez sur **Afficher tout** pour afficher l'historique de tous les travaux SnapCenter.

### Alertes

La mosaïque alertes affiche les dernières alertes critiques et d'avertissement non résolues pour les hôtes et le serveur SnapCenter.

Le nombre total d'alertes critiques et de catégories d'avertissement s'affiche en haut de l'écran. En cliquant sur les totaux critiques ou d'avertissement, vous accédez à la page alertes avec le filtre spécifique appliqué dans la page alertes.

En cliquant sur une alerte spécifique, vous accédez à la page alertes pour en savoir plus sur cette alerte. En cliquant sur **Afficher tout** en bas de l'écran, vous serez redirigé vers la page alertes pour obtenir une liste de toutes les alertes.

### Dernière synthèse de la protection

La dernière mosaïque de résumé de la protection vous donne l'état de protection pour toutes les entités auxquelles vous avez accès. Par défaut, l'affichage indique l'état de tous les plug-ins. Des informations d'état

sont fournies pour les ressources sauvegardées sur un stockage primaire comme snapshots et sur un stockage secondaire à l'aide des technologies SnapMirror et SnapVault. La disponibilité des informations d'état de protection pour le stockage secondaire dépend du type de plug-in sélectionné.



Si vous utilisez une règle de protection mirror-vault, les compteurs de la protection récapitulative sont affichés dans le tableau récapitulatif SnapVault et non dans le graphique SnapMirror.

L'état de protection des différents plug-ins est disponible en sélectionnant un plug-in dans le menu déroulant. Un graphique donut indique le pourcentage de ressources protégées pour le plug-in sélectionné. Un clic sur une tranche de donut vous redirige vers la page **Rapports > Plug-in**, qui fournit un rapport détaillé de toutes les activités de stockage primaire et secondaire pour le plug-in spécifié.



Les rapports sur le stockage secondaire s'appliquent uniquement à SnapVault. Les rapports SnapMirror ne sont pas pris en charge.



SAP HANA fournit des informations sur l'état de la protection pour le stockage principal et secondaire pour les snapshots. Seul l'état de protection du stockage primaire est disponible pour les sauvegardes basées sur des fichiers.

État de la protection	Le stockage primaire	Le stockage secondaire
Échec	Nombre d'entités faisant partie d'un groupe de ressources, où le groupe de ressources a exécuté une sauvegarde, mais la sauvegarde a échoué.	Nombre d'entités ayant des sauvegardes qui n'ont pas pu être transférées vers une destination secondaire.
Réussi	Nombre d'entités dans un groupe de ressources où le groupe de ressources a été sauvegardé avec succès.	Nombre d'entités ayant des sauvegardes qui ont été transférées avec succès vers une destination secondaire.
Non configuré	Nombre d'entités qui ne font partie d'aucun groupe de ressources et qui n'ont pas été sauvegardées.	Nombre d'entités faisant partie d'un ou de plusieurs groupes de ressources qui ne sont pas configurés pour que les sauvegardes soient transférées vers une destination secondaire.
Non lancé	Nombre d'entités faisant partie d'un groupe de ressources, mais aucune sauvegarde n'a été exécutée.	Sans objet



Si vous utilisez SnapCenter Server 4.2 et une version antérieure du plug-in (antérieure à 4.2) pour créer des sauvegardes, la vignette **dernière version de protection Summary** n'affiche pas l'état de protection SnapMirror de ces sauvegardes.

## Emplois

La mosaïque travaux fournit un récapitulatif des tâches de sauvegarde, de restauration et de clonage auxquelles vous avez accès. Vous pouvez personnaliser l'intervalle de temps de n'importe quel rapport à l'aide du menu déroulant. Les options de période sont fixées aux 24 dernières heures, aux 7 derniers jours et aux 30 derniers jours. Le rapport par défaut affiche les tâches de protection des données exécutées au cours des 7 derniers jours.

Les informations sur les tâches de sauvegarde, de restauration et de clonage sont affichées dans des graphiques en donut. Un clic sur une tranche de donut vous redirige vers la page Monitor avec des filtres de travail pré-appliqués à la sélection.

État des tâches	Description
Échec	Nombre de travaux ayant échoué.
Avertissement	Nombre de travaux ayant rencontré une erreur.
Réussi	Nombre de travaux terminés avec succès.
Exécution	Nombre de travaux en cours d'exécution.

## Stockage

Le module stockage affiche le stockage primaire et secondaire consommé par les tâches de protection sur une période de 90 jours, décrit sous forme graphique les tendances de consommation et calcule les économies en termes de stockage primaire. Les informations de stockage sont mises à jour toutes les 24 heures à 12 h du matin

Le total de consommation de la journée, qui comprend le nombre total de sauvegardes disponibles en SnapCenter et leur taille occupée, s'affiche en haut de l'écran. Une sauvegarde peut avoir plusieurs snapshots associés et le nombre de copies reflète le même. Cela s'applique aux snapshots primaires et secondaires. Par exemple, vous avez créé 10 sauvegardes, dont 2 sont supprimées en raison de la conservation des sauvegardes basée sur des règles et 1 sauvegarde est explicitement supprimée par vous. Ainsi, le nombre de 7 sauvegardes s'affiche avec la taille occupée par ces 7 sauvegardes.

Le facteur d'économie du stockage pour le stockage primaire est le rapport entre la capacité logique (économies de clones et de copies Snapshot et espace de stockage consommé) et la capacité physique du stockage primaire. Un graphique à barres illustre les économies de stockage réalisées.

Le graphique linéaire trace séparément la consommation de stockage primaire et secondaire, jour par jour, sur une période de 90 jours. Passez le pointeur de la souris sur les graphiques pour obtenir des résultats détaillés au jour le jour.



Si vous utilisez SnapCenter Server 4.2 et une version antérieure du plug-in (antérieure à 4.2) pour créer des sauvegardes, la vignette **Storage** n'affiche pas le nombre de sauvegardes, l'espace de stockage utilisé par ces sauvegardes, les économies de snapshots, les économies de clonage et la taille de la copie Snapshot.

## Configuration

La mosaïque de configuration fournit des informations d'état consolidées pour tous les hôtes de cluster

Windows et autonomes actifs que SnapCenter gère et auxquels vous avez accès. Cela inclut les informations sur l'état du plug-in associées à ces hôtes.

En cliquant sur le nombre adjacent aux hôtes, vous redirige vers la section hôtes gérés de la page hôtes. De là, vous pouvez obtenir des informations détaillées pour un hôte sélectionné.

Cet affichage présente également la somme des SVM ONTAP autonomes et des SVM Cluster ONTAP que SnapCenter gère et auxquels vous avez accès. Cliquez sur le nombre à côté de SVM pour vous rediriger vers la page systèmes de stockage. De là, vous pouvez obtenir des informations détaillées pour un SVM sélectionné.

L'état de configuration de l'hôte est présenté en rouge (critique), jaune (avertissement) et vert (actif), ainsi que le nombre d'hôtes dans chaque état. Des messages d'état sont fournis pour chaque état.

<b>État de la configuration</b>	<b>Description</b>
Mise à niveau obligatoire	Le nombre d'hôtes exécutant des plug-ins non pris en charge et nécessitant une mise à niveau. Un plug-in non pris en charge n'est pas compatible avec cette version de SnapCenter.
Migration obligatoire	Le nombre d'hôtes exécutant des plug-ins non pris en charge et qui doivent être migrations ? Un plug-in non pris en charge n'est pas compatible avec cette version de SnapCenter.
Aucun plug-in installé	Le nombre d'hôtes ajoutés correctement, mais les plug-ins doivent être installés, ou l'installation des plug-ins a échoué.
Suspendu	Nombre d'hôtes dont les horaires sont suspendus et en cours de maintenance.
Arrêté	Le nombre d'hôtes actifs, mais les services de plug-in ne sont pas en cours d'exécution.
Hôte arrêté	Nombre d'hôtes qui sont en panne ou inaccessibles.
Mise à niveau disponible (en option)	Nombre d'hôtes dans lesquels une version plus récente du plug-in est disponible pour la mise à niveau.
Migration disponible (facultatif)	Nombre d'hôtes dans lesquels une version plus récente du plug-in est disponible pour la migration.
Configurer le répertoire du journal	Nombre d'hôtes dans lesquels le répertoire du journal doit être configuré pour que SCSQL puisse effectuer une sauvegarde du journal de transactions.

État de la configuration	Description
Configurer les plug-ins VMware	Nombre d'hôtes dans lesquels le plug-in SnapCenter pour VMware vSphere doit être ajouté.
Inconnu	Nombre d'hôtes enregistrés mais l'installation n'est pas encore déclenchée.
Exécution	Le nombre d'hôtes actifs et de plug-ins s'exécute. Et dans le cas des plug-ins SCSQL, le répertoire de journaux et l'hyperviseur sont configurés.
Installation/désinstallation de modules externes	Nombre d'hôtes où l'installation ou la désinstallation du plug-in est en cours.

## Comment afficher les informations sur le tableau de bord

Dans le volet de navigation de gauche de SnapCenter, vous pouvez afficher les différentes mosaïques de tableau de bord, ainsi que les détails système associés. Le nombre d'affichages disponibles dans le tableau de bord est fixe et ne peut pas être modifié. Le contenu fourni sur chaque écran dépend du contrôle d'accès basé sur des rôles (RBAC).

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
2. Cliquez sur les zones actives de chaque écran pour obtenir des informations supplémentaires.

Par exemple, si vous cliquez sur un graphique donut dans **Jobs**, vous redirige vers la page Monitor pour plus d'informations sur votre sélection. En cliquant sur un graphique de donuts dans **Résumé de la protection**, vous redirige vers la page Rapports, qui peut fournir plus d'informations sur votre sélection.

## Rapports d'état des requêtes des travaux à partir du tableau de bord

Vous pouvez demander des rapports sur les tâches de sauvegarde, de restauration et de clonage à partir de la page Tableau de bord. Cette fonction est utile si vous souhaitez identifier le nombre total de tâches réussies ou ayant échoué dans votre environnement SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**
2. Localisez la mosaïque travaux dans le tableau de bord, puis sélectionnez **Backup**, **Restore** ou **Clone**.
3. Dans le menu déroulant, sélectionnez la période pour laquelle vous souhaitez obtenir des informations sur les tâches : 24 heures, 7 jours ou 30 jours.

Les systèmes affichent un graphique donut couvrant les données.

4. Cliquez sur la tranche donut représentant les informations de travail pour lesquelles vous souhaitez obtenir un rapport.

Lorsque vous cliquez sur le graphique donut, vous êtes redirigé de la page Tableau de bord vers la page moniteur. La page moniteur affiche les travaux dont l'état est sélectionné dans le graphique donut.

5. Dans la liste de la page moniteur, cliquez sur un travail spécifique pour le sélectionner.
6. En haut de la page moniteur, cliquez sur **Rapports**.

## Résultat

Le rapport affiche des informations uniquement pour le travail que vous avez sélectionné. Vous pouvez consulter le rapport ou le télécharger sur votre système local.

## Demander des rapports d'état de protection à partir du tableau de bord

Vous pouvez demander des informations sur la protection des ressources gérées par des plug-ins spécifiques à l'aide du tableau de bord. Seules les sauvegardes de données sont considérées pour la synthèse de la protection des données.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
2. Recherchez la dernière vignette protection Summary dans le tableau de bord et utilisez le menu déroulant pour sélectionner un plug-in.

Le tableau de bord affiche un tableau des beignets pour les ressources sauvegardées dans le stockage primaire et, le cas échéant, le plug-in, un tableau des beignets pour les ressources sauvegardées dans le stockage secondaire.



Les rapports sur la protection des données sont disponibles uniquement pour certains types de plug-ins. La spécification de **tous les plug-ins** n'est pas prise en charge.

3. Cliquez sur la coupe donut représentant l'état pour lequel vous voulez un rapport.

Lorsque vous cliquez sur le graphique donut, vous êtes redirigé de la page Tableau de bord vers les rapports, puis vers la page Plug-in. Le rapport affiche uniquement l'état du plug-in sélectionné. Vous pouvez consulter le rapport ou le télécharger sur votre système local.



La redirection vers la page Reports pour les graphiques SnapMirror et la sauvegarde SAP HANA basée sur les fichiers n'est pas prise en charge.

## Gérer le RBAC

SnapCenter permet de modifier les rôles, les utilisateurs et les groupes.

### Modifier un rôle

Vous pouvez modifier un rôle SnapCenter pour supprimer des utilisateurs ou des groupes et modifier les autorisations associées au rôle. Il est particulièrement utile de modifier des rôles lorsque vous voulez modifier

ou supprimer les autorisations utilisées par un rôle entier.

### Avant de commencer

Vous devez avoir ouvert une session en tant que rôle « SnapCenterAdmin ».



Vous ne pouvez ni modifier ni supprimer les autorisations pour le rôle SnapCenterAdmin.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **rôles**.
3. Dans le champ Nom du rôle, cliquez sur le rôle à modifier.
4. Select **tous les membres de ce rôle peuvent voir les objets d'autres membres** pour permettre aux autres membres du rôle d'afficher les ressources telles que les volumes et les hôtes après avoir actualisé la liste des ressources.

Désélectionnez cette option si vous ne souhaitez pas que les membres de ce rôle voient les objets auxquels les autres membres sont affectés.



Lorsque cette option est activée, il n'est pas nécessaire d'attribuer aux utilisateurs un accès aux objets ou aux ressources si les utilisateurs appartiennent au même rôle que l'utilisateur qui a créé les objets ou les ressources.

5. Dans la page Role Details (Détails du rôle), modifiez les autorisations ou annulez l'affectation des membres selon les besoins.
6. Cliquez sur **soumettre**.

## Modifier les utilisateurs et les groupes

Vous pouvez modifier les utilisateurs ou les groupes SnapCenter pour modifier leur rôle et leurs ressources.

### Avant de commencer

Vous devez être connecté en tant qu'administrateur SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **utilisateurs et accès**.
3. Dans la liste Nom d'utilisateur ou de groupe, cliquez sur l'utilisateur ou le groupe que vous souhaitez modifier.
4. Dans la page Détails de l'utilisateur ou du groupe, modifiez les rôles et les actifs.
5. Cliquez sur **soumettre**.

## Gérer les hôtes

Vous pouvez ajouter des hôtes et installer des packages plug-in SnapCenter, ajouter un serveur de vérification, supprimer des hôtes, migrer des tâches de sauvegarde et mettre à jour l'hôte pour mettre à niveau des modules plug-in ou ajouter de nouveaux modules

plug-in. Selon le plug-in que vous utilisez, vous pouvez également provisionner des disques, gérer des partages SMB, gérer des groupes initiateurs (igroups), gérer des sessions iSCSI et migrer des données.

<b>Vous pouvez effectuer ces tâches...</b>	<b>Pour Microsoft Exchange Server</b>	<b>Pour Microsoft SQL Server</b>	<b>Pour Microsoft Windows</b>	<b>Pour Oracle Database</b>	<b>Pour les bases de données SAP HANA</b>	<b>Pour les plug-ins NetApp pris en charge</b>	<b>Pour DB2</b>	<b>Pour PostgreSQL</b>	<b>Pour MySQL</b>
Ajoutez des hôtes et installez le package de plug-in	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.
Mettre à jour les informations ESXi pour un hôte	Non	Oui.	Non	Non	Non	Non	Non	Non	Non
Suspendre les plannings et placer les hôtes en mode de maintenance	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.
Modifiez les hôtes en ajoutant, mettant à niveau ou supprimant des plug-ins	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.
Supprimer des hôtes de SnapCenter	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.	Oui.

<b>Vous pouvez effectuer ces tâches...</b>	<b>Pour Microsoft Exchange Server</b>	<b>Pour Microsoft SQL Server</b>	<b>Pour Microsoft Windows</b>	<b>Pour Oracle Database</b>	<b>Pour les bases de données SAP HANA</b>	<b>Pour les plug-ins NetApp pris en charge</b>	<b>Pour DB2</b>	<b>Pour PostgreSQL</b>	<b>Pour MySQL</b>
Démarrer les services de plug-in (s'applique uniquement aux plug-ins s'exécutant sur un hôte Windows)	Oui.	Oui.	Oui.	Non	Oui.	Oui.	Oui.	Oui.	Oui.
Provisionner les disques	Non	Non	Oui.	Non	Non	Non	Non	Non	Non
Gérer les partages SMB	Non	Non	Oui.	Non	Non	Non	Non	Non	Non
Gestion des iGroups	Non	Non	Oui.	Non	Non	Non	Non	Non	Non
Gérez les sessions iSCSI	Non	Non	Oui.	Non	Non	Non	Non	Non	Non

## Actualiser les informations de la machine virtuelle

Vous devez actualiser les informations de votre machine virtuelle lorsque les informations d'identification de VMware vCenter changent ou que l'hôte de la base de données ou du système de fichiers redémarre. La mise à jour des informations de votre machine virtuelle dans SnapCenter établit la communication avec VMware vSphere vCenter et obtient les informations d'identification vCenter.



Les disques RDM sont gérés par le plug-in SnapCenter pour Microsoft Windows, installé sur l'hôte de base de données. Pour gérer RDM, le plug-in SnapCenter pour Microsoft Windows communique avec le serveur vCenter qui gère l'hôte de base de données.

### Étapes

1. Dans le volet de navigation de gauche de SnapCenter, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Dans la page hôtes gérés, sélectionnez l'hôte à mettre à jour.
4. Cliquez sur **Actualiser VM**.

## Modifier les hôtes du plug-in

Après l'installation d'un plug-in, vous pouvez modifier les détails sur les hôtes du plug-in, le cas échéant. Vous pouvez modifier les informations d'identification, le chemin d'installation, les plug-ins, les détails du répertoire des journaux du plug-in SnapCenter pour Microsoft SQL Server, le compte de service géré de groupe (GMSA) et le port du plug-in.



Vérifiez que la version du plug-in est identique à celle de la version du serveur SnapCenter.

### À propos de cette tâche

- Vous ne pouvez modifier un port de plug-in qu'après l'installation du plug-in.

Vous ne pouvez pas modifier le port du plug-in lorsque les opérations de mise à niveau sont en cours.

- Lors de la modification d'un port de plug-in, vous devez prendre en compte les scénarios de restauration de port suivants :
  - Dans une configuration autonome, si SnapCenter ne change pas le port d'un des composants, l'opération échoue et l'ancien port est conservé pour tous les composants.

Si le port a été modifié pour tous les composants mais que l'un des composants ne parvient pas à démarrer avec le nouveau port, alors l'ancien port est conservé pour tous les composants. Par exemple, si vous souhaitez modifier le port pour deux plug-ins sur l'hôte autonome et que SnapCenter ne parvient pas à appliquer le nouveau port à l'un des plug-ins, l'opération échoue (avec un message d'erreur approprié) et l'ancien port est conservé pour les deux plug-ins.

- Dans une configuration en cluster, si SnapCenter ne change pas le port du plug-in installé sur l'un des nœuds, l'opération échoue et l'ancien port est conservé pour tous les nœuds.

Par exemple, si le plug-in est installé sur quatre nœuds dans une configuration en cluster, et si le port n'est pas modifié pour l'un des nœuds, l'ancien port est conservé pour tous les nœuds.

Lorsque les plug-ins sont installés avec GMSA, vous pouvez modifier dans les fenêtres **plus d'options**. Lorsque les plug-ins sont installés sans GMSA, vous pouvez spécifier le compte GMSA pour l'utiliser comme compte de service de plug-in.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Vérifiez que **Managed Hosts** est sélectionné en haut.
3. Sélectionnez l'hôte pour lequel vous souhaitez modifier un champ.

Un seul champ peut être modifié à la fois.

4. Cliquez sur **soumettre**.

## Résultat

L'hôte est validé et ajouté au serveur SnapCenter.

