



Documentation Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/active-iq-unified-manager-916/index.html> on October 15, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation Active IQ Unified Manager	1
Notes de version	2
Commencer	3
Instructions de démarrage rapide pour les installations VMware	3
Configuration requise	3
Installer Active IQ Unified Manager	3
Instructions de démarrage rapide pour les installations Linux	4
Configuration requise	4
Installer Active IQ Unified Manager	4
Instructions de démarrage rapide pour les installations Windows	5
Configuration requise	5
Installer Active IQ Unified Manager	6
Installer Unified Manager sur les systèmes VMware vSphere	7
Introduction à Active IQ Unified Manager	7
À quoi sert le serveur Unified Manager	7
Aperçu de la séquence d'installation	7
Conditions requises pour l'installation d'Unified Manager	8
Infrastructure virtuelle et exigences matérielles	8
Configuration requise pour le logiciel et l'installation de VMware	10
Navigateurs pris en charge	10
Exigences relatives au protocole et au port	11
Complétez la feuille de travail	14
Installer, mettre à niveau et supprimer le logiciel Unified Manager	16
Aperçu du processus de déploiement	16
Déployer Unified Manager	17
Mettre à niveau Unified Manager	21
Redémarrer la machine virtuelle Unified Manager	24
Supprimer Unified Manager	24
Installer Unified Manager sur les systèmes Linux	25
Introduction à Active IQ Unified Manager	25
À quoi sert le serveur Unified Manager	25
Aperçu de la séquence d'installation	25
Conditions requises pour l'installation d'Unified Manager	26
Infrastructure virtuelle et exigences matérielles	26
Logiciels Linux et exigences d'installation	28
Navigateurs pris en charge	31
Exigences relatives au protocole et au port	31
Complétez la feuille de travail	34
Installer, mettre à niveau et supprimer le logiciel Unified Manager	36
Aperçu du processus d'installation	36
Configurer les référentiels de logiciels requis	37
Exigences SELinux sur les partages NFS et CIFS	39
Installer Unified Manager sur les systèmes Linux	42

Mettre à niveau Unified Manager sur Red Hat Enterprise Linux	48
Mettre à niveau les produits tiers après l'installation d'Unified Manager	54
Redémarrer Unified Manager	54
Supprimer Unified Manager	55
Supprimer l'utilisateur umadmin personnalisé et le groupe de maintenance	56
Installer Unified Manager sur les systèmes Windows	57
Introduction à Active IQ Unified Manager	57
À quoi sert le serveur Unified Manager	57
Aperçu de la séquence d'installation	57
Conditions requises pour l'installation d'Unified Manager	58
Infrastructure virtuelle et exigences matérielles	58
Logiciel Windows et configuration requise pour son installation	60
Navigateurs pris en charge	61
Exigences relatives au protocole et au port	62
Complétez la feuille de travail	65
Installer, mettre à niveau et supprimer le logiciel Unified Manager	67
Aperçu du processus d'installation	67
Installer Unified Manager sur Windows	68
Changer le mot de passe JBoss	71
Chemin de mise à niveau pris en charge pour les versions d'Unified Manager	72
Mettre à niveau Unified Manager	73
Mettre à niveau les produits tiers	74
Désinstaller les produits tiers	75
Redémarrer Unified Manager	76
Désinstaller Unified Manager	77
Effectuer des tâches de configuration et d'administration	78
Configurer Active IQ Unified Manager	78
Aperçu de la séquence de configuration	78
Accéder à l'interface Web d'Unified Manager	78
Effectuer la configuration initiale de l'interface Web d'Unified Manager	79
Ajouter des clusters	81
Configurer Unified Manager pour envoyer des notifications d'alerte	83
Modifier le mot de passe de l'utilisateur local	92
Définir le délai d'inactivité de la session	93
Définir le délai d'expiration de la session via la CLI	93
Modifier le nom d'hôte d'Unified Manager	94
Activer et désactiver la gestion du stockage basée sur des politiques	98
Configurer la sauvegarde d'Unified Manager	99
Gérer les paramètres des fonctionnalités	99
Activer la gestion du stockage basée sur des politiques	100
Activer la passerelle API	100
Spécifier le délai d'inactivité	101
Activer les événements du portail Active IQ	101
Activer et désactiver les paramètres de sécurité pour la conformité	102
Activer et désactiver le téléchargement de scripts	103

Ajouter une bannière de connexion	103
Utiliser la console de maintenance	103
Quelles fonctionnalités la console de maintenance fournit-elle ?	104
Ce que fait l'utilisateur de maintenance	104
Capacités de diagnostic utilisateur	104
Accéder à la console de maintenance	104
Accéder à la console de maintenance à l'aide de la console vSphere VM	105
Menus de la console de maintenance	106
Modifier le mot de passe de l'utilisateur de maintenance sous Windows	111
Modifier le mot de passe umadmin sur les systèmes Linux	112
Modifier les ports utilisés par Unified Manager pour les protocoles HTTP et HTTPS	112
Ajouter des interfaces réseau	113
Ajouter de l'espace disque au répertoire de la base de données Unified Manager	114
Gérer l'accès des utilisateurs	117
Ajouter des utilisateurs	117
Modifier les paramètres utilisateur	119
Afficher les utilisateurs	119
Supprimer des utilisateurs ou des groupes	120
Qu'est-ce que RBAC	120
À quoi sert le contrôle d'accès basé sur les rôles ?	120
Définitions des types d'utilisateurs	121
Définitions des rôles d'utilisateur	121
Rôles et capacités des utilisateurs d'Unified Manager	122
Gérer les paramètres d'authentification SAML	124
Exigences relatives aux fournisseurs d'identité	125
Activer l'authentification SAML	126
Modifier le fournisseur d'identité utilisé pour l'authentification SAML	127
Mettre à jour les paramètres d'authentification SAML après la modification du certificat de sécurité d'Unified Manager	128
Désactiver l'authentification SAML	129
Désactiver l'authentification SAML depuis la console de maintenance	130
Page d'authentification SAML	130
Gérer l'authentification	131
Modifier les serveurs d'authentification	132
Supprimer les serveurs d'authentification	132
Authentification avec Active Directory ou OpenLDAP	132
Journalisation d'audit	133
Page d'authentification à distance	136
Gérer les certificats de sécurité	139
Afficher le certificat de sécurité HTTPS	139
Télécharger une demande de signature de certificat HTTPS	139
Installer un certificat HTTPS signé et renvoyé par une autorité de certification	140
Installer un certificat HTTPS généré à l'aide d'outils externes	141
Descriptions des pages pour la gestion des certificats	143
Surveiller et gérer le stockage	146

Introduction à Active IQ Unified Manager	146
Introduction à la surveillance de l'état de santé Active IQ Unified Manager	146
Introduction à la surveillance des performances Active IQ Unified Manager	147
Utiliser les API REST d'Unified Manager	148
À quoi sert le serveur Unified Manager	148
Comprendre l'interface utilisateur	149
Dispositions de fenêtres typiques	149
Personnalisation de la disposition des fenêtres	150
Utiliser l'aide du gestionnaire unifié	151
Ajoutez vos sujets d'aide favoris à vos favoris	152
Rechercher des objets de stockage	152
Exporter les données de stockage sous forme de rapports	153
Filtrer le contenu de la page d'inventaire	155
Afficher les événements actifs depuis la cloche de notification	156
Surveiller et gérer les clusters depuis le tableau de bord	156
Page du tableau de bord	157
Gérez les problèmes ou les fonctionnalités ONTAP directement depuis Unified Manager	161
Gérer les clusters	168
Comment fonctionne le processus de découverte de cluster	168
Afficher la liste des clusters surveillés	169
Ajouter des clusters	170
Modifier les clusters	172
Supprimer les clusters	173
Redécouvrir les clusters	173
Surveiller l'infrastructure virtuelle VMware	174
Ce qui n'est pas pris en charge	176
Afficher et ajouter vCenter Server	177
Supprimer vCenter Server	179
Surveiller les machines virtuelles	179
Afficher l'infrastructure virtuelle dans une configuration de reprise après sinistre	181
Provisionner et gérer les charges de travail	183
Aperçu des charges de travail	184
Niveaux de service de performance	191
Gérer les politiques d'efficacité du stockage	198
Gérer et surveiller les configurations MetroCluster	200
Comportement du volume lors du basculement et du retour en arrière	201
Définitions de l'état de connectivité du cluster pour la configuration MetroCluster sur FC	203
Définitions de l'état de mise en miroir des données pour MetroCluster sur FC	204
Surveiller les configurations de MetroCluster	204
Surveiller la réplication de MetroCluster	207
Gérer les quotas	208
Quelles sont les limites de quota	208
Afficher les quotas des utilisateurs et des groupes d'utilisateurs	209
Créer des règles pour générer des adresses e-mail	209
Créer un format de notification par e-mail pour les quotas d'utilisateurs et de groupes d'utilisateurs	210

Modifier les adresses e-mail des quotas d'utilisateur et de groupe	210
En savoir plus sur les quotas	211
Description des boîtes de dialogue des quotas	212
Dépannage	215
Ajouter de l'espace disque au répertoire de la base de données Unified Manager	215
Modifier l'intervalle de collecte des statistiques de performances	219
Modifier la durée pendant laquelle Unified Manager conserve les données d'événements et de performances	220
Erreur d'authentification inconnue	221
Utilisateur non trouvé	221
Problème lors de l'ajout de LDAP à l'aide d'autres services d'authentification	221
Problème de rotation des journaux du SDK NetApp Manageability sur les systèmes Windows	222
Gérer les événements et les alertes	223
Gérer les événements	223
Quels sont les événements de la plateforme Active IQ	223
Quels sont les événements du système de gestion des événements ?	223
Que se passe-t-il lorsqu'un événement est reçu	229
Afficher les événements et les détails des événements	231
Afficher les événements non attribués	231
Reconnaître et résoudre les événements	231
Attribuer des événements à des utilisateurs spécifiques	232
Désactiver les événements indésirables	233
Résoudre les problèmes à l'aide de la correction automatique d'Unified Manager	234
Activer et désactiver les rapports d'événements Active IQ	235
Télécharger un nouveau fichier de règles Active IQ	236
Comment les événements de la plateforme Active IQ sont générés	237
Résoudre les événements de la plateforme Active IQ	237
Configurer les paramètres de conservation des événements	238
Qu'est-ce qu'une fenêtre de maintenance Unified Manager	238
Gérer les événements des ressources du système hôte	241
En savoir plus sur les événements	241
Liste des événements et types de gravité	247
Description des fenêtres d'événements et des boîtes de dialogue	309
Gérer les alertes	322
Que sont les alertes	322
Quelles informations sont contenues dans un e-mail d'alerte	323
Ajouter des alertes	323
Ajouter des alertes pour les événements de performance	326
Alertes de test	327
Activer et désactiver les alertes pour les événements résolus et obsolètes	328
Exclure les volumes de destination de reprise après sinistre de la génération d'alertes	328
Afficher les alertes	329
Modifier les alertes	329
Supprimer les alertes	330
Description des fenêtres d'alerte et des boîtes de dialogue	330

Gérer les scripts	336
Comment fonctionnent les scripts avec les alertes	337
Ajouter des scripts	338
Supprimer les scripts	339
Exécution du script de test	339
Commandes CLI Unified Manager prises en charge	340
Description des fenêtres de script et des boîtes de dialogue	346
Surveiller et gérer les performances du cluster	348
Introduction à la surveillance des performances Active IQ Unified Manager	348
Fonctionnalités de surveillance des performances d'Unified Manager	348
Interfaces Unified Manager utilisées pour gérer les performances du système de stockage	349
Activité de collecte de données sur la configuration et les performances des clusters	349
Qu'est-ce qu'un cycle de collecte de continuité des données	351
Ce que signifie l'horodatage dans les données et événements collectés	352
Naviguer dans les flux de travail de performance dans l'interface graphique d'Unified Manager	352
Connectez-vous à l'interface utilisateur	353
Interface graphique et chemins de navigation	353
Rechercher des objets de stockage	359
Filtrer le contenu de la page d'inventaire	360
Surveiller les performances du cluster à partir du tableau de bord	362
Comprendre les panneaux de performances sur le tableau de bord	362
Messages et descriptions des bannières de performance	363
Modifier l'intervalle de collecte des statistiques de performances	363
Dépanner les charges de travail à l'aide de l'analyseur de charge de travail	364
Quelles données l'analyseur de charge de travail affiche-t-il ?	365
Quand dois-je utiliser l'analyseur de charge de travail	367
Utiliser l'analyseur de charge de travail	367
Surveiller les performances du cluster à partir de la page de destination du cluster de performances	367
Comprendre la page de destination du cluster de performance	368
Page de destination du cluster de performance	368
Surveiller les performances à l'aide des pages d'inventaire des performances	373
Afficher les pages d'inventaire des performances pour tous les objets de stockage	374
Contenu de la page d'inventaire des performances de raffinement	380
Comprendre les recommandations d'Unified Manager pour hiérarchiser les données vers le cloud	382
Surveiller les performances à l'aide des pages de l'Explorateur de performances	384
Comprendre l'objet racine	384
Appliquer un filtrage pour réduire la liste des objets corrélés dans la grille	385
Spécifier une plage de temps pour les objets corrélés	385
Définir la liste des objets corrélés pour la comparaison graphique	387
Comprendre les graphiques de compteurs	388
Types de graphiques de compteurs de performances	389
Sélectionnez les graphiques de performances à afficher	392
Développer le volet Graphiques de compteur	392
Modifiez la focalisation des graphiques de compteur sur une période de temps plus courte	393
Afficher les détails de l'événement dans la chronologie des événements	393

Graphiques de compteurs Vue zoom	394
Afficher la latence du volume par composant de cluster	396
Afficher le trafic IOPS SVM par protocole	397
Consultez les graphiques de volume et de latence LUN pour vérifier la garantie de performances	398
Afficher les performances de tous les clusters SAN Array	398
Afficher les IOPS des nœuds en fonction des charges de travail qui résident uniquement sur le nœud local	399
Composants des pages de destination d'objets	400
Gérer les performances à l'aide des informations du groupe de politiques QoS	405
Comment la qualité de service du stockage peut contrôler le débit de la charge de travail	406
Afficher tous les groupes de politiques QoS disponibles sur tous les clusters	407
Afficher les volumes ou les LUN qui se trouvent dans le même groupe de politiques QoS	407
Afficher les paramètres du groupe de politiques QoS appliqués à des volumes ou des LUN spécifiques	408
Afficher les graphiques de performances pour comparer les volumes ou les LUN qui se trouvent dans le même groupe de stratégies QoS	409
Comment les différents types de politiques QoS sont affichés dans les graphiques de débit	409
Afficher les paramètres minimum et maximum de qualité de service de la charge de travail dans l'Explorateur de performances	411
Gérer les performances à l'aide de la capacité de performance et des informations IOPS disponibles	412
Quelle est la capacité de performance utilisée	413
Que signifie la valeur de la capacité de performance utilisée	414
Quels sont les IOPS disponibles	415
Afficher les valeurs utilisées de la capacité de performance des nœuds et des agrégats	416
Afficher les valeurs IOPS disponibles pour les nœuds et les agrégats	417
Consultez les graphiques des compteurs de capacité de performance pour identifier les problèmes	417
Capacité de performance utilisée, conditions de seuil de performance	419
Utilisez le compteur de capacité de performance utilisée pour gérer les performances	420
Comprendre et utiliser la page Planification du basculement de nœud	421
Utilisez la page Planification du basculement des nœuds pour déterminer les actions correctives	421
Composants de la page de planification du basculement de nœud	421
Utiliser une politique de seuil avec la page Planification du basculement de nœud	423
Utilisez le tableau de répartition de la capacité de performance utilisée pour la planification du basculement	423
Collecter des données et surveiller les performances de la charge de travail	425
Types de charges de travail surveillées par Unified Manager	425
Valeurs de mesure des performances de la charge de travail	426
Quelle est la plage de performances attendue	428
Comment la prévision de latence est utilisée dans l'analyse des performances	429
Comment Unified Manager utilise la latence de la charge de travail pour identifier les problèmes de performances	430
Comment les opérations de cluster peuvent affecter la latence de la charge de travail	431
Surveillance des performances des configurations MetroCluster	432
Comprendre les événements et les alertes de performance	433
Sources d'événements de performance	433

Types de gravité des événements de performance	434
Modifications de configuration détectées par Unified Manager	435
Types de politiques de seuil de performance définies par le système	435
Analyse et notification des événements de performance	438
Comment Unified Manager détermine l'impact sur les performances d'un événement	440
Composants de cluster et pourquoi ils peuvent être en conflit	441
Rôles des charges de travail impliquées dans un événement de performance	443
Gérer les seuils de performance	444
Comment fonctionnent les politiques de seuil de performance définies par l'utilisateur	445
Que se passe-t-il lorsqu'une politique de seuil de performance est violée ?	447
Quels compteurs de performance peuvent être suivis à l'aide de seuils	447
Quels objets et compteurs peuvent être utilisés dans les politiques de seuil combinées	450
Créer des politiques de seuil de performance définies par l'utilisateur	450
Attribuer des politiques de seuil de performance aux objets de stockage	452
Afficher les politiques de seuil de performance	453
Modifier les politiques de seuil de performance définies par l'utilisateur	453
Supprimer les politiques de seuil de performance des objets de stockage	454
Que se passe-t-il lorsqu'une politique de seuil de performance est modifiée	454
Qu'advient-il des politiques de seuil de performance lorsqu'un objet est déplacé ?	455
Analyser les événements de performance	456
Afficher des informations sur les événements de performance	456
Analyser les événements à partir de seuils de performance définis par l'utilisateur	457
Analyser les événements à partir des seuils de performance définis par le système	458
Analyser les événements à partir de seuils de performance dynamiques	464
Résoudre les événements de performance	472
Confirmez que la latence est dans la plage attendue	472
Examiner l'impact des modifications de configuration sur les performances de la charge de travail ...	472
Options permettant d'améliorer les performances de la charge de travail côté client	473
Vérifiez les problèmes de client ou de réseau	473
Vérifiez si d'autres volumes du groupe de politiques QoS présentent une activité inhabituellement élevée	473
Déplacer les interfaces logiques (LIF)	474
Exécutez les opérations d'efficacité du stockage à des heures moins chargées	475
Ajouter des disques et réaffecter des données	476
Comment l'activation du cache Flash sur un nœud peut améliorer les performances de la charge de travail	476
Comment l'activation de Flash Pool sur un agrégat de stockage peut améliorer les performances de la charge de travail	477
Vérification de l'état de la configuration de MetroCluster	477
Vérification de la configuration de MetroCluster	477
Déplacer les charges de travail vers un autre agrégat	478
Déplacer les charges de travail vers un autre nœud	479
Déplacer les charges de travail vers un agrégat sur un nœud différent	481
Déplacer les charges de travail vers un nœud dans une autre paire HA	482
Déplacer les charges de travail vers un autre nœud dans une autre paire HA	484

Utilisez les paramètres de stratégie QoS pour prioriser le travail sur ce nœud	486
Supprimer les volumes et les LUN inactifs	486
Ajouter des disques et effectuer une reconstruction de la disposition globale	487
Configurer une connexion entre un serveur Unified Manager et un fournisseur de données externe.	487
Données de performance pouvant être envoyées à un serveur externe	487
Configurer Graphite pour recevoir les données de performance d'Unified Manager	489
Configurer une connexion d'un serveur Unified Manager à un fournisseur de données externe	490
Surveiller et gérer la santé du cluster.	493
Introduction à la surveillance de l'état de santé Active IQ Unified Manager	493
Capacité physique et logique	493
Unités de mesure de capacité	493
Fonctionnalités de surveillance de l'état de santé d'Unified Manager	494
Interfaces Unified Manager utilisées pour gérer l'état du système de stockage	495
Gestion et surveillance des clusters et de la santé des objets du cluster	496
Comprendre la surveillance des clusters	496
Afficher la liste et les détails des clusters.	498
Vérifier la santé des clusters dans une configuration MetroCluster.	498
Afficher l'état de santé et de capacité de tous les clusters SAN Array	500
Afficher la liste et les détails des nœuds	501
Générer un rapport d'inventaire matériel pour le renouvellement du contrat	502
Afficher la liste et les détails des machines virtuelles de stockage	502
Voir la liste globale et les détails	503
Afficher les informations sur la capacité de FabricPool	503
Afficher les détails du pool de stockage	505
Afficher la liste des volumes et les détails	505
Afficher les détails sur les actions NFS	506
Afficher les détails des actions SMB/CIFS.	507
Afficher la liste des copies Snapshot	508
Supprimer les copies instantanées	508
Calculer l'espace récupérable pour les copies Snapshot	509
Description des fenêtres et des boîtes de dialogue des objets de cluster.	510
Flux de travail et tâches de santé communs d'Unified Manager	510
Surveiller et résoudre les problèmes de disponibilité des données	511
Résoudre les problèmes de capacité	518
Gérer les seuils de santé	520
Gérer les objectifs de sécurité du cluster.	525
Gérer les opérations de sauvegarde et de restauration.	538
Gérer les scripts.	554
Gérer et surveiller les groupes	557
Prioriser les événements des objets de stockage à l'aide d'annotations.	566
Envoyer un package d'assistance via l'interface Web et la console de maintenance	575
Tâches et informations liées à plusieurs flux de travail	582
Protéger et restaurer les données	641
Créer, surveiller et dépanner les relations de protection	641
Types de protection SnapMirror	641

Configurer les relations de protection dans Unified Manager	643
Effectuer un basculement et une restauration de la relation de protection	645
Résoudre un échec de tâche de protection	649
Résoudre les problèmes de décalage	653
Gérer et surveiller les relations de protection	654
Afficher l'état de protection du volume	654
Afficher les relations de protection du volume	657
Surveiller les LUN dans une relation de groupe de cohérence	657
Créer une relation de protection SnapVault à partir de la vue Santé : Tous les volumes	658
Créer une relation de protection SnapVault à partir de la page Détails du volume/de l'état de santé ..	659
Créer une relation de protection SnapMirror à partir de la vue Santé : Tous les volumes	660
Créer une relation de protection SnapMirror à partir de la page Détails du volume/de l'état de santé ..	662
Créer une relation SnapMirror avec une réplication flexible en fonction des versions	663
Créer des relations SnapMirror avec une réplication flexible en fonction des versions avec option de sauvegarde	664
Configurer les paramètres d'efficacité de destination	665
Créer des planifications SnapMirror et SnapVault	666
Créer des relations en cascade ou en éventail pour étendre la protection à partir d'une relation de protection existante	666
Modifier les relations de protection à partir de la page Relations de volume	667
Modifier les relations de protection à partir de la page Détails du volume/de la santé	668
Créer une politique SnapMirror pour maximiser l'efficacité du transfert	668
Créer une politique SnapVault pour maximiser l'efficacité du transfert	669
Annuler un transfert de protection des données actif à partir de la page Relations de volume	669
Annuler un transfert de protection des données actif à partir de la page Détails du volume/de la santé	670
Suspendre une relation de protection à partir de la page Relations de volume	671
Suspendre une relation de protection à partir de la page de détails Volume/Santé	672
Rompre une relation SnapMirror à partir de la page Relations de volume	673
Supprimer une relation de protection de la page Relations de volume	673
Reprendre les transferts programmés sur une relation suspendue à partir de la page Relations de volume	674
Reprendre les transferts programmés sur une relation suspendue à partir de la page Détails du volume/de la santé	674
Initialiser ou mettre à jour les relations de protection à partir de la page Relations de volume	675
Initialiser ou mettre à jour les relations de protection à partir de la page Détails du volume/de la santé	676
Resynchroniser les relations de protection à partir de la page Relations de volume	677
Relations de protection inverse à partir de la page Relations de volume	678
Restaurer les données à l'aide des pages de détails Volume et Volume/Santé	679
Que sont les pools de ressources	680
Créer des pools de ressources	681
Modifier les pools de ressources	681
Afficher l'inventaire des pools de ressources	682
Ajouter des membres au pool de ressources	682
Supprimer les agrégats des pools de ressources	682
Supprimer les pools de ressources	683