## Démarrez ou redémarrez les services du plug-in

Le démarrage des services du plug-in SnapCenter vous permet de démarrer les services s'ils ne sont pas en cours d'exécution ou de les redémarrer s'ils sont en cours d'exécution. Il se peut que vous souhaitiez redémarrer les services une fois la maintenance effectuée.

Vous devez vous assurer qu'aucun travail n'est en cours d'exécution lors du redémarrage des services.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Dans la page hôtes gérés, sélectionnez l'hôte que vous souhaitez démarrer.
4. Cliquez sur  l'icône et cliquez sur **Démarrer le service** ou **redémarrer le service**.

Vous pouvez démarrer ou redémarrer le service de plusieurs hôtes simultanément.

## Suspendre les planifications pour la maintenance de l'hôte

Lorsque vous souhaitez empêcher l'hôte d'exécuter des tâches SnapCenter planifiées, vous pouvez placer votre hôte en mode maintenance. Avant de mettre à niveau les plug-ins ou si vous effectuez des tâches de maintenance sur les hôtes,



Vous ne pouvez pas suspendre les planifications d'un hôte qui est arrêté car SnapCenter ne peut pas communiquer avec cet hôte.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Dans la page hôtes gérés, sélectionnez l'hôte que vous souhaitez suspendre.
4. Cliquez sur l'  icône, puis cliquez sur **suspendre la planification** pour placer l'hôte de ce plug-in en mode de maintenance.

Vous pouvez interrompre la planification de plusieurs hôtes simultanément.



Vous n'avez pas besoin d'arrêter le service de plug-in en premier. Le service du plug-in peut être en cours d'exécution ou arrêté.

## Résultat

Une fois les planifications suspendues sur l'hôte, la page hôtes gérés affiche **suspendu** dans le champ d'état global de l'hôte.

Une fois la maintenance de l'hôte terminée, vous pouvez mettre l'hôte hors mode maintenance en cliquant sur

**Activer le programme.** Vous pouvez activer la planification de plusieurs hôtes simultanément.

## Opérations prises en charge à partir de la page Ressources

Pour découvrir les ressources et exécuter les opérations de protection des données, consultez la page Ressources. Les opérations que vous pouvez effectuer diffèrent en fonction du plug-in que vous utilisez pour gérer vos ressources.

À partir de la page Ressources, vous pouvez effectuer les tâches suivantes :

<b>Vous pouvez effectuer ces tâches...</b>	<b>Pour Microsoft Exchange Server</b>	<b>Pour Microsoft SQL Server</b>	<b>Pour Microsoft Windows</b>	<b>Pour Oracle Database</b>	<b>Pour les bases de données SAP HANA</b>
Déterminer si des ressources sont disponibles pour les sauvegardes	Oui.	Oui.	Oui.	Oui.	Oui.
Sauvegarde à la demande d'une ressource	Oui.	Oui.	Oui.	Oui.	Oui.
Effectuez des restaurations à partir des sauvegardes	Oui.	Oui.	Oui.	Oui.	Oui.
Sauvegardes clones	Non	Oui.	Oui.	Oui.	Oui.
Gérer les sauvegardes	Oui.	Oui.	Oui.	Oui.	Oui.
Gérer les clones	Non	Oui.	Oui.	Oui.	Oui.
Gestion des règles	Oui.	Oui.	Oui.	Oui.	Oui.
Gérer les connexions de stockage	Oui.	Oui.	Oui.	Oui.	Oui.
Montez les sauvegardes	Non	Non	Non	Oui.	Non
Démonter les sauvegardes	Non	Non	Non	Oui.	Non

<b>Vous pouvez effectuer ces tâches...</b>	<b>Pour Microsoft Exchange Server</b>	<b>Pour Microsoft SQL Server</b>	<b>Pour Microsoft Windows</b>	<b>Pour Oracle Database</b>	<b>Pour les bases de données SAP HANA</b>
Afficher les détails	Oui.	Oui.	Oui.	Oui.	Oui.

## Gestion des règles

Vous pouvez détacher des stratégies d'une ressource ou d'un groupe de ressources, modifier, supprimer, afficher et copier.

### Modifier des règles

Vous pouvez modifier les options de réplication, les paramètres de rétention des snapshots, le nombre de tentatives d'erreur ou les informations relatives aux scripts lorsqu'une règle est attachée à un groupe de ressources ou de ressources. Vous ne pouvez modifier le type de planification (fréquence) qu'après avoir désolidariser une stratégie.

#### À propos de cette tâche

La modification du type de planification dans une stratégie nécessite des étapes supplémentaires car le serveur SnapCenter enregistre le type de planification uniquement au moment où la stratégie est associée à une ressource ou à un groupe de ressources.

<b>Les fonctions que vous recherchez...</b>	<b>Alors...</b>
Ajouter un type d'horaire supplémentaire	<p>Créez une nouvelle stratégie et joignez-la aux ressources ou aux groupes de ressources nécessaires.</p> <p>Par exemple, si une stratégie de groupe de ressources spécifie uniquement les sauvegardes horaires et que vous souhaitez ajouter également des sauvegardes quotidiennes, vous pouvez créer une stratégie avec un type de planification quotidien et l'ajouter au groupe de ressources. Le groupe de ressources aurait alors deux politiques : horaire et quotidien.</p>

Les fonctions que vous recherchez...	Alors...
Supprimer ou modifier un type d'horaire	<p>Effectuez les opérations suivantes :</p> <ol style="list-style-type: none"> <li>1. Détachez la stratégie de chaque groupe de ressources et de ressources qui utilise cette stratégie.</li> <li>2. Modifier le type de planification.</li> <li>3. Joignez à nouveau la stratégie à toutes les ressources et à tous les groupes de ressources.</li> </ol> <p>Par exemple, si une stratégie spécifie des sauvegardes horaires et que vous souhaitez les modifier en sauvegardes quotidiennes, vous devez d'abord détacher la stratégie.</p>

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Sélectionnez la stratégie, puis cliquez sur **Modifier**.
4. Modifiez les informations, puis cliquez sur **Terminer**.

### Détacher les polices

Vous pouvez détacher des stratégies d'une ressource ou d'un groupe de ressources à chaque fois que vous ne souhaitez plus que ces stratégies régissent la protection des données pour les ressources. Vous devez détacher une stratégie avant de pouvoir la supprimer ou avant de modifier le type de planification.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Sélectionnez le groupe de ressources, puis cliquez sur **Modifier le groupe de ressources**.
4. Dans la page stratégies de l'assistant Modifier le groupe de ressources, décochez la case en regard des stratégies que vous souhaitez détacher.
5. Apportez toute modification supplémentaire au groupe de ressources dans le reste de l'assistant, puis cliquez sur **Terminer**.

### Supprimer des règles

Si vous n'avez plus besoin de règles, vous pouvez les supprimer.

### Avant de commencer

Vous devez détacher la stratégie des groupes de ressources ou de ressources si la stratégie est associée à des groupes de ressources ou de ressources.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **stratégies**.
3. Sélectionnez la stratégie, puis cliquez sur **Supprimer**.
4. Cliquez sur **Oui**.

## Gérer les groupes de ressources

Vous pouvez effectuer diverses opérations sur des groupes de ressources.

Vous pouvez effectuer les tâches suivantes associées aux groupes de ressources :

- Modifiez un groupe de ressources en sélectionnant le groupe de ressources et en cliquant sur **Modifier le groupe de ressources** pour modifier les informations fournies lors de la création du groupe de ressources.



Vous pouvez modifier le planning lors de la modification du groupe de ressources. Toutefois, pour modifier le type de planification, vous devez modifier la stratégie.



Si vous supprimez des ressources d'un groupe de ressources, les paramètres de conservation de sauvegarde définis dans les stratégies actuellement associées au groupe de ressources continueront d'être appliqués aux ressources supprimées.

- Créez une sauvegarde d'un groupe de ressources.
- Créer un clone d'une sauvegarde.

Vous pouvez cloner à partir des sauvegardes existantes de SQL, Oracle, des systèmes de fichiers Windows, des applications personnalisées et des ressources de base de données SAP HANA ou des groupes de ressources.

- Créer un clone d'un groupe de ressources.

Cette opération n'est prise en charge que pour les groupes de ressources SQL (qui ne contiennent que des bases de données). Vous pouvez configurer une planification de clonage d'un groupe de ressources (cycle de vie du clone).

- Empêcher le démarrage des opérations planifiées sur les groupes de ressources.
- Supprimer un groupe de ressources.

## Arrêter et reprendre les opérations sur les groupes de ressources

Vous pouvez désactiver temporairement les opérations planifiées de démarrer sur un groupe de ressources. Vous pouvez activer ces opérations plus tard que vous le souhaitez.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Sélectionnez le groupe de ressources et cliquez sur **Maintenance**.

4. Cliquez sur **OK**.

Si vous souhaitez reprendre les opérations sur le groupe de ressources que vous avez mis en mode maintenance, sélectionnez le groupe de ressources et cliquez sur **production**.

## Supprimer des groupes de ressources

Vous pouvez supprimer un groupe de ressources si vous n'avez plus besoin de protéger les ressources du groupe de ressources. Vous devez vous assurer que les groupes de ressources sont supprimés avant de supprimer des plug-ins de SnapCenter.

### À propos de cette tâche

Vous devez supprimer manuellement tous les clones créés pour l'une des ressources du groupe de ressources. Vous pouvez également forcer la suppression de toutes les sauvegardes, métadonnées, règles et snapshots associés au groupe de ressources.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez **Groupe de ressources** dans la liste **Affichage**.
3. Sélectionnez le groupe de ressources, puis cliquez sur **Supprimer**.
4. Facultatif : cochez la case **Supprimer les sauvegardes et détacher les stratégies associées à ce groupe de ressources** pour supprimer toutes les sauvegardes, métadonnées, stratégies et instantanés associés au groupe de ressources.
5. Cliquez sur **OK**.

## Gérer les sauvegardes

Vous pouvez renommer et supprimer des sauvegardes. Vous pouvez également supprimer plusieurs sauvegardes simultanément.

### Renommer les sauvegardes

Vous pouvez renommer les sauvegardes si vous voulez fournir un meilleur nom pour améliorer la capacité de recherche.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource ou le groupe de ressources dans la liste.

La page topologie des ressources ou des groupes de ressources s'affiche. Si la ressource ou le groupe de ressources n'est pas configuré pour la protection des données, l'assistant de protection s'affiche à la place de la page de topologie.

4. Dans la vue gérer les copies, sélectionnez **sauvegardes** dans les systèmes de stockage principaux.

Vous ne pouvez pas renommer les sauvegardes qui se trouvent sur le système de stockage secondaire.

Si vous avez catalogué les sauvegardes des bases de données Oracle à l'aide d'Oracle Recovery Manager (RMAN), vous ne pouvez pas renommer ces sauvegardes cataloguées.

5. Sélectionnez la sauvegarde, puis cliquez sur .

6. Dans le champ **Renommer la sauvegarde sous**, saisissez un nouveau nom et cliquez sur **OK**.

## Supprimer les sauvegardes

Vous pouvez supprimer des sauvegardes si vous n'avez plus besoin de sauvegarder pour d'autres opérations de protection des données.

### Avant de commencer

Vous devez avoir supprimé les clones associés avant de supprimer une sauvegarde.



Si une sauvegarde est associée à une ressource clonée, vous ne pouvez pas la supprimer.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource ou le groupe de ressources dans la liste.

La page topologie des ressources ou des groupes de ressources s'affiche.

4. Dans la vue gérer les copies, sélectionnez **sauvegardes** dans les systèmes de stockage principaux.

Vous ne pouvez pas supprimer les sauvegardes qui se trouvent sur le système de stockage secondaire.

5. Sélectionnez la sauvegarde, puis cliquez sur .

Si vous supprimez une sauvegarde de base de données SAP HANA, les catalogues SAP HANA associés de la sauvegarde sont également supprimés.



Si la dernière sauvegarde restante est supprimée, les entrées du catalogue HANA associées ne peuvent pas être supprimées.

6. Cliquez sur **OK**.



Si certaines sauvegardes de base de données obsolètes se trouvent dans SnapCenter qui ne disposent pas des sauvegardes correspondantes sur le système de stockage, vous devez utiliser la commande `remove-smbbackup` pour nettoyer ces entrées de sauvegarde obsolètes. Si les sauvegardes obsolètes ont été cataloguées, elles seront décataloguées à partir de la base de données du catalogue de reprise.

## Déposer la protection

Supprimer la protection supprime toutes les sauvegardes et détache toutes les règles. Avant de supprimer la protection, assurez-vous que les sauvegardes ne sont pas montées et qu'aucun clone n'est associé à la sauvegarde.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource ou le groupe de ressources dans la liste.  
  
La page topologie des ressources ou des groupes de ressources s'affiche.
4. Sélectionnez la sauvegarde et cliquez sur **Supprimer la protection**.

## Supprimer les clones

Vous pouvez supprimer les clones si vous les trouvez devenus superflus.

### À propos de cette tâche

Vous ne pouvez pas supprimer des clones qui agissent comme la source pour d'autres clones.

Par exemple, si la base de données de production est db1, la base de données clone1 est clonée à partir de la sauvegarde de db1, puis clone1 est protégée. La base de données clone2 est clonée à partir de la sauvegarde de clone1. Si vous décidez de supprimer clone1, vous devez d'abord supprimer clone2, puis supprimer clone1.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Dans la page Ressources, sélectionnez la ressource ou le groupe de ressources dans la liste déroulante **Affichage**.
3. Sélectionnez la ressource ou le groupe de ressources dans la liste.  
  
La page topologie de ressource ou de groupe de ressources s'affiche.
4. Dans la vue gérer les copies, sélectionnez **clones** dans les systèmes de stockage primaire ou secondaire (mis en miroir ou répliqué).
5. Sélectionnez le clone, puis cliquez sur .  
  
Si vous supprimez des clones de base de données SAP HANA, effectuez les opérations suivantes dans la page Delete Clone :
  - a. Dans le champ **Pre clone delete**, entrez les commandes à exécuter avant de supprimer le clone.
  - b. Dans le champ **Unmount**, entrez la commande pour démonter le clone avant de supprimer le clone.
6. Cliquez sur **OK**.

## Après la fin

Parfois, les systèmes de fichiers ne sont pas supprimés. Vous devez augmenter la valeur du paramètre `CLONE_DELETE_DELAY` en exécutant la commande suivante : `./sccli Set-SmConfigSettings`



Le paramètre `CLONE_DELETE_DELAY` indique le nombre de secondes d'attente après la suppression du clone d'application et avant de lancer la suppression du système de fichiers.

Après avoir modifié la valeur du paramètre, redémarrer le service SnapCenter Plug-in Loader (SPL).

## Surveillez les tâches, les plannings, les événements et les journaux

Vous pouvez surveiller la progression de vos travaux, obtenir des informations sur les tâches planifiées et vérifier les événements et les journaux à partir de la page Monitor.

### Surveiller les tâches

Vous pouvez afficher des informations sur les tâches de sauvegarde, de clonage, de restauration et de vérification SnapCenter. Vous pouvez filtrer cette vue en fonction de la date de début et de fin, du type de tâche, du groupe de ressources, de la stratégie ou du plug-in SnapCenter. Vous pouvez également obtenir des détails supplémentaires et des fichiers journaux pour les travaux spécifiés.

Vous pouvez également surveiller les tâches liées aux opérations SnapMirror et SnapVault.



Vous ne pouvez contrôler que les travaux que vous avez créés et qui sont pertinents pour vous, sauf si vous avez reçu un rôle d'administrateur SnapCenter ou un autre super utilisateur.

Vous pouvez effectuer les tâches suivantes associées aux tâches de surveillance :

- Surveillance des opérations de sauvegarde, de clonage, de restauration et de vérification
- Afficher les détails du travail et les rapports.
- Arrêter une tâche planifiée.

### Gérer les tâches de sauvegarde planifiées

À partir de la version SnapCenter 6.0.1, un nouveau paramètre **JobConcurrencyThreshold** a été introduit, qui définit un seuil pour le nombre de travaux programmés pouvant s'exécuter à tout moment. Cela vous permet de contrôler le nombre de sauvegardes que vous souhaitez exécuter en fonction de la configuration matérielle de votre système.

La valeur par défaut attribuée à **JobConcurrencyThreshold** est 0 et est désactivée. Vous pouvez activer en attribuant une valeur si vous observez une dégradation des performances pendant la fenêtre de sauvegarde planifiée.



Si vous activez **JobConcurrencyThreshold** pour gérer des tâches simultanées, SnapCenter ne vous permet pas de contrôler l'ordre des sauvegardes et les sauvegardes peuvent ne pas être déclenchées au même moment que celui spécifié dans le planning.

## Étapes

1. Définissez la valeur du paramètre *JobConcurrencyThreshold* situé dans *C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config*.
2. Recyclez le pool d'applications SnapCenter en cliquant sur IIS > pools d'applications > SnapCenter > redémarrer.
3. Redémarrez le service Web SnapCenter en cliquant sur IIS > sites > SnapCenter > redémarrer.

## Gérer les tâches obsolètes

Les travaux obsolètes sont créés à la suite d'interruptions dans SnapCenter ou de mises à jour incorrectes des travaux. À partir de la version SnapCenter 6.0.1, un planning prédéfini est introduit pour nettoyer ces tâches obsolètes bloquées pendant plus de 72 heures. Vous pouvez modifier la fréquence de programmation en modifiant le paramètre configurable **CleanUpStaleJobsIntervalHours**.

Vous pouvez déclencher le nettoyage à la demande en exécutant le programme à partir de **moniteur > programmes > SnapCenter\_StaleJobCleanUp**.

### Étapes

1. Définissez la valeur du paramètre *CleanUpStaleJobsIntervalHours* situé dans *C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config*.
2. Recyclez le pool d'applications SnapCenter en cliquant sur IIS > pools d'applications > SnapCenter > redémarrer.
3. Redémarrez le service Web SnapCenter en cliquant sur IIS > sites > SnapCenter > redémarrer.

## Surveiller les plannings

Vous pouvez afficher les horaires actuels pour déterminer le moment où l'opération démarre, le moment où elle a été exécutée pour la dernière fois et le moment où elle s'exécute ensuite. Vous pouvez également déterminer l'hôte sur lequel l'opération s'exécute, ainsi que le groupe de ressources et les informations de stratégie de l'opération.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **plannings**.
3. Sélectionnez le groupe de ressources et le type de planification.
4. Afficher la liste des opérations planifiées.

## Contrôle des événements

Vous pouvez afficher la liste des événements SnapCenter dans le système, par exemple lorsqu'un utilisateur crée un groupe de ressources ou lorsqu'il lance des activités, comme par exemple lors de la création d'une sauvegarde planifiée. Vous pouvez afficher les événements pour déterminer si une opération telle qu'une sauvegarde ou une restauration est en cours.

### À propos de cette tâche

Toutes les informations sur le travail s'affichent sur la page événements. Par exemple, lorsqu'une tâche de sauvegarde démarre, un événement « démarrage de sauvegarde » s'affiche. À la fin de la sauvegarde, un événement « sauvegarde terminée » s'affiche.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page moniteur, cliquez sur **Événements**.
3. (Facultatif) dans la zone filtre, entrez la date de début ou de fin, la catégorie d'événement (comme la sauvegarde, le groupe de ressources ou la stratégie) et le niveau de gravité, puis cliquez sur **appliquer**. Vous pouvez également saisir des caractères dans la zone de recherche.
4. Afficher la liste des événements.

## Surveiller les journaux

Vous pouvez afficher et télécharger les journaux du serveur SnapCenter, les journaux des agents de l'hôte SnapCenter et les journaux des plug-ins. Vous pouvez afficher les journaux pour faciliter le dépannage.

### À propos de cette tâche

Vous pouvez filtrer les journaux pour afficher uniquement un niveau de sévérité spécifique du journal :

- Débogage
- Info
- Avertissement
- Erreur
- Mortel

Vous pouvez également obtenir des journaux au niveau des tâches, par exemple des journaux qui vous aident à résoudre le problème d'échec d'une tâche de sauvegarde. Pour les journaux au niveau des travaux, utilisez l'option **moniteur > travaux**.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
2. Dans la page travaux, sélectionnez un travail et cliquez sur Télécharger les journaux.

Le dossier compressé téléchargé contient les journaux des travaux et les journaux courants. Le nom du dossier compressé contient l'ID du travail et le type de travail sélectionnés.

3. Dans la page moniteur, cliquez sur **Logs**.
4. Sélectionnez le type de journal, l'hôte et l'instance.

Si vous sélectionnez le type de journal comme **plugin**, vous pouvez sélectionner un hôte ou un plug-in SnapCenter. Vous ne pouvez pas le faire si le type de journal est **Server**.

5. Pour filtrer les journaux par source, message ou niveau de journal spécifique, cliquez sur l'icône de filtre située en haut de l'en-tête de colonne.

Pour afficher tous les journaux, choisissez **supérieur ou égal à** comme Debug niveau.

6. Cliquez sur **Actualiser**.
7. Afficher la liste des journaux
8. Cliquez sur **Télécharger** pour télécharger les journaux.

Le dossier compressé téléchargé contient les journaux des travaux et les journaux courants. Le nom du

dossier compressé contient l'ID du travail et le type de travail sélectionnés.

Dans les grandes configurations pour des performances optimales, vous devez définir au niveau minimal les paramètres de journalisation de SnapCenter en utilisant la cmdlet PowerShell.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```



Pour accéder aux informations d'intégrité ou de configuration après la fin d'un travail de basculement, exécutez l'applet de commande `Get-SmRepositoryConfig`.

## Supprimer les travaux et les journaux de SnapCenter

Vous pouvez supprimer des tâches de sauvegarde, de restauration, de clonage et de vérification ainsi que des journaux de SnapCenter. SnapCenter stocke les journaux des tâches qui ont réussi et échoué indéfiniment, sauf si vous les supprimez. Il se peut que vous souhaitiez les supprimer pour réapprovisionner le stockage.

### À propos de cette tâche

Aucun travail ne doit être en cours d'exécution. Vous pouvez supprimer un travail spécifique en fournissant un ID de travail ou en supprimant des travaux au cours d'une période donnée.

Il n'est pas nécessaire de placer l'hôte en mode de maintenance pour supprimer des travaux.

### Étapes

1. Lancer PowerShell.
2. Dans l'invite de commande, entrez : `Open-SMConnection`
3. Dans l'invite de commande, entrez : `Remove-SmJobs`
4. Dans le volet de navigation de gauche, cliquez sur **moniteur**.
5. Dans la page moniteur, cliquez sur **travaux**.
6. Dans la page travaux, vérifiez l'état du travail.

### Informations associées

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Présentation des fonctionnalités de reporting SnapCenter

SnapCenter propose toute une gamme d'options de création de rapports qui vous permettent de surveiller et de gérer l'état de santé de votre système et sa réussite.

Type de rapport	Description
Rapport de sauvegarde	Le rapport de sauvegarde fournit des données globales concernant les tendances en matière de sauvegarde de votre environnement SnapCenter, le taux de réussite des sauvegardes, ainsi que des informations sur chaque sauvegarde effectuée au cours de la période spécifiée. Si une sauvegarde est supprimée, le rapport n'affiche aucune information d'état pour la sauvegarde supprimée. Le rapport de sauvegarde détaillé fournit des informations détaillées sur une tâche de sauvegarde spécifiée et répertorie les ressources sauvegardées avec succès et les ressources qui ont échoué.
Rapport sur les clones	Le rapport de clonage fournit des données globales relatives aux tendances de clonage de votre environnement SnapCenter, au taux de réussite des clones et à certaines informations sur chaque tâche de clonage effectuée pendant la période spécifiée. Si un clone est supprimé, le rapport n'affiche aucune information d'état pour le clone supprimé. Le rapport de clonage détaillé fournit des informations détaillées sur l'état du clone, de l'hôte de clonage et de la tâche de clonage spécifié. En cas d'échec d'une tâche, le rapport de clonage détaillé affiche des informations sur l'échec.
Restaurer le rapport	Le rapport de restauration fournit des informations générales sur les tâches de restauration. Le rapport de restauration détaillé fournit des détails sur une tâche de restauration spécifiée, notamment le nom d'hôte, le nom de sauvegarde, le début et la durée de la tâche, ainsi que l'état de chaque tâche. En cas d'échec d'une tâche, le rapport Restore Detail Report affiche des informations sur l'échec.
Rapport sur la protection	Ces rapports fournissent des informations détaillées sur la protection des ressources gérées par toutes les instances de plug-in SnapCenter. Ce rapport fournit des informations sur la protection des ressources gérées par toutes les instances de plug-in. Vous pouvez voir une présentation, des détails des ressources non protégées, des ressources qui n'ont pas été sauvegardées lorsque le rapport a été généré, des ressources d'un groupe de ressources pour lequel les opérations de sauvegarde ont échoué et l'état SnapVault.

Type de rapport	Description
Rapport planifié	<p>Ces rapports sont planifiés pour être exécutés régulièrement comme par jour, par semaine ou par mois. Les rapports sont générés automatiquement à la date et à l'heure spécifiées et le rapport est envoyé aux personnes concernées par courrier électronique. Vous pouvez activer, désactiver, modifier ou supprimer les planifications. Le programme activé peut être exécuté à la demande en cliquant sur le bouton <b>Exécuter maintenant</b>. L'administrateur peut exécuter n'importe quel programme, mais le rapport généré contiendra des données en fonction de l'autorisation fournie par l'utilisateur qui a créé le planning.</p> <p>Tout autre utilisateur autre que l'administrateur pourra voir ou modifier le planning en fonction de son autorisation. Si tous les membres de ce rôle peuvent voir l'option objets d'autres membres est sélectionnée sur la page Ajouter un rôle, les autres membres du rôle pourront voir et modifier.</p>

## Accédez aux rapports

Le tableau de bord de SnapCenter vous permet d'obtenir une brève présentation de l'état de santé de votre système. Le tableau de bord vous permet d'accéder à davantage d'informations. Vous pouvez également accéder directement aux rapports détaillés.

Vous pouvez accéder aux rapports par l'une des méthodes suivantes :

- Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**, puis cliquez sur **dernier diagramme à secteurs de protection** pour afficher plus de détails dans la page Rapports.
- Dans le volet de navigation de gauche, cliquez sur **Rapports**.

## Filtrez votre rapport

Vous pouvez filtrer les données de votre rapport en fonction d'une plage de paramètres, en fonction du niveau de détail et de la durée des informations dont vous avez besoin.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Rapports**.
2. Si la vue des paramètres ne s'affiche pas, cliquez sur l'icône **Activer/Désactiver la zone des paramètres** dans la barre d'outils du rapport.
3. Spécifiez la plage horaire pour laquelle vous souhaitez exécuter votre rapport. + si vous omettez la date de fin, vous récupérez toutes les informations disponibles.
4. Filtrez les informations de votre rapport en fonction de l'un des critères suivants :
  - Groupe de ressources
  - Hôte

- Politique
- Ressource
- État
- Nom du plug-in

5. Cliquez sur **appliquer**.

## Exporter ou imprimer des rapports

L'exportation de rapports SnapCenter vous permet d'afficher le rapport dans divers formats de rechange. Vous pouvez également imprimer des rapports.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Rapports**.
2. Dans la barre d'outils des rapports, effectuez l'une des opérations suivantes :
  - Cliquez sur l'icône **Activer/Désactiver l'aperçu avant impression** pour prévisualiser un rapport imprimable.
  - Sélectionnez un format dans la liste déroulante icône **Exporter** pour exporter un rapport vers un autre format.
3. Pour imprimer un rapport, cliquez sur l'icône **Imprimer**.
4. Pour afficher un résumé de rapport spécifique, faites défiler jusqu'à la section appropriée du rapport.

## Configurez le serveur SMTP pour les notifications par e-mail

Vous pouvez spécifier le serveur SMTP à utiliser pour envoyer des rapports de tâches de protection des données à vous-même ou à d'autres personnes. Vous pouvez également envoyer un e-mail de test pour vérifier la configuration. Les paramètres sont appliqués globalement à toute tâche SnapCenter pour laquelle vous configurez la notification par e-mail.

Cette option permet de configurer le serveur SMTP pour l'envoi de tous les rapports de tâches de protection des données. Toutefois, si vous souhaitez que des mises à jour régulières des tâches de protection des données SnapCenter pour une ressource particulière vous soient envoyées ou à d'autres personnes afin de surveiller l'état de ces mises à jour, vous pouvez configurer l'option pour envoyer les rapports SnapCenter par e-mail lors de la création d'un groupe de ressources.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Paramètres globaux**.
3. Entrez le serveur SMTP et cliquez sur **Enregistrer**.
4. Pour envoyer un e-mail de test, saisissez l'adresse e-mail de et à laquelle vous allez envoyer l'e-mail, saisissez l'objet, puis cliquez sur **Envoyer**.

## Configurez l'option pour envoyer des rapports par e-mail

Si vous souhaitez que des mises à jour régulières des tâches de protection des données SnapCenter vous soient envoyées ou à d'autres personnes afin de surveiller l'état de ces mises à jour, vous pouvez configurer l'option pour envoyer les rapports SnapCenter par e-mail lorsque vous créez un groupe de ressources.

## Avant de commencer

Vous devez avoir configuré votre serveur SMTP dans la page Paramètres globaux sous Paramètres.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Ressources**, puis sélectionnez le plug-in approprié dans la liste.
2. Sélectionnez le type de ressource à afficher et cliquez sur **Nouveau groupe de ressources**, ou sélectionnez un groupe de ressources existant et cliquez sur **Modifier** pour configurer les rapports électroniques pour un groupe de ressources existant.
3. Dans le panneau notification de l'assistant Nouveau groupe de ressources, sélectionnez dans le menu déroulant si vous souhaitez recevoir des rapports toujours, en cas d'échec, en cas d'échec ou d'avertissement.
4. Saisissez l'adresse de l'e-mail d'envoi, l'adresse à laquelle l'e-mail est envoyé et l'objet de l'e-mail.

## Gérer le référentiel du serveur SnapCenter

Les informations relatives aux différentes opérations effectuées à partir de SnapCenter sont stockées dans le référentiel de base de données du serveur SnapCenter. Vous devez créer des sauvegardes du référentiel pour protéger le serveur SnapCenter contre la perte de données.

Le référentiel SnapCenter Server est parfois appelé base de données NSM.

## Conditions préalables à la protection du référentiel SnapCenter

Votre environnement doit respecter certaines conditions préalables pour la protection du référentiel SnapCenter.

- Gestion des connexions des serveurs virtuels de stockage

Vous devez configurer les informations d'identification du stockage.

- Provisionner les hôtes

Au moins un disque de stockage NetApp doit être présent sur l'hôte du référentiel SnapCenter. Si aucun disque NetApp n'est présent sur l'hôte de référentiel SnapCenter, vous devez en créer un.

Pour plus d'informations sur l'ajout d'hôtes, la configuration des connexions SVM et le provisionnement des hôtes, consultez les instructions d'installation.

- Provisionnement d'une LUN iSCSI ou d'un VMDK

Pour une configuration haute disponibilité, vous pouvez provisionner un LUN iSCSI ou un VMDK sur l'un des serveurs SnapCenter.

## Sauvegarder le référentiel SnapCenter

La sauvegarde du référentiel SnapCenter Server permet de le protéger contre la perte de données. Vous pouvez sauvegarder le référentiel en exécutant l'applet de commande *Protect-SmRepository*.

## À propos de cette tâche

La cmdlet *Protect-SmRepository* exécute les tâches suivantes :

- Crée un groupe de ressources et une stratégie
- Crée un programme de sauvegarde pour le référentiel SnapCenter

### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, établissez une session à l'aide de l'applet de commande *Open-SmConnection*, puis saisissez vos informations d'identification.
3. Sauvegardez le référentiel à l'aide de l'applet de commande *Protect-SmRepository* et des paramètres requis.

## Afficher les sauvegardes du référentiel SnapCenter

Vous pouvez afficher la liste des sauvegardes du référentiel de base de données du serveur SnapCenter en exécutant l'applet de commande *get-SmRepositoryBackups*.

Les sauvegardes du référentiel sont créées en fonction du programme spécifié dans l'applet de commande *Protect-SmRepository*.

### Étapes

1. Lancer PowerShell.
2. À partir de l'invite de commande, entrez l'applet de commande suivante, puis fournissez les informations d'identification pour vous connecter au serveur SnapCenter : *Open-SMConnection*
3. Répertoriez toutes les sauvegardes de base de données SnapCenter disponibles à l'aide de l'applet de commande *get-SmRepositoryBackups*.

## Restaurez le référentiel de base de données SnapCenter

Vous pouvez restaurer le référentiel SnapCenter en exécutant l'applet de commande *Restore-SmRepositoryBackup*.

Lorsque vous restaurez le référentiel SnapCenter, les autres opérations SnapCenter en cours d'exécution seront affectées car, pendant l'opération de restauration, la base de données du référentiel n'est pas accessible.

### Étapes

1. Lancer PowerShell.
2. À partir de l'invite de commande, entrez l'applet de commande suivante, puis fournissez les informations d'identification pour vous connecter au serveur SnapCenter : *Open-SMConnection*
3. Restaurez la sauvegarde du référentiel à l'aide de l'applet de commande *Restore-SmRepositoryBackup*.

L'applet de commande suivante restaure le référentiel de base de données SnapCenter MySQL à partir des sauvegardes existantes sur LUN iSCSI ou VMDK :

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mvax3550-s09_09-15-2016_10.32.00.4445
```

L'applet de commande ci-dessous restaure la base de données SnapCenter MySQL lorsque les fichiers de sauvegarde sont supprimés accidentellement dans la LUN iSCSI. Pour VMDK, restaurez manuellement la sauvegarde à partir de snapshots ONTAP.

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mvax3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```



La sauvegarde utilisée pour effectuer l'opération de restauration du référentiel ne sera pas répertoriée lorsque les sauvegardes du référentiel sont récupérées après l'opération de restauration.

## Migrer le référentiel SnapCenter

Vous pouvez migrer le référentiel de base de données du serveur SnapCenter de l'emplacement par défaut vers un autre disque. Vous pouvez migrer le référentiel lorsque vous souhaitez le transférer sur un disque avec plus d'espace.

### Étapes

1. Arrêtez le service MYSQL57 sous Windows.
2. Localisez le répertoire des données MySQL.

Vous pouvez généralement trouver le répertoire de données à l'adresse C:\ProgramData\MySQL\MySQL Server 5.7\Data.

3. Copiez le répertoire de données MySQL vers le nouvel emplacement, par exemple, E:\Data\nsm.
4. Cliquez avec le bouton droit de la souris sur le nouveau répertoire, puis sélectionnez **Propriétés > sécurité** pour ajouter le compte de serveur local Service réseau au nouveau répertoire, puis attribuez le contrôle total du compte.
5. Renommez le répertoire de base de données d'origine, par exemple nsm\_copy.
6. À partir d'une invite de commande Windows, créez un lien de répertoire symbolique à l'aide de la commande *mklink*.

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
```

7. Démarrez le service MYSQL57 sous Windows.
8. Vérifiez que la modification de l'emplacement de la base de données a réussi en se connectant à SnapCenter et en vérifiant les entrées du référentiel, ou en vous connectant à l'utilitaire MySQL et en vous connectant au nouveau référentiel.
9. Supprimez le répertoire de référentiel de base de données original, renommé (nsm\_copy).

## Réinitialisez le mot de passe du référentiel SnapCenter

Le mot de passe de la base de données du référentiel du serveur MySQL est généré automatiquement lors de l'installation du serveur SnapCenter à partir de SnapCenter 4.2. Ce mot de passe généré automatiquement n'est en aucun cas connu de l'utilisateur SnapCenter. Si vous souhaitez accéder à la base de données du référentiel, vous devez réinitialiser le mot de passe.

### Avant de commencer

Vous devez disposer des privilèges d'administrateur SnapCenter pour réinitialiser le mot de passe.

### Étapes

1. Lancer PowerShell.
2. À partir de l'invite de commande, entrez la commande suivante, puis fournissez les informations d'identification pour vous connecter au serveur SnapCenter : *Open-SMConnection*
3. Réinitialisez le mot de passe du référentiel : *set-SmRepositoryPassword*

La commande suivante réinitialise le mot de passe du référentiel :