Surveiller les relations de protection de reprise après sinistre des machines virtuelles de stockage . . .	683
Comprendre les associations de machines virtuelles de stockage	686
Exigences relatives aux SVM et aux pools de ressources pour prendre en charge les services de stockage	688
Quels sont les emplois	689
Surveiller les emplois	689
Voir les détails du poste	689
Abandonner les tâches	690
Réessayer une tâche de protection ayant échoué	690
Description des fenêtres et boîtes de dialogue des relations de protection	691
Générer des rapports personnalisés	734
Rapports du gestionnaire unifié	734
Points d'accès pour la génération de rapports	734
Comprendre les rapports	736
Comprendre la relation entre la vue et le rapport	736
Types de rapports	737
Limitations des rapports	739
Travailler avec des rapports	739
Flux de travail du rapport	739
Démarrage rapide des rapports	740
Rechercher un rapport planifié	743
Personnaliser les rapports	743
Télécharger les rapports	747
Rapports de planification	747
Planifier un rapport	748
Gérer les calendriers de rapports	750
Exemples de rapports personnalisés	752
Personnaliser les rapports de stockage en cluster	753
Personnaliser les rapports de capacité globale	756
Personnaliser les rapports de capacité de volume	758
Personnaliser les rapports de capacité Qtree	761
Personnaliser les rapports de partage NFS	762
Personnaliser les rapports de VM de stockage	764
Personnaliser les rapports de relation de volume	765
Personnaliser les rapports de performances de volume	769
Exemples de rapports Microsoft Excel	770
Créer un rapport pour afficher un tableau et un graphique de capacité globale	770
Créer un rapport pour afficher les graphiques de capacité totale agrégée par rapport à la capacité disponible	773
Créer un rapport pour afficher les graphiques de capacité de volume disponibles	776
Créer un rapport pour afficher les agrégats qui ont le plus d'IOPS disponibles	779
Gérer le stockage à l'aide des API REST	781
Démarrer avec les API REST Active IQ Unified Manager	781
Audience pour ce contenu	781
Accès et catégories de l'API Active IQ Unified Manager	781

Services REST proposés dans Active IQ Unified Manager	783
Version de l'API dans Active IQ Unified Manager	784
Ressources de stockage dans ONTAP	784
Accès et authentification de l'API REST dans Active IQ Unified Manager	785
Authentification	787
Codes d'état HTTP utilisés dans Active IQ Unified Manager	788
Recommandations d'utilisation des API pour Active IQ Unified Manager	789
Journaux de dépannage	790
Objets de travail processus asynchrones	790
Bonjour serveur API	791
API REST d'Unified Manager	795
Gérer les objets de stockage dans un centre de données à l'aide d'API	796
Accéder aux API ONTAP via un accès proxy	803
Effectuer des tâches administratives à l'aide d'API	806
Gérer les utilisateurs à l'aide des API	808
Afficher les indicateurs de performance à l'aide des API	809
Afficher les tâches et les détails du système	820
Gérer les événements et les alertes à l'aide d'API	821
Gérer les charges de travail à l'aide d'API	824
Flux de travail API courants pour la gestion du stockage	833
Comprendre les appels API utilisés dans les workflows	833
Déterminer les problèmes d'espace dans les agrégats à l'aide d'API	834
Déterminer les problèmes dans les objets de stockage à l'aide des API d'événements	836
Dépanner les volumes ONTAP à l'aide des API de passerelle	837
Workflows API pour la gestion de la charge de travail	841
Mentions légales	868
Copyright	868
Marques de commerce	868
Brevets	868
Politique de confidentialité	868
Open source	868

Documentation Active IQ Unified Manager

Notes de version

Fournit un résumé des nouvelles fonctionnalités, des limitations et des problèmes connus pour Active IQ Unified Manager 9.16.

Pour plus d'informations, consultez le ["Notes de version Active IQ Unified Manager"](#) .

Commencer

Instructions de démarrage rapide pour les installations VMware

Vous pouvez télécharger le .tar fichier contenant un certificat racine, un README fichier et un OVA fichier et déployez Unified Manager en tant qu'appliance virtuelle.

Configuration requise

- Système d'exploitation : VMware ESXi 8.0
- RAM : 12 Go
- CPU : 9572 MHz au total
- Espace disque disponible : 5 Go (provisionnement léger), 152 Go (provisionnement épais)

Pour connaître la configuration système requise détaillée, consultez le ["Conditions requises pour l'installation d'Unified Manager"](#) et ["Matrice d'interopérabilité"](#).

Installer Active IQ Unified Manager

Téléchargez le programme d'installation

1. Téléchargez le .tar fichier contenant un certificat racine, un README fichier et un OVA déposer.
2. Enregistrez le fichier dans un répertoire local ou un répertoire réseau accessible à votre client vSphere.
3. Dans le répertoire où vous avez téléchargé le .tar fichier, entrez le `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` commande. + Le requis OVA fichier, un certificat racine et un README les fichiers sont décompressés dans le répertoire cible.

Vérifier l'intégrité

Vous pouvez vérifier l'intégrité du OVA fichier en suivant les étapes fournies dans le README déposer.

Installer Unified Manager

1. Dans le client vSphere, cliquez sur **Fichier > Déployer le modèle OVF**.
2. Localisez le fichier OVA et utilisez l'assistant pour déployer l'appliance virtuelle sur le serveur ESXi.
3. Sur la page Détails de l'évaluation, dans la section Éditeur, le message Entrust Code Signing - OVCS2 (Trusted certificate) confirme l'intégrité du fichier téléchargé OVA déposer. Pour le message Entrust Code Signing - OVCS2 (Invalid certificate), mettez à niveau VMware vCenter Server vers la version 7.0U3E ou supérieure.
4. Sur la page Personnaliser le modèle, dans l'onglet Propriétés, renseignez les champs selon les besoins du type d'installation que vous effectuez :
 - Pour une configuration statique, saisissez les informations requises dans tous les champs. L'ajout d'informations pour le champ **DNS secondaire** n'est pas obligatoire.
 - Pour DHCP utilisant IPv4, n'ajoutez aucune information dans aucun champ.

- Pour DHCP utilisant IPv6, cochez la case « Activer l'adressage IPv6 automatique ». N'ajoutez aucune information dans aucun autre champ.

5. Allumez la VM.
6. Cliquez sur l'onglet Console pour afficher le processus de démarrage initial.
7. Configurer le fuseau horaire.
8. Saisissez un nom d'utilisateur et un mot de passe de maintenance Unified Manager.

À la fin de l'installation, les informations pour se connecter à l'interface Web d'Unified Manager s'affichent.

Instructions de démarrage rapide pour les installations Linux

Vous pouvez télécharger le package d'installation et installer Unified Manager sur une plate-forme Red Hat Enterprise Linux physique ou virtuelle.

Configuration requise

- Système d'exploitation : Red Hat Enterprise Linux versions 8.x et 9.4, basées sur l'architecture x86_64, installées à l'aide de l'environnement de base « Serveur avec interface graphique » de l'option **Sélection de logiciel** du programme d'installation du système d'exploitation.
- RAM : 12 Go, CPU : 9 572 MHz au total
- Espace disque libre : 100 Go d'espace disque dans le /opt/netapp/data répertoire, 50 Go dans la partition racine. Pour montage séparé /opt et /var/log répertoires, assurez-vous que /opt a 15 Go, /var/log dispose de 16 Go et /tmp dispose de 10 Go d'espace libre.

Pour connaître la configuration système requise détaillée et obtenir des informations sur l'installation du produit dans un site sécurisé, consultez le ["Conditions requises pour l'installation d'Unified Manager"](#) et le ["Matrice d'interopérabilité"](#).

Installer Active IQ Unified Manager

Téléchargez le programme d'installation

1. Téléchargez le ActiveIQUnifiedManager-`<version>`.zip package d'installation avec certificat de signature de code(.pem) et la signature numérique(.sig).
2. Dans le répertoire où vous avez téléchargé le fichier d'installation, exécutez :

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

Vérifier l'intégrité

Exécutez les commandes suivantes pour vérifier l'intégrité du package d'installation :

- Courir `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` pour créer un fichier avec la clé publique du certificat de signature de code.
- Courir `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` pour vérifier la signature

sur le package d'installation.

Vérifier la configuration du référentiel

Les procédures de configuration d'un référentiel Red Hat Enterprise Linux sont spécifiques au site. Vous pouvez utiliser le `pre_install_check.sh` script inclus dans le package d'installation pour vérifier la configuration de votre système d'exploitation. Si votre système est connecté à Internet, vous recevez automatiquement des instructions pour configurer le référentiel Red Hat Enterprise Linux.

```
# sudo ./pre_install_check.sh
```

Installer Unified Manager

Unified Manager utilise le `yum` utilitaire permettant d'installer le logiciel et tout logiciel dépendant. Étant donné qu'il existe différentes images de Red Hat Enterprise Linux, les packages installés dépendent des logiciels présents dans les images. Le `yum` L'utilitaire détermine les packages logiciels dépendants pour l'installation. Si vous avez besoin de plus d'informations sur les packages logiciels dépendants, consultez le ["Logiciels Linux et exigences d'installation"](#).

Pour installer Unified Manager, exécutez la commande suivante, soit en tant qu'utilisateur root, soit en utilisant `sudo`, à partir du répertoire où le fichier d'installation a été décompressé :

```
# yum install netapp-um<version>.x86_64.rpm
```

ou

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

À la fin de l'installation, les informations pour se connecter à l'interface Web d'Unified Manager s'affichent. Si vous ne parvenez pas à vous connecter à l'interface Web, reportez-vous à la `README` fichier fourni avec le logiciel pour plus d'informations sur les restrictions du port 443.

Instructions de démarrage rapide pour les installations Windows

Vous pouvez télécharger le package d'installation et installer Unified Manager pour surveiller et résoudre les problèmes de capacité de stockage des données, de disponibilité, de performances et de protection.

Configuration requise

- Systèmes d'exploitation
 - Microsoft Windows Server 2019 Édition Standard et Datacenter
 - Microsoft Windows Server 2022 Édition Standard et Datacenter

Unified Manager est pris en charge sur le système d'exploitation Windows 64 bits pour les langues suivantes :

- English
- japonais

- chinois simplifié
- RAM : 12 Go
- CPU : 9572 MHz au total
- Espace disque libre : 100 Go d'espace disque pour le répertoire d'installation, 50 Go d'espace disque pour le répertoire de données MySQL

Pour connaître la configuration système requise détaillée, consultez le ["Conditions requises pour l'installation d'Unified Manager"](#) et ["Matrice d'interopérabilité"](#) .

Installer Active IQ Unified Manager

Téléchargez le programme d'installation

1. Téléchargez le `ActiveIQUnifiedManager-<version>.exe` paquet d'installation.
2. Copiez le fichier d'installation dans un répertoire du système cible.

Installer Unified Manager

Pour installer Unified Manager, assurez-vous que Microsoft .NET 4.5.2 ou une version ultérieure est installé. Dans le cadre du processus d'installation, Unified Manager installe d'autres packages tiers selon les besoins. Pour plus d'informations sur les packages logiciels dépendants, reportez-vous au ["Logiciel Windows et configuration requise pour son installation"](#) .

1. Connectez-vous à Windows à l'aide du compte administrateur local par défaut.
2. Dans le répertoire où vous avez téléchargé le fichier d'installation, cliquez avec le bouton droit de la souris et exécutez le fichier exécutable Unified Manager (.exe) en tant qu'administrateur.
3. Lorsque vous y êtes invité, saisissez le nom d'utilisateur et le mot de passe pour créer l'utilisateur de maintenance Unified Manager.
4. Dans l'assistant de connexion à la base de données, entrez le mot de passe root MySQL.
5. Suivez les instructions restantes pour terminer l'installation.
6. Cliquez sur **Terminer** à la fin de l'installation et l'interface Web d'Unified Manager s'affiche.

Installer Unified Manager sur les systèmes VMware vSphere

Introduction à Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous permet de surveiller et de gérer l'état et les performances de vos systèmes de stockage ONTAP à partir d'une interface unique. Vous pouvez déployer Unified Manager sur un serveur Linux, sur un serveur Windows ou en tant qu'appliance virtuelle sur un hôte VMware.

Une fois l'installation terminée et les clusters que vous souhaitez gérer ajoutés, Unified Manager fournit une interface graphique qui affiche la capacité, la disponibilité, la protection et l'état des performances des systèmes de stockage surveillés.

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

À quoi sert le serveur Unified Manager

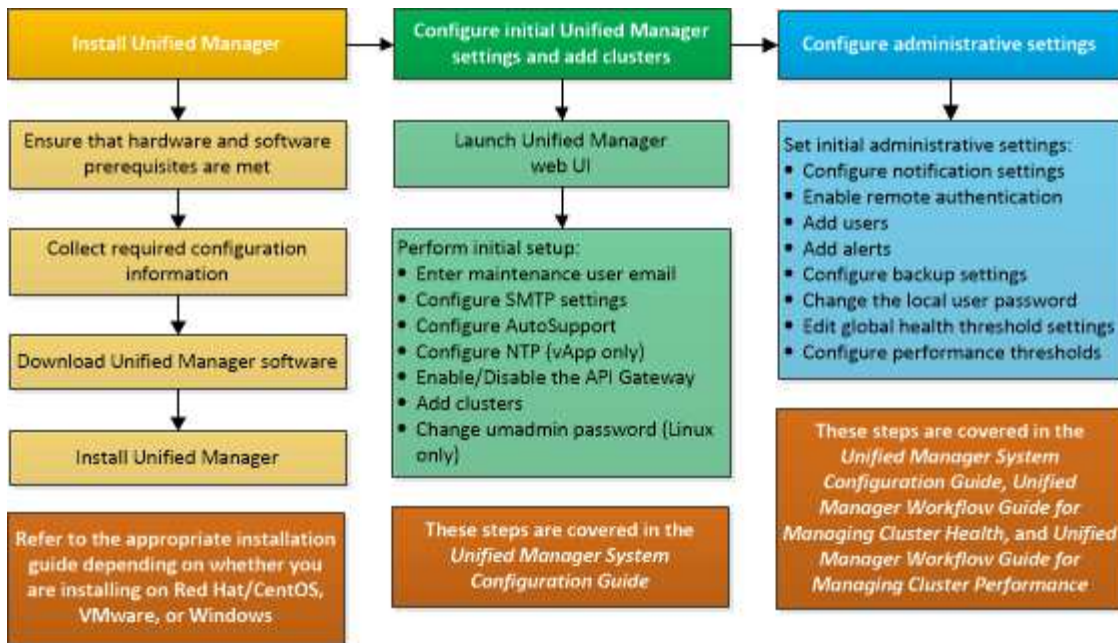
L'infrastructure du serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations du cluster, stocke les données dans la base de données et analyse les données pour voir s'il existe des problèmes de cluster.

Aperçu de la séquence d'installation

Le flux de travail d'installation décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.

Ces sections décrivent chacun des éléments affichés dans le flux de travail ci-dessous.



Conditions requises pour l'installation d'Unified Manager

Avant de commencer le processus d'installation, assurez-vous que le serveur sur lequel vous souhaitez installer Unified Manager répond aux exigences spécifiques en matière de logiciel, de matériel, de processeur et de mémoire.

NetApp ne prend en charge aucune modification du code d'application Unified Manager. Si vous devez appliquer des mesures de sécurité au serveur Unified Manager, vous devez apporter ces modifications au système d'exploitation sur lequel Unified Manager est installé.

Pour plus de détails sur l'application des mesures de sécurité au serveur Unified Manager, consultez l'article de la base de connaissances.

["Prise en charge des mesures de sécurité appliquées à Active IQ Unified Manager pour Clustered Data ONTAP"](#)

Informations connexes

Pour plus d'informations, voir ["Outil de matrice d'interopérabilité NetApp"](#)

Infrastructure virtuelle et exigences matérielles

L'installation d'Unified Manager sur une infrastructure virtuelle ou un système physique doit répondre aux exigences minimales en matière de mémoire, de processeur et d'espace disque.

Le tableau suivant affiche les valeurs recommandées pour les ressources de mémoire, de processeur et d'espace disque. Ces valeurs ont été qualifiées afin qu'Unified Manager atteigne des niveaux de performance acceptables.

Configuration matérielle	Paramètres recommandés
BÉLIER	12 Go (exigence minimale 8 Go)
Processeurs	4 processeurs
Capacité du cycle du processeur	9572 MHz au total (exigence minimale 9572 MHz)
Espace disque libre	• 5 Go (provisionnement léger) • 152 Go (provisionnement épais)

Unified Manager peut être installé sur des systèmes dotés d'une petite quantité de mémoire, mais les 12 Go de RAM recommandés garantissent que suffisamment de mémoire est disponible pour des performances optimales et que le système peut accueillir des clusters et des objets de stockage supplémentaires à mesure que votre configuration se développe. Vous ne devez définir aucune limite de mémoire sur la machine virtuelle sur laquelle Unified Manager est déployé et ne devez activer aucune fonctionnalité (par exemple, le gonflage) qui empêche le logiciel d'utiliser la mémoire allouée sur le système.

De plus, il existe une limite au nombre de nœuds qu'une seule instance d'Unified Manager peut surveiller avant d'installer une deuxième instance d'Unified Manager. Pour plus d'informations, voir ["Guide des meilleures pratiques d'Unified Manager"](#).

L'échange de pages mémoire a un impact négatif sur les performances du système et de l'application de gestion. La concurrence pour des ressources CPU qui ne sont pas disponibles en raison de l'utilisation globale de l'hôte peut dégrader les performances.

Exigence d'utilisation dédiée

Le système physique ou virtuel sur lequel vous installez Unified Manager doit être utilisé exclusivement pour Unified Manager et ne doit pas être partagé avec d'autres applications. D'autres applications peuvent consommer des ressources système et réduire considérablement les performances d'Unified Manager.

Besoins d'espace pour les sauvegardes

Si vous prévoyez d'utiliser la fonction de sauvegarde et de restauration d'Unified Manager, allouez une capacité supplémentaire afin que le répertoire ou le disque « data » dispose de 150 Go d'espace. Une sauvegarde peut être écrite vers une destination locale ou vers une destination distante. La meilleure pratique consiste à identifier un emplacement distant externe au système hôte Unified Manager disposant d'un minimum de 150 Go d'espace.

Exigences relatives à la connectivité de l'hôte

Le système physique ou le système virtuel sur lequel vous installez Unified Manager doit être configuré de manière à ce que vous puissiez réussir `ping` le nom de l'hôte de l'hôte lui-même. Dans le cas d'une configuration IPv6, vous devez vérifier que `ping6` au nom d'hôte est réussi pour garantir que l'installation d'Unified Manager réussit.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web du produit. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, vous devez obtenir le nom d'hôte à partir du DNS.

Si vous prévoyez d'autoriser les utilisateurs à accéder à Unified Manager en utilisant le nom court au lieu d'utiliser le nom de domaine complet (FQDN) ou l'adresse IP, votre configuration réseau doit résoudre ce nom court en un FQDN valide.

Configuration requise pour le logiciel et l'installation de VMware

Le système VMware vSphere sur lequel vous installez Unified Manager nécessite une version spécifique du système d'exploitation et des versions spécifiques du logiciel de support.

Logiciel du système d'exploitation

Le système d'exploitation pris en charge est VMware ESXi 8.0.



Unified Manager OVA sur les systèmes VMware vSphere exécute Debian OS 12 (bookworm) en interne. Pour plus d'informations sur les versions du matériel de machine virtuelle que les versions prises en charge des serveurs ESXi peuvent prendre en charge, reportez-vous à la documentation VMware.

Les versions suivantes de vSphere sont prises en charge :

- VMware vCenter Server 7.0 et 8.0

Consultez la matrice d'interopérabilité pour obtenir la liste complète et la plus récente des versions ESXi prises en charge.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

L'heure du serveur VMware ESXi doit être la même que l'heure du serveur NTP pour que le dispositif virtuel fonctionne correctement. La synchronisation de l'heure du serveur VMware ESXi avec l'heure du serveur NTP évite une panne de temps.

Conditions d'installation

VMware High Availability pour l'appliance virtuelle Unified Manager est pris en charge.

Si vous déployez une banque de données NFS sur un système de stockage exécutant le logiciel ONTAP , utilisez le plug-in NetApp NFS pour VMware VAAI pour utiliser le provisionnement statique.

Si le déploiement échoue dans votre environnement haute disponibilité en raison de ressources insuffisantes, vous devrez peut-être modifier les options de la machine virtuelle des fonctionnalités du cluster en désactivant la priorité de redémarrage de la machine virtuelle et en laissant la réponse d'isolement de l'hôte activée.



Lors de l'installation ou de la mise à niveau d'Unified Manager, les logiciels tiers et les correctifs de sécurité requis sont automatiquement installés ou mis à niveau sur un système VMware vSphere. Étant donné que les processus d'installation et de mise à niveau d'Unified Manager contrôlent ces composants, vous ne devez pas tenter une installation ou une mise à niveau autonome d'un composant tiers.

Navigateurs pris en charge

Pour accéder à l'interface Web d'Unified Manager, utilisez un navigateur pris en charge.

La matrice d'interopérabilité contient la liste des versions de navigateur prises en charge.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit que les fonctionnalités du logiciel s'affichent correctement.

Si vous prévoyez de configurer Unified Manager pour l'authentification SAML, afin qu'un fournisseur d'identité (IdP) puisse authentifier les utilisateurs, vous devez également vérifier la liste des navigateurs pris en charge par l'IdP.

Exigences relatives au protocole et au port

Les ports et protocoles requis permettent la communication entre le serveur Unified Manager et les systèmes de stockage gérés, les serveurs et d'autres composants.

Connexions au serveur Unified Manager

Dans les installations classiques, vous n'avez pas besoin de spécifier de numéros de port lors de la connexion à l'interface utilisateur Web d'Unified Manager, car les ports par défaut sont toujours utilisés. Par exemple, étant donné qu'Unified Manager tente toujours de s'exécuter sur son port par défaut, vous pouvez saisir `https://<host>` au lieu de `https://<host>:443`.

Le serveur Unified Manager utilise des protocoles spécifiques pour accéder aux interfaces suivantes :

Interface	Protocole	Port	Description
Interface utilisateur Web d'Unified Manager	HTTP	80	Utilisé pour accéder à l'interface Web d'Unified Manager ; redirige automatiquement vers le port sécurisé 443.
Interface utilisateur Web et programmes Unified Manager utilisant des API	HTTPS	443	Utilisé pour accéder en toute sécurité à l'interface utilisateur Web d'Unified Manager ou pour effectuer des appels API ; les appels API ne peuvent être effectués qu'à l'aide de HTTPS.
Console de maintenance	SSH/SFTP	22	Utilisé pour accéder à la console de maintenance et récupérer les bundles de support.
Ligne de commande Linux	SSH/SFTP	22	Utilisé pour accéder à la ligne de commande Red Hat Enterprise Linux et récupérer les bundles de support.