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: *****
ConfirmPassword: *****
Successfully updated the MySQL server password.
```

### Informations associées

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Gérer les ressources des domaines non fiables

Outre la gestion des hôtes dans les domaines de confiance Active Directory (AD), SnapCenter gère aussi les hôtes dans plusieurs domaines AD non fiables. Les domaines AD non fiables doivent être enregistrés auprès du serveur SnapCenter. SnapCenter prend en charge les utilisateurs et groupes de plusieurs domaines AD non approuvés.

Vous pouvez installer le serveur SnapCenter sur un ordinateur qui se trouve dans un domaine ou un groupe de travail. Pour installer le serveur SnapCenter, vous devez spécifier les informations d'identification du domaine si la machine se trouve dans un domaine ou les informations d'identification de l'administrateur local si la machine est dans un groupe de travail.

Les groupes Active Directory (AD) appartenant à des domaines non enregistrés auprès du serveur SnapCenter ne sont pas pris en charge. Bien que vous puissiez créer des rôles SnapCenter avec ces groupes AD, la connexion au serveur SnapCenter échoue avec le message d'erreur suivant : l'utilisateur que vous essayez de vous connecter n'appartient à aucun rôle. Veuillez contacter votre administrateur système.

## Modifier les domaines non fiables

Vous pouvez modifier un domaine non approuvé lorsque vous souhaitez mettre à jour les adresses IP du contrôleur de domaine ou le nom de domaine complet (FQDN).

### À propos de cette tâche

Après avoir modifié le FQDN, les ressources associées (hôtes, utilisateurs et groupes) peuvent ne pas fonctionner comme prévu.

Pour modifier un domaine non fiable, vous pouvez utiliser l'interface utilisateur SnapCenter ou les applets de commande PowerShell.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Paramètres globaux**.
3. Dans la page Paramètres globaux, cliquez sur **Paramètres de domaine**.

4. Cliquez sur  , puis fournissez les détails suivants :

Pour ce champ...	Procédez comme ça...
FQDN du domaine	Spécifiez le FQDN, puis cliquez sur <b>résoudre</b> .
Adresses IP du contrôleur de domaine	Si le FQDN du domaine ne peut pas être résolu, spécifiez une ou plusieurs adresses IP du contrôleur de domaine.

5. Cliquez sur **OK**.

## Annuler l'inscription des domaines Active Directory non fiables

Vous pouvez annuler l'enregistrement d'un domaine Active Directory non fiable si vous ne souhaitez pas utiliser les ressources associées à ce domaine.

### Avant de commencer

Vous devez avoir supprimé les hôtes, les utilisateurs, les groupes et les informations d'identification associés au domaine non fiable.

### À propos de cette tâche

- Une fois le domaine non enregistré du serveur SnapCenter, les utilisateurs de ce domaine ne peuvent pas accéder au serveur SnapCenter.
- Si des ressources sont associées (hôtes, utilisateurs et groupes), après l'annulation de l'enregistrement du domaine, les actifs ne seront pas opérationnels.
- Pour annuler l'enregistrement d'un domaine non fiable, vous pouvez utiliser l'interface utilisateur SnapCenter ou les applets de commande PowerShell.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page Paramètres, cliquez sur **Paramètres globaux**.
3. Dans la page Paramètres globaux, cliquez sur **Paramètres de domaine**.
4. Dans la liste des domaines, sélectionnez le domaine que vous souhaitez annuler l'enregistrement.
5. Cliquez sur  , puis sur **OK**.

## Gestion du système de stockage

Après avoir ajouté le système de stockage, vous pouvez modifier la configuration et les connexions du système de stockage ou supprimer le système de stockage.

### Modifier la configuration du système de stockage

Vous pouvez utiliser SnapCenter pour modifier la configuration de votre système de stockage si vous souhaitez modifier le nom d'utilisateur, le mot de passe, la plate-forme, le port, le protocole, Délai d'expiration, adresse IP préférée ou options de messagerie.

#### À propos de cette tâche

Vous pouvez modifier les connexions de stockage d'un utilisateur individuel ou d'un groupe. Si vous appartenez à un ou plusieurs groupes disposant de l'autorisation d'utiliser le même système de stockage, le nom de la connexion de stockage s'affiche plusieurs fois dans la liste des connexions de stockage, une fois pour chaque groupe ayant l'autorisation d'accéder au système de stockage.

#### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Systems**.
2. Dans la page Storage Systems (systèmes de stockage), dans la liste déroulante **Type**, effectuez l'une des opérations suivantes :

Sélectionner...	Étapes...
SVM ONTAP	<p>Pour afficher tous les SVM (Storage Virtual machines) qui ont été ajoutés et modifier la configuration requise des SVM.</p> <ol style="list-style-type: none"> <li>a. Dans la page Storage Connections, cliquez sur le nom du SVM approprié.</li> <li>b. Effectuez l'une des opérations suivantes : <ul style="list-style-type: none"> <li>◦ Si le SVM ne fait pas partie d'un cluster, sur la page Modifier un système de stockage, modifier les configurations telles que nom d'utilisateur, mot de passe, paramètres EMS et AutoSupport, plateforme, protocole, port, timeout, Et IP préférée.</li> <li>◦ Si le SVM fait partie d'un cluster, dans la page Modifier un système de stockage, sélectionnez <b>gérer SVM indépendamment</b> et modifiez les configurations comme nom d'utilisateur, mot de passe, EMS et AutoSupport, plateforme, protocole, port, timeout, Et IP préférée.</li> </ul> </li> </ol> <p>Après avoir modifié le SVM pour être géré de façon indépendante, si vous décidez de le gérer via un cluster, supprimez le SVM et cliquez sur <b>redécouvrir</b>. Le SVM sera ajouté au cluster ONTAP.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 20px;"> <p> Lorsqu'un mot de passe du système de stockage est mis à jour dans l'interface utilisateur graphique SnapCenter, redémarrez les services SMCORE de chaque plug-in ou hôte serveur car le mot de passe mis à jour ne reflète pas SMCORE et les tâches de sauvegarde échoueront avec une erreur d'identification incorrecte.</p> </div>

Sélectionner...	Étapes...
Clusters ONTAP	<p>Pour afficher tous les clusters qui ont été ajoutés et modifier la configuration de cluster requise.</p> <ol style="list-style-type: none"> <li>Dans la page connexions de stockage, cliquez sur le nom du cluster.</li> <li>Dans la page Modifier le système de stockage, cliquez sur l'icône Modifier en regard de Nom d'utilisateur et modifiez le nom d'utilisateur et le mot de passe.</li> <li>Sélectionnez ou effacez les paramètres EMS et AutoSupport.</li> <li>Cliquez sur <b>plus d'options</b> et modifiez d'autres configurations telles que la plate-forme, le protocole, le port, le délai d'attente et l'adresse IP préférée.</li> </ol>

3. Cliquez sur **soumettre**.

## Supprimez le système de stockage

Vous pouvez utiliser SnapCenter pour supprimer tout système de stockage inutilisé.

### À propos de cette tâche

Vous pouvez supprimer des connexions de stockage pour un utilisateur individuel ou pour un groupe. Si vous appartenez à un ou plusieurs groupes avec l'autorisation d'utiliser le même système de stockage, le nom du système de stockage s'affiche plusieurs fois dans la liste des connexions de stockage, une fois pour chaque groupe avec l'autorisation du système de stockage.



Lorsque vous supprimez un système de stockage, toutes les opérations qui sont en cours d'exécution sur ce système échouent.

### Étapes

- Dans le volet de navigation de gauche, cliquez sur **Storage Systems**.
- Dans la page systèmes de stockage, dans la liste déroulante **Type**, sélectionnez **SVM ONTAP** ou **clusters ONTAP**.
- Sur la page Storage Connections, cochez la case en regard du SVM, ou du cluster que vous souhaitez supprimer.



On ne peut pas sélectionner le SVM qui fait partie d'un cluster.

- Cliquez sur **Supprimer**.
- Dans la page Supprimer les paramètres de connexion du système de stockage, cliquez sur **OK**.



Si un SVM est supprimé du cluster ONTAP à l'aide de l'interface graphique de ONTAP, dans l'interface graphique de SnapCenter, cliquez sur **redécouvrez** pour mettre à jour la liste des SVM.

## Prise en charge de REST API

Par défaut, toutes les connexions des systèmes ASA, AFF ou FAS à ONTAP passent par ZAPI. L'API REST peut être activée pour des versions spécifiques d'ONTAP.

SnapCenter exploite les API REST pour effectuer toutes les opérations sur les systèmes ASA r2, qui ne prennent pas en charge les ZAPI.

Vous pouvez modifier les clés de configuration dans les fichiers de configuration suivants :

- IsRestEnabledForStorageConnection

La valeur par défaut est FALSE.

- MinOntapVersionToUseRest

La valeur par défaut est 9.13.1.

### Activez la connexion via l'API REST

1. Définissez IsRestEnabledForStorageConnection sur true.
2. Ajoutez la clé dans SMCoreServiceHost.dll.config et SnapDriveService.dll.config sur le serveur et les hôtes de plug-in Windows.

```
<add key="IsRestEnabledForStorageConnection" value="true" />
```

### Limiter la connexion via l'API REST à une version spécifique de ONTAP

1. Définissez le paramètre de configuration MinontapVersionToUseREST sur true.
2. Ajoutez la clé dans SMCoreServiceHost.dll.config et SnapDriveService.dll.config sur le serveur et les hôtes de plug-in Windows.

```
<add key="MinOntapVersionToUseREST" value="9.13.1" />
```

3. Redémarrez le service pour SmCore sur le serveur et le plug-in et le service SnapDrive sur la machine du plug-in.

## Gérer la collecte de données EMS

Vous pouvez planifier et gérer la collecte de données EMS (Event Management System) à l'aide des applets de commande PowerShell. La collecte des données EMS implique la collecte de détails sur le serveur SnapCenter, les modules du plug-in SnapCenter installés, les hôtes et des informations similaires, puis leur envoi à un SVM (Storage Virtual machine) ONTAP spécifié.



L'utilisation de l'UC du système est élevée lorsque la tâche de collecte des données est en cours. Le taux d'utilisation du processeur reste élevé tant que l'opération est en cours, quelle que soit la taille des données.

## Arrêter la collecte de données EMS

La collecte de données EMS est activée par défaut et s'exécute tous les sept jours après la date d'installation. Vous pouvez désactiver la collecte de données à tout moment à l'aide de la cmdlet PowerShell *Disable-SmDataCollectionEMS*.

### Étapes

1. À partir d'une ligne de commande PowerShell, établissez une session avec SnapCenter en entrant *Open-SmConnection*.
2. Désactivez la collecte de données EMS en entrant *Disable-SmDataCollectionEms*.

## Démarrer la collecte de données EMS

La collecte de données EMS est activée par défaut et est planifiée pour s'exécuter tous les sept jours à compter de la date d'installation. Si vous l'avez désactivé, vous pouvez relancer la collecte de données EMS en utilisant la commande *Enable-SmDataCollectionEMS* cmdlet.

L'autorisation event NetApp ONTAP generate-AutoSupport-log a été accordée à l'utilisateur SVM (Storage Virtual machine).

### Étapes

1. À partir d'une ligne de commande PowerShell, établissez une session avec SnapCenter en entrant *Open-SmConnection*.
2. Activez la collecte de données EMS en entrant *Enable-SmDataCollectionEMS*.

## Modifier la planification de la collecte de données EMS et le SVM cible

Vous pouvez utiliser les applets de commande PowerShell pour modifier la planification de la collecte de données EMS ou la machine virtuelle de stockage cible (SVM).

### Étapes

1. À partir d'une ligne de commande PowerShell, pour établir une session avec SnapCenter, entrez l'applet de commande *Open-SmConnection*.
2. Pour modifier la cible de collecte de données EMS, entrez la commande *set-SmDataCollectionEmsTarget* cmdlet.
3. Pour modifier le planning de collecte de données EMS, entrez la commande *set-SmDataCollectionEmsSchedule* cmdlet.

## Surveiller l'état de la collecte de données EMS

Vous pouvez surveiller l'état de votre collecte de données EMS à l'aide de plusieurs applets de commande PowerShell. Vous pouvez obtenir des informations sur le planning, la cible de machine virtuelle de stockage et l'état.

### Étapes

1. À partir d'une ligne de commande PowerShell, établissez une session avec SnapCenter en entrant *Open-*

*SmConnection*.

2. Récupérez des informations sur le planning de collecte de données EMS en entrant *get-SmDataCollectionEmsSchedule*.
3. Récupérez des informations sur l'état de la collecte de données EMS en entrant *get-SmDataCollectionEmsStatus*.
4. Récupérez des informations sur la cible de collecte de données EMS en entrant *get-SmDataCollectionEmsTarget*.

### **Informations associées**

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

# Mise à niveau de SnapCenter Server et des plug-ins

## Configurer SnapCenter pour vérifier les mises à jour disponibles

SnapCenter communique régulièrement avec le site de support NetApp pour vous informer des mises à jour logicielles disponibles. Vous pouvez également créer un planning pour spécifier l'intervalle dans lequel vous souhaitez recevoir des informations sur les mises à jour disponibles.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Paramètres**.
2. Dans la page **Paramètres**, cliquez sur **logiciel**.

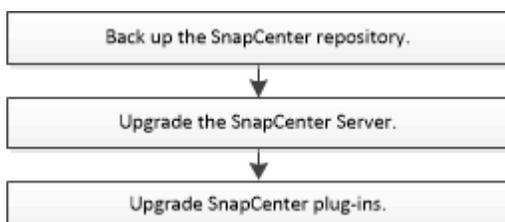
La page logiciels disponibles affiche les modules d'extension disponibles, les versions disponibles et leur état d'installation.

3. Cliquez sur **Rechercher les mises à jour** pour voir si des versions plus récentes de modules enfichables sont disponibles.
4. Cliquez sur **Programmer les mises à jour** pour créer un programme afin de spécifier l'intervalle dans lequel vous souhaitez recevoir des informations sur les mises à jour disponibles :
  - a. Sélectionnez l'intervalle dans **Rechercher les mises à jour**.
  - b. Sélectionnez les informations d'identification Windows pour l'administration du serveur SnapCenter et cliquez sur **OK**.

## Mise à niveau du workflow

Chaque version de SnapCenter contient un serveur SnapCenter et un pack de plug-in mis à jour. Les mises à jour des modules d'extension sont distribuées avec le programme d'installation de SnapCenter. Vous pouvez configurer SnapCenter pour vérifier les mises à jour disponibles.

Le workflow montre les différentes tâches nécessaires à la mise à niveau du serveur SnapCenter et des modules de plug-in.



## Chemins de mise à niveau pris en charge

Le chemin de mise à niveau vous permet de savoir à partir de quelles versions antérieures de SnapCenter vous pouvez mettre à niveau vers les dernières versions de SnapCenter et quelles versions des plug-ins sont

prises en charge.

Si vous utilisez la version du serveur SnapCenter...	Vous pouvez directement mettre à niveau SnapCenter Server vers...	Versions de plug-in prises en charge
5.0	6,0	<ul style="list-style-type: none"><li>• 5.0</li><li>• 6,0</li></ul>
	6.0.1	<ul style="list-style-type: none"><li>• 6.0.1</li></ul>
	6,1	<ul style="list-style-type: none"><li>• 6,1</li></ul>
6,0	6.0.1	<ul style="list-style-type: none"><li>• 6,0</li><li>• 6.0.1</li></ul>
	6,1	<ul style="list-style-type: none"><li>• 6,1</li></ul>
6.0.1	6,1	<ul style="list-style-type: none"><li>• 6.0.1</li><li>• 6,1</li></ul>

Pour plus d'informations sur la mise à niveau du plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Mettez à niveau le plug-in SnapCenter pour VMware vSphere](#)".

## Mettez à niveau le serveur SnapCenter sur l'hôte Windows

Vous devez mettre à niveau le serveur SnapCenter pour accéder aux dernières fonctionnalités et améliorations fournies dans la dernière version.

### Avant de commencer

- Mettez à jour l'hôte SnapCenter Server avec les dernières mises à jour Windows et assurez-vous qu'il n'y a pas de redémarrages système en attente.
- Assurez-vous qu'aucune autre opération n'est en cours d'exécution avant de démarrer la mise à niveau.
- Installez ASP.NET Core Runtime 8.0.12 (et tous les correctifs 8.0.x ultérieurs) Hosting Bundle et PowerShell 7.4.2 ou version ultérieure.
- Sauvegardez la base de données du référentiel SnapCenter (MySQL) après vous être assuré qu'aucune tâche n'est en cours d'exécution. Ceci est recommandé avant la mise à niveau de SnapCenter Server et du plug-in Exchange.

Pour plus d'informations, reportez-vous à la section "[Sauvegarder le référentiel SnapCenter](#)".

- Sauvegardez tous les fichiers de configuration SnapCenter modifiés que vous avez modifiés sur l'hôte SnapCenter Server ou sur l'hôte du plug-in.

Exemples de fichiers de configuration SnapCenter : SnapDriveService.exe.config, SMCOREServiceHost.exe.config, etc.

- Si vous avez installé plusieurs versions du plug-in personnalisé dans SnapCenter 5.0, avant de procéder à

la mise à niveau vers la version 6.0 ou une version ultérieure, vous devez exécuter les applets de commande PowerShell pour supprimer toutes les versions antérieures du plug-in personnalisé (à l'exception de la dernière) du référentiel SnapCenter (base de données NSM).

- Courir `Open-SmConnection` et connectez-vous en utilisant les informations d'identification du rôle `SnapCenterAdmin`
- Courir `Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>`

Pour plus d'informations, consultez "[La mise à niveau vers SnapCenter 6.0 ou version ultérieure échoue](#)".

## Description de la tâche

- Lors de la mise à niveau, SnapCenter exécute un script SQL pour mettre à jour les données Exchange dans la base de données NSM, en convertissant le DAG et le nom court de l'hôte en FQDN. Ceci s'applique uniquement si vous utilisez SnapCenter Server avec le plug-in Exchange.
- Si vous avez placé manuellement l'hôte du serveur en mode maintenance, après la mise à niveau, sélectionnez **Hôtes > Activer la planification** pour sortir l'hôte du serveur du mode maintenance.
- Pour les programmes de sauvegarde et de vérification existants avec les prescripteurs et les postscripts activés dans la stratégie, les opérations de sauvegarde continueront de fonctionner après la mise à niveau.

Dans la page **Détails du travail**, un message d'avertissement recommande au client de copier les scripts dans `LE_CHEMIN_SCRIPTS` et de modifier la stratégie pour fournir un chemin relatif au `CHEMIN_SCRIPTS`. Pour le travail de cycle de vie du clone, un message d'avertissement s'affiche au niveau du sous-travail.

## Étapes

1. Téléchargez le pack d'installation du serveur SnapCenter depuis le site de support NetApp.

<https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab>

2. Créez une copie de l'adresse `web.config` située à l'adresse `C:\Program Files\NetApp\SnapCenter\WebApp`.
3. Exportez les planifications de l'hôte du plug-in SnapCenter à partir du Planificateur de tâches Windows pour les restaurer en cas d'échec de la mise à niveau.

```
md d:\\SCBackup` `schtasks /query /xml /TN taskname >>
"D:\\SCBackup\\taskname.xml"
```

4. Créez le vidage de la base de données SnapCenter MySQL si la sauvegarde du référentiel n'est pas configurée.

```
md d:\\SCBackup` `mysqldump --all-databases --single-transaction --add-drop
-database --triggers --routines --events -u root -p >
D:\\SCBackup\\SCRepoBackup.dmp
```

Lorsque vous y êtes invité, entrez le mot de passe.

5. Double-cliquez sur le fichier `.exe` téléchargé pour lancer la mise à niveau de SnapCenter Server.

Une fois la mise à niveau démarrée, SnapCenter exécute des vérifications préalables. Si le système ne répond pas aux exigences minimales, SnapCenter affiche des messages d'erreur ou d'avertissement.

Vous pouvez ignorer les avertissements et continuer l'installation, mais vous devez corriger toutes les erreurs.



SnapCenter continue d'utiliser le mot de passe de la base de données du référentiel MySQL Server existant fourni lors de l'installation de la version antérieure de SnapCenter Server.

## 6. Sélectionnez **Mettre à niveau**.

Si vous sélectionnez **Annuler** à n'importe quelle étape, SnapCenter arrête la mise à niveau. Cela ne ramènera pas le serveur SnapCenter à son état précédent.

**Meilleure pratique** : déconnectez-vous et reconnectez-vous, ou ouvrez un nouveau navigateur pour accéder à l'interface utilisateur de SnapCenter .

### Une fois que vous avez terminé

- Si le plug-in est installé à l'aide d'un utilisateur sudo, vous devez copier les clés sha224 disponibles dans `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` pour mettre à jour le fichier `/etc/sudoers`.
- Vous devez effectuer une nouvelle découverte des ressources sur l'hôte du serveur.

Si SnapCenter affiche l'état de l'hôte du serveur comme arrêté, attendez un certain temps et effectuez une nouvelle découverte. Vous pouvez également modifier la valeur du paramètre **HostRefreshInterval** (la valeur par défaut est 3600 secondes) sur n'importe quelle valeur supérieure à 10 minutes.

- Si la mise à niveau échoue, nettoyez l'installation ayant échoué, réinstallez la version antérieure de SnapCenter et restaurez la base de données NSM à l'état dans lequel elle se trouvait auparavant.
- Après la mise à niveau de l'hôte serveur, vous devez également mettre à niveau les plug-ins avant d'ajouter un système de stockage.

## Mettez à niveau le serveur SnapCenter sur un hôte Linux

Vous pouvez utiliser le fichier d'installation du serveur SnapCenter pour mettre à niveau le serveur SnapCenter.

### Étapes

1. Effectuez l'une des actions de mise à niveau du serveur SnapCenter.

Si vous souhaitez effectuer...	Procédez comme ça...
Mise à niveau non interactive	<pre>sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DUPGRADE=&lt;value&gt; -DINSTALL_LOG_NAME=&lt;filename&gt;</pre> <p>Exemple : <code>sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log</code></p> <p>Les journaux seront stockés à <i>/var/opt/snapcenter/logs</i>.</p> <p>Paramètres à transmettre pour la mise à niveau :</p> <ul style="list-style-type: none"> <li>• <code>DINSTALL_LOG_NAME</code> : nom du fichier journal dans lequel les journaux d'installation seront stockés.</li> <li>• <code>DUPGRADE</code> : la valeur par défaut est 0. Spécifiez ce paramètre et sa valeur comme tout entier autre que 0 pour mettre à niveau le serveur SnapCenter.</li> </ul>
Installation interactive	<pre>./snapcenter-linux-server- (e18/e19/sles15).bin</pre> <p>Vous serez invité à confirmer la mise à niveau. Entrez une valeur autre que 0 pour confirmer la mise à niveau du serveur SnapCenter.</p>



Vous devez vous déconnecter puis vous connecter à SnapCenter, ou fermer puis ouvrir un nouveau navigateur pour accéder à l'interface graphique de SnapCenter.

## Mettez à niveau vos modules d'extension

Les modules d'extension sont distribués dans le cadre de la mise à niveau de SnapCenter.

Il n'est pas nécessaire de mettre manuellement chaque hôte de plug-in à mettre à niveau en mode maintenance car la procédure de mise à niveau place vos hôtes de plug-in Windows, Linux ou AIX en mode maintenance. Le mode de maintenance empêche l'exécution de tâches planifiées sur l'hôte du plug-in pendant la mise à niveau.

### Avant de commencer

- Si vous êtes un utilisateur non-root disposant d'un accès aux machines Linux, vous devez mettre à jour le fichier `/etc/sudoers` avec les dernières valeurs de somme de contrôle avant d'effectuer l'opération de mise à niveau.
- Par défaut, SnapCenter détecte `JAVA_HOME` à partir de l'environnement. Si vous souhaitez utiliser un `JAVA_HOME` fixe et si vous mettez à niveau les plug-ins sur un hôte Linux, vous devez ajouter

manuellement le paramètre SKIP\_JAVAHOME\_UPDATE dans le fichier *spl.properties* situé à */var/opt/snapcenter/spl/etc/* et définir la valeur SUR TRUE.

La valeur de JAVA\_HOME est mise à jour lorsque le plug-in est mis à niveau ou lorsque le service SnapCenter Plug-in Loader (SPL) redémarre. Avant de mettre à niveau ou de redémarrer la SPL, si vous ajoutez le paramètre SKIP\_JAVAHOME\_UPDATE et définissez la valeur SUR TRUE, la valeur de JAVA\_HOME n'est pas mise à jour.

- Vous devez avoir sauvegardé tous les fichiers de configuration SnapCenter que vous avez modifiés sur l'hôte du serveur SnapCenter ou sur l'hôte du plug-in.

Exemples de fichiers de configuration SnapCenter : SnapDriveService.exe.config, SMCoreserviceHost.exe.config, etc.

## Description de la tâche

- Pour le plug-in SnapCenter pour Microsoft SQL Server, le plug-in SnapCenter pour Microsoft Exchange Server et le plug-in SnapCenter pour Microsoft Windows, il est recommandé de mettre à niveau à la fois le serveur et les hôtes du plug-in vers la dernière version pour que LE CHEMIN\_SCRIPTS s'exécute.

Pour les programmes de sauvegarde et de vérification existants avec les prescripteurs et les postscripts activés dans la stratégie, les opérations de sauvegarde continueront de fonctionner après la mise à niveau.

Dans la page **Détails du travail**, un message d'avertissement recommande au client de copier les scripts dans LE CHEMIN\_SCRIPTS et de modifier la stratégie pour fournir un chemin relatif au CHEMIN\_SCRIPTS. Pour le travail de cycle de vie du clone, un message d'avertissement s'affiche au niveau du sous-travail.

## Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts > Managed Hosts**.
2. Mettez à niveau les hôtes en effectuant l'une des tâches suivantes :
  - Si la colonne État global affiche « mise à niveau disponible » pour l'un des plug-ins hôtes, cliquez sur le nom d'hôte du plug-in et effectuez les opérations suivantes :
    - i. Cliquez sur **plus d'options**.
    - ii. Sélectionnez **Ignorer les contrôles préalables** si vous ne souhaitez pas valider si l'hôte du plug-in répond aux exigences de mise à niveau du plug-in.
    - iii. Cliquez sur **Upgrade**.
  - Si vous souhaitez mettre à niveau plusieurs hôtes, sélectionnez tous les hôtes, cliquez sur , puis cliquez sur **mettre à niveau > OK**.

Tous les services associés sont redémarrés lors de la mise à niveau du plug-in.



Tous les plug-ins du package sont sélectionnés. Seuls les plug-ins installés avec la version précédente de SnapCenter sont mis à niveau et les plug-ins restants ne sont pas installés. Vous devez utiliser l'option **Ajouter des plug-ins** pour installer un nouveau plug-in.

Si vous n'avez pas coché la case **Ignorer les précontrôles**, l'hôte du plug-in est validé pour vérifier s'il répond aux exigences d'installation du plug-in. Si les exigences minimales ne sont pas remplies, des messages d'erreur ou d'avertissement appropriés s'affichent. Après avoir résolu le problème, cliquez

sur **Upgrade**.



Si l'erreur est liée à l'espace disque ou à la mémoire RAM, vous pouvez mettre à jour le fichier web.config situé à C:\Program Files\NetApp\SnapCenter WebApp, ou les fichiers de configuration PowerShell situés à C:\Windows\System32\PowerShell\Windowsv1.0\modules\SnapCenter\ pour modifier les valeurs par défaut. Si l'erreur est liée aux paramètres restants, vous devez corriger le problème, puis valider à nouveau les exigences.

# Mise à jour technologique

## Mise à jour technologique de l'hôte du serveur SnapCenter

Lorsque l'hôte du serveur SnapCenter nécessite une actualisation, vous pouvez installer la même version du serveur SnapCenter sur le nouvel hôte, puis exécuter les API pour sauvegarder le serveur SnapCenter à partir de l'ancien serveur et le restaurer sur le nouveau serveur.

### Étapes

1. Déployez le nouvel hôte et effectuez les tâches suivantes :
  - a. Installez la même version du serveur SnapCenter.
  - b. (Facultatif) configurez les certificats CA et activez le protocole SSL bidirectionnel. Pour plus d'informations, reportez-vous à la section ["Configurer le certificat CA"](#) et ["Configurer et activer le protocole SSL bidirectionnel"](#).
  - c. (Facultatif) configurez l'authentification multifacteur. Pour plus d'informations, reportez-vous à la section ["Activez l'authentification multifacteur"](#).
2. Connectez-vous en tant qu'utilisateur Admin SnapCenter.
3. Créez une sauvegarde du serveur SnapCenter sur l'ancien hôte à l'aide de l'API:  
`/<snapcenter_version>/server/backup` Ou de l'applet de commande: `New-SmServerBackup`.



Avant de procéder à la sauvegarde, suspendez toutes les tâches planifiées et assurez-vous qu'aucune tâche n'est en cours d'exécution.



Si vous souhaitez restaurer la sauvegarde sur le serveur SnapCenter en cours d'exécution sur un nouveau domaine, vous devez ajouter le nouvel utilisateur de domaine dans l'ancien hôte SnapCenter et attribuer le rôle d'administrateur SnapCenter avant de procéder à une sauvegarde.

4. Copiez la sauvegarde de l'ancien hôte vers le nouvel hôte.
5. Restaurez la sauvegarde du serveur SnapCenter sur le nouvel hôte à l'aide de l'API  
`/<snapcenter_version>/server/restore` : ou de l'applet de commande : `Restore-SmServerBackup`.

Par défaut, la restauration mettra à jour la nouvelle URL du serveur SnapCenter dans tous les hôtes. Si vous voulez ignorer la mise à jour, utilisez l'attribut `-SkipSMSURLInHosts` et mettez à jour séparément l'URL du serveur en utilisant l'API: `/<snapcenter_version>/server/configureurl` Ou l'applet de commande: `Set-SmServerConfig`.



Si l'hôte du plug-in ne parvient pas à résoudre le nom d'hôte du serveur, connectez-vous à chacun des hôtes du plug-in et ajoutez l'entrée `etc/host` pour la nouvelle adresse IP au format `<New IP> SC_Server_Name`.



Les entrées du serveur `etc/host` ne seront pas restaurées. Vous pouvez le restaurer manuellement à partir de l'ancien serveur.

Si la sauvegarde est restaurée sur le serveur SnpCenter qui s'exécute sur un nouveau domaine et si vous

souhaitez continuer à utiliser les anciens utilisateurs de domaine, vous devez enregistrer l'ancien domaine dans le nouveau serveur SnapCenter.



Si vous avez mis à jour manuellement le fichier web.config dans l'ancien hôte SnapCenter, les mises à jour ne seront pas copiées sur le nouvel hôte. Vous devez effectuer manuellement les mêmes modifications dans le fichier web.config du nouvel hôte.

6. Si vous avez ignoré la mise à jour de l'URL du serveur SnapCenter ou si l'un des hôtes était en panne pendant le processus de restauration, mettez à jour le nouveau nom du serveur dans tous les hôtes ou hôtes spécifiés gérés par SnapCenter à l'aide de l'API:

`/<snapcenter_version>/server/configureurl` Ou de l'applet de commande: `Set-SmServerConfig`.

7. Activez les travaux planifiés sur tous les hôtes à partir du nouveau serveur SnapCenter.

## Mise à jour technologique d'un nœud dans un cluster F5

Vous pouvez procéder à une actualisation technologique de n'importe quel nœud du cluster F5 en supprimant le nœud et en ajoutant le nouveau nœud. Si le nœud qui doit être actualisé est actif, activez un autre nœud du cluster, puis supprimez-le.

Pour plus d'informations sur l'ajout d'un nœud à un cluster F5, reportez-vous à la section "[Configurer les serveurs SnapCenter pour la haute disponibilité à l'aide de F5](#)".



Si l'url du cluster F5 change, l'url peut être mise à jour dans tous les hôtes à l'aide de l'API: `/<snapcenter_version>/server/configureurl` Ou de l'applet de commande: `Set-SmServerConfig`.

## Mise hors service de l'ancien hôte du serveur SnapCenter

Vous pouvez supprimer l'ancien hôte du serveur SnapCenter après avoir vérifié que le nouveau serveur SnapCenter est en cours d'exécution et que tous les hôtes du plug-in peuvent communiquer avec le nouvel hôte du serveur SnapCenter.

## Restauration vers l'ancien hôte du serveur SnapCenter

En cas de problème, vous pouvez ramener l'ancien hôte du serveur SnapCenter en mettant à jour l'URL du serveur SnapCenter dans tous les hôtes à l'aide de l'API:

`/<snapcenter_version>/server/configureurl` Ou de l'applet de commande: `Set-SmServerConfig`.

## Reprise après incident

### Reprise après incident d'un hôte SnapCenter autonome

Vous pouvez effectuer une reprise sur incident en restaurant la sauvegarde du serveur sur le nouvel hôte.

#### Avant de commencer

Assurez-vous que vous disposez d'une sauvegarde de l'ancien serveur SnapCenter.

#### Étapes

1. Déployez le nouvel hôte et effectuez les tâches suivantes :
  - a. Installez la même version du serveur SnapCenter.

- b. Configurez les certificats CA et activez le protocole SSL bidirectionnel. Pour plus d'informations, reportez-vous à la section ["Configurer le certificat CA"](#) et ["Configurer et activer le protocole SSL bidirectionnel"](#).
2. Copiez l'ancienne sauvegarde du serveur SnapCenter sur le nouvel hôte.
3. Connectez-vous en tant qu'utilisateur Admin SnapCenter.
4. Restaurez la sauvegarde du serveur SnapCenter sur le nouvel hôte à l'aide de l'API `/<snapcenter_version>/server/restore` : ou de l'applet de commande : `Restore-SmServerBackup`.

Par défaut, la restauration mettra à jour la nouvelle URL du serveur SnapCenter dans tous les hôtes. Si vous voulez ignorer la mise à jour, utilisez l'attribut `-SkipSMSURLInHosts` et mettez à jour séparément l'URL du serveur en utilisant l'API: `/<snapcenter_version>/server/configureurl` Ou l'applet de commande: `Set-SmServerConfig`.



Si l'hôte du plug-in ne parvient pas à résoudre le nom d'hôte du serveur, connectez-vous à chacun des hôtes du plug-in et ajoutez l'entrée `etc/host` pour la nouvelle adresse IP au format `<New IP> SC_Server_Name`.



Les entrées du serveur `etc/host` ne seront pas restaurées. Vous pouvez le restaurer manuellement à partir de l'ancien serveur.

5. Si vous avez ignoré la mise à jour de l'URL ou si l'un des hôtes était en panne pendant le processus de restauration, mettez à jour le nouveau nom de serveur dans tous les hôtes ou hôtes spécifiés gérés par SnapCenter à l'aide de l'API: `/<snapcenter_version>/server/configureurl` Ou de l'applet de commande: `Set-SmServerConfig`.

## Reprise après incident du cluster SnapCenter F5

Vous pouvez effectuer une reprise sur incident en restaurant la sauvegarde du serveur sur le nouvel hôte, puis en convertissant l'hôte autonome en cluster.

### Avant de commencer

Assurez-vous que vous disposez d'une sauvegarde de l'ancien serveur SnapCenter.

### Étapes

1. Déployez le nouvel hôte et effectuez les tâches suivantes :
  - a. Installez la même version du serveur SnapCenter.
  - b. Configurez les certificats CA et activez le protocole SSL bidirectionnel. Pour plus d'informations, reportez-vous à la section ["Configurer le certificat CA"](#) et ["Configurer et activer le protocole SSL bidirectionnel"](#).
2. Copiez l'ancienne sauvegarde du serveur SnapCenter sur le nouvel hôte.
3. Connectez-vous en tant qu'utilisateur Admin SnapCenter.
4. Restaurez la sauvegarde du serveur SnapCenter sur le nouvel hôte à l'aide de l'API `/<snapcenter_version>/server/restore` : ou de l'applet de commande : `Restore-SmServerBackup`.

Par défaut, la restauration mettra à jour la nouvelle URL du serveur SnapCenter dans tous les hôtes. Si vous voulez ignorer la mise à jour, utilisez l'attribut `-SkipSMSURLInHosts` et mettez à jour séparément l'URL du serveur en utilisant l'API: `/<snapcenter_version>/server/configureurl` Ou l'applet de

commande: *Set-SmServerConfig*.



Si l'hôte du plug-in ne parvient pas à résoudre le nom d'hôte du serveur, connectez-vous à chacun des hôtes du plug-in et ajoutez l'entrée *etc/host* pour la nouvelle adresse IP au format <New IP> SC\_Server\_Name.



Les entrées du serveur *etc/host* ne seront pas restaurées. Vous pouvez le restaurer manuellement à partir de l'ancien serveur.

5. Si vous avez ignoré la mise à jour de l'URL ou si l'un des hôtes était en panne pendant le processus de restauration, mettez à jour le nouveau nom de serveur dans tous les hôtes ou hôtes spécifiés gérés par SnapCenter à l'aide de l'API: `/<snapcenter_version>/server/configureurl` Ou de l'applet de commande: *Set-SmServerConfig*.
6. Convertir l'hôte autonome en cluster F5.

Pour plus d'informations sur la configuration de F5, reportez-vous à la section "[Configurer les serveurs SnapCenter pour la haute disponibilité à l'aide de F5](#)".

### Informations associées

Pour plus d'informations sur les API, vous devez accéder à la page swagger. voir "[Comment accéder aux API REST à l'aide de la page Web de l'API swagger](#)".

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous référer au "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".

## Mise à jour technologique des hôtes du plug-in SnapCenter

Lorsque les hôtes du plug-in SnapCenter doivent être renouvelés, vous devez déplacer les ressources de l'ancien hôte vers le nouvel hôte. Une fois le nouvel hôte ajouté à SnapCenter, il découvre toutes les ressources, mais sera traité comme de nouvelles ressources.

### Description de la tâche

Vous devez exécuter l'API ou l'applet de commande qui prendra l'ancien nom d'hôte et le nouveau nom d'hôte en entrée, comparer les ressources par nom et rééditer les objets des ressources correspondantes de l'ancien hôte vers le nouvel hôte. Les ressources correspondantes seront marquées comme protégées.

- Le paramètre *IsDryRun* est défini sur vrai par défaut et identifie les ressources correspondantes de l'ancien et du nouvel hôte.

Après avoir vérifié les ressources correspondantes, vous devez définir le paramètre *IsDryRun* sur Faux pour rééditer les objets des ressources correspondantes de l'ancien hôte vers le nouvel hôte.

- Le paramètre *AutoMigrateManuallyAddedResources* est défini sur vrai par défaut et copie automatiquement les ressources ajoutées manuellement depuis l'ancien hôte vers le nouvel hôte.

Le paramètre *AutoMigrationManuallyAddedResources* ne s'applique qu'aux ressources Oracle et SAP HANA.

- Le paramètre *SQLInstanceMapping* doit être utilisé si le nom de l'instance est différent entre l'ancien hôte

et le nouvel hôte. S'il s'agit d'une instance par défaut, utilisez *default\_instance* comme nom d'instance.

La mise à jour technologique est prise en charge pour les plug-ins SnapCenter suivants :

- Plug-in SnapCenter pour Microsoft SQL Server
  - Si les bases de données SQL sont protégées au niveau de l'instance et que, dans le cadre de l'actualisation technologique de l'hôte, seules des ressources partielles sont déplacées vers le nouvel hôte, la protection au niveau de l'instance existante est convertie en protection de groupe de ressources et les instances des deux hôtes sont ajoutées au groupe de ressources.
  - Si un hôte SQL (par exemple host1) est utilisé comme planificateur ou serveur de vérification pour les ressources d'un autre hôte (par exemple host2), alors lors de l'actualisation technologique sur host1, le planning ou les détails de vérification ne seront pas migrés et continueront à s'exécuter sur host1. Si vous devez modifier, vous devez le modifier manuellement dans les hôtes respectifs.
  - Si vous utilisez la configuration des instances de cluster de basculement SQL (FCI), vous pouvez effectuer la mise à jour technologique en ajoutant le nouveau nœud au cluster FCI et en actualisant l'hôte de plug-in dans SnapCenter.
  - Si vous utilisez la configuration de SQL Availability Group (AG), aucune mise à jour technologique n'est requise. Vous pouvez ajouter le nouveau nœud à AG et actualiser l'hôte dans SnapCenter.
- Plug-in SnapCenter pour Windows
- Plug-in SnapCenter pour bases de données Oracle

Si vous utilisez la configuration d'Oracle Real application Cluster (RAC), vous pouvez effectuer la mise à jour technologique en ajoutant le nouveau nœud au cluster RAC et en actualisant l'hôte du plug-in dans SnapCenter.

- Plug-in SnapCenter pour base de données SAP HANA

Les cas d'utilisation pris en charge sont les suivants :

- Migration des ressources d'un hôte vers un autre hôte.
- Migration des ressources de plusieurs hôtes vers un ou moins d'hôtes.
- Migration des ressources d'un hôte vers plusieurs hôtes.

Les scénarios pris en charge sont les suivants :

- Le nouvel hôte a un nom différent de celui de l'ancien hôte
- L'hôte existant a été renommé

### **Avant de commencer**

Comme ce flot de travaux modifie les données dans le référentiel SnapCenter, il est recommandé de sauvegarder le référentiel SnapCenter. En cas de problème de données, le référentiel SnapCenter peut revenir à l'état antérieur à l'aide de la sauvegarde.

Pour plus d'informations, reportez-vous à la section "[Sauvegarder le référentiel SnapCenter](#)".

### **Étapes**

1. Déployez le nouvel hôte et installez l'application.
2. Suspendre les planifications de l'ancien hôte.
3. Déplacez les ressources requises de l'ancien hôte vers le nouvel hôte.

- a. Place les bases de données requises sur le nouvel hôte à partir du même stockage.
  - Assurez-vous que le stockage est mappé sur le même lecteur ou sur le même chemin de montage que celui de l'ancien hôte. Si le stockage n'est pas mappé correctement, les sauvegardes créées dans l'ancien hôte ne peuvent pas être utilisées pour la restauration.



Par défaut, Windows attribue automatiquement le lecteur disponible suivant.

- Si la reprise sur incident du stockage est activée, le stockage respectif doit être monté sur le nouvel hôte.
- b. Vérifiez la compatibilité en cas de modification de la version de l'application.
  - c. Uniquement pour l'hôte du plug-in Oracle, assurez-vous que les UID et les GID d'Oracle et de ses utilisateurs de groupe sont identiques à ceux de l'ancien hôte.

Pour plus d'informations, reportez-vous à :

- ["Comment migrer la base de données SQL de l'ancien hôte vers le nouvel hôte"](#)
- ["Comment migrer une base de données Oracle de l'ancien hôte vers le nouvel hôte"](#)
- ["Comment intégrer la base de données SAP HANA au nouvel hôte"](#)

4. Ajoutez le nouvel hôte à SnapCenter.
5. Vérifiez si toutes les ressources sont découvertes.
6. Exécutez l'API d'actualisation de l'hôte `/<snapcenter_version>/techrefresh/host` : ou l'applet de commande : `Invoke-SmTechRefreshHost`.



La séquence sèche est activée par défaut et les ressources correspondantes à réassocier sont identifiées. Vous pouvez vérifier les ressources en exécutant l'API `'/jobs/{jobid}'` ou l'applet de commande `get-SmJobSummaryReport`.

Si vous avez migré les ressources de plusieurs hôtes, vous devez exécuter l'API ou l'applet de commande pour tous les hôtes. Si le lecteur ou le chemin de montage du nouvel hôte n'est pas le même que l'ancien hôte, les opérations de restauration suivantes échoueront :

- La restauration SQL sur place échouera. Toutefois, la fonction RTAL peut être utilisée.
- La restauration des bases de données Oracle et SAP HANA échoue.

Si vous souhaitez migrer vers plusieurs hôtes, vous devez effectuer toutes les étapes à partir de l'étape 1 pour tous les hôtes.



Vous pouvez exécuter l'API ou l'applet de commande sur le même hôte plusieurs fois. Elle sera réactivée uniquement si une nouvelle ressource est identifiée.

7. (Facultatif) supprimez l'ancien ou les anciens hôtes de SnapCenter.

### Informations associées

Pour plus d'informations sur les API , vous devez accéder à la page swagger . voir ["Comment accéder aux API REST à l'aide de la page Web de l'API swagger"](#).

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous référer au ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

# Mise à jour technologique du système de stockage

Une fois le stockage actualisé en mode technologique, les données sont migrées vers le nouveau système de stockage et les hôtes d'application sont montés avec un nouveau système de stockage. Le workflow de sauvegarde SnapCenter identifie le nouveau stockage et crée le snapshot si le nouveau stockage est enregistré dans SnapCenter.

Vous pouvez restaurer, monter et cloner les nouvelles sauvegardes créées après l'actualisation du stockage. Cependant, ces opérations échouent lorsqu'elles sont effectuées sur les sauvegardes créées avant l'actualisation du stockage, car les sauvegardes possèdent les anciens détails du stockage. Vous devez exécuter l'API ou le cmdlet de mise à jour technologique du stockage pour mettre à jour les anciennes sauvegardes dans SnapCenter avec les nouveaux détails de stockage.

La mise à jour technologique est prise en charge pour les plug-ins SnapCenter suivants :

- Plug-in SnapCenter pour Microsoft SQL Server
- Plug-in SnapCenter pour Windows
- Plug-in SnapCenter pour bases de données Oracle
- Plug-in SnapCenter pour base de données SAP HANA
- Plug-in SnapCenter pour Microsoft Exchange Server

Les cas d'utilisation pris en charge sont les suivants :

- Actualisation du stockage primaire

La mise à jour technologique du stockage est prise en charge pour remplacer le stockage primaire par un nouveau stockage. Vous ne pouvez pas convertir le stockage secondaire existant en stockage principal.

- Actualisation du stockage secondaire

## Mettre à jour les sauvegardes du stockage primaire

Une fois le stockage actualisé en mode technologique, vous devez exécuter l'API ou le cmdlet de mise à jour technologique pour mettre à jour les anciennes sauvegardes dans SnapCenter avec les nouveaux détails du stockage.

### Avant de commencer

Comme ce flot de travaux modifie les données dans le référentiel SnapCenter, il est recommandé de sauvegarder le référentiel SnapCenter. En cas de problème de données, le référentiel SnapCenter peut revenir à l'état antérieur à l'aide de la sauvegarde.

Pour plus d'informations, reportez-vous à la section "[Sauvegarder le référentiel SnapCenter](#)".

### Étapes

1. Migrez les données de l'ancien stockage vers le nouveau.

Pour plus d'informations sur la migration, reportez-vous à :

- "[Comment migrer les données vers un nouveau stockage](#)"
- "[Comment copier un volume et conserver toutes les copies Snapshot ?](#)"

2. Mettez l'hôte en mode de maintenance.
3. Montez le nouveau stockage sur les hôtes respectifs et faites apparaître les bases de données.

Le nouveau stockage doit être connecté à l'hôte de la même manière qu'auparavant. Par exemple, s'il était connecté en tant que SAN, il doit être connecté en tant que SAN.

Le nouveau système de stockage doit être monté sur le même disque ou chemin que l'ancien système de stockage.

4. Vérifiez que toutes les ressources sont opérationnelles.
5. Ajoutez le nouveau stockage dans SnapCenter.

Assurez-vous de disposer d'un nom de SVM unique sur tous les clusters dans SnapCenter. Si vous utilisez le même nom de SVM dans le nouveau stockage et si tous les volumes de la SVM peuvent être migrés avant d'exécuter l'actualisation du stockage, il est ensuite recommandé de supprimer le SVM de l'ancien cluster et de redécouvrir l'ancien cluster en SnapCenter qui supprimera le SVM du cache.

6. Mettre l'hôte en mode de production.
7. Dans SnapCenter, créez une sauvegarde des ressources dont le stockage est migré. Une nouvelle sauvegarde est nécessaire pour que SnapCenter puisse identifier l'empreinte de stockage la plus récente et elle sera utilisée pour mettre à jour les métadonnées des anciennes sauvegardes existantes.



Chaque fois qu'une nouvelle LUN est connectée à l'hôte, elle possède un nouveau numéro de série. Lors de la découverte du système de fichiers Windows, SnapCenter traite chaque numéro de série unique comme une nouvelle ressource. Lors de la mise à jour technologique du stockage, lorsque la LUN du nouveau stockage est connectée à l'hôte avec la même lettre ou le même chemin de lecteur, la découverte du système de fichiers Windows dans SnapCenter marque la ressource existante comme supprimée, même si elle est montée avec la même lettre de lecteur ou le même chemin et affiche la nouvelle LUN comme nouvelle ressource. Comme la ressource est marquée comme supprimée, elle ne sera pas prise en compte pour la mise à jour technologique de stockage dans SnapCenter et toutes les sauvegardes de l'ancienne ressource seront perdues. Lorsqu'une actualisation du stockage se produit, pour les ressources du système de fichiers Windows, la détection des ressources ne doit pas être effectuée avant l'exécution de l'API ou de l'applet de commande d'actualisation du stockage.

8. Exécutez l'API d'actualisation du stockage :

`/<snapcenter_version>/techrefresh/primarystorage` ou l'applet de commande : `Invoke-SmTechRefreshPrimaryStorage`.



Si la ressource est configurée avec une règle de réplication activée, la dernière sauvegarde après l'actualisation du stockage doit contenir des détails sur le stockage secondaire.

- a. Si vous utilisez la configuration des instances de cluster de basculement SQL (FCI), les sauvegardes sont conservées au niveau du cluster. Vous devez fournir le nom du cluster comme entrée pour la mise à jour technologique du stockage.
- b. Si vous utilisez la configuration de SQL Availability Group (AG), les sauvegardes sont conservées au niveau du nœud. Vous devez fournir le nom du nœud en tant qu'entrée pour la mise à jour technologique du stockage.
- c. Si vous utilisez la configuration Oracle Real application clusters (RAC), vous pouvez effectuer une mise à jour technologique du stockage sur n'importe quel nœud.

Par défaut, l'attribut *IsDryRun* est défini sur vrai. Elle identifie les ressources pour lesquelles le stockage est actualisé. Vous pouvez afficher les détails de la ressource et du stockage modifié en exécutant l'API «<SnapCenter\_version>/jobs/{jobid} » ou l'applet de commande *get-SmJobSummaryReport*.

9. Après avoir vérifié les détails du stockage, définissez l'attribut *IsDryRun* sur Faux et exécutez l'API d'actualisation du stockage : `/<snapcenter_version>/techrefresh/primarystorage` ou l'applet de commande : *Invoke-SmTechRefreshPrimaryStorage*.

Les détails de stockage des anciennes sauvegardes seront mis à jour.

Vous pouvez exécuter l'API ou l'applet de commande sur le même hôte plusieurs fois. Les détails du stockage des anciennes sauvegardes seront mis à jour uniquement si le stockage est actualisé.



Impossible de migrer la hiérarchie des clones dans ONTAP. Si des métadonnées de clone sont présentes dans SnapCenter dans le stockage en cours de migration, la ressource clonée sera marquée comme ressource indépendante. Les clones des métadonnées de clone seront supprimés de manière récursive.

10. (Facultatif) si tous les snapshots ne sont pas déplacés de l'ancien stockage primaire vers le nouveau stockage primaire, exécutez l'API suivante : `/<snapcenter_version>/hosts/primarybackupsexistencecheck` ou l'applet de commande *Invoke-SmPrimaryBackupsExistenceCheck*.

Cette opération permet d'effectuer le contrôle de l'existence des snapshots sur le nouveau stockage primaire et de marquer les sauvegardes respectives indisponibles pour toute opération dans SnapCenter.

## Mettre à jour les sauvegardes du stockage secondaire

Une fois le stockage actualisé en mode technologique, vous devez exécuter l'API ou le cmdlet de mise à jour technologique pour mettre à jour les anciennes sauvegardes dans SnapCenter avec les nouveaux détails du stockage.

### Avant de commencer

Comme ce flot de travaux modifie les données dans le référentiel SnapCenter, il est recommandé de sauvegarder le référentiel SnapCenter. En cas de problème de données, le référentiel SnapCenter peut revenir à l'état antérieur à l'aide de la sauvegarde.

Pour plus d'informations, reportez-vous à la section "[Sauvegarder le référentiel SnapCenter](#)".

### Étapes

1. Migrez les données de l'ancien stockage vers le nouveau.

Pour plus d'informations sur la migration, reportez-vous à :

- "[Comment migrer les données vers un nouveau stockage](#)"
- "[Comment copier un volume et conserver toutes les copies Snapshot ?](#)"

2. Établissez la relation SnapMirror entre le stockage primaire et le nouveau stockage secondaire et assurez-vous que la relation fonctionne correctement.
3. Dans SnapCenter, créez une sauvegarde des ressources dont le stockage est migré.

Une nouvelle sauvegarde est nécessaire pour que SnapCenter puisse identifier l'empreinte de stockage la

plus récente et elle sera utilisée pour mettre à jour les métadonnées des anciennes sauvegardes existantes.



Vous devez attendre que cette opération soit terminée. Si vous passez à l'étape suivante avant la fin de l'opération, SnapCenter déserre complètement les anciennes métadonnées du snapshot secondaire.

4. Une fois la sauvegarde de toutes les ressources d'un hôte créée, exécutez l'API d'actualisation du stockage secondaire : `/<snapcenter_version>/techrefresh/secondarystorage` ou l'applet de commande : *Invoke-SmTechRefreshSecondaryStorage*.

Ceci mettra à jour les détails de stockage secondaire des anciennes sauvegardes de l'hôte donné.

Si vous souhaitez exécuter cette opération au niveau des ressources, cliquez sur **Refresh** pour chaque ressource afin de mettre à jour les métadonnées de stockage secondaire.

5. Une fois les anciennes sauvegardes mises à jour, vous pouvez rompre l'ancienne relation de stockage secondaire avec la sauvegarde principale.

# Désinstaller SnapCenter Server et les plug-ins

## Désinstallez les modules du plug-in SnapCenter

### Conditions préalables à la suppression d'un hôte

Vous pouvez supprimer des hôtes et désinstaller des plug-ins ou des modules externes individuels à l'aide de l'interface graphique de SnapCenter. Vous pouvez également désinstaller des plug-ins ou modules externes individuels sur des hôtes distants à l'aide de l'interface de ligne de commande (CLI) de votre hôte SnapCenter Server ou à l'aide de l'option Windows **Désinstaller un programme** localement sur n'importe quel hôte.

Avant de supprimer un hôte du serveur SnapCenter, vous devez remplir les conditions préalables.

- Vous devez vous connecter en tant qu'administrateur.
- Vous devez vous assurer que les travaux de découverte ne sont pas en cours d'exécution sur l'hôte.
- Un rôle avec les autorisations requises doit être attribué pour supprimer tous les objets associés à l'hôte. Dans le cas contraire, l'opération de retrait échoue.
- Vous devez confirmer l'empreinte si la clé SSH a été modifiée après l'ajout de l'hôte à SnapCenter.
- Vous devez confirmer l'empreinte si l'hôte SnapCenter est mis à niveau vers une version plus récente de SnapCenter, mais que l'hôte du plug-in exécute toujours une version antérieure du plug-in.

### Conditions préalables pour supprimer un hôte à l'aide du contrôle d'accès basé sur les rôles

- Vous devez avoir ouvert une session à l'aide d'un rôle RBAC qui dispose d'autorisations en lecture, suppression de l'hôte, installation, désinstallation du plug-in et suppression d'objets.

Les objets peuvent être clonés, sauvegarde, groupe de ressources, système de stockage, etc.

- Vous devez avoir ajouté l'utilisateur RBAC au rôle RBAC.
- Vous devez affecter l'utilisateur RBAC à l'hôte, au plug-in, aux identifiants, aux groupes de ressources et au système de stockage (pour les clones) à supprimer.
- Vous devez avoir ouvert une session SnapCenter en tant qu'utilisateur RBAC.

### Conditions préalables pour supprimer un hôte avec clones créés à partir de l'opération de cycle de vie du clonage

- Vous devez avoir créé des tâches de clonage avec la gestion du cycle de vie des clones pour les bases de données SQL.
- Vous devez avoir créé un rôle RBAC avec la lecture et la suppression du clone, la lecture et la suppression de ressources, la lecture et la suppression du groupe de ressources, la lecture et la suppression du stockage, le provisionnement en lecture et suppression, le montage, le démontage, l'installation et la désinstallation de plug-ins, les autorisations de lecture et de suppression de l'hôte.
- Vous devez avoir affecté l'utilisateur RBAC au rôle RBAC.
- Vous devez avoir attribué l'utilisateur RBAC à l'hôte, au plug-in SnapCenter pour Microsoft SQL Server, aux informations d'identification, au groupe de ressources sur le cycle de vie des clones et au système de stockage.

- Vous devez avoir ouvert une session SnapCenter en tant qu'utilisateur RBAC.

Pour plus d'informations sur la désinstallation du plug-in SnapCenter pour VMware vSphere, reportez-vous à la section "[Suppression du plug-in SnapCenter pour VMware vSphere](#)".

## Supprimer un hôte

Lorsque le serveur SnapCenter supprime un hôte, il supprime d'abord la sauvegarde, les clones, les tâches de clonage, les groupes de ressources et les ressources répertoriées pour cet hôte sur la page Ressources SnapCenter, puis désinstalle les modules du plug-in sur l'hôte.

### Description de la tâche

- Si vous supprimez un hôte, les sauvegardes, clones et groupes de ressources associés à cet hôte sont également supprimés.
- Lorsque vous supprimez les groupes de ressources, tous les plannings associés sont également supprimés.
- Si l'hôte dispose d'un groupe de ressources partagé avec un autre hôte et que vous supprimez l'hôte, le groupe de ressources est également supprimé.
- Vous devez utiliser la cmdlet *Remove-SmHost* pour supprimer les hôtes du plug-in désaffectés ou inaccessibles.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous référer au "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)"

- Le temps nécessaire pour supprimer un hôte dépend du nombre de sauvegardes et des paramètres de rétention. En effet, les instantanés sont supprimés de chacun des contrôleurs et les métadonnées sont nettoyées.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page **hosts**, cliquez sur **Managed Hosts**.
3. Sélectionnez l'hôte à supprimer, puis cliquez sur **Supprimer**.
4. Pour les clusters Oracle RAC, pour supprimer le logiciel SnapCenter de tous les hôtes du cluster, sélectionnez **inclure tous les hôtes du cluster**.

Vous pouvez également supprimer un nœud d'un cluster et ainsi supprimer tous les nœuds un par un.

5. Cliquez sur **OK**.



Lorsque vous désinstallez et réinstallez les plug-ins hôtes sur un cluster, les ressources du cluster ne sont pas automatiquement découvertes. Sélectionnez le nom d'hôte du cluster, puis cliquez sur **Actualiser les ressources** pour découvrir automatiquement les ressources du cluster.

## Désinstallez les plug-ins à l'aide de l'interface graphique de SnapCenter

Lorsque vous décidez de ne plus avoir besoin d'un plug-in individuel ou d'un module externe, vous pouvez le désinstaller à l'aide de l'interface SnapCenter.

### Avant de commencer

- Vous devez avoir supprimé les groupes de ressources du module d'extension que vous désinstallez.
- Vous devez avoir détaché les stratégies associées aux groupes de ressources du module externe que vous désinstallez.

### Description de la tâche

Vous pouvez désinstaller un plug-in individuel. Par exemple, vous devrez peut-être désinstaller le plug-in SnapCenter pour Microsoft SQL Server car un hôte manque de ressources et vous souhaitez déplacer ce plug-in vers un hôte plus puissant. Vous pouvez également désinstaller tout un module externe. Par exemple, vous devrez peut-être désinstaller le module de plug-ins SnapCenter pour Linux, qui inclut le plug-in SnapCenter pour Oracle Database et le plug-in SnapCenter pour UNIX.

- La suppression d'un hôte inclut la désinstallation de tous les plug-ins.

Lorsque vous supprimez un hôte de SnapCenter, SnapCenter désinstalle tous les modules du plug-in sur l'hôte avant de supprimer l'hôte.

- L'interface graphique de SnapCenter supprime les plug-ins d'un hôte à la fois.

Lorsque vous utilisez l'interface graphique SnapCenter, vous ne pouvez désinstaller les plug-ins que sur un seul hôte à la fois. Toutefois, plusieurs opérations de désinstallation peuvent être exécutées en même temps.

Vous pouvez également désinstaller un plug-in à partir de plusieurs hôtes à l'aide de l'applet de commande *Uninstall-SmHostPackage* et des paramètres requis. Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant *get-Help nom\_commande*. Vous pouvez également vous reporter à la "[Guide de référence de l'applet de commande du logiciel SnapCenter](#)".



La désinstallation du module de plug-ins SnapCenter pour Windows à partir d'un hôte sur lequel le serveur SnapCenter est installé endommagera l'installation du serveur SnapCenter. Ne désinstallez pas le module de plug-ins SnapCenter pour Windows, sauf si vous êtes certain que vous n'avez plus besoin du serveur SnapCenter.

### Étapes

1. Dans le volet de navigation de gauche, cliquez sur **hosts**.
2. Dans la page hôtes, cliquez sur **Managed Hosts**.
3. Dans la page hôtes gérés, sélectionnez l'hôte à partir duquel vous souhaitez désinstaller le module externe ou le module externe.
4. À côté du plug-in que vous souhaitez supprimer, cliquez sur **Remove > Submit**.

### Une fois que vous avez terminé

Patientez 5 minutes avant de réinstaller le plug-in sur cet hôte. Cette période est suffisante pour que l'interface graphique de SnapCenter actualise l'état de l'hôte géré. L'installation échoue si vous réinstallez immédiatement le plug-in.

Si vous désinstallez le module de plug-ins SnapCenter pour Linux, des fichiers journaux spécifiques à la désinstallation sont disponibles à l'adresse suivante : `/Custom_location/snapcenter/log`.

## Désinstallez les plug-ins Windows à l'aide de l'applet de commande PowerShell

Vous pouvez désinstaller des modules externes individuels ou désinstaller des modules externes d'un ou plusieurs hôtes à l'aide de l'applet de commande `Uninstall-SmHostPackage` de l'interface de ligne de commande de l'hôte SnapCenter Server.

Vous devez vous connecter à SnapCenter en tant qu'utilisateur de domaine disposant des droits d'administrateur local sur chaque hôte sur lequel vous souhaitez désinstaller les plug-ins.

### Étapes

1. Lancer PowerShell.
2. Sur l'hôte du serveur SnapCenter, entrez la commande : `Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME`, puis entrez vos informations d'identification.
3. Désinstallez les plug-ins Windows à l'aide de l'applet de commande `Uninstall-SmHostPackage` et des paramètres requis.

Les informations relatives aux paramètres pouvant être utilisés avec la cmdlet et leurs descriptions peuvent être obtenues en exécutant `get-Help nom_commande`. Vous pouvez également vous référer au ["Guide de référence de l'applet de commande du logiciel SnapCenter"](#).

## Désinstallez les plug-ins localement sur un hôte

Vous pouvez désinstaller les plug-ins SnapCenter localement sur un hôte si vous ne pouvez pas accéder à l'hôte à partir du serveur SnapCenter.

### Description de la tâche

La meilleure pratique pour désinstaller des plug-ins individuels ou des modules externes consiste à utiliser l'interface graphique SnapCenter ou l'applet de commande `Uninstall-SmHostPackage` sur l'interface de ligne de commande de l'hôte SnapCenter Server. Ces procédures permettent au serveur SnapCenter de rester à jour en cas de modification.

Toutefois, il peut être rare de devoir désinstaller des plug-ins localement. Par exemple, vous avez peut-être exécuté une tâche de désinstallation à partir du serveur SnapCenter, mais la tâche a échoué, ou vous avez désinstallé votre serveur SnapCenter et les plug-ins orphelins restent sur un hôte.



La désinstallation d'un module de plug-in localement sur un hôte ne supprime pas les données associées à l'hôte, par exemple les tâches planifiées et les métadonnées de sauvegarde.



N'essayez pas de désinstaller localement le module de plug-ins SnapCenter pour Windows à partir du panneau de configuration. Vous devez utiliser l'interface graphique SnapCenter pour vous assurer que le plug-in SnapCenter pour Microsoft Windows est correctement désinstallé.

### Étapes

1. Sur le système hôte, accédez au panneau de configuration et cliquez sur **Désinstaller un programme**.
2. Dans la liste de programmes, sélectionnez le module SnapCenter ou le module externe que vous souhaitez désinstaller, puis cliquez sur **Désinstaller**.

Windows désinstalle tous les plug-ins du package sélectionné.

## Désinstallez le package de plug-ins pour Linux ou AIX à l'aide de l'interface de ligne de commande

Vous pouvez désinstaller SnapCenter Plug-ins Package pour Linux ou SnapCenter Plug-ins Package pour AIX à l'aide de l'interface de ligne de commande.

### Avant de commencer

- Assurez-vous d'avoir supprimé les travaux planifiés
- Assurez-vous que toutes les tâches en cours d'exécution sont terminées.

### Étape

Exécutez `/Custom_location/NetApp/snapcenter/SPL/installation/plugins/Uninstall` pour désinstaller.

## Désinstallez le serveur SnapCenter sur l'hôte Windows

Si vous ne souhaitez plus utiliser le serveur SnapCenter pour gérer les tâches de protection des données, vous pouvez désinstaller le serveur SnapCenter à l'aide du panneau de configuration programmes et fonctionnalités de l'hôte du serveur SnapCenter. La désinstallation du serveur SnapCenter supprime tous ses composants.

### Avant de commencer

- Assurez-vous que vous disposez d'au moins 2 Go d'espace libre sur le lecteur sur lequel le serveur SnapCenter est installé.
- Assurez-vous que le domaine dans lequel le serveur SnapCenter est installé n'est pas supprimé.

Si vous supprimez le domaine sur lequel le serveur SnapCenter a été installé, puis essayez de le désinstaller, l'opération échoue.

- Vous devez avoir sauvegardé la base de données du référentiel car la base de données du référentiel sera nettoyée et désinstallée.

### Étapes

1. Sur l'hôte du serveur SnapCenter, accédez au panneau de configuration.
2. Assurez-vous que vous êtes dans la vue **Catégorie**.
3. Sous programmes, cliquez sur **Désinstaller un programme**.

La fenêtre programmes et fonctionnalités s'ouvre.

4. Sélectionnez le serveur NetApp SnapCenter, puis cliquez sur **Désinstaller**.

À partir de SnapCenter 4.2, lorsque vous désinstallez le serveur SnapCenter, tous ses composants, y compris la base de données du référentiel du serveur MySQL, sont désinstallés.

- Pour supprimer le nœud NLB d'un cluster NLB, vous devez redémarrer l'hôte du serveur SnapCenter. Si vous ne redémarrez pas l'hôte, vous risquez de rencontrer un échec si vous essayez de réinstaller le serveur SnapCenter.
- Vous devez désinstaller manuellement .NET Framework qui n'est pas supprimé pendant la

désinstallation.

## Désinstallez le serveur SnapCenter sur l'hôte Linux

Si vous ne souhaitez plus utiliser le serveur SnapCenter pour gérer les tâches de protection des données, vous pouvez désinstaller le serveur SnapCenter. La désinstallation du serveur SnapCenter supprime tous ses composants.

### Étapes

1. Effectuez l'une des actions nécessaires pour désinstaller le serveur SnapCenter.

Si vous souhaitez effectuer...	Procédez comme ça...
Désinstallation non interactive	<pre>\$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1</pre> <p>Exemple : sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</p>
Désinstallation interactive	<pre>\$ sudo &lt;USER_INSTALL_DIR&gt;/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</pre> <p>Entrez une valeur autre que 0 dans l'entrée de confirmation pour confirmer la désinstallation.</p>

# Automatisez à l'aide d'API REST

## Automatisation SnapCenter via les API REST

Vous pouvez utiliser des API REST pour effectuer plusieurs opérations de gestion du SnapCenter. Les API REST sont exposées via la page Web de swagger. Vous pouvez accéder à la page Web swagger disponible à l'adresse `https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` pour afficher la documentation de L'API REST, ainsi que pour émettre manuellement un appel d'API.

Les plug-ins qui prennent en charge les API REST sont les suivants :

- Le plug-in pour Microsoft SQL Server
- Plug-in pour base de données SAP HANA
- Plug-in pour Oracle Database

Pour plus d'informations sur le plug-in SnapCenter pour les API REST VMware vSphere, consultez la section ["Plug-in SnapCenter pour les API REST VMware vSphere"](#)

## Comment accéder de manière native à l'API REST de SnapCenter

Vous pouvez accéder directement à l'API REST de SnapCenter via n'importe quel langage de programmation qui prend en charge un client REST. Il s'agit de Python, PowerShell et Java.

## Base de services Web REST

Representational State Transfer (REST) est un style qui permet de créer des applications Web distribuées. Lorsqu'il est appliqué à la conception d'une API de services Web, il établit un ensemble de technologies et de meilleures pratiques pour l'exposition des ressources basées sur serveur et la gestion de leurs États. Il utilise des protocoles et des normes standard traditionnels pour offrir une base flexible de gestion de SnapCenter.

### Ressources et représentation d'état

Les ressources sont les composants de base d'un système basé sur le Web. Lors de la création d'une application de services Web REST, les premières tâches de conception incluent :

#### Identification des ressources système ou serveur

Chaque système utilise et gère les ressources. Une ressource peut être un fichier, une transaction commerciale, un processus ou une entité administrative. L'une des premières tâches de conception d'une application basée sur des services Web REST consiste à identifier les ressources.

## Définition des États de ressource et des opérations d'état associées

Les ressources se trouvent toujours dans un des États finis. Les États, ainsi que les opérations associées utilisées pour affecter les changements d'état, doivent être clairement définis.

## Terminaux URI

Chaque ressource REST doit être définie et mise à disposition à l'aide d'un schéma d'adressage bien défini. Les noeuds finaux où les ressources sont situées et identifiées utilisent un URI (Uniform Resource Identifier).

L'URI fournit un cadre général pour créer un nom unique pour chaque ressource du réseau. L'URL (Uniform Resource Locator) est un type d'URI utilisé avec les services Web pour identifier et accéder aux ressources. Les ressources sont généralement exposées dans une structure hiérarchique similaire à un répertoire de fichiers.

## Messages HTTP

Le protocole HTTP (Hypertext Transfer Protocol) est le protocole utilisé par le client et le serveur de services Web pour échanger des messages de requête et de réponse sur les ressources.

Dans le cadre de la conception d'une application de services Web, les méthodes HTTP sont mappées aux ressources et aux actions de gestion d'état correspondantes. Le HTTP est sans état. Par conséquent, pour associer un ensemble de requêtes et de réponses associées dans le cadre d'une transaction, des informations supplémentaires doivent être incluses dans les en-têtes HTTP des flux de données de requête et de réponse.

## Formatage JSON

Bien que l'information puisse être structurée et transférée de plusieurs façons entre un client de services Web et un serveur, l'option la plus populaire est JavaScript Object notation (JSON).

JSON est une norme de l'industrie qui représente les structures de données simples en texte brut et permet de transférer les informations d'état décrivant les ressources. L'API REST de SnapCenter utilise JSON pour formater les données présentes dans le corps de chaque requête et réponse HTTP.

## Caractéristiques opérationnelles de base

Alors QUE REST établit un ensemble commun de technologies et de meilleures pratiques, les détails de chaque API peuvent varier en fonction des choix de conception.

## Transaction d'API de demande et de réponse

Chaque appel de l'API REST est exécuté sous forme de requête HTTP vers le système du serveur SnapCenter, qui génère une réponse associée au client. Cette paire de demandes et de réponses est considérée comme une transaction API.

Avant d'utiliser l'API, vous devez connaître les variables d'entrée disponibles pour contrôler une requête et le contenu de la sortie de réponse.

## Prise en charge des opérations CRUD

Chaque ressource disponible via l'API REST SnapCenter est accessible selon le modèle CRUD :

- Création
- Lecture
- Mise à jour
- Supprimer

Pour certaines ressources, seul un sous-ensemble des opérations est pris en charge.

## Identifiants d'objets

Un identifiant unique est attribué à chaque instance de ressource ou objet lors de sa création. Dans la plupart des cas, l'identificateur est un UUID 128 bits. Ces identifiants sont globalement uniques dans un serveur SnapCenter spécifique.

Après l'émission d'un appel API qui crée une nouvelle instance d'objet, une URL avec l'ID associé est renvoyée à l'appelant dans l'en-tête d'emplacement de la réponse HTTP. Vous pouvez extraire l'identificateur et l'utiliser sur les appels suivants lorsque vous faites référence à l'instance de ressource.



Le contenu et la structure interne des identificateurs d'objet peuvent changer à tout moment. Vous ne devez utiliser les identificateurs sur les appels API applicables que si nécessaire lorsque vous faites référence aux objets associés.

## Instances et collections d'objets

Selon le chemin de ressource et la méthode HTTP, un appel API peut s'appliquer à une instance d'objet spécifique ou à une collection d'objets.

## Opérations synchrones et asynchrones

SnapCenter effectue une requête HTTP reçue d'un client de manière synchrone ou asynchrone.

### Traitement synchrone

SnapCenter exécute la demande immédiatement et répond avec un code d'état HTTP 200 ou 201 s'il réussit.

Chaque demande utilisant la méthode GET est toujours effectuée de manière synchrone. En outre, les demandes qui utilisent POST sont conçues pour s'exécuter de manière synchrone si elles doivent se terminer en moins de deux secondes.

### Traitement asynchrone

Si une demande asynchrone est valide, SnapCenter crée une tâche d'arrière-plan pour traiter la demande et un objet de travail pour ancrer la tâche. Le code d'état HTTP 202 est renvoyé à l'appelant avec l'objet travail. Vous devez récupérer l'état du travail pour déterminer le succès ou l'échec.

Les demandes qui utilisent les méthodes POST et DELETE sont conçues pour s'exécuter de manière asynchrone si elles devraient prendre plus de deux secondes.

## Sécurité

La sécurité fournie avec l'API REST repose principalement sur les fonctionnalités de sécurité disponibles avec SnapCenter. La sécurité suivante est utilisée par l'API :

## Sécurité de la couche de transport

Tout le trafic envoyé sur le réseau entre le serveur SnapCenter et le client est généralement chiffré à l'aide du protocole TLS, selon les paramètres de configuration de SnapCenter.

## Authentification HTTP

Au niveau HTTP, l'authentification de base est utilisée pour les transactions API. Un en-tête HTTP avec le nom d'utilisateur et le mot de passe dans une chaîne base64 est ajouté à chaque requête.

# Variables d'entrée contrôlant une requête API

Vous pouvez contrôler le traitement d'un appel API à l'aide de paramètres et de variables définis dans la requête HTTP.

## Méthodes HTTP

Les méthodes HTTP prises en charge par l'API REST de SnapCenter sont répertoriées dans le tableau suivant.



Toutes les méthodes HTTP ne sont pas disponibles sur chacun des terminaux REST.

Méthode HTTP	Description
OBTENEZ	Récupère les propriétés d'un objet sur une instance ou une collection de ressources.
POST	Crée une nouvelle instance de ressource en fonction de l'entrée fournie.
SUPPRIMER	Supprime une instance de ressource existante.
EN	Modifie une instance de ressource existante.

## En-têtes de demande

Vous devez inclure plusieurs en-têtes dans la requête HTTP.

### Type de contenu

Si le corps de la demande inclut JSON, cet en-tête doit être défini sur *application/json*.

### Accepter

Cet en-tête doit être réglé sur *application/json*.

### Autorisation

L'authentification de base doit être définie avec le nom d'utilisateur et le mot de passe codés en tant que chaîne base64.

## Corps de la demande

Le contenu du corps de la demande varie en fonction de l'appel spécifique. Le corps de requête HTTP comprend l'un des éléments suivants :

- Objet JSON avec variables d'entrée
- Vide

## Filtrage d'objets

Lors de l'émission d'un appel API utilisant GET, vous pouvez limiter ou filtrer les objets renvoyés en fonction de n'importe quel attribut. Par exemple, vous pouvez spécifier une valeur exacte à associer :