Interface	Protocole	Port	Description
Syslog	UDP	514	Utilisé pour accéder aux messages EMS basés sur un abonnement à partir des systèmes ONTAP et pour créer des événements basés sur les messages.
REPOS	HTTPS	9443	Utilisé pour accéder aux événements EMS basés sur l'API REST en temps réel à partir de systèmes ONTAP authentifiés.
base de données MySQL	MySQL	3306	Utilisé pour activer l'accès à OnCommand Workflow Automation et aux services API OnCommand à Unified Manager.
Courtier AMQP QPID	TCP/IP	56072	Utilisé pour la communication de messages internes.
Courtier AMQP QPID	WebSocket sur TCP	56080	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud).
Courtier AMQP QPID	WebSocket sur TCP	56443	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud). La communication sur ce port prend en charge le cryptage fourni par TLS ou SSL.



Le port par défaut pour MySQL, 3306, est limité uniquement à localhost lors de l'installation d'Unified Manager sur les systèmes VMware vSphere. Cela n'a aucun impact sur les scénarios de mise à niveau, où la configuration précédente est conservée. Cette configuration peut être modifiée et la connexion peut être rendue disponible à d'autres hôtes en utilisant le `Control access to MySQL port 3306` option sur la console de maintenance. Pour plus d'informations, voir "[Options de menu supplémentaires](#)". Les ports utilisés pour la communication HTTP et HTTPS (ports 80 et 443) peuvent être modifiés à l'aide de la console de maintenance Unified Manager. Pour plus d'informations, voir "[Menus de la console de maintenance](#)".

Connexions depuis le serveur Unified Manager

Vous devez configurer votre pare-feu pour ouvrir les ports qui permettent la communication entre le serveur Unified Manager et les systèmes de stockage gérés, les serveurs et d'autres composants. Si un port n'est pas ouvert, la communication échoue.

Selon votre environnement, vous pouvez choisir de modifier les ports et les protocoles utilisés par le serveur Unified Manager pour se connecter à des destinations spécifiques.

Le serveur Unified Manager se connecte à l'aide des protocoles et ports suivants aux systèmes de stockage gérés, aux serveurs et aux autres composants :

Destination	Protocole	Port	Description
Système de stockage	HTTPS	443/TCP	Utilisé pour surveiller et gérer les systèmes de stockage.  Si vous utilisez ce port ou tout autre port pour vous connecter au serveur VMware vCenter ou ESXi, assurez-vous que le port est disponible et peut être connecté sur un site sécurisé.
Système de stockage	NDMP	10 000/TCP	Utilisé pour certaines opérations de restauration d'instantanés.
Serveur AutoSupport	HTTPS	443	Utilisé pour envoyer des informations AutoSupport . Nécessite un accès Internet pour exécuter cette fonction.

Destination	Protocole	Port	Description
Serveur d'authentification	LDAP	389	Utilisé pour effectuer des demandes d'authentification et des demandes de recherche d'utilisateurs et de groupes.
LDAPS	636	Utilisé pour la communication LDAP sécurisée.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	Expéditeur de trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Utilisé pour envoyer des notifications d'alerte SNMP.	Serveur fournisseur de données externe
TCP	2003	Utilisé pour envoyer des données de performances à un fournisseur de données externe, tel que Graphite.	serveur NTP
NTP	123/UDP	Utilisé pour synchroniser l'heure sur le serveur Unified Manager avec un serveur de temps NTP externe. (Systèmes VMware uniquement)	Syslog

Complétez la feuille de travail

Avant d'installer et de configurer Unified Manager, vous devez disposer d'informations spécifiques sur votre environnement. Vous pouvez enregistrer les informations dans la feuille de travail.

Informations d'installation d'Unified Manager

Les détails requis pour installer Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Adresse IP du serveur ESXi	
Héberger un nom de domaine entièrement qualifié	

Système sur lequel le logiciel est déployé	Votre valeur
Adresse IP de l'hôte	
Masque de réseau	
Adresse IP de la passerelle	
Adresse DNS principale	
Adresse DNS secondaire	
Rechercher des domaines	
Nom d'utilisateur de maintenance	
Mot de passe de l'utilisateur de maintenance	

Informations de configuration d'Unified Manager

Les détails pour configurer Unified Manager après l'installation. Certaines valeurs sont facultatives selon votre configuration.

Paramètre	Votre valeur
Adresse e-mail de l'utilisateur de maintenance	
serveur NTP	
Nom d'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
Port SMTP	25 (valeur par défaut)
E-mail à partir duquel les notifications d'alerte sont envoyées	
Nom d'hôte ou adresse IP du serveur d'authentification	
Nom de l'administrateur Active Directory ou nom distinctif de liaison LDAP	

Paramètre	Votre valeur
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom distinctif de base du serveur d'authentification	
URL du fournisseur d'identité (IdP)	
Métadonnées du fournisseur d'identité (IdP)	
Adresses IP des hôtes de destination des interruptions SNMP	
Port SNMP	

Informations sur le cluster

Les détails des systèmes de stockage que vous gérez à l'aide d'Unified Manager.

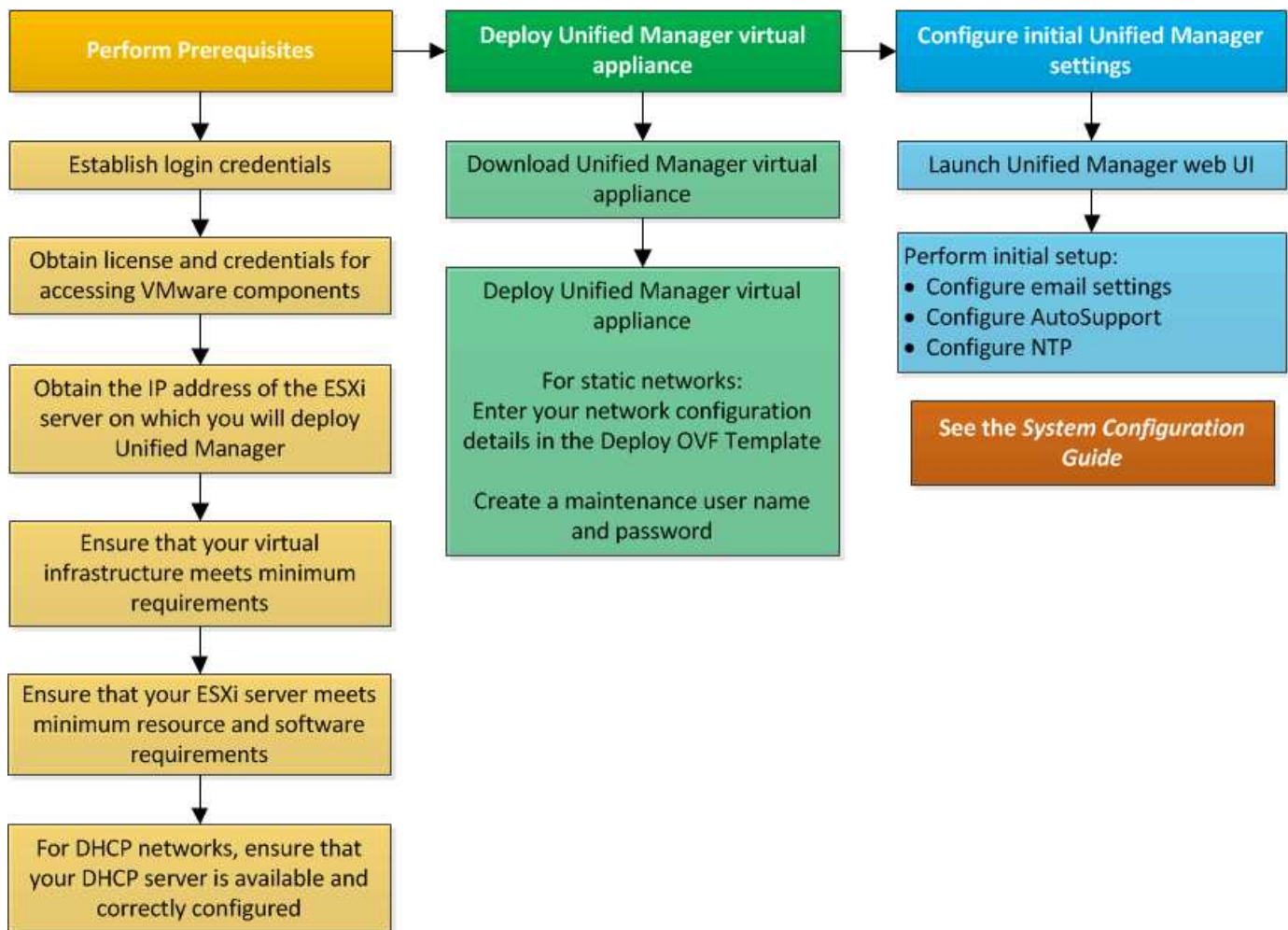
Groupe 1 de N	Votre valeur
Nom d'hôte ou adresse IP de gestion du cluster	
 L'administrateur doit avoir reçu le rôle « admin ».	
Mot de passe administrateur ONTAP	
Protocole	HTTPS

Installer, mettre à niveau et supprimer le logiciel Unified Manager

Sur les systèmes VMware vSphere, vous pouvez installer Unified Manager, effectuer une mise à niveau vers une version plus récente du logiciel ou supprimer l'appliance virtuelle Unified Manager (vApp).

Aperçu du processus de déploiement

Le flux de travail de déploiement décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.



Déployer Unified Manager

Le déploiement d'Unified Manager comprend le téléchargement du logiciel, le déploiement de l'appliance virtuelle, la création d'un nom d'utilisateur et d'un mot de passe de maintenance et l'exécution de la configuration initiale dans l'interface utilisateur Web.

Avant de commencer

- Vous devez vérifier et compléter la configuration système requise pour le déploiement.

Voir "[Configuration requise](#)".

- Assurez-vous d'avoir les informations suivantes :
 - Informations de connexion pour le site de support NetApp
 - Informations d'identification pour accéder à VMware vCenter Server et vSphere Web Client
 - Adresse IP du serveur ESXi sur lequel vous déployez l'appliance virtuelle Unified Manager
 - Détails sur le centre de données, tels que l'espace de stockage dans la banque de données et les besoins en mémoire
 - IPv6 doit être activé sur l'hôte si vous prévoyez d'utiliser l'adressage IPv6.

Vous pouvez déployer Unified Manager en tant qu'appliance virtuelle sur un serveur VMware ESXi.

Vous devez accéder à la console de maintenance en utilisant la console VMware et non en utilisant SSH.



À partir de Unified Manager 9.8, VMware Tools a été remplacé par Open VM Tools (`open-vm-tools`). Vous n'avez plus besoin d'installer VMware Tools dans le cadre de l'installation car `open-vm-tools` est inclus avec le package d'installation d'Unified Manager.

Une fois le déploiement et la configuration initiale terminés, vous pouvez soit ajouter des clusters, soit configurer des paramètres réseau supplémentaires dans la console de maintenance, puis accéder à l'interface utilisateur Web.

Étapes

1. Suivez les étapes dans "[Télécharger Unified Manager](#)".
2. De plus, suivez les étapes de "[Déployer l'appliance virtuelle Unified Manager](#)".

Téléchargez le fichier d'installation d'Unified Manager

Téléchargez le fichier d'installation d'Unified Manager à partir du site de support NetApp pour déployer Unified Manager en tant qu'appliance virtuelle.

Avant de commencer

Vous devez disposer des informations de connexion pour le site de support NetApp.

Le fichier d'installation est un `.tar` fichier contenant un certificat racine, un `README` fichier et un `OVA` fichier contenant le logiciel Unified Manager configuré pour une appliance virtuelle.

Étapes

1. Connectez-vous au site de support NetApp et accédez à la page de téléchargement d'Unified Manager :

"[Site de support NetApp](#)"
2. Sélectionnez la version requise d'Unified Manager et acceptez le contrat de licence utilisateur final (CLUF).
3. Téléchargez et enregistrez le `.tar` fichier pour l'installation de VMware vSphere dans un répertoire local ou un répertoire réseau accessible à votre client vSphere.
4. Vérifiez la somme de contrôle pour vous assurer que le logiciel a été téléchargé correctement.
5. Accédez au répertoire dans lequel vous avez téléchargé le `.tar` fichier et entrez la commande suivante dans votre fenêtre de terminal pour développer le bundle Unified Manager :

```
tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
```

Le requis `OVA` fichier, un certificat racine et un `README` les fichiers pour Unified Manager sont décompressés dans le répertoire cible.

6. Vérifier l'intégrité du `OVA` fichier en suivant les étapes fournies dans le `README` déposer.

Déployer l'appliance virtuelle Unified Manager

Après avoir téléchargé le fichier d'installation, vous déployez Unified Manager en tant qu'appliance virtuelle. Utilisez vSphere Web Client pour déployer l'appliance virtuelle sur

un serveur ESXi. Lorsque vous déployez l'appliance virtuelle, une machine virtuelle est créée.

Avant de commencer

Vous devriez revoir la configuration requise. Apportez les modifications nécessaires avant de déployer l'appliance virtuelle Unified Manager.

Voir ["Exigences en matière d'infrastructure virtuelle"](#) .

Voir ["Configuration requise pour le logiciel et l'installation de VMware"](#) .

Si vous utilisez le protocole DHCP (Dynamic Host Configuration Protocol), assurez-vous que le serveur DHCP est disponible et que les configurations de la carte réseau DHCP et de la machine virtuelle (VM) sont correctes. DHCP est configuré par défaut.

Si vous utilisez une configuration réseau statique, assurez-vous que l'adresse IP n'est pas dupliquée dans le même sous-réseau et que les entrées de serveur DNS appropriées ont été configurées.

Obtenez les informations suivantes avant de déployer l'appliance virtuelle :

- Informations d'identification pour accéder à VMware vCenter Server et vSphere Web Client
- Adresse IP du serveur ESXi sur lequel vous déployez l'appliance virtuelle Unified Manager
- Détails sur le centre de données, tels que la disponibilité de l'espace de stockage
- Si vous n'utilisez pas DHCP, obtenez les adresses IPv4 ou IPv6 des périphériques réseau auxquels vous prévoyez de vous connecter :
 - Nom de domaine entièrement qualifié (FQDN) de l'hébergeur
 - Adresse IP de l'hôte
 - Masque de réseau
 - Adresse IP de la passerelle par défaut
 - Adresses DNS primaires et secondaires
 - Rechercher des domaines

À partir de Unified Manager 9.8, VMware Tools a été remplacé par Open VM Tools (*open-vm-tools*). Vous n'avez pas besoin d'installer VMware Tools dans le cadre du processus d'installation car *open-vm-tools* est inclus avec le package d'installation d'Unified Manager.

Lorsque l'appliance virtuelle est déployée, un certificat auto-signé unique pour l'accès HTTPS est généré. Lorsque vous accédez à l'interface Web d'Unified Manager, vous pouvez voir un avertissement de navigateur concernant des certificats non approuvés.

VMware High Availability pour l'appliance virtuelle Unified Manager est pris en charge.

Étapes

1. Dans le client vSphere, cliquez sur **Fichier > Déployer le modèle OVF**.
2. Terminez l'assistant de déploiement du modèle OVF pour déployer l'appliance virtuelle Unified Manager.

Sur la page Détails de l'évaluation :

- Vérifiez les détails de la section Éditeur. Le message **Entrust Code Signing - OVCS2 (certificat de confiance)** confirme l'intégrité du fichier téléchargé OVA déposer. + Si vous voyez le message **Entrust**

Code Signing - OVCS2 (certificat non valide), mettez à niveau VMware vCenter Server vers la version 7.0U3E ou supérieure.

Sur la page Personnaliser le modèle :

- Laissez tous les champs vides lorsque vous utilisez l'adressage DHCP et IPv4.
 - Cochez la case « Activer l'adressage IPv6 automatique » et laissez tous les autres champs vides lorsque vous utilisez l'adressage DHCP et IPv6.
 - Si vous souhaitez utiliser une configuration réseau statique, vous pouvez remplir les champs de cette page et ces paramètres seront appliqués lors du déploiement. Assurez-vous que l'adresse IP est unique à l'hôte sur lequel elle est déployée, qu'elle n'est pas déjà utilisée et qu'elle dispose d'une entrée DNS valide.
3. Une fois l'appliance virtuelle Unified Manager déployée sur le serveur ESXi, mettez sous tension la machine virtuelle en cliquant avec le bouton droit sur la machine virtuelle, puis en sélectionnant **Mettre sous tension**.



Si l'opération de mise sous tension échoue en raison de ressources insuffisantes, ajoutez des ressources, puis réessayez l'installation.

4. Cliquez sur l'onglet **Console**.

Le processus de démarrage initial prend quelques minutes.

5. Pour configurer votre fuseau horaire, entrez votre zone géographique et votre ville ou région comme demandé dans la fenêtre de la console VM.

Toutes les informations de date affichées utilisent le fuseau horaire configuré pour Unified Manager, quel que soit le paramètre de fuseau horaire sur vos appareils gérés. Si vos systèmes de stockage et le serveur de gestion sont configurés avec le même serveur NTP, ils font référence au même instant dans le temps, même s'ils apparaissent différemment. Par exemple, si vous créez une copie instantanée à l'aide d'un périphérique configuré avec un fuseau horaire différent de celui du serveur de gestion, l'horodatage correspond à l'heure du serveur de gestion.

6. Si aucun service DHCP n'est disponible ou s'il y a une erreur dans les détails de la configuration du réseau statique, sélectionnez l'une des options suivantes :

Si vous utilisez...	Alors fais ceci...
DHCP	Sélectionnez Réessayer DHCP. Si vous prévoyez d'utiliser DHCP, vous devez vous assurer qu'il est correctement configuré. Si vous utilisez un réseau compatible DHCP, les entrées du nom de domaine complet et du serveur DNS sont automatiquement transmises à l'appliance virtuelle. Si DHCP n'est pas correctement configuré avec DNS, le nom d'hôte « UnifiedManager » est automatiquement attribué et associé au certificat de sécurité. Si vous n'avez pas configuré de réseau compatible DHCP, vous devez saisir manuellement les informations de configuration réseau.

Si vous utilisez...	Alors fais ceci...
Une configuration de réseau statique	a. Sélectionnez Entrez les détails de la configuration du réseau statique. Le processus de configuration prend quelques minutes. b. Confirmez les valeurs que vous avez saisies et sélectionnez Y.

7. À l'invite, entrez un nom d'utilisateur de maintenance, puis cliquez sur **Entrée**.

Le nom de l'utilisateur de maintenance doit commencer par une lettre de a à z, suivie de n'importe quelle combinaison de -, a à z ou 0 à 9.

8. À l'invite, entrez un mot de passe, puis cliquez sur **Entrée**.

La console VM affiche l'URL de l'interface utilisateur Web d'Unified Manager.

Vous pouvez accéder à l'interface utilisateur Web pour effectuer la configuration initiale d'Unified Manager, comme décrit dans le ["Configuration Active IQ Unified Manager"](#).

Mettre à niveau Unified Manager

Vous pouvez mettre à niveau Active IQ Unified Manager vers la version 9.16 à partir de la version 9.13 ou 9.14 uniquement.

Pendant le processus de mise à niveau, Unified Manager n'est pas disponible. Vous devez terminer toutes les opérations en cours avant de mettre à niveau Unified Manager.

Si Unified Manager est associé à une instance d' OnCommand Workflow Automation et que de nouvelles versions du logiciel sont disponibles pour les deux produits, vous devez déconnecter les deux produits, puis configurer une nouvelle connexion Workflow Automation après avoir effectué les mises à niveau. Si vous effectuez une mise à niveau vers un seul des produits, vous devez vous connecter à Workflow Automation après la mise à niveau et vérifier qu'il acquiert toujours des données à partir d'Unified Manager.

Étapes

1. Suivez les étapes dans ["Téléchargez l'image ISO d'Unified Manager"](#).
2. De plus, suivez les étapes décrites dans ["Mettre à niveau Unified Manager"](#).

Chemin de mise à niveau pris en charge pour les versions d'Unified Manager

Active IQ Unified Manager prend en charge un chemin de mise à niveau spécifique pour chaque version.

Toutes les versions d'Unified Manager ne peuvent pas effectuer une mise à niveau sur place vers des versions ultérieures. Les mises à niveau d'Unified Manager sont limitées à un modèle N-2, ce qui signifie qu'une mise à niveau ne peut être effectuée que dans les 2 prochaines versions sur toutes les plates-formes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.16 à partir d'Unified Manager 9.13 et 9.14 uniquement.

Si vous exécutez une version antérieure aux versions prises en charge, votre instance Unified Manager devra d'abord être mise à niveau vers l'une des versions prises en charge, puis mise à niveau vers la version actuelle.

Par exemple, si votre version installée est Unified Manager 9.9 et que vous souhaitez effectuer une mise à niveau vers Unified Manager 9.14, vous devez suivre une séquence de mises à niveau.

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.11 → 9.13
2. Mise à niveau 9.13 → 9.14
3. Mise à niveau 9.13 → 9.16
4. Mise à niveau 9.14 → 9.16

Pour plus d'informations sur la matrice de chemin de mise à niveau, consultez ceci ["article de la base de connaissances \(KB\)"](#) .

Téléchargez le fichier de mise à niveau d'Unified Manager

Avant de mettre à niveau Unified Manager, téléchargez le fichier de mise à niveau d'Unified Manager à partir du site de support NetApp .

Avant de commencer

Vous devez disposer des informations de connexion pour le site de support NetApp .

Étapes

1. Connectez-vous au site de support NetApp :

["Site de support NetApp"](#)

2. Accédez à la page de téléchargement pour mettre à niveau Unified Manager sur VMware vSphere.
3. Téléchargez le .iso image à mettre à niveau et enregistrez-la dans un répertoire local ou un répertoire réseau accessible à votre client vSphere.
4. Vérifiez la somme de contrôle pour vous assurer que le logiciel a été téléchargé correctement.

Mettre à niveau l'appliance virtuelle Unified Manager

Vous pouvez mettre à niveau l'appliance virtuelle Active IQ Unified Manager des versions 9.13 ou 9.14 vers la version 9.16.

Avant de commencer

Assurez-vous de ce qui suit :

- Vous avez téléchargé le fichier de mise à niveau, l'image ISO à partir du site de support NetApp .
- Le système sur lequel vous mettez à niveau Unified Manager répond aux exigences système et logicielles.

Voir ["Exigences en matière d'infrastructure virtuelle"](#) .

Voir ["Configuration requise pour le logiciel et l'installation de VMware"](#) .

- Pour les utilisateurs de vSphere 6.5 et versions ultérieures, vous avez installé la console distante VMware

(VMRC).

- Lors de la mise à niveau, vous serez peut-être invité à confirmer si vous souhaitez conserver les paramètres par défaut précédents pour la conservation des données de performances pendant 13 mois ou les modifier à 6 mois. Après confirmation, les données de performances historiques sont purgées après 6 mois.
- Vous disposez des informations suivantes :
 - Informations de connexion pour le site de support NetApp
 - Informations d'identification pour accéder à VMware vCenter Server et vSphere Web Client
 - Informations d'identification pour l'utilisateur de maintenance d'Unified Manager

Pendant le processus de mise à niveau, Unified Manager n'est pas disponible. Vous devez terminer toutes les opérations en cours avant de mettre à niveau Unified Manager.