```
<field>=<query value>
```

En plus d'une correspondance exacte, d'autres opérateurs sont disponibles pour renvoyer un ensemble d'objets sur une plage de valeurs. L'API REST SnapCenter prend en charge les opérateurs de filtrage indiqués dans le tableau ci-dessous.

Opérateur	Description
=	Égal à
<	Inférieur à
>	Supérieur à
≤	Inférieur ou égal à
≥	Supérieur ou égal à
MISE À JOUR	Ou
!	Différent de
*	Un caractère générique gourmand

Vous pouvez également renvoyer une collection d'objets en fonction de la définition ou non d'un champ spécifique à l'aide du mot clé **null** ou de sa négation **!null** dans le cadre de la requête.



Les champs qui ne sont pas définis sont généralement exclus des requêtes correspondantes.

## Demande de champs d'objet spécifiques

Par défaut, l'émission d'un appel API à l'aide DE GET renvoie uniquement les attributs qui identifient de manière unique l'objet ou les objets. Cet ensemble minimal de champs sert de clé pour chaque objet et varie en fonction du type d'objet. Vous pouvez sélectionner d'autres propriétés d'objet à l'aide de l' `fields` paramètre de requête des manières suivantes :

### Champs communs ou standard

Spécifiez `fields=*` pour récupérer les champs d'objet les plus couramment utilisés. Ces champs sont généralement conservés dans la mémoire du serveur local ou nécessitent peu de traitement pour accéder à. Ce sont les mêmes propriétés que pour un objet après avoir utilisé GET avec une clé de chemin d'URL (UUID).

## Tous les champs

Spécifiez **fields=\*\*** pour récupérer tous les champs d'objet, y compris ceux nécessitant un traitement de serveur supplémentaire pour accéder.

## Sélection de champ personnalisée

Utilisez **fields=<nom\_champ>** pour spécifier le champ exact souhaité. Lorsque vous demandez plusieurs champs, les valeurs doivent être séparées par des virgules sans espaces.



Vous devez toujours identifier les champs spécifiques que vous souhaitez. Vous ne devez récupérer que l'ensemble des champs communs ou tous les champs, le cas échéant. Les champs sont classés comme communs et renvoyés à l'aide de *fields=\**, lesquels sont déterminés par NetApp en fonction de l'analyse des performances internes. La classification d'un champ pourrait changer dans les versions futures.

## Tri des objets dans le jeu de sortie

Les enregistrements d'une collection de ressources sont renvoyés dans l'ordre par défaut défini par l'objet. Vous pouvez modifier la commande à l'aide de la `order_by` paramètre de requête avec le nom de champ et la direction de tri comme suit :