Si vous avez associé Workflow Automation et Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans Workflow Automation.

Étapes

1. Dans le client vSphere, cliquez sur **Accueil > Inventaire > VM et modèles**.
2. Sélectionnez la machine virtuelle (VM) sur laquelle le dispositif virtuel Unified Manager est installé.
3. Si la machine virtuelle Unified Manager est en cours d'exécution, accédez à **Résumé > Commandes > Arrêter l'invité**.
4. Créez une copie de sauvegarde, telle qu'un instantané ou un clone, de la machine virtuelle Unified Manager pour créer une sauvegarde cohérente avec l'application.
5. Depuis le client vSphere, mettez sous tension la machine virtuelle Unified Manager.
6. Lancez la console distante VMware.
7. Cliquez sur l'icône **CDROM** et sélectionnez **Se connecter au fichier image disque (.iso)**.
8. Sélectionnez le `ActiveIQUnifiedManager-<version>-virtual-update.iso` fichier et cliquez sur **Ouvrir**.
9. Cliquez sur l'onglet **Console**.
10. Connectez-vous à la console de maintenance Unified Manager.
11. Dans le menu principal, sélectionnez **Mettre à niveau**.

Un message s'affiche indiquant qu'Unified Manager ne sera pas disponible pendant le processus de mise à niveau et qu'il reprendra une fois terminé.
12. Taper `y` pour continuer.

Un avertissement s'affiche, vous rappelant de sauvegarder la machine virtuelle sur laquelle réside l'appliance virtuelle.
13. Taper `y` pour continuer.

Le processus de mise à niveau et le redémarrage des services Unified Manager peuvent prendre plusieurs minutes.
14. Appuyez sur n'importe quelle touche pour continuer.

Vous êtes automatiquement déconnecté de la console de maintenance.

15. **Facultatif** : connectez-vous à la console de maintenance et vérifiez la version d'Unified Manager.

Vous pouvez lancer l'interface utilisateur Web dans une nouvelle fenêtre sur un navigateur Web pris en charge et vous connecter pour utiliser la version mise à niveau d'Unified Manager. Notez que vous devez attendre la fin du processus de découverte avant d'effectuer une tâche dans l'interface utilisateur.

Redémarrer la machine virtuelle Unified Manager

Vous pouvez redémarrer la machine virtuelle (VM) Unified Manager à partir de la console de maintenance. Vous devez redémarrer la machine virtuelle après avoir généré un nouveau certificat de sécurité ou s'il y a un problème avec la machine virtuelle.

Avant de commencer

- L'appareil virtuel doit être sous tension.
- Vous devez être connecté à la console de maintenance Unified Manager en tant qu'utilisateur de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere en utilisant l'option VMware **Redémarrer l'invité**. Se référer à "[l'applet de commande Restart-VMGuest dans la référence de l'applet de commande VMware vSphere PowerCLI de Broadcom](#)."

Étapes

1. Dans la console de maintenance, sélectionnez **Configuration système > Redémarrer la machine virtuelle**.
2. Démarrez l'interface Web d'Unified Manager à partir de votre navigateur et connectez-vous.

Supprimer Unified Manager

Vous pouvez désinstaller Unified Manager en supprimant la machine virtuelle (VM) sur laquelle le logiciel Unified Manager est installé.

Avant de commencer

- Vous devez disposer des informations d'identification pour accéder à VMware vCenter Server et vSphere Web Client.
- Toute connexion active du serveur Unified Manager à un serveur Workflow Automation doit être fermée.
- Tous les clusters (sources de données) doivent être supprimés du serveur Unified Manager avant de supprimer la machine virtuelle (VM).

Étapes

1. Utilisez la console de maintenance Unified Manager pour vérifier que le serveur Unified Manager ne dispose pas d'une connexion active à un fournisseur de données externe.
2. Dans le client vSphere, cliquez sur **Accueil > Inventaire > VM et modèles**.
3. Sélectionnez la machine virtuelle que vous souhaitez supprimer et cliquez sur l'onglet **Résumé**.
4. Si la machine virtuelle est en cours d'exécution, cliquez sur **Alimentation > Arrêter l'invité**.
5. Cliquez avec le bouton droit sur la machine virtuelle que vous souhaitez supprimer, puis cliquez sur **Supprimer du disque**.

Installer Unified Manager sur les systèmes Linux

Introduction à Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous permet de surveiller et de gérer l'état et les performances de vos systèmes de stockage ONTAP à partir d'une interface unique. Vous pouvez déployer Unified Manager sur un serveur Linux, sur un serveur Windows ou en tant qu'appliance virtuelle (vApp) sur un hôte VMware.

Une fois l'installation terminée et les clusters que vous souhaitez gérer ajoutés, Unified Manager fournit une interface graphique qui affiche la capacité, la disponibilité, la protection et l'état des performances des systèmes de stockage surveillés.

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

À quoi sert le serveur Unified Manager

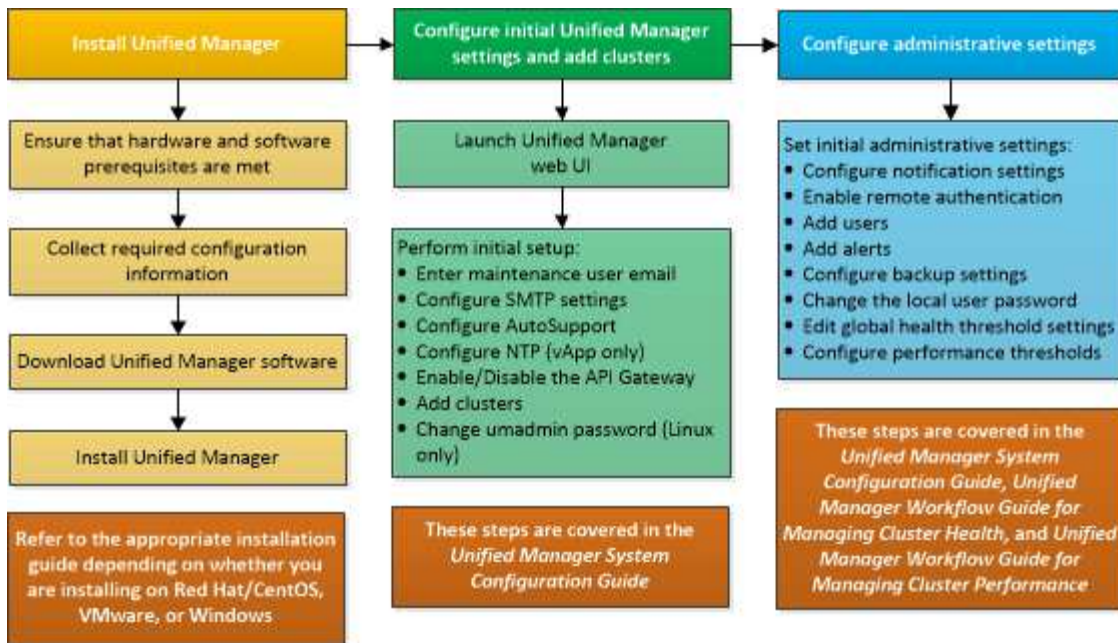
L'infrastructure du serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations du cluster, stocke les données dans la base de données et analyse les données pour voir s'il existe des problèmes de cluster.

Aperçu de la séquence d'installation

Le flux de travail d'installation décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.

Ces sections décrivent chacun des éléments affichés dans le flux de travail ci-dessous.



Conditions requises pour l'installation d'Unified Manager

Avant de commencer le processus d'installation, assurez-vous que le serveur sur lequel vous souhaitez installer Unified Manager répond aux exigences spécifiques en matière de logiciel, de matériel, de processeur et de mémoire.

NetApp ne prend en charge aucune modification du code d'application Unified Manager. Si vous devez appliquer des mesures de sécurité au serveur Unified Manager, vous devez apporter ces modifications au système d'exploitation sur lequel Unified Manager est installé.

Pour plus de détails sur l'application des mesures de sécurité au serveur Unified Manager, consultez l'article de la base de connaissances.

["Prise en charge des mesures de sécurité appliquées à Active IQ Unified Manager pour Clustered Data ONTAP"](#)

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

Infrastructure virtuelle et exigences matérielles

L'installation d'Unified Manager sur une infrastructure virtuelle ou un système physique doit répondre aux exigences minimales en matière de mémoire, de processeur et d'espace disque.

Le tableau suivant affiche les valeurs recommandées pour les ressources de mémoire, de processeur et d'espace disque. Ces valeurs ont été qualifiées afin qu'Unified Manager atteigne des niveaux de performance acceptables.

Configuration matérielle	Paramètres recommandés
BÉLIER	12 Go (exigence minimale 8 Go)
Processeurs	4 processeurs
Capacité du cycle du processeur	9572 MHz au total (exigence minimale 9572 MHz)
Espace disque libre	150 Go, où la capacité est répartie comme suit : • 50 Go alloués à la partition racine • 100 Go d'espace disque libre alloués au <code>/opt/netapp/data</code> répertoire, qui est monté sur un lecteur LVM ou sur un disque local distinct connecté au système cible  Pour montage séparé <code>/opt</code> et <code>/var/log</code> répertoires, assurez-vous que <code>/opt</code> a 15 Go et <code>/var/log</code> dispose de 16 Go d'espace libre. Le <code>/tmp</code> le répertoire doit avoir au moins 10 Go d'espace libre.

Unified Manager peut être installé sur des systèmes dotés d'une petite quantité de mémoire, mais les 12 Go de RAM recommandés garantissent que suffisamment de mémoire est disponible pour des performances optimales et que le système peut accueillir des clusters et des objets de stockage supplémentaires à mesure que votre configuration se développe. Vous ne devez définir aucune limite de mémoire sur la machine virtuelle sur laquelle Unified Manager est déployé et ne devez activer aucune fonctionnalité (par exemple, le gonflage) qui empêche le logiciel d'utiliser la mémoire allouée sur le système.

De plus, il existe une limite au nombre de nœuds qu'une seule instance d'Unified Manager peut surveiller avant d'installer une deuxième instance d'Unified Manager. Pour plus d'informations, consultez le *Guide des meilleures pratiques*.

["Rapport technique 4621 : Guide des meilleures pratiques pour Unified Manager"](#)

L'échange de pages mémoire a un impact négatif sur les performances du système et de l'application de gestion. La concurrence pour des ressources CPU qui ne sont pas disponibles en raison de l'utilisation globale de l'hôte peut dégrader les performances.

Exigence d'utilisation dédiée

Le système physique ou virtuel sur lequel vous installez Unified Manager doit être utilisé exclusivement pour Unified Manager et ne doit pas être partagé avec d'autres applications. D'autres applications peuvent consommer des ressources système et réduire considérablement les performances d'Unified Manager.

Besoins d'espace pour les sauvegardes

Si vous prévoyez d'utiliser la fonction de sauvegarde et de restauration d'Unified Manager, allouez une capacité supplémentaire afin que le répertoire ou le disque « data » dispose de 150 Go d'espace. Une sauvegarde peut être écrite vers une destination locale ou vers une destination distante. La meilleure pratique

consiste à identifier un emplacement distant externe au système hôte Unified Manager disposant d'un minimum de 150 Go d'espace.

Exigences relatives à la connectivité de l'hôte

Le système physique ou le système virtuel sur lequel vous installez Unified Manager doit être configuré de manière à ce que vous puissiez réussir `ping` le nom de l'hôte de l'hôte lui-même. Dans le cas d'une configuration IPv6, vous devez vérifier que `ping6` au nom d'hôte est réussi pour garantir que l'installation d'Unified Manager réussit.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web du produit. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, vous devez obtenir le nom d'hôte à partir du DNS.

Si vous prévoyez d'autoriser les utilisateurs à accéder à Unified Manager en utilisant le nom court au lieu d'utiliser le nom de domaine complet (FQDN) ou l'adresse IP, votre configuration réseau doit résoudre ce nom court en un FQDN valide.

Logiciels Linux et exigences d'installation

Le système Linux sur lequel vous installez Unified Manager nécessite des versions spécifiques du système d'exploitation et des logiciels de support.

Logiciel du système d'exploitation

Le système Linux doit avoir les versions suivantes du système d'exploitation et des logiciels de support installés :

- Red Hat Enterprise Linux versions 8.x et 9.4, basées sur l'architecture x86_64.

Consultez la matrice d'interopérabilité pour obtenir la liste complète et la plus récente des versions de Red Hat Enterprise Linux prises en charge.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

Le serveur doit être dédié à l'exécution d'Unified Manager. Aucune autre application ne doit être installée sur le serveur. Il est possible qu'un scanner de vulnérabilité comme Qualys soit installé sur votre système Linux en raison des réglementations de l'entreprise. Vous devez désactiver le scanner de vulnérabilité avant d'installer Unified Manager pour éviter l'échec de l'installation.



Les scanners de vulnérabilité (tels que Qualys) peuvent entraîner une utilisation élevée du processeur lors de l'analyse de la machine virtuelle (VM) soit en interne (lorsque Unified Manager et le scanner de vulnérabilité sont installés sur la même VM) soit en externe (lorsque Unified Manager et le scanner de vulnérabilité sont installés sur deux serveurs différents et le scanner de vulnérabilité analyse la VM sur laquelle Unified Manager est installé). Ce problème entraîne souvent une absence de réponse de la machine virtuelle et affecte les services Unified Manager. Par conséquent, NetApp recommande de désactiver le scanner de vulnérabilité dans la machine virtuelle sur laquelle Unified Manager est installé. Si la désactivation du scanner n'est pas une option, analysez la machine virtuelle en dehors des heures ouvrables et redémarrez les services une fois l'analyse terminée.

Logiciels tiers

Unified Manager est déployé sur un serveur Web WildFly. WildFly 26.1.3 est fourni et configuré avec Unified Manager.

Les packages tiers suivants sont requis, mais ne sont pas inclus avec Unified Manager. Ces packages sont automatiquement installés par le `yum` installateur lors de l'installation, à condition que vous ayez configuré les référentiels comme mentionné dans les sections suivantes.

- MySQL Community Edition version 8.4.4 (à partir du référentiel MySQL)
- OpenJDK version 11.0.25 (à partir du référentiel Red Hat Extra Enterprise Linux Server)
- Python 3.9.x (à partir du référentiel Red Hat Extra Enterprise Linux Server)
- p7zip version 16.02 ou ultérieure (à partir du référentiel Red Hat Extra Packages pour Enterprise Linux)



Vous devez arrêter une instance en cours d'exécution d'Unified Manager avant de mettre à niveau un logiciel tiers. Une fois l'installation du logiciel tiers terminée, vous pouvez redémarrer Unified Manager.

Exigences d'autorisation de l'utilisateur

L'installation d'Unified Manager sur un système Linux peut être effectuée par l'utilisateur root ou par des utilisateurs non root à l'aide de l' `sudo` commande.

De plus, l'installation par défaut d'Unified Manager inclut l'utilisateur `umadmin` (utilisateur de maintenance par défaut) et l'utilisateur `jboss` dans les fichiers `sudoers` (`ocum_sudoers` et `ocie_sudoers`) dans le `/etc/sudoers.d/` annuaire. Si vous supprimez ce contenu de votre environnement en raison de politiques de sécurité ou d'un outil de surveillance de sécurité, vous devez le rajouter. Vous devez conserver la configuration `sudoers` car certaines opérations Unified Manager nécessitent ces privilèges `sudo`.

Conditions d'installation

Les meilleures pratiques pour l'installation de Red Hat Enterprise Linux et des référentiels associés sur votre système sont répertoriées ci-dessous. Les systèmes installés ou configurés différemment, ou déployés hors site (dans le cloud), peuvent nécessiter des étapes supplémentaires et Unified Manager peut ne pas fonctionner correctement dans de tels déploiements.

- Vous devez installer Red Hat Enterprise Linux conformément aux meilleures pratiques de Red Hat et sélectionner les options par défaut suivantes, ce qui nécessite de sélectionner l'environnement de base « Serveur avec interface graphique ».
- Lors de l'installation d'Unified Manager sur Red Hat Enterprise Linux, le système doit avoir accès au référentiel approprié afin que le programme d'installation puisse accéder et installer toutes les dépendances logicielles requises.
- Pour le `yum` Pour rechercher les logiciels dépendants dans les référentiels Red Hat Enterprise Linux, vous devez avoir enregistré le système lors de l'installation de Red Hat Enterprise Linux ou ultérieurement en utilisant un abonnement Red Hat valide.

Consultez la documentation Red Hat pour plus d'informations sur Red Hat Subscription Manager.

- Vous devez activer le référentiel Extra Packages for Enterprise Linux (EPEL) pour installer avec succès les utilitaires tiers requis sur votre système.

Si le référentiel EPEL n'est pas configuré sur votre système, vous devez télécharger et configurer

manuellement le référentiel.

Voir ["Configuration manuelle du référentiel EPEL"](#) .

- Si la version correcte de MySQL n'est pas installée, vous devez activer le référentiel MySQL pour installer avec succès le logiciel MySQL sur votre système.

Si le référentiel MySQL n'est pas configuré sur votre système, vous devez télécharger et configurer manuellement le référentiel.

Voir ["Configuration manuelle du référentiel MySQL"](#) .

- Vous ne devez installer qu'une seule version de Java sur votre hôte Unified Manager ; sinon, le système risque de ne pas être en mesure de déterminer quelle version utiliser. Voir ["Après la mise à jour de Java sur l'hôte Active IQ Unified Manager , les services ne démarrent pas"](#) .

Si votre système n'a pas accès à Internet et que les référentiels ne sont pas mis en miroir d'un système connecté à Internet vers un système non connecté, vous devez suivre les instructions d'installation pour déterminer les dépendances logicielles externes de votre système. Vous pouvez ensuite télécharger le logiciel requis sur le système connecté à Internet et copier le `.rpm` fichiers sur le système sur lequel vous prévoyez d'installer Unified Manager. Pour télécharger les artefacts et les packages, vous devez utiliser le `yum install` commande. Vous devez vous assurer que les deux systèmes exécutent la même version du système d'exploitation et que la licence d'abonnement correspond à la version Red Hat Enterprise Linux appropriée.



Vous ne devez pas installer le logiciel tiers requis à partir de référentiels autres que ceux répertoriés ici. Les logiciels installés à partir des référentiels Red Hat sont conçus explicitement pour Red Hat Enterprise Linux et sont conformes aux meilleures pratiques de Red Hat (dispositions de répertoires, autorisations, etc.). Les logiciels provenant d'autres emplacements peuvent ne pas suivre ces directives, ce qui peut entraîner l'échec de l'installation d'Unified Manager ou entraîner des problèmes lors des mises à niveau futures.

Exigence du port 443

Les images génériques de Red Hat Enterprise Linux peuvent bloquer l'accès externe au port 443. En raison de cette restriction, vous ne pourrez peut-être pas vous connecter à l'interface Web de l'administrateur après l'installation d'Unified Manager. L'exécution de la commande suivante permet d'accéder au port 443 pour tous les utilisateurs et applications externes sur un Red Hat Enterprise Linux générique.

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd --reload
```

Vous devez installer Red Hat Enterprise Linux avec l'environnement de base « Serveur avec interface graphique ». Il fournit les commandes utilisées par les instructions d'installation de Unified Manager. D'autres environnements de base peuvent nécessiter l'installation de commandes supplémentaires pour valider ou terminer l'installation. Si le `firewall-cmd` n'est pas disponible sur votre système, vous devez l'installer en exécutant la commande suivante :

```
# sudo yum install firewalld
```

Contactez votre service informatique avant d'exécuter les commandes pour voir si vos politiques de sécurité nécessitent une procédure différente.



THP (Transparent Huge Pages) doit être désactivé sur les systèmes Red Hat. Lorsqu'elle est activée, elle peut dans certains cas entraîner l'arrêt d'Unified Manager lorsque certains processus consomment trop de mémoire et sont interrompus.

Navigateurs pris en charge

Pour accéder à l'interface Web d'Unified Manager, utilisez un navigateur pris en charge.

La matrice d'interopérabilité contient la liste des versions de navigateur prises en charge.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit que les fonctionnalités du logiciel s'affichent correctement.

Si vous prévoyez de configurer Unified Manager pour l'authentification SAML, afin qu'un fournisseur d'identité (IdP) puisse authentifier les utilisateurs, vous devez également vérifier la liste des navigateurs pris en charge par l'IdP.

Exigences relatives au protocole et au port

Les ports et protocoles requis permettent la communication entre le serveur Unified Manager et les systèmes de stockage gérés, les serveurs et d'autres composants.

Connexions au serveur Unified Manager

Dans les installations classiques, vous n'avez pas besoin de spécifier de numéros de port lors de la connexion à l'interface utilisateur Web d'Unified Manager, car les ports par défaut sont toujours utilisés. Par exemple, étant donné qu'Unified Manager tente toujours de s'exécuter sur son port par défaut, vous pouvez saisir `https://<host>` au lieu de `https://<host>:443`.

Le serveur Unified Manager utilise des protocoles spécifiques pour accéder aux interfaces suivantes :

Interface	Protocole	Port	Description
Interface utilisateur Web d'Unified Manager	HTTP	80	Utilisé pour accéder à l'interface Web d'Unified Manager ; redirige automatiquement vers le port sécurisé 443.
Interface utilisateur Web et programmes Unified Manager utilisant des API	HTTPS	443	Utilisé pour accéder en toute sécurité à l'interface utilisateur Web d'Unified Manager ou pour effectuer des appels API ; les appels API ne peuvent être effectués qu'à l'aide de HTTPS.

Interface	Protocole	Port	Description
Console de maintenance	SSH/SFTP	22	Utilisé pour accéder à la console de maintenance et récupérer les bundles de support.
Ligne de commande Linux	SSH/SFTP	22	Utilisé pour accéder à la ligne de commande Red Hat Enterprise Linux et récupérer les bundles de support.
base de données MySQL	MySQL	3306	Utilisé pour activer l'accès à OnCommand Workflow Automation et aux services API OnCommand à Unified Manager.
Syslog	UDP	514	Utilisé pour accéder aux messages EMS basés sur un abonnement à partir des systèmes ONTAP et pour créer des événements basés sur les messages.
REPOS	HTTPS	9443	Utilisé pour accéder aux événements EMS basés sur l'API REST en temps réel à partir de systèmes ONTAP authentifiés.
base de données MySQL	MySQL	3306	Utilisé pour activer l'accès à OnCommand Workflow Automation et aux services API OnCommand à Unified Manager.
Courtier AMQP QPID	TCP/IP	56072	Utilisé pour la communication de messages internes.
Courtier AMQP QPID	WebSocket sur TCP	56080	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud).

Interface	Protocole	Port	Description
Courtier AMQP QPID	WebSocket sur TCP	56443	Utilisé pour écouter sur ce port les messages reçus d'ONTAP (agent cloud). La communication sur ce port prend en charge le cryptage fourni par TLS ou SSL.



Le port par défaut pour MySQL, 3306, est limité uniquement à localhost lors de l'installation d'Unified Manager sur les systèmes Linux. Cela n'a aucun impact sur les scénarios de mise à niveau, où la configuration précédente est conservée. Cette configuration peut être modifiée et la connexion peut être rendue disponible à d'autres hôtes en utilisant le `Control access to MySQL port 3306` option sur la console de maintenance. Pour plus d'informations, voir "[Options de menu supplémentaires](#)". Les ports utilisés pour la communication HTTP et HTTPS (ports 80 et 443) peuvent être modifiés à l'aide de la console de maintenance Unified Manager. Pour plus d'informations, voir "[Menus de la console de maintenance](#)".

Connexions depuis le serveur Unified Manager

Vous devez configurer votre pare-feu pour ouvrir les ports qui permettent la communication entre le serveur Unified Manager et les systèmes de stockage gérés, les serveurs et d'autres composants. Si un port n'est pas ouvert, la communication échoue.

Selon votre environnement, vous pouvez choisir de modifier les ports et les protocoles utilisés par le serveur Unified Manager pour se connecter à des destinations spécifiques.

Le serveur Unified Manager se connecte à l'aide des protocoles et ports suivants aux systèmes de stockage gérés, aux serveurs et aux autres composants :

Destination	Protocole	Port	Description
Système de stockage	HTTPS	443/TCP	Utilisé pour surveiller et gérer les systèmes de stockage.
Système de stockage	NDMP	10 000/TCP	Utilisé pour certaines opérations de restauration d'instantanés.
Serveur AutoSupport	HTTPS	443	Utilisé pour envoyer des informations AutoSupport . Nécessite un accès Internet pour exécuter cette fonction.

Destination	Protocole	Port	Description
Serveur d'authentification	LDAP	389	Utilisé pour effectuer des demandes d'authentification et des demandes de recherche d'utilisateurs et de groupes.
LDAPS	636	Utilisé pour la communication LDAP sécurisée.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	Expéditeur de trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Utilisé pour envoyer des notifications d'alerte SNMP.	Serveur fournisseur de données externe
TCP	2003	Utilisé pour envoyer des données de performances à un fournisseur de données externe, tel que Graphite.	serveur NTP
NTP	123/UDP	Utilisé pour synchroniser l'heure sur le serveur Unified Manager avec un serveur de temps NTP externe. (Systèmes VMware uniquement)	Syslog

Complétez la feuille de travail

Avant d'installer et de configurer Unified Manager, vous devez disposer d'informations spécifiques sur votre environnement. Vous pouvez enregistrer les informations dans la feuille de travail.

Informations d'installation d'Unified Manager

Les détails requis pour installer Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Héberger un nom de domaine entièrement qualifié	
Adresse IP de l'hôte	

Système sur lequel le logiciel est déployé	Votre valeur
Masque de réseau	
Adresse IP de la passerelle	
Adresse DNS principale	
Adresse DNS secondaire	
Rechercher des domaines	
Nom d'utilisateur de maintenance	
Mot de passe de l'utilisateur de maintenance	

Informations de configuration d'Unified Manager

Les détails pour configurer Unified Manager après l'installation. Certaines valeurs sont facultatives selon votre configuration.

Paramètre	Votre valeur
Adresse e-mail de l'utilisateur de maintenance	
Nom d'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
Port SMTP	25 (valeur par défaut)
E-mail à partir duquel les notifications d'alerte sont envoyées	
Nom d'hôte ou adresse IP du serveur d'authentification	
Nom de l'administrateur Active Directory ou nom distinctif de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom distinctif de base du serveur d'authentification	

Paramètre	Votre valeur
URL du fournisseur d'identité (IdP)	
Métadonnées du fournisseur d'identité (IdP)	
Adresses IP des hôtes de destination des interruptions SNMP	
Port SNMP	

Informations sur le cluster

Les détails des systèmes de stockage que vous gérez à l'aide d'Unified Manager.

Groupe 1 de N	Votre valeur
Nom d'hôte ou adresse IP de gestion du cluster	
 L'administrateur doit avoir reçu le rôle « admin ». Nom d'utilisateur de l'administrateur ONTAP	
Mot de passe administrateur ONTAP	
Protocole	HTTPS

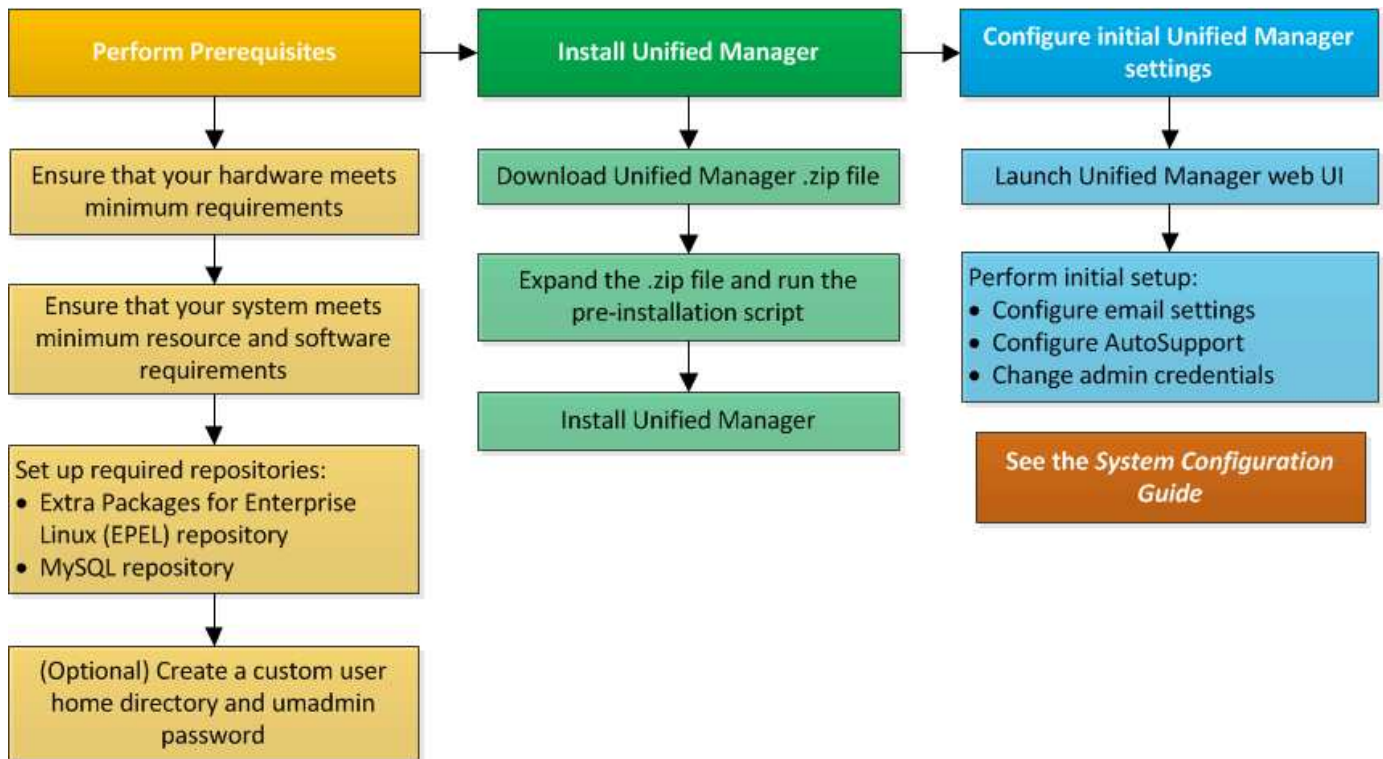
Installer, mettre à niveau et supprimer le logiciel Unified Manager

Sur les systèmes Linux, vous pouvez installer le logiciel Unified Manager, effectuer une mise à niveau vers une version plus récente du logiciel ou supprimer Unified Manager.

Unified Manager peut être installé sur les serveurs Red Hat Enterprise Linux. Le serveur Linux sur lequel vous installez Unified Manager peut être exécuté sur une machine physique ou sur une machine virtuelle exécutée sur VMware ESXi, Microsoft Hyper-V ou Citrix XenServer.

Aperçu du processus d'installation

Le flux de travail d'installation décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.



Configurer les référentiels de logiciels requis

Le système doit avoir accès à certains référentiels afin que le programme d'installation puisse accéder et installer toutes les dépendances logicielles requises.

Configurer manuellement le référentiel EPEL

Si le système sur lequel vous installez Unified Manager n'a pas accès au référentiel Extra Packages for Enterprise Linux (EPEL), vous devez télécharger et configurer manuellement le référentiel pour une installation réussie.

Le référentiel EPEL donne accès aux utilitaires tiers requis qui doivent être installés sur votre système. Vous utilisez le référentiel EPEL pour installer Unified Manager sur un système Red Hat Enterprise Linux.

Étapes

1. Téléchargez le référentiel EPEL pour votre installation. Pour la version 8, téléchargez-la depuis :

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

Pour la version 9, téléchargez-la depuis :

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

2. Configurer le référentiel EPEL :

```
yum install epel-release-latest-<version>.noarch.rpm
```

Pour les systèmes Red Hat Enterprise Linux 8, si vous disposez de référentiels internes avec des packages RPM modulaires, par exemple, `javapackages-filesystem-<version>.module.rpm`, assurez-vous

que les métadonnées des packages modulaires sont également disponibles dans le même référentiel.

Configurer manuellement le référentiel MySQL

Si le système sur lequel vous installez Unified Manager n'a pas accès au référentiel MySQL Community Edition, vous devez télécharger et configurer manuellement le référentiel pour une installation réussie.

Le référentiel MySQL donne accès au logiciel MySQL requis qui doit être installé sur votre système.



Cette tâche peut échouer si le système ne dispose pas de connectivité Internet. Reportez-vous à la documentation MySQL si le système sur lequel vous installez Unified Manager ne dispose pas d'accès Internet.

Étapes

1. Téléchargez le référentiel MySQL approprié pour votre installation. Pour la version 8, téléchargez-la depuis :

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/8/x86_64/mysql84-community-release-el8-1.noarch.rpm
```

Pour la version 9, téléchargez-la depuis :

```
wget http://repo.mysql.com/yum/mysql-8.4-community/el/9/x86_64/mysql84-community-release-el9-1.noarch.rpm
```

2. Configurer le référentiel MySQL :

```
yum install mysql84-community-release-.noarch.rpm
```

Pour le système Red Hat Enterprise Linux 8, si vous disposez de référentiels internes avec java-11-openjdk, p7zip et d'autres packages logiciels fournis par le référentiel AppStream, vous devez désactiver votre référentiel AppStream et installer MySQL Community Server. Exécutez la commande suivante :

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install mysql-community-server
```

Si vous recevez une erreur concernant une clé manquante ou une non-concordance de clé et que votre installation échoue, essayez ces étapes :

- Sur un système connecté, importez la clé MySQL mise à jour en exécutant la commande suivante :

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```

- Sur un système qui ne dispose pas de connectivité Internet, mettez à jour votre fichier de dépôt MySQL et désactivez `gpgcheck` en marquant `gpgcheck=0`.

Exigences SELinux sur les partages NFS et CIFS

Si vous envisagez de monter `/opt/netapp` ou `/opt/netapp/data` sur un périphérique NAS ou SAN, et que vous avez activé SELinux, vous devez tenir compte de quelques considérations.

Si vous envisagez de monter `/opt/netapp` ou `/opt/netapp/data` à partir de n'importe où ailleurs que le système de fichiers racine, et que SELinux est activé dans votre environnement, vous devez définir le contexte correct pour les répertoires montés. Pour le scénario applicable à votre environnement, suivez ces étapes pour définir et confirmer le contexte SELinux correct.

Configurer le contexte SELinux lorsque `/opt/netapp/data` est monté

Si vous avez monté `/opt/netapp/data` dans votre système et SELinux est configuré pour `Enforcing`, assurez-vous que le type de contexte SELinux pour `/opt/netapp/data` est réglé sur `mysqld_db_t`, qui est l'élément de contexte par défaut pour l'emplacement des fichiers de base de données.

1. Exécutez cette commande pour vérifier le contexte :

```
ls -dZ /opt/netapp/data
```

Un exemple de sortie :

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
/opt/netapp/data
```



Dans cette sortie, le contexte est `default_t`. Vous devriez changer ce contexte en `mysqld_db_t`.

2. Effectuez ces étapes pour définir le contexte en fonction de la façon dont vous avez monté `/opt/netapp/data`.
 - a. Exécutez les commandes suivantes pour définir le contexte sur `mysqld_db_t` :

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"
`restorecon -R -v /opt/netapp/data
```
 - b. Si vous avez configuré `/opt/netapp/data` dans `/etc/fstab`, vous devriez éditer le `/etc/fstab` déposer. Pour le `/opt/netapp/data/` option de montage, ajoutez l'étiquette MySQL comme :

```
context=system_u:object_r:mysqld_db_t:s0
```
 - c. Démonter et remonter `/opt/netapp/data/` pour activer le contexte.
 - d. Si vous disposez d'un montage NFS direct, exécutez la commande suivante pour définir le contexte sur `mysqld_db_t` :

```
mount <nfsshare>:/<mountpoint> /opt/netapp/data -o
context=system_u:object_r:mysqld_db_t:s0
```

3. Vérifiez si le contexte est correctement défini :

```
ls -dZ /opt/netapp/data/
```

Un exemple de sortie :

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_db_t:s0
/opt/netapp/data/
```

Configurer le contexte SELinux lorsque /opt/netapp est monté, et /opt/netapp/data/ est également monté séparément

Dans ce scénario, vous devez d'abord définir le contexte pour /opt/netapp/data/ comme décrit dans la section précédente. Après avoir défini le contexte correct pour /opt/netapp/data/ , assurez-vous que le répertoire parent /opt/netapp n'a pas le contexte SELinux défini sur file_t .

Étapes

1. Exécutez cette commande pour vérifier le contexte :

```
ls -dZ /opt/netapp
```

Un exemple de sortie :

```
drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
```

Dans cette sortie, le contexte est file_t devrait être changé. Les commandes suivantes définissent le contexte sur usr_t . Vous pouvez définir le contexte sur n'importe quelle valeur autre que file_t en fonction de vos exigences de sécurité.

2. Effectuez ces étapes pour définir le contexte, en fonction de la façon dont vous avez monté /opt/netapp

.

a. Exécutez les commandes suivantes pour définir le contexte :

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. Si vous avez configuré /opt/netapp dans /etc/fstab , vous devriez éditer le /etc/fstab déposer. Pour le /opt/netapp option de montage, ajoutez l'étiquette MySQL comme :

```
context=system_u:object_r:usr_t:s0
```

2. Démonter, puis remonter /opt/netapp pour activer le contexte.

3. Si vous disposez d'un montage NFS direct, exécutez la commande suivante pour définir le contexte :

```
mount <nfsshare>:<mountpoint> /opt/netapp -o
context=system_u:object_r:usr_t:s0
```

a. Vérifiez si le contexte est correctement défini :

```
ls -dZ /opt/netapp
```

Un exemple de sortie

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

Configurer le contexte SELinux lorsque /opt/netapp est monté, et /opt/netapp/data/ n'est pas monté séparément

Si vous avez monté /opt/netapp dans votre système et SELinux est configuré pour Enforcing, assurez-vous que le type de contexte SELinux pour /opt/netapp est réglé sur `mysqld_db_t`, qui est l'élément de contexte par défaut pour l'emplacement des fichiers de base de données.

Étapes

1. Exécutez cette commande pour vérifier le contexte :

```
ls -dZ /opt/netapp
```

Un exemple de sortie :

```
drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
```



Dans cette sortie, le contexte est `default_t`. Vous devriez changer ce contexte en `mysqld_db_t`.

2. Procédez comme suit pour définir le contexte en fonction de la façon dont vous avez monté /opt/netapp :

a. Exécutez les commandes suivantes pour définir le contexte sur `mysqld_db_t` :

```
semanage fcontext -a -t mysqld_db_t "/opt/netapp"  
`restorecon -R -v /opt/netapp
```

b. Si vous avez configuré /opt/netapp dans /etc/fstab, éditer le /etc/fstab déposer. Pour le /opt/netapp/ option de montage, ajoutez l'étiquette MySQL comme :

```
context=system_u:object_r:mysqld_db_t:s0
```

c. Démonter, puis remonter /opt/netapp/ pour activer le contexte.

d. Si vous disposez d'un montage NFS direct, exécutez la commande suivante pour définir le contexte sur `mysqld_db_t` :

```
mount <nfsshare>:<mountpoint> /opt/netapp -o  
context=system_u:object_r:mysqld_db_t:s0
```

3. Vérifiez si le contexte est correctement défini :

```
ls -dZ /opt/netapp/
```

Un exemple de sortie :

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysql_d_db_t:s0 /opt/netapp/
```

Installer Unified Manager sur les systèmes Linux

Il est important que vous compreniez que la séquence d'étapes pour télécharger et installer Unified Manager varie en fonction de votre scénario d'installation.

Créez un répertoire personnel utilisateur et un mot de passe umadmin personnalisés avant l'installation

Vous pouvez créer un répertoire personnel personnalisé et définir votre propre mot de passe utilisateur umadmin avant d'installer Unified Manager. Cette tâche est facultative, mais certains sites peuvent avoir besoin de la flexibilité nécessaire pour remplacer les paramètres par défaut de l'installation d'Unified Manager.

Avant de commencer

- Le système doit répondre aux exigences décrites dans ["Configuration matérielle requise"](#).
- Vous devez pouvoir vous connecter en tant qu'utilisateur root au système Red Hat Enterprise Linux.

L'installation par défaut d'Unified Manager exécute les tâches suivantes :

- Crée l'utilisateur umadmin avec `/home/umadmin` comme répertoire personnel.
- Attribue le mot de passe par défaut « admin » à l'utilisateur umadmin.

Parce que certains environnements d'installation restreignent l'accès à `/home`, l'installation échoue. Vous devez créer le répertoire personnel dans un emplacement différent. De plus, certains sites peuvent avoir des règles concernant la complexité des mots de passe ou exiger que les mots de passe soient définis par les administrateurs locaux plutôt que par le programme d'installation.

Si votre environnement d'installation nécessite que vous remplaciez ces paramètres d'installation par défaut, suivez ces étapes pour créer un répertoire personnel personnalisé et définir le mot de passe de l'utilisateur umadmin.

Lorsque ces informations sont définies avant l'installation, le script d'installation découvre ces paramètres et utilise les valeurs définies au lieu d'utiliser les paramètres d'installation par défaut.

De plus, l'installation par défaut d'Unified Manager inclut l'utilisateur umadmin dans les fichiers `sudoers` (`ocum_sudoers` et `ocie_sudoers`) dans le `/etc/sudoers.d/` annuaire. Si vous supprimez ce contenu de votre environnement en raison de politiques de sécurité ou d'un outil de surveillance de sécurité, vous devez le rajouter. Vous devez conserver la configuration `sudoers` car certaines opérations Unified Manager nécessitent ces privilèges `sudo`.

Les politiques de sécurité de votre environnement ne doivent pas restreindre les privilèges `sudo` pour l'utilisateur de maintenance d'Unified Manager. Certaines opérations d'Unified Manager peuvent échouer si les privilèges sont restreints. Vérifiez que vous êtes en mesure d'exécuter la commande `sudo` suivante lorsque vous êtes connecté en tant qu'utilisateur umadmin après une installation réussie.

```
sudo systemctl status ocie
```

Cette commande doit renvoyer l'état approprié du service ocie sans aucune erreur.

Étapes

1. Connectez-vous en tant qu'utilisateur root au serveur.
2. Créez le compte de groupe umadmin appelé « maintenance » :

```
groupadd maintenance
```

3. Créez le compte utilisateur « umadmin » dans le groupe de maintenance sous un répertoire personnel de votre choix :

```
adduser --home <home_directory> -g maintenance umadmin
```

4. Définir le mot de passe umadmin :

```
passwd umadmin
```

Le système vous invite à saisir une nouvelle chaîne de mot de passe pour l'utilisateur umadmin.

Après avoir installé Unified Manager, vous devez spécifier le shell de connexion de l'utilisateur umadmin.

Télécharger Unified Manager

Vous devez télécharger le Unified Manager .zip fichier du site de support NetApp pour installer Unified Manager.

Avant de commencer

Vous devez disposer des informations de connexion pour le site de support NetApp .

Vous téléchargez le package d'installation d'Unified Manager pour le système Red Hat Enterprise Linux.

Étapes

1. Connectez-vous au site de support NetApp et accédez à la page de téléchargement d'Unified Manager :

["Site de support NetApp"](#)

2. Sélectionnez la version requise d'Unified Manager et acceptez le contrat de licence utilisateur final (CLUF).
3. Téléchargez le fichier d'installation d'Unified Manager pour Linux et enregistrez-le .zip fichier dans un répertoire sur le système cible.



- Assurez-vous de télécharger la version correcte du fichier d'installation pour votre système Red Hat Enterprise Linux. Selon que vous avez installé Red Hat Enterprise Linux 8 ou 9, assurez-vous de télécharger la version appropriée d'Unified Manager .zip déposer.
- NetApp vous recommande de télécharger le certificat de signature de code(.pem) et la signature numérique(.sig) avec le .zip déposer.

4. Vérifiez la somme de contrôle pour l'intégrité du logiciel téléchargé.
5. Si vous avez téléchargé le certificat de signature de code et la signature numérique, vous pouvez vérifier l'intégrité du fichier d'installation. Vous pouvez utiliser les commandes suivantes pour vérifier l'intégrité du

fichier d'installation :

- Cette commande crée un fichier avec la clé publique du certificat de signature de code :

```
openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >  
<public_key_file_name>
```

- Où **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** est le fichier qui contient le certificat de signature de code.
- Cette commande vérifie la signature sur le fichier d'installation :

```
openssl dgst -sha256 -verify <public_key_file_name> -signature  
<signature_file_name> ActiveIQUnifiedManager-<version>.zip
```

Le message similaire à `Verified Ok` confirme que le fichier d'installation peut être utilisé en toute sécurité.

Installer Unified Manager

Vous pouvez installer Unified Manager sur une plate-forme Red Hat Enterprise Linux physique ou virtuelle.

Avant de commencer

- Le système sur lequel vous souhaitez installer Unified Manager doit répondre aux exigences système et logicielles.

Voir "[Configuration matérielle requise](#)".

Voir "[Logiciels Linux et exigences d'installation](#)".

- Vous devez avoir téléchargé le Unified Manager .zip fichier du site de support NetApp vers le système cible.
- Vous auriez dû vérifier l'intégrité du fichier téléchargé .zip déposer.
- Vous devez disposer d'un navigateur Web pris en charge.
- Votre logiciel d'émulation de terminal doit avoir le défilement arrière activé.

Le système Red Hat Enterprise Linux peut avoir toutes les versions requises des logiciels de support requis (Java, MySQL, utilitaires supplémentaires) installées, seulement certains des logiciels requis installés, ou peut être un système nouvellement installé sans aucun des logiciels requis installés.

Étapes

1. Connectez-vous au serveur sur lequel vous installez Unified Manager.
2. Saisissez les commandes appropriées pour évaluer quels logiciels pourraient nécessiter une installation ou une mise à niveau sur le système cible pour prendre en charge l'installation :

Logiciel requis et version minimale	Commande pour vérifier le logiciel et la version
Version 11.0.25 d'OpenJDK	<code>java -version</code>
MySQL 8.4.4 Édition communautaire	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16.02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

- Si la version installée de MySQL est antérieure à MySQL 8.4.4 Community Edition, entrez la commande suivante pour la désinstaller :

```
rpm -e <mysql_package_name>
```

Si vous recevez des erreurs de dépendance, vous devez ajouter le `--nodeps` option pour désinstaller le composant.

- Accédez au répertoire dans lequel vous avez téléchargé l'installation `.zip` fichier et développez le bundle Unified Manager :

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Le requis `.rpm` les modules pour Unified Manager sont décompressés dans le répertoire cible.

- Vérifiez que le module suivant est disponible dans le répertoire :

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

- Exécutez le script de pré-installation pour vous assurer qu'aucun paramètre de configuration système ni aucun logiciel installé ne pourrait entrer en conflit avec l'installation d'Unified Manager :

```
sudo ./pre_install_check.sh
```

Le script de pré-installation vérifie que le système dispose d'un abonnement Red Hat Enterprise Linux valide et qu'il a accès aux référentiels logiciels requis. Si le script identifie des problèmes, vous devez les résoudre avant d'installer Unified Manager.

Pour le système Red Hat Enterprise Linux 8, si vous disposez de référentiels internes avec JDK 11 - OpenJDK, p7zip et d'autres packages logiciels fournis par le référentiel AppStream, vous devez désactiver votre référentiel AppStream et installer MySQL Community Server. Exécutez la commande suivante :

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
mysql-community-server
```

- Facultatif :** vous devez effectuer l'étape 7 uniquement si votre système n'est pas connecté à Internet et que vous devez télécharger manuellement les packages requis pour votre installation. Si votre système dispose d'un accès Internet et que tous les packages requis sont disponibles, passez à l'étape 8. Pour les

systèmes qui ne sont pas connectés à Internet ou qui n'utilisent pas les référentiels Red Hat Enterprise Linux, procédez comme suit pour déterminer si des packages requis manquent, puis téléchargez ces packages :

- a. Sur le système sur lequel vous installez Unified Manager, affichez la liste des packages disponibles et non disponibles :

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

Les éléments de la section « Installation : » sont les packages disponibles dans le répertoire actuel, et les éléments de la section « Installation des dépendances : » sont les packages manquants sur votre système.