```
order_by=<field name> asc|desc
```

Par exemple, vous pouvez trier le champ de type par ordre décroissant, suivi d'un ID par ordre croissant :

```
order_by=type desc, id asc
```

- Si vous spécifiez un champ de tri sans fournir de direction, les valeurs sont triées par ordre croissant.
- Lorsque vous ajoutez plusieurs paramètres, vous devez séparer les champs par une virgule.

## Pagination lors de la récupération d'objets dans une collection

Lors de l'émission d'un appel API à l'aide DE GET pour accéder à une collection d'objets du même type, SnapCenter tente de renvoyer le plus grand nombre possible d'objets en fonction de deux contraintes. Vous pouvez contrôler chacune de ces contraintes à l'aide de paramètres de requête supplémentaires sur la demande. La première contrainte atteinte pour une demande GET spécifique met fin à la demande et limite donc le nombre d'enregistrements renvoyés.



Si une demande se termine avant de passer à l'itération de tous les objets, la réponse contient le lien nécessaire pour récupérer le lot d'enregistrements suivant.

## Limitation du nombre d'objets

Par défaut, SnapCenter renvoie un maximum de 10,000 objets pour une requête GET. Vous pouvez modifier cette limite à l'aide du paramètre `max_records` query. Par exemple :

```
max_records=20
```

Le nombre d'objets effectivement renvoyés peut être inférieur au maximum en vigueur, en fonction de la contrainte de temps associée ainsi que du nombre total d'objets dans le système.

## Limitation du temps utilisé pour récupérer les objets

Par défaut, SnapCenter renvoie le plus grand nombre d'objets possible dans le temps imparti pour la demande GET. Le délai par défaut est de 15 secondes. Vous pouvez modifier cette limite à l'aide du paramètre `return_timeout` query. Par exemple :