- b. Sur un système disposant d'un accès Internet, téléchargez les packages manquants :

```
yum install <package_name> --downloadonly --downloadaddir=.
```



Étant donné que le plug-in « yum-plugin-downloadonly » n'est pas toujours activé sur les systèmes Red Hat Enterprise Linux, vous devrez peut-être activer la fonctionnalité permettant de télécharger un package sans l'installer :

```
yum install yum-plugin-downloadonly
```

- a. Copiez les packages manquants du système connecté à Internet vers votre système d'installation.

8. En tant qu'utilisateur root ou en utilisant `sudo`, exécutez la commande suivante pour installer le logiciel :

```
yum install netapp-um<version>.x86_64.rpm
```

Cette commande installe les packages .rpm, tous les autres logiciels de support nécessaires et le logiciel Unified Manager.

Si l'installation échoue avec l'erreur GPG NOKEY, utilisez `rpm --import` pour importer les clés depuis une URL :

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2023
```



N'essayez pas d'effectuer l'installation en utilisant des commandes alternatives (telles que `rpm -ivh`). Une installation réussie de Unified Manager sur un système Red Hat Enterprise Linux nécessite que tous les fichiers Unified Manager et les fichiers associés soient installés dans un ordre spécifique dans une structure de répertoire spécifique qui est appliquée automatiquement par le `yum install netapp-um<version>.x86_64.rpm` commande.

9. Ne tenez pas compte de la notification par courrier électronique qui s'affiche immédiatement après les messages d'installation.

L'e-mail informe l'utilisateur root d'un échec initial de la tâche cron, ce qui n'a aucun effet négatif sur l'installation.

10. Une fois les messages d'installation terminés, faites défiler les messages jusqu'à ce que vous voyiez le message dans lequel le système affiche une adresse IP ou une URL pour l'interface utilisateur Web d'Unified Manager, le nom d'utilisateur de maintenance (umadmin) et un mot de passe par défaut.

Le message est similaire au suivant :

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/      (if using IPv4)
https://[default_ip_address]/    (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. Enregistrez l'adresse IP ou l'URL, le nom d'utilisateur attribué (umadmin) et le mot de passe actuel.
12. Si vous avez créé un compte utilisateur umadmin avec un répertoire personnel personnalisé avant d'installer Unified Manager, vous devez spécifier le shell de connexion de l'utilisateur umadmin :

```
usermod -s /bin/maintenance-user-shell.sh umadmin
```

Accédez à l'interface utilisateur Web pour modifier le mot de passe par défaut de l'utilisateur umadmin et effectuez la configuration initiale d'Unified Manager, comme décrit dans "[Configuration Active IQ Unified Manager](#)". Il est obligatoire de changer le mot de passe par défaut de l'utilisateur umadmin.

Utilisateurs créés lors de l'installation d'Unified Manager

Lorsque vous installez Unified Manager sur Red Hat Enterprise Linux, les utilisateurs suivants sont créés par Unified Manager et des utilitaires tiers : umadmin, jboss et mysql.

- **umadmin**

Utilisé pour se connecter à Unified Manager pour la première fois. Cet utilisateur se voit attribuer un rôle d'utilisateur « Administrateur d'application » et est configuré comme type « Utilisateur de maintenance ». Cet utilisateur est créé par Unified Manager.

- **jboss**

Utilisé pour exécuter les services Unified Manager liés à l'utilitaire JBoss. Cet utilisateur est créé par Unified Manager.

- **mysql**

Utilisé pour exécuter les requêtes de base de données MySQL d'Unified Manager. Cet utilisateur est créé par l'utilitaire tiers MySQL.

En plus de ces utilisateurs, Unified Manager crée également des groupes correspondants : maintenance, jboss et mysql. Les groupes de maintenance et jboss sont créés par Unified Manager, tandis que le groupe mysql est créé par un utilitaire tiers.



Si vous avez créé un répertoire personnel personnalisé et défini votre propre mot de passe utilisateur umadmin avant d'installer Unified Manager, le programme d'installation ne recrée pas le groupe de maintenance ni l'utilisateur umadmin.

Changer le mot de passe JBoss

Vous pouvez réinitialiser le mot de passe JBoss spécifique à l'instance défini lors de l'installation. Vous pouvez réinitialiser le mot de passe en option, au cas où votre site nécessiterait cette fonctionnalité de sécurité pour remplacer le paramètre d'installation d'Unified Manager. Cette opération modifie également le mot de passe que JBoss utilise pour accéder à MySQL.

- Vous devez disposer d'un accès utilisateur root au système Red Hat Enterprise Linux sur lequel Unified Manager est installé.
- Vous devez pouvoir accéder au NetApp fourni `password.sh` script dans le répertoire `/opt/netapp/essentials/bin`.

Étapes

1. Connectez-vous en tant qu'utilisateur root sur le système.
2. Arrêtez les services Unified Manager en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

N'arrêtez pas le logiciel MySQL associé.

3. Entrez la commande suivante pour lancer le processus de changement de mot de passe :

```
/opt/netapp/essentials/bin/password.sh resetJBossPassword
```

4. Lorsque vous y êtes invité, saisissez le nouveau mot de passe JBoss, puis saisissez-le une deuxième fois pour confirmation.

Notez que le mot de passe doit comporter entre 8 et 16 caractères et doit contenir au moins un chiffre, une majuscule et une minuscule, ainsi qu'au moins un de ces caractères spéciaux :

```
!@%^*-_=[]:<>./~/+
```

5. Une fois le script terminé, démarrez les services Unified Manager en entrant les commandes suivantes dans l'ordre indiqué :

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. Une fois tous les services démarrés, vous pouvez vous connecter à l'interface utilisateur d'Unified Manager.

Mettre à niveau Unified Manager sur Red Hat Enterprise Linux

Vous pouvez mettre à niveau Unified Manager lorsqu'une nouvelle version est disponible.

Les versions de correctifs du logiciel Unified Manager, lorsqu'elles sont fournies par NetApp, sont installées à l'aide de la même procédure que les nouvelles versions.

Si Unified Manager est associé à une instance d' OnCommand Workflow Automation et que de nouvelles versions du logiciel sont disponibles pour les deux produits, vous devez déconnecter les deux produits, puis configurer une nouvelle connexion Workflow Automation après avoir effectué les mises à niveau. Si vous effectuez une mise à niveau vers un seul des produits, vous devez vous connecter à Workflow Automation après la mise à niveau et vérifier qu'il acquiert toujours des données à partir d'Unified Manager.

Chemin de mise à niveau pris en charge pour les versions d'Unified Manager

Active IQ Unified Manager prend en charge un chemin de mise à niveau spécifique pour chaque version.

Toutes les versions d'Unified Manager ne peuvent pas effectuer une mise à niveau sur place vers des versions ultérieures. Les mises à niveau d'Unified Manager sont limitées à un modèle N-2, ce qui signifie qu'une mise à niveau ne peut être effectuée que dans les 2 prochaines versions sur toutes les plates-formes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.16 à partir d'Unified Manager 9.13 et 9.14 uniquement.

Si vous exécutez une version antérieure aux versions prises en charge, votre instance Unified Manager devra d'abord être mise à niveau vers l'une des versions prises en charge, puis mise à niveau vers la version actuelle.

Par exemple, si votre version installée est Unified Manager 9.9 et que vous souhaitez effectuer une mise à niveau vers Unified Manager 9.14, vous devez suivre une séquence de mises à niveau.

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.11 → 9.13
2. Mise à niveau 9.13 → 9.14
3. Mise à niveau 9.13 → 9.16
4. Mise à niveau 9.14 → 9.16

Pour plus d'informations sur la matrice de chemin de mise à niveau, consultez ceci ["article de la base de connaissances \(KB\)"](#) .

Mettre à niveau Unified Manager

Vous pouvez effectuer une mise à niveau d'Unified Manager 9.13 ou 9.14 vers 9.16 en téléchargeant et en exécutant le fichier d'installation sur la plate-forme Linux.

Avant de commencer

- Le système sur lequel vous mettez à niveau Unified Manager doit répondre aux exigences système et logicielles.

Voir ["Configuration matérielle requise"](#) .

Voir ["Logiciels Linux et exigences d'installation"](#) .

- Vous devez disposer d'un abonnement au gestionnaire d'abonnements Red Hat Enterprise Linux.
- Vous devez installer ou mettre à niveau vers la version correcte d'OpenJDK avant de mettre à niveau Unified Manager.

Voir ["Mise à niveau du JRE sous Linux"](#) .

- Pour éviter toute perte de données, vous devez avoir créé une sauvegarde de la base de données Unified Manager au cas où un problème surviendrait lors de la mise à niveau. NetApp vous recommande de déplacer le fichier de sauvegarde depuis le `/opt/netapp/data` répertoire vers un emplacement externe.
- Lors de la mise à niveau, vous serez peut-être invité à confirmer si vous souhaitez conserver les paramètres par défaut précédents pour la conservation des données de performances pendant 13 mois ou les modifier à 6 mois. Après confirmation, les données de performances historiques sont purgées après 6 mois.
- Vous devez avoir terminé toutes les opérations en cours, car Unified Manager n'est pas disponible pendant le processus de mise à niveau.
- MySQL Community Edition est automatiquement mis à niveau lors de la mise à niveau d'Unified Manager. Si la version installée de MySQL sur votre système est antérieure à 8.4.4, le processus de mise à niveau d'Unified Manager met automatiquement à niveau MySQL vers 8.4.4.

Étapes

1. Connectez-vous au serveur cible Red Hat Enterprise Linux.
2. Téléchargez le pack Unified Manager sur le serveur.

Voir ["Téléchargement d'Unified Manager pour Linux"](#) .

3. Accédez au répertoire cible et développez le bundle Unified Manager :

```
unzip ActiveIQUnifiedManager-<version>.zip
```

Les modules RPM requis pour Unified Manager sont décompressés dans le répertoire cible.

4. Vérifiez que le module suivant est disponible dans le répertoire :

```
ls *.rpm
```

```
netapp-um<version>.x86_64.rpm
```

5. Exécutez le script de pré-installation pour vous assurer qu'aucun paramètre de configuration système ni aucun logiciel installé ne pourrait entrer en conflit avec la mise à niveau :

```
sudo ./pre_install_check.sh
```

Le script de pré-installation vérifie que le système dispose d'un abonnement Red Hat Enterprise Linux valide et qu'il a accès aux référentiels logiciels requis. Si le script identifie des problèmes, vous devez les résoudre et poursuivre la mise à niveau.

Si des paquets manquants sont détectés, effectuez les étapes mentionnées dans ["Étapes supplémentaires à effectuer pour les packages manquants"](#) . S'il n'y a aucun paquet manquant, passez aux étapes suivantes.

6. Mettez à niveau Unified Manager à l'aide du script suivant :

```
upgrade.sh
```

Ce script exécute automatiquement les modules RPM, en mettant à niveau les logiciels de support nécessaires et les modules Unified Manager qui s'exécutent sur eux. De plus, le script de mise à niveau vérifie s'il existe des paramètres de configuration système ou des logiciels installés susceptibles d'entrer en conflit avec la mise à niveau. Si le script identifie des problèmes, vous devez les résoudre avant de

mettre à niveau Unified Manager. Si vous avez déjà installé des packages, tels que *net-snmp* avant de mettre à niveau Unified Manager, la dépendance MySQL peut désinstaller le package pendant la mise à niveau. Vous devez réinstaller le package manuellement pour continuer à l'utiliser.

7. Une fois la mise à niveau terminée, faites défiler les messages jusqu'à ce que vous voyiez le message affichant une adresse IP ou une URL pour l'interface utilisateur Web d'Unified Manager, le nom d'utilisateur de maintenance (umadmin) et le mot de passe par défaut.

Le message est similaire au suivant :

```
Active IQ Unified Manager upgraded successfully.  
Use a web browser and one of the following URLs to access the Unified  
Manager GUI:
```

```
https://default_ip_address/      (if using IPv4)  
https://[default_ip_address]/    (if using IPv6)  
https://fully_qualified_domain_name/
```

Saisissez l'adresse IP ou l'URL spécifiée dans une nouvelle fenêtre d'un navigateur Web pris en charge pour démarrer l'interface utilisateur Web d'Unified Manager, puis connectez-vous en utilisant le même nom d'utilisateur de maintenance (umadmin) et le même mot de passe que ceux que vous avez définis précédemment.

Étapes supplémentaires à effectuer pour les packages manquants

Si des packages manquants sont détectés sur votre site lors de la mise à niveau, ou si votre système n'est pas connecté à Internet, ou si vous n'utilisez pas les référentiels Red Hat Enterprise Linux, procédez comme suit pour déterminer s'il vous manque des packages requis et téléchargez ces packages.



Ces étapes doivent être effectuées après l'étape 5 de la procédure principale. Cette procédure met à niveau Unified Manager et vous n'avez pas besoin d'exécuter d'étapes supplémentaires pour la mise à niveau.

1. Consultez la liste des packages disponibles et indisponibles :

```
yum install netapp-um<version>.x86_64.rpm --assumeno
```

Les éléments de la section « Installation : » sont les packages disponibles dans le répertoire actuel, et les éléments de la section « Installation des dépendances : » sont les packages manquants sur votre système.

2. Sur un autre système disposant d'un accès Internet, exécutez la commande suivante pour télécharger les packages manquants.

```
yum install package_name --downloadonly --downloadaddir=.
```

Les packages sont téléchargés dans le répertoire spécifié comme `--downloadaddir=.`

Étant donné que le plug-in « yum-plugin-downloadonly » n'est pas toujours activé sur les systèmes Red Hat Enterprise Linux, vous devrez peut-être activer la fonctionnalité permettant de télécharger un package sans l'installer :


```
yum install yum-plugin-downloadonly
```

3. Copiez les packages téléchargés dans le répertoire où vous avez décompressé le bundle Unified Manager sur le système d'installation.
4. Changez de répertoire vers ce répertoire et exécutez la commande suivante pour installer les packages manquants, ainsi que leurs dépendances.

```
yum install *.rpm
```

5. Démarrez le serveur Unified Manager. Exécutez ces commandes :

```
systemctl start ocie
```

```
systemctl start ocieau
```

Ce processus termine le processus de mise à niveau d'Unified Manager. Saisissez l'adresse IP ou l'URL spécifiée dans une nouvelle fenêtre d'un navigateur Web pris en charge pour démarrer l'interface utilisateur Web d'Unified Manager, puis connectez-vous en utilisant le même nom d'utilisateur de maintenance (umadmin) et le même mot de passe que ceux que vous avez définis précédemment.

Mettre à niveau le système d'exploitation hôte de Red Hat Enterprise Linux 7.x vers 8.x

Si vous avez précédemment installé Unified Manager sur un système Red Hat Enterprise Linux 7.x et que vous devez effectuer une mise à niveau vers Red Hat Enterprise Linux 8.x, vous devez suivre l'une des procédures répertoriées dans cette rubrique. Dans les deux cas, vous devez créer une sauvegarde de Unified Manager sur le système Red Hat Enterprise Linux 7.x, puis restaurer la sauvegarde sur un système Red Hat Enterprise Linux 8.x. Notez que les versions prises en charge de Red Hat Enterprise Linux vont de 8.0 à 8.10.

La différence entre les deux options répertoriées ci-dessous est que dans un cas, vous effectuez la restauration d'Unified Manager sur un nouveau serveur 8.x, et dans l'autre cas, vous effectuez l'opération de restauration sur le même serveur.

Étant donné que cette tâche nécessite la création d'une sauvegarde d'Unified Manager sur le système Red Hat Enterprise Linux 7.x, vous devez créer la sauvegarde uniquement lorsque vous êtes prêt à terminer l'intégralité du processus de mise à niveau afin qu'Unified Manager soit hors ligne pendant la période la plus courte possible. Des lacunes dans les données collectées apparaissent dans l'interface utilisateur d'Unified Manager pendant la période pendant laquelle le système Red Hat Enterprise Linux 7.x est arrêté et avant le démarrage du nouveau Red Hat Enterprise Linux 8.x.

Voir "[Gestion des opérations de sauvegarde et de restauration](#)" si vous avez besoin de consulter des instructions détaillées pour les processus de sauvegarde et de restauration.

Suivez ces étapes si vous disposez d'un système de secours sur lequel vous pouvez installer le logiciel Red Hat Enterprise Linux 8.x afin de pouvoir effectuer la restauration d'Unified Manager sur ce système pendant que le système Red Hat Enterprise Linux 7.x est toujours disponible.

1. Installez et configurez un nouveau serveur avec le logiciel Red Hat Enterprise Linux 8.x.

Voir "[Logiciels Linux et exigences d'installation](#)".

2. Sur le système Red Hat Enterprise Linux 8.x, installez la même version du logiciel Unified Manager que celle que vous avez sur le système Red Hat Enterprise Linux 7.x existant.

Voir ["Installation d'Unified Manager sur Linux"](#) .

Ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification une fois l'installation terminée. Le fichier de sauvegarde renseigne ces informations pendant le processus de restauration.

3. Sur le système Red Hat Enterprise Linux 7.x, à partir du menu Administration de l'interface utilisateur Web, créez une sauvegarde Unified Manager, puis copiez le fichier de sauvegarde(. 7z fichier) et le contenu du répertoire du référentiel de base de données(/database-dumps-repo sous-répertoire) vers un emplacement externe.
4. Sur le système Red Hat Enterprise Linux 7.x, arrêtez Unified Manager.
5. Sur le système Red Hat Enterprise Linux 8.x, copiez le fichier de sauvegarde(. 7z fichier) depuis l'emplacement externe vers /opt/netapp/data/ocum-backup/ et les fichiers du référentiel de base de données vers le /database-dumps-repo sous-répertoire sous le /ocum-backup annuaire.
6. Entrez la commande suivante pour restaurer la base de données Unified Manager à partir du fichier de sauvegarde :

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. Saisissez l'adresse IP ou l'URL dans votre navigateur Web pour démarrer l'interface Web d'Unified Manager, puis connectez-vous au système.

Une fois que vous avez vérifié que le système fonctionne correctement, vous pouvez supprimer Unified Manager du système Red Hat Enterprise Linux 7.x.

Mise à niveau du système d'exploitation hôte sur le même serveur

Suivez ces étapes si vous ne disposez pas d'un système de secours sur lequel vous pouvez installer le logiciel Red Hat Enterprise Linux 8.x.

1. Depuis le menu Administration de l'interface Web, créez une sauvegarde Unified Manager, puis copiez le fichier de sauvegarde(. 7z fichier) et le contenu du répertoire du référentiel de base de données(/database-dumps-repo sous-répertoire) vers un emplacement externe.
2. Supprimez l'image Red Hat Enterprise Linux 7.x du système et effacez complètement le système.
3. Installez et configurez le logiciel Red Hat Enterprise Linux 8.x sur le même système.

Voir ["Logiciels Linux et exigences d'installation"](#) .

4. Sur le système Red Hat Enterprise Linux 8.x, installez la même version du logiciel Unified Manager que celle que vous aviez sur le système Red Hat Enterprise Linux 7.x.

Voir ["Installation d'Unified Manager sur Linux"](#) .

Ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification une fois l'installation terminée. Le fichier de sauvegarde renseigne ces informations pendant le processus de restauration.

5. Copier le fichier de sauvegarde(. 7z fichier) de l'emplacement externe vers /opt/netapp/data/ocum-backup/ et les fichiers du référentiel de base de données vers le /database-dumps-repo sous-

répertoire sous le /ocum-backup annuaire.

6. Entrez la commande suivante pour restaurer la base de données Unified Manager à partir du fichier de sauvegarde :

```
um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
```

7. Saisissez l'adresse IP ou l'URL dans votre navigateur Web pour démarrer l'interface Web d'Unified Manager, puis connectez-vous au système.

Mettre à niveau les produits tiers après l'installation d'Unified Manager

Vous pouvez mettre à niveau des produits tiers, tels que JRE, lorsque Unified Manager est déjà installé sur les systèmes Linux.

Les entreprises qui développent ces produits tiers signalent régulièrement des vulnérabilités de sécurité. Vous pouvez mettre à niveau vers des versions plus récentes de ce logiciel à votre rythme.

Mettre à niveau OpenJDK sur Linux

Vous pouvez effectuer une mise à niveau vers une version plus récente d'OpenJDK sur le serveur Linux sur lequel Unified Manager est installé pour obtenir des correctifs pour les vulnérabilités de sécurité.

Avant de commencer

Vous devez disposer des privilèges root pour le système Linux sur lequel Unified Manager est installé.

Vous pouvez mettre à jour les versions d'OpenJDK au sein des familles de versions. Par exemple, vous pouvez effectuer une mise à niveau d'OpenJDK 11.0.14 vers OpenJDK 11.0.17, mais vous ne pouvez pas effectuer une mise à niveau directement d'OpenJDK 11 vers OpenJDK 12.

Étapes

1. Connectez-vous en tant qu'utilisateur root sur la machine hôte Unified Manager.
2. Téléchargez la version appropriée d'OpenJDK (64 bits) sur le système cible.
3. Arrêter les services Unified Manager :

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

4. Installez la dernière version d'OpenJDK sur le système.
5. Démarrez les services Unified Manager :

```
systemctl start ocie
```

```
systemctl start ocieau
```

Redémarrer Unified Manager

Vous devrez peut-être redémarrer Unified Manager après avoir apporté des modifications

de configuration.

Avant de commencer

Vous devez disposer d'un accès utilisateur root au serveur Red Hat Enterprise Linux sur lequel Unified Manager est installé.

Étapes

1. Connectez-vous en tant qu'utilisateur root au serveur sur lequel vous souhaitez redémarrer le service Unified Manager.
2. Arrêtez le service Unified Manager et le service MySQL associé dans cet ordre :

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

```
systemctl stop mysqld
```

3. Démarrez les services MySQL et Unified Manager dans cet ordre :

```
systemctl start mysqld
```

```
systemctl start ocie
```

```
systemctl start ocieau
```



`mysqld` est un programme démon requis pour démarrer et arrêter le serveur MySQL.

Supprimer Unified Manager

Vous pouvez arrêter et désinstaller Unified Manager de l'hôte Red Hat Enterprise Linux avec une seule commande.

Avant de commencer

- Vous devez disposer d'un accès utilisateur root au serveur à partir duquel vous souhaitez supprimer Unified Manager.
- Security-Enhanced Linux (SELinux) doit être désactivé sur le système Linux. Modifiez le mode d'exécution de SELinux sur « Permissif » en utilisant la `setenforce 0` commande.
- Tous les clusters (sources de données) doivent être supprimés du serveur Unified Manager avant de supprimer le logiciel.
- Vous devez supprimer manuellement les règles de pare-feu créées pour autoriser ou bloquer le port MySQL 3306. Les règles du pare-feu ne sont pas supprimées automatiquement.

Étapes

1. Connectez-vous en tant qu'utilisateur root au serveur sur lequel vous souhaitez supprimer Unified Manager.
2. Arrêtez et supprimez Unified Manager du serveur :

```
rpm -e netapp-um
```

Cette étape supprime tous les packages NetApp RPM associés. Il ne supprime pas les modules logiciels prérequis, tels que Java, MySQL et p7zip.

3. **Facultatif** : si nécessaire, supprimez les modules logiciels de support, tels que Java, MySQL et p7zip :

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-  
common mysql-community-libs java-x.y
```

Une fois cette opération terminée, le logiciel est supprimé. Toutes les données de la `/opt/netapp/data` le répertoire est déplacé vers le `/opt/netapp/data/BACKUP` dossier après la désinstallation. La désinstallation d'Unified Manager supprime également les packages Java et MySQL, sauf si les packages sont requis et utilisés par une autre application sur le système. Cependant, les données MySQL ne sont pas supprimées.