```
return_timeout=5
```

Le nombre d'objets effectivement renvoyés peut être inférieur au maximum en vigueur, en fonction de la contrainte associée sur le nombre d'objets ainsi que du nombre total d'objets dans le système.

## Rétrécir le jeu de résultats

Si nécessaire, vous pouvez combiner ces deux paramètres avec des paramètres de requête supplémentaires pour affiner le jeu de résultats. Par exemple, le suivant renvoie jusqu'à 10 événements EMS générés après le temps spécifié :

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Vous pouvez émettre plusieurs demandes de page via les objets. Chaque appel d'API suivant doit utiliser une nouvelle valeur de temps basée sur le dernier événement du dernier jeu de résultats.

## Propriétés de taille

Les valeurs d'entrée utilisées avec certains appels API ainsi que certains paramètres de requête sont numériques. Au lieu de fournir un entier en octets, vous pouvez éventuellement utiliser un suffixe comme indiqué dans le tableau suivant.

Suffixe	Description
KO	Ko kilo-octets (1024 octets) ou kibioctets
MO	Mo mégaoctets (Ko x 1024 octets) ou mébioctets
GO	Go gigaoctets (Mo x 1024 octets) ou gibioctets
TO	To Teroctets (Go x 1024 bytes) ou tébioctets
PO	PB po (TB x 1024 bytes) ou pemabmabl

## Interprétation d'une réponse API

Chaque requête d'API génère une réponse au client. Vous devez examiner la réponse pour déterminer si elle a réussi et récupérer des données supplémentaires si nécessaire.

## Code d'état HTTP

Les codes d'état HTTP utilisés par l'API REST de SnapCenter sont décrits ci-dessous.

Code	Description
200	OK indique que les appels qui ne créent pas d'objet ont réussi.

Code	Description
201	Un objet créé a été créé. L'en-tête d'emplacement de la réponse inclut l'identifiant unique de l'objet.
202	Accepté Une tâche d'arrière-plan a été démarrée pour exécuter la demande, mais n'a pas encore été terminée.
400	Demande incorrecte l'entrée de demande n'est pas reconnue ou est inappropriée.
401	L'authentification utilisateur non autorisée a échoué.
403	Accès interdit en raison d'une erreur d'autorisation (RBAC).
404	Introuvable la ressource mentionnée dans la demande n'existe pas.
405	Méthode non autorisée la méthode HTTP de la requête n'est pas prise en charge pour la ressource.
409	Conflit une tentative de création d'un objet a échoué car un objet différent doit d'abord être créé ou l'objet demandé existe déjà.
500	Erreur interne Une erreur interne générale s'est produite au niveau du serveur.

## En-têtes de réponse

Plusieurs en-têtes sont inclus dans la réponse HTTP générée par le SnapCenter.

### Emplacement

Lorsqu'un objet est créé, l'en-tête d'emplacement inclut l'URL complète du nouvel objet, y compris l'identifiant unique attribué à l'objet.

### Type de contenu

Cela sera normalement `application/json`.

## Corps de réponse

Le contenu du corps de réponse résultant d'une requête API diffère selon l'objet, le type de traitement et le succès ou l'échec de la requête. La réponse est toujours affichée au format JSON.

### Objet unique

Un objet peut être renvoyé avec un ensemble de champs en fonction de la requête. Par exemple, vous pouvez utiliser OBTENIR pour extraire les propriétés sélectionnées d'un cluster à l'aide de l'identifiant unique.

### Objets multiples

Plusieurs objets d'une collection de ressources peuvent être renvoyés. Dans tous les cas, un format cohérent est utilisé avec `num_records` indique le nombre d'enregistrements et d'enregistrements contenant un tableau

des instances d'objet. Par exemple, vous pouvez extraire les nœuds définis dans un cluster spécifique.

## Objet travail

Si un appel API est traité de manière asynchrone, un objet travail est renvoyé, qui ancre la tâche d'arrière-plan. Par exemple, la demande DE CORRECTIF utilisée pour mettre à jour la configuration du cluster est traitée de manière asynchrone et renvoie un objet travail.

## Objet erreur

Si une erreur se produit, un objet erreur est toujours renvoyé. Par exemple, vous recevrez une erreur lors de la tentative de modification d'un champ non défini pour un cluster.

## Vide

Dans certains cas, aucune donnée n'est renvoyée et le corps de réponse inclut un objet JSON vide.

## Erreurs

Si une erreur se produit, un objet d'erreur est renvoyé dans le corps de réponse.

## Format

Un objet d'erreur a le format suivant :

```
"error": {
 "message": "<string>",
 "code": <integer>[,
 "target": "<string>"]
}
```

Vous pouvez utiliser la valeur de code pour déterminer le type ou la catégorie d'erreur générale, et le message pour déterminer l'erreur spécifique. Lorsqu'il est disponible, le champ cible inclut l'entrée utilisateur spécifique associée à l'erreur.

## Codes d'erreur courants

Les codes d'erreur courants sont décrits dans le tableau suivant. Certains appels API peuvent inclure des codes d'erreur supplémentaires.

Code	Description
409	Un objet ayant le même identifiant existe déjà.
400	La valeur d'un champ n'est pas valide ou est manquante ou un champ supplémentaire a été fourni.
400	L'opération n'est pas prise en charge.
405	Impossible de trouver un objet avec l'identificateur spécifié.
403	L'autorisation d'effectuer la demande est refusée.

Code	Description
409	La ressource est en cours d'utilisation.

## API REST prises en charge pour SnapCenter Server et les plug-ins

Les ressources disponibles via l'API REST de SnapCenter sont organisées par catégories, comme affichées sur la page de documentation de l'API SnapCenter. Une brève description de chacune des ressources avec les chemins de ressources de base est présentée ci-dessous, ainsi que des considérations d'utilisation supplémentaires, le cas échéant.

### Auth

Vous pouvez utiliser cette API pour vous connecter au serveur SnapCenter. Cette API renvoie un jeton d'autorisation d'utilisateur utilisé pour authentifier les requêtes suivantes.

### Domaines

Vous pouvez utiliser des API pour effectuer différentes opérations.

- Récupérer tous les domaines dans SnapCenter
- récupérer les détails d'un domaine spécifique
- enregistrer ou annuler l'enregistrement d'un domaine
- modifier un domaine

### Emplois

Vous pouvez utiliser des API pour effectuer différentes opérations.

- Récupérer tous les travaux dans SnapCenter
- récupérer l'état d'un travail
- annuler ou arrêter un travail

### Paramètres

Vous pouvez utiliser des API pour effectuer différentes opérations.

- enregistrer, modifier ou supprimer une information d'identification
- Affiche les informations d'identification enregistrées dans le serveur SnapCenter
- configurer les paramètres de notification
- Récupère des informations sur le serveur SMTP actuellement configuré pour envoyer des notifications par e-mail et affiche le nom du serveur SMTP, le nom des destinataires et le nom de l'expéditeur
- Affiche la configuration de l'authentification multifacteur (MFA) pour la connexion au serveur SnapCenter
- Activer ou désactiver l'authentification multifacteur pour la connexion au serveur SnapCenter

- Créez le fichier de configuration requis pour configurer MFA

## Hôtes

Vous pouvez utiliser des API pour effectuer différentes opérations.

- Interroger tous les hôtes SnapCenter
- Supprimer un ou plusieurs hôtes de SnapCenter
- récupérer un hôte par son nom
- récupérer toutes les ressources d'un hôte
- Récupérer une ressource à l'aide de l'ID de ressource
- récupérer les détails de la configuration du plug-in
- configurer l'hôte du plug-in
- Récupérer toutes les ressources du plug-in pour l'hôte Microsoft SQL Server
- Récupérez toutes les ressources du plug-in pour l'hôte de base de données Oracle
- récupérez toutes les ressources du plug-in pour l'hôte d'application personnalisé
- Récupérer toutes les ressources du plug-in pour l'hôte SAP HANA
- récupérer les plug-ins installés
- installez les plug-ins sur un hôte existant
- mettre à niveau le package hôte
- supprimez les plug-ins d'un hôte existant
- ajout d'un plug-in sur un hôte
- ajouter ou modifier un hôte
- Obtenir la signature de l'hôte Linux
- Enregistrez la signature de l'hôte Linux
- mettre l'hôte en mode maintenance ou production
- démarrez ou redémarrez les services du plug-in sur l'hôte
- renommer un hôte

## Ressources

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupérer toutes les ressources
- Récupérer une ressource à l'aide de l'ID de ressource
- Récupérer toutes les ressources du plug-in pour l'hôte Microsoft SQL Server
- Récupérez toutes les ressources du plug-in pour l'hôte de base de données Oracle
- récupérez toutes les ressources du plug-in pour l'hôte d'application personnalisé
- Récupérer toutes les ressources du plug-in pour l'hôte SAP HANA
- Récupérer une ressource Microsoft SQL Server à l'aide d'une clé
- récupérer une ressource personnalisée à l'aide d'une clé

- modifiez une ressource du plug-in pour l'hôte d'application personnalisé
- supprimez une ressource du plug-in pour l'hôte d'application personnalisé à l'aide d'une clé
- Récupérez une ressource SAP HANA à l'aide d'une clé
- Modifiez une ressource du plug-in pour l'hôte SAP HANA
- Supprimez une ressource du plug-in pour l'hôte SAP HANA à l'aide d'une clé
- Récupérez une ressource Oracle à l'aide d'une clé
- Créez une ressource de volume d'application Oracle
- Modifier une ressource de volume d'application Oracle
- Supprimez une ressource de volume d'application Oracle à l'aide d'une clé
- Récupérez les détails secondaires de la ressource Oracle
- Sauvegardez la ressource Microsoft SQL Server à l'aide du plug-in pour Microsoft SQL Server
- Sauvegardez la ressource Oracle à l'aide du plug-in pour la base de données Oracle
- sauvegardez la ressource personnalisée à l'aide du plug-in pour une application personnalisée
- Configurez la base de données SAP HANA
- Configurez la base de données Oracle
- Restaurez une sauvegarde de base de données SQL
- Restaurez une sauvegarde de base de données Oracle
- restaurez une sauvegarde d'application personnalisée
- Créez une ressource SAP HANA
- protégez une ressource personnalisée à l'aide du plug-in pour une application personnalisée
- Protection d'une ressource Microsoft SQL Server à l'aide du plug-in pour Microsoft SQL Server
- Modifier une ressource Microsoft SQL Server protégée
- Supprimez la protection des ressources Microsoft SQL Server
- Protection d'une ressource Oracle à l'aide du plug-in pour base de données Oracle
- Modifier une ressource Oracle protégée
- Supprimez la protection de la ressource Oracle
- clonez une ressource à partir de la sauvegarde à l'aide du plug-in pour une application personnalisée
- Cloner un volume d'application Oracle à partir de la sauvegarde à l'aide du plug-in pour la base de données Oracle
- Clonage d'une ressource Microsoft SQL Server à partir de la sauvegarde à l'aide du plug-in pour Microsoft SQL Server
- Création d'un cycle de vie de clonage d'une ressource Microsoft SQL Server
- Modification du cycle de vie du clone d'une ressource Microsoft SQL Server
- Supprimer le cycle de vie du clone d'une ressource Microsoft SQL Server
- Déplacez une base de données Microsoft SQL Server existante d'un disque local vers un LUN NetApp
- Créez un fichier de spécification clone pour une base de données Oracle
- Lancer une tâche d'actualisation du clone à la demande d'une ressource Oracle
- Créez une ressource Oracle à partir de la sauvegarde à l'aide du fichier de spécification clone

- restaure la base de données sur le réplica secondaire et la joint à nouveau au groupe de disponibilité
- Créez une ressource de volume d'application Oracle

## Sauvegardes

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupérez les détails de la sauvegarde par nom, type, plug-in, ressource ou date
- récupérer toutes les sauvegardes
- récupérer les détails de la sauvegarde
- renommer ou supprimer des sauvegardes
- Montez une sauvegarde Oracle
- Démontez une sauvegarde Oracle
- Cataloguer une sauvegarde Oracle
- Décataloguer une sauvegarde Oracle
- procurez-vous toutes les sauvegardes nécessaires pour effectuer une restauration instantanée

## Clones

Vous pouvez utiliser des API pour effectuer différentes opérations.

- Créer, afficher, modifier et supprimer le fichier de spécifications du clone de base de données Oracle
- Afficher la hiérarchie des clones des bases de données Oracle
- récupérer les informations du clone
- récupérer tous les clones
- supprimer les clones
- Récupère les détails du clone par ID
- Lancer une tâche d'actualisation du clone à la demande d'une ressource Oracle
- Cloner une ressource Oracle à partir de la sauvegarde à l'aide du fichier de spécification clone

## Répartition des clones

Vous pouvez utiliser des API pour effectuer différentes opérations.

- estimez l'opération de séparation des clones de la ressource clonée
- récupère l'état d'une opération de fractionnement de clone
- démarrer ou arrêter une opération de fractionnement du clone

## Groupes de ressources

Vous pouvez utiliser des API pour effectuer différentes opérations.

- extraire les détails de tous les groupes de ressources
- récupérez le groupe de ressources par nom

- créez un groupe de ressources pour le plug-in pour l'application personnalisée
- Créez un groupe de ressources pour le plug-in pour Microsoft SQL Server
- Créez un groupe de ressources pour le plug-in pour la base de données Oracle
- modifiez un groupe de ressources pour le plug-in pour l'application personnalisée
- Modifiez un groupe de ressources pour le plug-in pour Microsoft SQL Server
- Modifier un groupe de ressources pour le plug-in pour la base de données Oracle
- Créez, modifiez ou supprimez le cycle de vie d'un clone d'un groupe de ressources pour le plug-in pour Microsoft SQL Server
- sauvegarder un groupe de ressources
- mettez le groupe de ressources en mode maintenance ou production
- supprimer un groupe de ressources

## Stratégies

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupérer les détails de la police
- récupérer les détails de la stratégie par nom
- suppression d'une stratégie
- créer une copie d'une règle de gestion existante
- créez ou modifiez des règles pour le plug-in pour l'application personnalisée
- Créez ou modifiez des règles pour le plug-in pour Microsoft SQL Server
- Créez ou modifiez des règles pour le plug-in pour la base de données Oracle
- Créez ou modifiez des règles pour le plug-in pour la base de données SAP HANA

## Stockage

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupérer tous les partages
- récupérer un partage par nom
- créer ou supprimer un partage
- récupérer les informations relatives au stockage
- récupérer les détails du stockage par nom
- créer, modifier ou supprimer un stockage
- découvrir les ressources sur un cluster de stockage
- récupérer les ressources sur un cluster de stockage

## Partagez

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupérer les détails d'un partage

- récupérer les détails de tous les partages
- créer ou supprimer un partage sur le stockage
- récupérer un partage par nom

## Plug-ins

Vous pouvez utiliser des API pour effectuer différentes opérations.

- répertoriez tous les plug-ins d'un hôte
- Récupérer une ressource Microsoft SQL Server à l'aide d'une clé
- modifiez une ressource personnalisée à l'aide d'une clé
- supprimer une ressource personnalisée à l'aide d'une clé
- Récupérez une ressource SAP HANA à l'aide d'une clé
- Modifiez une ressource SAP HANA à l'aide d'une clé
- Supprimez une ressource SAP HANA à l'aide d'une clé
- Récupérer une ressource Oracle à l'aide d'une clé
- Modifiez une ressource de volume d'application Oracle à l'aide d'une clé
- Supprimez une ressource de volume d'application Oracle à l'aide d'une clé
- Sauvegardez la ressource Microsoft SQL Server à l'aide du plug-in pour Microsoft SQL Server et d'une clé
- Sauvegardez la ressource Oracle à l'aide du plug-in pour la base de données Oracle et d'une clé
- sauvegardez la ressource d'application personnalisée à l'aide du plug-in pour une application personnalisée et une clé
- Configurez la base de données SAP HANA à l'aide d'une clé
- Configurez la base de données Oracle à l'aide d'une clé
- restaurez une sauvegarde d'application personnalisée à l'aide d'une clé
- Créez une ressource SAP HANA
- Créez une ressource de volume d'application Oracle
- protégez une ressource personnalisée à l'aide du plug-in pour une application personnalisée
- Protection d'une ressource Microsoft SQL Server à l'aide du plug-in pour Microsoft SQL Server
- Modifier une ressource Microsoft SQL Server protégée
- Supprimez la protection des ressources Microsoft SQL Server
- Protection d'une ressource Oracle à l'aide du plug-in pour base de données Oracle
- Modifier une ressource Oracle protégée
- Supprimez la protection de la ressource Oracle
- clonez une ressource à partir de la sauvegarde à l'aide du plug-in pour une application personnalisée
- Cloner un volume d'application Oracle à partir de la sauvegarde à l'aide du plug-in pour la base de données Oracle
- Clonage d'une ressource Microsoft SQL Server à partir de la sauvegarde à l'aide du plug-in pour Microsoft SQL Server
- Création d'un cycle de vie de clonage d'une ressource Microsoft SQL Server

- Modification du cycle de vie du clone d'une ressource Microsoft SQL Server
- Supprimer le cycle de vie du clone d'une ressource Microsoft SQL Server
- Créez un fichier de spécification clone pour une base de données Oracle
- Lancement d'un cycle de vie du clone à la demande d'une ressource Oracle
- Cloner une ressource Oracle à partir de la sauvegarde à l'aide du fichier de spécification clone

## Rapports

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupère les rapports des opérations de sauvegarde, de restauration et de clonage pour les plug-ins respectifs
- ajouter, exécuter, supprimer ou modifier des plannings
- récupérer les données des rapports programmés

## Alertes

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupère toutes les alertes
- Récupère les alertes par ID
- Supprime plusieurs alertes ou une alerte par ID

## RBAC

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupère les détails des utilisateurs, groupes et rôles
- ajouter ou supprimer des utilisateurs
- attribuer l'utilisateur au rôle
- annuler l'affectation de l'utilisateur au rôle
- créer, modifier ou supprimer des rôles
- affecter un groupe à un rôle
- annuler l'affectation d'un groupe à un rôle
- ajouter ou supprimer des groupes
- créer une copie d'un rôle existant
- affecter ou désaffecter des ressources à l'utilisateur ou au groupe

## Configuration

Vous pouvez utiliser des API pour effectuer différentes opérations.

- afficher les paramètres de configuration
- modifiez les paramètres de configuration

## CertificateSettings

Vous pouvez utiliser des API pour effectuer différentes opérations.

- Afficher l'état du certificat pour le serveur SnapCenter ou l'hôte du plug-in
- Modifiez les paramètres de certificat pour le serveur SnapCenter ou l'hôte du plug-in

## Référentiel

Vous pouvez utiliser des API pour effectuer différentes opérations.

- récupérer les sauvegardes du référentiel
- afficher les informations de configuration relatives au référentiel
- Protégez et restaurez le référentiel SnapCenter
- Déprotégez le référentiel SnapCenter
- reconstruction et basculement du référentiel

## Version

Vous pouvez utiliser cette API pour afficher la version de SnapCenter.

## Comment accéder aux API REST à l'aide de la page Web de l'API swagger

Les API REST sont exposées via la page Web de swagger. Vous pouvez accéder à la page Web swagger pour afficher les API REST du serveur SnapCenter et pour émettre manuellement un appel d'API. Vous pouvez utiliser des API REST pour gérer votre SnapCenter Server ou effectuer des opérations de protection des données.

Vous devez connaître l'adresse IP de gestion ou le nom de domaine du serveur SnapCenter sur lequel vous souhaitez exécuter les API REST.

Vous n'avez pas besoin d'autorisations spéciales pour exécuter le client de l'API REST. N'importe quel utilisateur peut accéder à la page Web de swagger. Les autorisations respectives sur les objets accessibles via l'API REST sont basées sur l'utilisateur qui génère le jeton pour se connecter à l'API REST.

### Étapes

1. À partir d'un navigateur, entrez l'URL pour accéder à la page Web swagger au format `https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/`.



Assurez-vous que l'URL de L'API REST ne comporte pas les caractères suivants : +, ., % et &.

2. Dans le champ **swagger Explore**, si la documentation de l'API swagger ne s'affiche pas automatiquement, saisissez :  
`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/SnapCenter.yaml`
3. Cliquez sur **Explorer**.

Une liste de types ou de catégories de ressources API s'affiche.

4. Cliquez sur un type de ressource API pour afficher les API dans ce type de ressource.

Si vous rencontrez un comportement inattendu lors de l'exécution d'API REST SnapCenter, vous pouvez utiliser les fichiers journaux pour identifier la cause du problème et le résoudre. Vous pouvez télécharger les fichiers journaux à partir de l'interface utilisateur de SnapCenter en cliquant sur **moniteur > journaux > Téléchargement**.

## Commencez avec l'API REST

Vous pouvez commencer rapidement à utiliser l'API REST de SnapCenter. L'accès à l'API fournit une perspective avant de commencer à l'utiliser avec les processus de workflow plus complexes dans une configuration en direct.

### Bonjour tout le monde

Vous pouvez exécuter une commande simple sur votre système pour commencer à utiliser l'API REST de SnapCenter et confirmer sa disponibilité.

#### Avant de commencer

- Assurez-vous que l'utilitaire Curl est disponible sur votre système.
- Adresse IP ou nom d'hôte du serveur SnapCenter
- Nom d'utilisateur et mot de passe d'un compte autorisé à accéder à l'API REST de SnapCenter.



Si vos informations d'identification incluent des caractères spéciaux, vous devez les formater de manière acceptable pour Curl, en fonction du shell que vous utilisez. Par exemple, vous pouvez insérer une barre oblique inverse avant chaque caractère spécial ou envelopper la totalité `username:password` chaîne de devis unique.

#### Étape

Sur l'interface de ligne de commande, exécutez les commandes suivantes pour récupérer les informations du plug-in :

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Exemple :

```
curl -X GET -u admin:password -k
"https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

# Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

## Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

["Avis pour SnapCenter 6.1"](#)

## Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.