Supprimer l'utilisateur umadmin personnalisé et le groupe de maintenance

Si vous avez créé un répertoire personnel personnalisé pour définir votre propre utilisateur umadmin et votre compte de maintenance avant d'installer Unified Manager, vous devez supprimer ces éléments après avoir désinstallé Unified Manager.

La désinstallation standard d'Unified Manager ne supprime pas un utilisateur umadmin ni un compte de maintenance définis sur mesure. Vous devez supprimer ces éléments manuellement.

Étapes

1. Connectez-vous en tant qu'utilisateur root au serveur Red Hat Enterprise Linux.
2. Supprimer l'utilisateur umadmin :

```
userdel umadmin
```

3. Supprimer le groupe de maintenance :

```
groupdel maintenance
```

Installer Unified Manager sur les systèmes Windows

Introduction à Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous permet de surveiller et de gérer l'état et les performances de vos systèmes de stockage ONTAP à partir d'une interface unique. Vous pouvez déployer Unified Manager sur un serveur Linux, sur un serveur Windows ou en tant qu'appliance virtuelle sur un hôte VMware.

Une fois l'installation terminée et les clusters que vous souhaitez gérer ajoutés, Unified Manager fournit une interface graphique qui affiche la capacité, la disponibilité, la protection et l'état des performances des systèmes de stockage surveillés.

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

À quoi sert le serveur Unified Manager

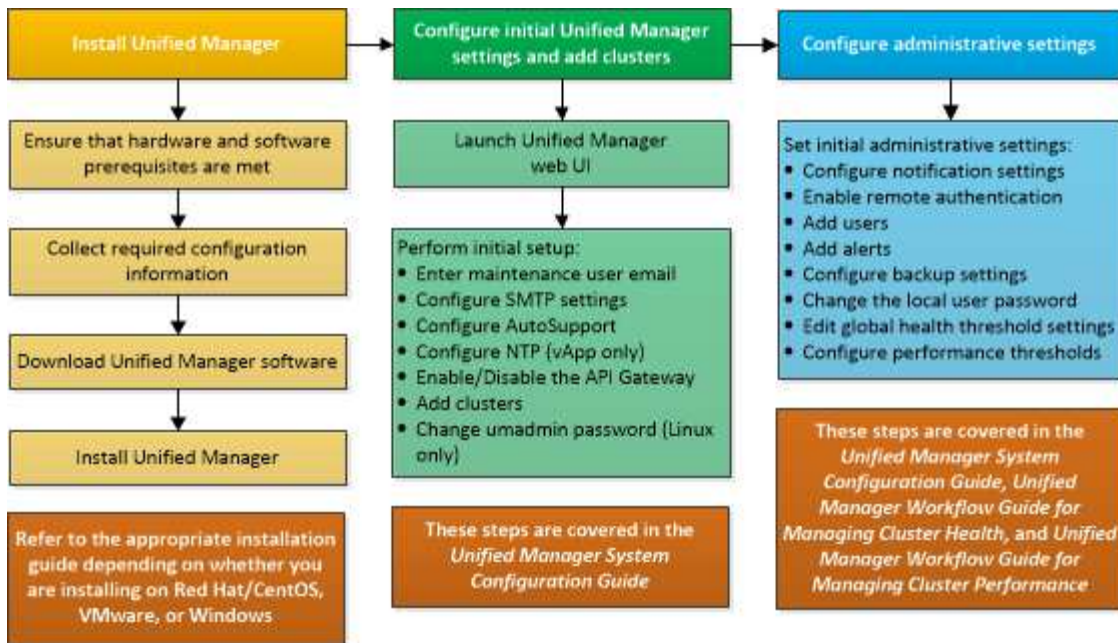
L'infrastructure du serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations du cluster, stocke les données dans la base de données et analyse les données pour voir s'il existe des problèmes de cluster.

Aperçu de la séquence d'installation

Le flux de travail d'installation décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.

Ces sections décrivent chacun des éléments affichés dans le flux de travail ci-dessous.



Conditions requises pour l'installation d'Unified Manager

Avant de commencer le processus d'installation, assurez-vous que le serveur sur lequel vous souhaitez installer Unified Manager répond aux exigences spécifiques en matière de logiciel, de matériel, de processeur et de mémoire.

NetApp ne prend en charge aucune modification du code d'application Unified Manager. Si vous devez appliquer des mesures de sécurité au serveur Unified Manager, vous devez apporter ces modifications au système d'exploitation sur lequel Unified Manager est installé.

Pour plus de détails sur l'application des mesures de sécurité au serveur Unified Manager, consultez l'article de la base de connaissances.

["Prise en charge des mesures de sécurité appliquées à Active IQ Unified Manager pour Clustered Data ONTAP"](#)

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

Infrastructure virtuelle et exigences matérielles

L'installation d'Unified Manager sur une infrastructure virtuelle ou un système physique doit répondre aux exigences minimales en matière de mémoire, de processeur et d'espace disque.

Le tableau suivant affiche les valeurs recommandées pour les ressources de mémoire, de processeur et d'espace disque. Ces valeurs ont été qualifiées afin qu'Unified Manager atteigne des niveaux de performance acceptables.

Configuration matérielle	Paramètres recommandés
BÉLIER	12 Go (exigence minimale 8 Go)
Processeurs	4 processeurs
Capacité du cycle du processeur	9572 MHz au total (exigence minimale 9572 MHz)
Espace disque libre	150 Go, où la capacité est répartie comme suit : • 100 Go d'espace disque pour le répertoire d'installation • 50 Go d'espace disque pour le répertoire de données MySQL

Unified Manager peut être installé sur des systèmes dotés d'une petite quantité de mémoire, mais les 12 Go de RAM recommandés garantissent que suffisamment de mémoire est disponible pour des performances optimales et que le système peut accueillir des clusters et des objets de stockage supplémentaires à mesure que votre configuration se développe. Vous ne devez définir aucune limite de mémoire sur la machine virtuelle sur laquelle Unified Manager est déployé et ne devez activer aucune fonctionnalité (par exemple, le gonflage) qui empêche le logiciel d'utiliser la mémoire allouée sur le système.

De plus, il existe une limite au nombre de nœuds qu'une seule instance d'Unified Manager peut surveiller avant d'installer une deuxième instance d'Unified Manager. Pour plus d'informations, consultez le *Guide des meilleures pratiques*.

["Rapport technique 4621 : Guide des meilleures pratiques pour Unified Manager"](#)

L'échange de pages mémoire a un impact négatif sur les performances du système et de l'application de gestion. La concurrence pour des ressources CPU qui ne sont pas disponibles en raison de l'utilisation globale de l'hôte peut dégrader les performances.

Exigence d'utilisation dédiée

Le système physique ou virtuel sur lequel vous installez Unified Manager doit être utilisé exclusivement pour Unified Manager et ne doit pas être partagé avec d'autres applications. D'autres applications peuvent consommer des ressources système et réduire considérablement les performances d'Unified Manager.

Besoins d'espace pour les sauvegardes

Si vous prévoyez d'utiliser la fonction de sauvegarde et de restauration d'Unified Manager, allouez une capacité supplémentaire afin que le répertoire ou le disque « data » dispose de 150 Go d'espace. Une sauvegarde peut être écrite vers une destination locale ou vers une destination distante. La meilleure pratique consiste à identifier un emplacement distant externe au système hôte Unified Manager disposant d'un minimum de 150 Go d'espace.

Exigences relatives à la connectivité de l'hôte

Le système physique ou le système virtuel sur lequel vous installez Unified Manager doit être configuré de manière à ce que vous puissiez réussir `ping` le nom de l'hôte de l'hôte lui-même. Dans le cas d'une configuration IPv6, vous devez vérifier que `ping6` au nom d'hôte est réussi pour garantir que l'installation d'Unified Manager réussit.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web du produit. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, vous devez obtenir le nom d'hôte à partir du DNS.

Si vous prévoyez d'autoriser les utilisateurs à accéder à Unified Manager en utilisant le nom court au lieu d'utiliser le nom de domaine complet (FQDN) ou l'adresse IP, votre configuration réseau doit résoudre ce nom court en un FQDN valide.

Logiciel Windows et configuration requise pour son installation

Pour une installation réussie d'Unified Manager sous Windows, vous devez vous assurer que le système sur lequel Unified Manager est installé répond aux exigences logicielles.

Logiciel du système d'exploitation

Vous pouvez installer Unified Manager sur les éditions Windows suivantes :

- Microsoft Windows Server 2019 Édition Standard et Datacenter
- Microsoft Windows Server 2022 Édition Standard et Datacenter

Unified Manager est pris en charge sur le système d'exploitation Windows 64 bits pour les langues suivantes :

- English
- japonais
- chinois simplifié

Consultez la matrice d'interopérabilité pour obtenir la liste complète et la plus récente des versions Windows prises en charge.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)



NetApp ne prend pas en charge l'installation d'Unified Manager à l'aide d'outils tiers, tels que Microsoft System Center Configuration Manager (SCCM).

Le serveur doit être dédié à l'exécution d'Unified Manager. Aucune autre application ne doit être installée sur le serveur. Il est possible qu'un logiciel antivirus actif soit installé sur votre système Windows en raison des réglementations de l'entreprise. Vous devez désactiver le logiciel antivirus avant d'installer Unified Manager pour éviter l'échec de l'installation.

Logiciels tiers

Les packages tiers suivants sont fournis avec Unified Manager. Si ces packages tiers ne sont pas installés sur votre système, Unified Manager les installe dans le cadre de l'installation.

- Packages redistribuables Microsoft Visual C++ pour Visual Studio 2015 version 14.26.28720.3
- MySQL Community Edition version 8.4.4
- Python 3.12.4
- Version 11.0.25 d'OpenJDK
- 7-zip version 23.01 ou ultérieure



À partir d'Unified Manager 9.5, OpenJDK est fourni dans le package d'installation d'Unified Manager et installé automatiquement. Oracle Java n'est pas pris en charge à partir de Unified Manager 9.5.

Si MySQL est préinstallé, vous devez vous assurer que :

- Il utilise le port par défaut.
- Les bases de données d'exemple ne sont pas installées.
- Le nom du service est « MYSQL84 ».

Unified Manager est déployé sur un serveur Web WildFly. WildFly 26.1.3 est fourni et configuré avec Unified Manager.



Vous devez arrêter une instance en cours d'exécution d'Unified Manager avant de mettre à niveau un logiciel tiers. Une fois l'installation du logiciel tiers terminée, vous pouvez redémarrer Unified Manager.

Conditions d'installation

- Microsoft .NET 4.5.2 ou supérieur doit être installé.
- Le répertoire doit être configuré avec 2 Go d'espace disque pour extraire les fichiers d'installation. Pour vérifier si le répertoire est créé, exécutez la commande suivante sur l'interface de ligne de commande : `echo %temp%`
- Vous devez réserver 2 Go d'espace disque sur le lecteur Windows pour la mise en cache des fichiers MSI d'Unified Manager.
- Le serveur Microsoft Windows sur lequel vous souhaitez installer Unified Manager doit être configuré avec un nom de domaine complet (FQDN) tel que `ping` les réponses au nom d'hôte et au FQDN réussissent.
- Vous devez désactiver le service de publication Web mondial Microsoft IIS et vous assurer que les ports 80 et 443 sont libres.
- Vous devez vous assurer que le paramètre Hôte de session Bureau à distance pour « Compatibilité RDS Windows Installer » est désactivé pendant l'installation.
- Le port UDP 514 doit être libre et ne doit être utilisé par aucun autre service.
- Vous devez désactiver tous les logiciels antivirus sur votre système avant d'installer Unified Manager. Une fois l'installation terminée, assurez-vous d'exclure manuellement les chemins suivants de l'analyse antivirus :
 - Répertoire de données Unified Manager, par exemple, `C:\ProgramData\NetApp\OnCommandAppData\`
 - Répertoire d'installation d'Unified Manager, par exemple, `\C:\Program Files\NetApp\`
 - Répertoire de données MySQL, par exemple, `C:\ProgramData\MySQL\MySQLServerData`

Navigateurs pris en charge

Pour accéder à l'interface Web d'Unified Manager, utilisez un navigateur pris en charge.

La matrice d'interopérabilité contient la liste des versions de navigateur prises en charge.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit que les fonctionnalités du logiciel s'affichent correctement.

Si vous prévoyez de configurer Unified Manager pour l'authentification SAML, afin qu'un fournisseur d'identité (IdP) puisse authentifier les utilisateurs, vous devez également vérifier la liste des navigateurs pris en charge par l'IdP.

Exigences relatives au protocole et au port

Les ports et protocoles requis permettent la communication entre le serveur Unified Manager et les systèmes de stockage gérés, les serveurs et d'autres composants.

Connexions au serveur Unified Manager

Dans les installations classiques, vous n'avez pas besoin de spécifier de numéros de port lors de la connexion à l'interface utilisateur Web d'Unified Manager, car les ports par défaut sont toujours utilisés. Par exemple, étant donné qu'Unified Manager tente toujours de s'exécuter sur son port par défaut, vous pouvez saisir `https://<host>` au lieu de `https://<host>:443`.

Le serveur Unified Manager utilise des protocoles spécifiques pour accéder aux interfaces suivantes :

Interface	Protocole	Port	Description
Interface utilisateur Web d'Unified Manager	HTTP	80	Utilisé pour accéder à l'interface Web d'Unified Manager ; redirige automatiquement vers le port sécurisé 443.
Interface utilisateur Web et programmes Unified Manager utilisant des API	HTTPS	443	Utilisé pour accéder en toute sécurité à l'interface utilisateur Web d'Unified Manager ou pour effectuer des appels API ; les appels API ne peuvent être effectués qu'à l'aide de HTTPS.
Console de maintenance	SSH/SFTP	22	Utilisé pour accéder à la console de maintenance et récupérer les bundles de support.
Ligne de commande Linux	SSH/SFTP	22	Utilisé pour accéder à la ligne de commande Red Hat Enterprise Linux et récupérer les bundles de support.

Interface	Protocole	Port	Description
Syslog	UDP	514	Utilisé pour accéder aux messages EMS basés sur un abonnement à partir des systèmes ONTAP et pour créer des événements basés sur les messages.
REPOS	HTTPS	9443	Utilisé pour accéder aux événements EMS basés sur l'API REST en temps réel à partir de systèmes ONTAP authentifiés.
base de données MySQL	MySQL	3306	Utilisé pour activer l'accès à OnCommand Workflow Automation et aux services API OnCommand à Unified Manager.
Courtier AMQP QPID	TCP/IP	56072	Utilisé pour la communication de messages internes.
Courtier AMQP QPID	WebSocket sur TCP	56080	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud).
Courtier AMQP QPID	WebSocket sur TCP	56443	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud). La communication sur ce port prend en charge le cryptage fourni par TLS ou SSL.



Le port par défaut de MySQL, 3306, est limité uniquement à localhost lors de l'installation d'Unified Manager sur les systèmes Windows. Activez le pare-feu pour restreindre l'accès au port MySQL, 3306, une fois l'installation terminée. Cela n'a aucun impact sur les scénarios de mise à niveau, où la configuration précédente est conservée. Cette configuration peut être modifiée et la connexion peut être rendue disponible à d'autres hôtes en utilisant le `Control access to MySQL port 3306` option sur la console de maintenance. Pour plus d'informations, voir "[Options de menu supplémentaires](#)". Les ports utilisés pour la communication HTTP et HTTPS (ports 80 et 443) peuvent être modifiés à l'aide de la console de maintenance Unified Manager. Pour plus d'informations, voir "[Configuration Active IQ Unified Manager](#)".

Connexions depuis le serveur Unified Manager

Vous devez configurer votre pare-feu pour ouvrir les ports qui permettent la communication entre le serveur Unified Manager et les systèmes de stockage gérés, les serveurs et d'autres composants. Si un port n'est pas ouvert, la communication échoue.

Selon votre environnement, vous pouvez choisir de modifier les ports et les protocoles utilisés par le serveur Unified Manager pour se connecter à des destinations spécifiques.

Le serveur Unified Manager se connecte à l'aide des protocoles et ports suivants aux systèmes de stockage gérés, aux serveurs et aux autres composants :

Destination	Protocole	Port	Description
Système de stockage	HTTPS	443/TCP	Utilisé pour surveiller et gérer les systèmes de stockage.
Système de stockage	NDMP	10 000/TCP	Utilisé pour certaines opérations de restauration d'instantanés.
Serveur AutoSupport	HTTPS	443	Utilisé pour envoyer des informations AutoSupport . Nécessite un accès Internet pour exécuter cette fonction.
Serveur d'authentification	LDAP	389	Utilisé pour effectuer des demandes d'authentification et des demandes de recherche d'utilisateurs et de groupes.
LDAPS	636	Utilisé pour la communication LDAP sécurisée.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	Expéditeur de trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Utilisé pour envoyer des notifications d'alerte SNMP.	Serveur fournisseur de données externe

Destination	Protocole	Port	Description
TCP	2003	Utilisé pour envoyer des données de performances à un fournisseur de données externe, tel que Graphite.	serveur NTP
NTP	123/UDP	Utilisé pour synchroniser l'heure sur le serveur Unified Manager avec un serveur de temps NTP externe. (Systèmes VMware uniquement)	Courtier AMQP QPID
TCP/IP	56072	Utilisé pour la communication de messages internes.	Courtier AMQP QPID
WebSocket sur TCP	56080	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud).	Courtier AMQP QPID
WebSocket sur TCP	56443	Utilisé pour écouter sur ce port les messages reçus d' ONTAP (agent cloud). La communication via ce port prend en charge le cryptage fourni par TLS ou SSL.	Syslog

Complétez la feuille de travail

Avant d'installer et de configurer Unified Manager, vous devez disposer d'informations spécifiques sur votre environnement. Vous pouvez enregistrer les informations dans la feuille de travail.

Informations d'installation d'Unified Manager

Les détails requis pour installer Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Héberger un nom de domaine entièrement qualifié	
Adresse IP de l'hôte	
Masque de réseau	

Système sur lequel le logiciel est déployé	Votre valeur
Adresse IP de la passerelle	
Adresse DNS principale	
Adresse DNS secondaire	
Rechercher des domaines	
Nom d'utilisateur de maintenance	
Mot de passe de l'utilisateur de maintenance	

Informations de configuration d'Unified Manager

Les détails pour configurer Unified Manager après l'installation. Certaines valeurs sont facultatives selon votre configuration.

Paramètre	Votre valeur
Adresse e-mail de l'utilisateur de maintenance	
Nom d'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
Port SMTP	25 (valeur par défaut)
E-mail à partir duquel les notifications d'alerte sont envoyées	
Nom d'hôte ou adresse IP du serveur d'authentification	
Nom de l'administrateur Active Directory ou nom distinctif de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom distinctif de base du serveur d'authentification	
URL du fournisseur d'identité (IdP)	

Paramètre	Votre valeur
Métadonnées du fournisseur d'identité (IdP)	
Adresses IP des hôtes de destination des interruptions SNMP	
Port SNMP	

Informations sur le cluster

Les détails des systèmes de stockage que vous gérez à l'aide d'Unified Manager.

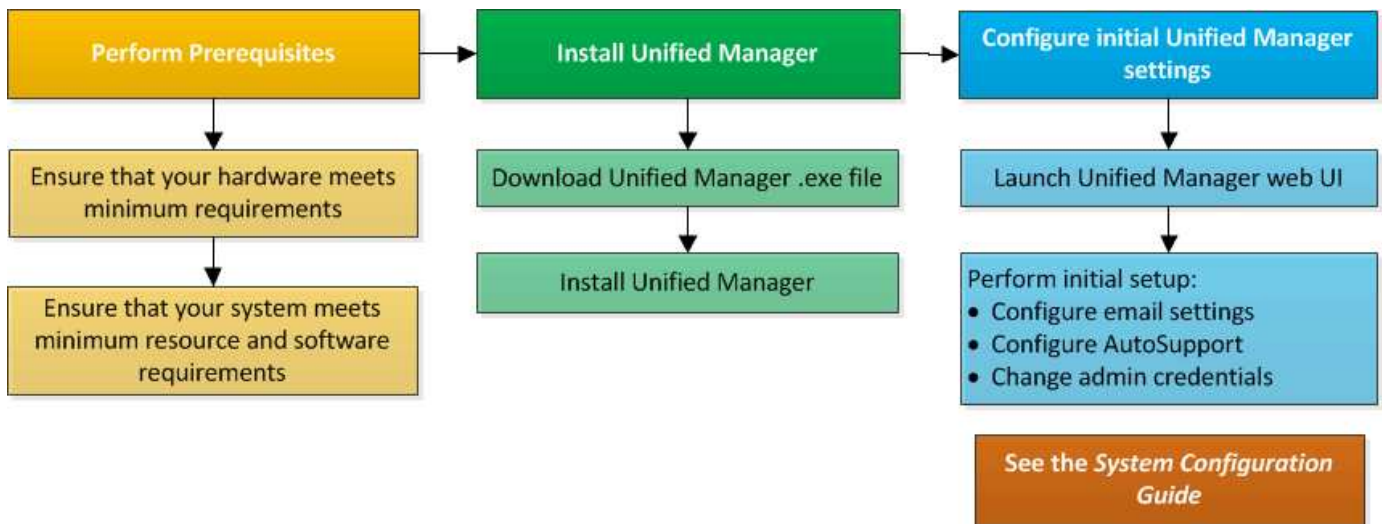
Groupe 1 de N	Votre valeur
Nom d'hôte ou adresse IP de gestion du cluster	
 L'administrateur doit avoir reçu le rôle « admin ».	
Mot de passe administrateur ONTAP	
Protocole	HTTPS

Installer, mettre à niveau et supprimer le logiciel Unified Manager

Vous pouvez installer Unified Manager, effectuer une mise à niveau vers une version plus récente ou supprimer l'application Unified Manager.

Aperçu du processus d'installation

Le flux de travail d'installation décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.



Installer Unified Manager sur Windows

Il est important que vous compreniez la séquence d'étapes pour télécharger et installer Unified Manager sur Windows.

Installer Unified Manager

Vous pouvez installer Unified Manager pour surveiller et résoudre les problèmes de capacité de stockage, de disponibilité, de performances et de protection des données.

Avant de commencer

- Le système sur lequel vous prévoyez d'installer Unified Manager doit répondre aux exigences système et logicielles.

Voir ["Configuration matérielle requise"](#) .

Voir ["Logiciel Windows et configuration requise pour son installation"](#) .



À partir d'Unified Manager 9.5, OpenJDK est fourni dans le package d'installation et installé automatiquement. Oracle Java n'est pas pris en charge à partir de Unified Manager 9.5.

- Vous devez disposer des privilèges d'administrateur Windows. Assurez-vous que votre nom d'utilisateur ne commence pas par un point d'exclamation « ! ». Installation of Unified Manager might fail if the user name of user running the installation begins with " !".
- Tous les clusters sont pris en charge, à l'exception des systèmes ASA r2.
- Vous devez disposer d'un navigateur Web pris en charge.
- Le mot de passe de l'utilisateur de maintenance d'Unified Manager doit comporter entre 8 et 20 caractères et contenir des lettres majuscules ou minuscules, des chiffres et des caractères spéciaux.
- Les caractères spéciaux suivants ne sont pas autorisés dans la chaîne de mot de passe pour l'utilisateur de maintenance ou pour l'utilisateur root MySQL : " ' ` % , = & < > | ^ \ / () [] ; :

Les caractères spéciaux suivants sont autorisés : ~ ! @ # \$ * - ? . + { }

Étapes

1. Connectez-vous à Windows à l'aide du compte administrateur local par défaut.
2. Connectez-vous au site de support NetApp et accédez à la page de téléchargement d'Unified Manager :

["Site de support NetApp"](#)

3. Sélectionnez la version requise d'Unified Manager et acceptez le contrat de licence utilisateur final (CLUF).
4. Téléchargez le fichier d'installation Windows ou le fichier zip d'Unified Manager dans un répertoire cible sur le système Windows.
5. Extrayez le fichier zip, si nécessaire, et accédez au répertoire où se trouve le fichier d'installation.
6. Cliquez avec le bouton droit de la souris et exécutez le fichier exécutable du programme d'installation d'Unified Manager (.exe) en tant qu'administrateur.

Unified Manager détecte les packages tiers manquants ou préinstallés et les répertorie. Si les packages tiers requis ne sont pas installés sur le système, Unified Manager les installe dans le cadre de l'installation.

7. Cliquez sur **Suivant**.
8. Saisissez le nom d'utilisateur et le mot de passe pour créer l'utilisateur de maintenance.
9. Dans l'assistant de connexion à la base de données, entrez le mot de passe root MySQL.
10. Cliquez sur **Modifier** pour spécifier un nouvel emplacement pour le répertoire d'installation d'Unified Manager et le répertoire de données MySQL.

Si vous ne modifiez pas le répertoire d'installation, Unified Manager est installé dans le répertoire d'installation par défaut.

11. Cliquez sur **Suivant**.
12. Dans l'assistant Prêt à installer Shield, cliquez sur **Installer**.
13. Une fois l'installation terminée, cliquez sur **Terminer**.
14. Si vous avez un logiciel antivirus actif installé sur votre système Windows, excluez manuellement les chemins suivants de l'analyse antivirus une fois l'installation terminée :
 - Répertoire de données Unified Manager
 - Répertoire d'installation d'Unified Manager
 - Répertoire de données MySQL

L'installation crée plusieurs répertoires :

- Répertoire d'installation

Il s'agit du répertoire racine d'Unified Manager, que vous avez spécifié lors de l'installation. Exemple:
C:\Program Files\NetApp\

- Répertoire de données MySQL

Il s'agit du répertoire dans lequel sont stockées les bases de données MySQL, que vous avez spécifiées lors de l'installation. Exemple: C:\ProgramData\MySQL\MySQLServerData\

- Répertoire Java

Il s'agit du répertoire dans lequel OpenJDK est installé. Exemple: C:\Program Files\NetApp\JDK\

- Répertoire de données d'application Unified Manager (appDataDir)

Il s'agit du répertoire dans lequel toutes les données générées par l'application sont stockées. Cela inclut les journaux, les packs d'assistance, les sauvegardes et toutes les autres données supplémentaires.

Exemple: C:\ProgramData\NetApp\OnCommandAppData\

Vous pouvez accéder à l'interface utilisateur Web pour effectuer la configuration initiale d'Unified Manager, comme décrit dans le ["Configuration Active IQ Unified Manager"](#).

Effectuer une installation sans assistance d'Unified Manager

Vous pouvez installer Unified Manager sans intervention de l'utilisateur en utilisant l'interface de ligne de commande. Vous pouvez terminer l'installation sans assistance en transmettant les paramètres sous forme de paires clé-valeur.

Étapes

1. Connectez-vous à l'interface de ligne de commande Windows en utilisant le compte administrateur local par défaut.
2. Accédez à l'emplacement où vous souhaitez installer Unified Manager et choisissez l'une des options suivantes :

Option	Instructions
Si des packages tiers sont préinstallés	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qn /l*v CompletePathForLogFile"</pre> Exemple: <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MySQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"</pre>

Option	Instructions
Si les packages tiers ne sont pas installés	<pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qr /l*v CompletePathForLogFile"</pre> Exemple: <pre>ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MySQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre>

Le /qr l'option permet d'activer le mode silencieux avec une interface utilisateur réduite. Une interface utilisateur de base s'affiche, qui montre la progression de l'installation. Vous n'êtes pas invité à effectuer des saisies. Si des packages tiers tels que JRE, MySQL et 7zip ne sont pas préinstallés, vous devez utiliser le /qr option. L'installation échoue si le /qn L'option est utilisée sur un serveur où les packages tiers ne sont pas installés.

Le /qn l'option permet d'activer le mode silencieux sans interface utilisateur. Aucune interface utilisateur ni aucun détail ne sont affichés lors de l'installation. Vous ne devez pas utiliser le /qn option lorsque les packages tiers ne sont pas installés.

3. Connectez-vous à l'interface utilisateur Web d'Unified Manager en utilisant l'URL suivante :

`https://IP address`

Changer le mot de passe JBoss

Vous pouvez réinitialiser le mot de passe JBoss spécifique à l'instance défini lors de l'installation. Vous pouvez réinitialiser le mot de passe en option, au cas où votre site nécessiterait cette fonctionnalité de sécurité pour remplacer le paramètre d'installation d'Unified Manager. Cette opération modifie également le mot de passe que JBoss utilise pour accéder à MySQL.

Avant de commencer

- Vous devez disposer des privilèges d'administrateur Windows pour le système sur lequel Unified Manager est installé.
- Vous devriez avoir le mot de passe de l'utilisateur root MySQL.
- Vous devriez pouvoir accéder au NetApp fourni `password.bat` script dans le répertoire

C:\Program Files\NetApp\essentials\bin.

Étapes

1. Connectez-vous en tant qu'utilisateur administrateur sur la machine hôte Unified Manager.
2. Utilisez la console des services Windows pour arrêter les services Unified Manager suivants :
 - Service d'acquisition NetApp Active IQ (Ocie-au)
 - Service de serveur de gestion NetApp Active IQ (Oncommandsvc)
3. Lancer le `password.bat` script pour démarrer le processus de changement de mot de passe :

```
C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
```

4. Lorsque vous y êtes invité, entrez le mot de passe de l'utilisateur root MySQL.
5. Lorsque vous y êtes invité, saisissez le nouveau mot de passe utilisateur JBoss, puis saisissez-le à nouveau pour confirmation.

Notez que le mot de passe doit comporter entre 8 et 16 caractères et doit contenir au moins un chiffre, une majuscule et une minuscule, ainsi qu'au moins un de ces caractères spéciaux :

!@%^*-_=[]:<>./~+

6. Une fois le script terminé, démarrez les services Unified Manager à l'aide de la console des services Windows :
 - Service de serveur de gestion NetApp Active IQ (Oncommandsvc)
 - Service d'acquisition NetApp Active IQ (Ocie-au)
7. Une fois tous les services démarrés, vous pouvez vous connecter à l'interface utilisateur d'Unified Manager.

Chemin de mise à niveau pris en charge pour les versions d'Unified Manager

Active IQ Unified Manager prend en charge un chemin de mise à niveau spécifique pour chaque version.

Toutes les versions d'Unified Manager ne peuvent pas effectuer une mise à niveau sur place vers des versions ultérieures. Les mises à niveau d'Unified Manager sont limitées à un modèle N-2, ce qui signifie qu'une mise à niveau ne peut être effectuée que dans les 2 prochaines versions sur toutes les plates-formes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.16 à partir d'Unified Manager 9.13 et 9.14 uniquement.

Si vous exécutez une version antérieure aux versions prises en charge, votre instance Unified Manager devra d'abord être mise à niveau vers l'une des versions prises en charge, puis mise à niveau vers la version actuelle.

Par exemple, si votre version installée est Unified Manager 9.9 et que vous souhaitez effectuer une mise à niveau vers Unified Manager 9.14, vous devez suivre une séquence de mises à niveau.

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.11 → 9.13
2. Mise à niveau 9.13 → 9.14

3. Mise à niveau 9.13 → 9.16

4. Mise à niveau 9.14 → 9.16

Pour plus d'informations sur la matrice de chemin de mise à niveau, consultez ceci ["article de la base de connaissances \(KB\)"](#) .

Mettre à niveau Unified Manager

Vous pouvez mettre à niveau Unified Manager 9.13 ou 9.14 vers 9.16 en téléchargeant et en exécutant le fichier d'installation sur la plate-forme Windows.

Avant de commencer

- Le système sur lequel vous mettez à niveau Unified Manager doit répondre aux exigences système et logicielles.

Voir ["Configuration matérielle requise"](#) .

Voir ["Logiciel Windows et configuration requise pour son installation"](#) .



À partir d'Unified Manager 9.5, OpenJDK est fourni dans le package d'installation et installé automatiquement. Oracle Java n'est pas pris en charge à partir de Unified Manager 9.5.



Assurez-vous que Microsoft .NET 4.5.2 ou supérieur est installé sur votre système avant de démarrer la mise à niveau.

- MySQL Community Edition est automatiquement mis à niveau lors de la mise à niveau d'Unified Manager. Si la version installée de MySQL sur votre système est antérieure à 8.4.4, le processus de mise à niveau d'Unified Manager met automatiquement à niveau MySQL vers 8.4.4. Vous ne devez pas exécuter une mise à niveau autonome d'une version antérieure de MySQL vers 8.4.4.
- Tous les clusters sont pris en charge, à l'exception des systèmes ASA r2.
- Vous devez disposer des privilèges d'administrateur Windows. Assurez-vous que votre nom d'utilisateur ne commence pas par un point d'exclamation « ! ». Installation of Unified Manager might fail if the user name of user running the installation begins with " !".
- Vous devez disposer d'informations d'identification valides pour vous connecter au site de support NetApp .
- Pour éviter toute perte de données, vous devez avoir créé une sauvegarde de la machine Unified Manager au cas où un problème surviendrait lors de la mise à niveau.
- Vous devez disposer de suffisamment d'espace disque disponible pour effectuer la mise à niveau.

L'espace disponible sur le lecteur d'installation doit être supérieur de 2,5 Go à la taille du répertoire de données. La mise à niveau s'arrête et affiche un message d'erreur indiquant la quantité d'espace à ajouter s'il n'y a pas suffisamment d'espace libre.

- Lors de la mise à niveau, vous serez peut-être invité à confirmer si vous souhaitez conserver les paramètres par défaut précédents pour la conservation des données de performances pendant 13 mois ou les modifier à 6 mois. Après confirmation, les données de performance historiques après 6 mois sont purgées.
- Avant la mise à niveau, vous devez fermer tous les fichiers ou dossiers ouverts dans *<InstallDir>\JDK* et *MySQL Data Directory*.

- Si vous disposez d'un logiciel antivirus actif installé sur votre système Windows, la mise à niveau d'Unified Manager peut échouer. Vous devez désactiver tous les logiciels antivirus sur votre système avant de mettre à niveau Unified Manager.

Pendant le processus de mise à niveau, Unified Manager n'est pas disponible. Vous devez terminer toutes les opérations en cours avant de mettre à niveau Unified Manager.

Si Unified Manager est associé à une instance d' OnCommand Workflow Automation et que de nouvelles versions du logiciel sont disponibles pour les deux produits, vous devez déconnecter les deux produits, puis configurer une nouvelle connexion Workflow Automation après avoir effectué les mises à niveau. Si vous effectuez une mise à niveau vers un seul des produits, vous devez vous connecter à Workflow Automation après la mise à niveau et vérifier qu'il acquiert toujours des données à partir d'Unified Manager.

Étapes

1. Connectez-vous au site de support NetApp et accédez à la page de téléchargement d'Unified Manager :

["Site de support NetApp"](#).

2. Sélectionnez la version requise d'Unified Manager et acceptez le contrat de licence utilisateur final (CLUF).
3. Téléchargez le fichier d'installation Windows ou le fichier zip d'Unified Manager dans un répertoire cible sur le système Windows. Extrayez le fichier zip, si nécessaire, et accédez au répertoire où se trouve le fichier d'installation. Cliquez avec le bouton droit de la souris et exécutez le fichier exécutable du programme d'installation d'Unified Manager (.exe) en tant qu'administrateur.

Unified Manager vous affiche le message suivant :

```
This setup will perform an upgrade of Unified Manager. Do you want to
continue?
```

4. Cliquez sur **Oui**, puis sur **Suivant**.
5. Saisissez le mot de passe root MySQL84 défini lors de l'installation, puis cliquez sur **Suivant**.
6. Lancez l'interface utilisateur Web dans une nouvelle fenêtre sur un navigateur Web pris en charge et connectez-vous pour utiliser la version mise à niveau d'Unified Manager.
7. Si vous avez un logiciel antivirus actif installé sur votre système Windows, assurez-vous d'exclure manuellement les chemins suivants de l'analyse antivirus une fois la mise à niveau terminée :
 - Répertoire de données Unified Manager
 - Répertoire d'installation d'Unified Manager
 - Répertoire de données MySQL



Pour effectuer une mise à niveau silencieuse d'Unified Manager, exécutez la commande suivante :

```
ActiveIQUnifiedManager-<version>.exe /s /v"MYSQL_PASSWORD=<password>
/qn /l*v <system_drive>:\install.log"
```

Mettre à niveau les produits tiers

Vous pouvez mettre à niveau des produits tiers, tels que JRE, sur Unified Manager lorsqu'ils sont installés sur des systèmes Windows.

Les entreprises qui développent ces produits tiers signalent régulièrement des vulnérabilités de sécurité. Vous pouvez mettre à niveau vers des versions plus récentes de ce logiciel à votre rythme.

Mettre à niveau OpenJDK

Vous pouvez effectuer une mise à niveau vers une version plus récente d'OpenJDK sur le serveur Windows sur lequel Unified Manager est installé pour obtenir des correctifs pour les vulnérabilités de sécurité.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows pour le système sur lequel Unified Manager est installé.

Vous pouvez mettre à jour les versions d'OpenJDK au sein des familles de versions. Par exemple, vous pouvez effectuer une mise à niveau d'OpenJDK 11.0.16 vers OpenJDK 11.0.18, mais vous ne pouvez pas effectuer une mise à niveau directement d'OpenJDK 11 vers OpenJDK 12.

Étapes

1. Connectez-vous en tant qu'utilisateur administrateur sur la machine hôte Unified Manager.
2. Téléchargez la version appropriée d'OpenJDK (64 bits) depuis le site OpenJDK sur le système cible.

Par exemple, téléchargez `jdk-11.0.18_windows-x64_bin.zip` from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html>.



Un compte Oracle est requis pour télécharger le fichier. Si vous n'avez pas de compte Oracle, accédez à "[Connexion au compte Oracle](#)" page pour en créer une.

3. Utilisez la console des services Windows pour arrêter les services Unified Manager suivants :
 - Service d'acquisition NetApp Active IQ (Ocie-au)
 - Service de serveur de gestion NetApp Active IQ (Oncommandsvc)
4. Développer le zip déposer.
5. Copiez les répertoires et les fichiers du résultat `jdk` répertoire (par exemple, `jdk-11.0.18` à l'emplacement où Java est installé. Exemple: `C:\Program Files\NetApp\JDK\`
6. Démarrez les services Unified Manager à l'aide de la console des services Windows :
 - Service de serveur de gestion NetApp Active IQ (Oncommandsvc)
 - Service d'acquisition NetApp Active IQ (Ocie-au)

Désinstaller les produits tiers

Après la mise à niveau d'Unified Manager, vous pouvez désinstaller des produits tiers, tels que Python ou Microsoft Visual C++ 2013. Ceci est facultatif.

Désinstaller Python

Étapes

1. Dans le **Panneau de configuration**, sélectionnez **Programmes > Programmes et fonctionnalités**.

2. Sélectionnez Python dans la liste des programmes.
3. Sélectionnez **Désinstaller ce programme**. Désinstallez toutes les versions de Python à l'exception de la 3.12. Assurez-vous de conserver la version 3.12 de Python.

Désinstaller Microsoft Visual C++ 2013

Étapes

1. Dans le **Panneau de configuration**, sélectionnez **Programmes > Programmes et fonctionnalités**.
2. Sélectionnez **Microsoft Visual C++ 2013** dans la liste des programmes.
3. Sélectionnez **Désinstaller ce programme**.

Redémarrer Unified Manager

Vous devrez peut-être redémarrer Unified Manager après avoir apporté des modifications de configuration.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Étapes

1. Connectez-vous à Windows à l'aide du compte administrateur local par défaut.
2. Arrêter les services Unified Manager :

Du...	Arrêtez les services dans l'ordre suivant...
Ligne de commande	a. <code>sc stop ocie-au</code> b. <code>sc stop Oncommandsvc</code>
Gestionnaire de services Microsoft	a. Service d'acquisition NetApp Active IQ (Ocie-au) b. Service de serveur de gestion NetApp Active IQ (Oncommandsvc)

3. Démarrez les services Unified Manager :

Du...	Démarrez les services dans l'ordre suivant...
Ligne de commande	a. <code>sc start Oncommandsvc</code> b. <code>sc start ocie-au</code>
Gestionnaire de services Microsoft	a. Service de serveur de gestion NetApp Active IQ (Oncommandsvc) b. Service d'acquisition NetApp Active IQ (Ocie-au)

Désinstaller Unified Manager

Vous pouvez désinstaller Unified Manager à l'aide de l'assistant Programmes et fonctionnalités ou en effectuant une désinstallation sans assistance à partir de l'interface de ligne de commande.

Avant de commencer

- Vous devez disposer des privilèges d'administrateur Windows.
- Tous les clusters (sources de données) doivent être supprimés du serveur Unified Manager avant de désinstaller le logiciel.
- Vous devez supprimer manuellement les règles de pare-feu créées pour autoriser ou bloquer le port MySQL 3306. Les règles du pare-feu ne sont pas supprimées automatiquement.

Étapes

1. Désinstallez Unified Manager en choisissant l'une des options suivantes :

- Si vous désinstallez Unified Manager à partir de l'assistant **Programmes et fonctionnalités**, procédez comme suit :
 - i. Accédez à **Panneau de configuration > Programmes et fonctionnalités**.
 - ii. Sélectionnez Active IQ Unified Manager et cliquez sur **Désinstaller**.
- Si vous désinstallez Unified Manager à partir de la ligne de commande, procédez comme suit :
 - i. Connectez-vous à la ligne de commande Windows à l'aide des privilèges d'administrateur.
 - ii. Accédez au répertoire Active IQ Unified Manager et exécutez la commande suivante :

```
msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v  
%systemdrive%\UmUnInstall.log
```

Si le contrôle de compte d'utilisateur (UAC) est activé sur le serveur et que vous êtes connecté en tant qu'utilisateur de domaine, vous devez utiliser la méthode de désinstallation par ligne de commande.

Unified Manager est désinstallé de votre système.

2. Désinstallez les packages et données tiers suivants qui ne sont pas supprimés lors de la désinstallation d'Unified Manager :

- Paquets tiers : JRE, MySQL, Microsoft Visual C++ 2015 Redistributable, Python et 7zip
- Données d'application MySQL générées par Unified Manager
- Journaux d'application et contenu du répertoire de données d'application

Effectuer des tâches de configuration et d'administration

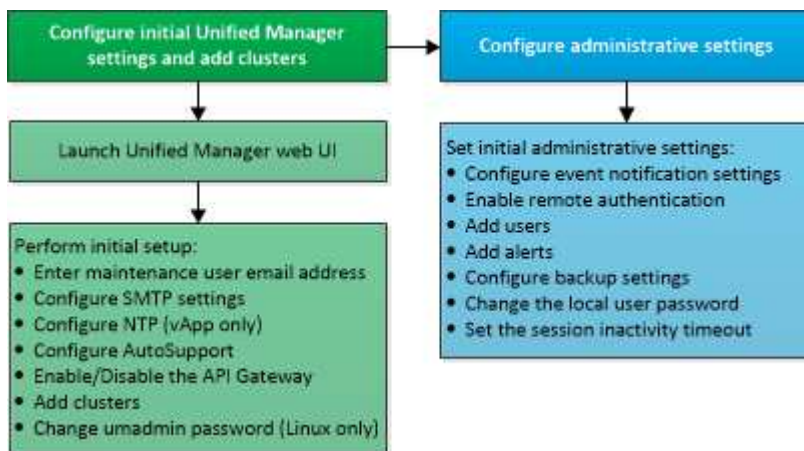
Configurer Active IQ Unified Manager

Après avoir installé Active IQ Unified Manager (anciennement OnCommand Unified Manager), vous devez terminer la configuration initiale (également appelée assistant de première expérience) pour accéder à l'interface utilisateur Web. Vous pouvez ensuite effectuer des tâches de configuration supplémentaires, telles que l'ajout de clusters, la configuration de l'authentification à distance, l'ajout d'utilisateurs et l'ajout d'alertes.

Certaines des procédures décrites dans ce manuel sont nécessaires pour terminer la configuration initiale de votre instance Unified Manager. D'autres procédures sont des paramètres de configuration recommandés qui sont utiles à configurer sur votre nouvelle instance ou qu'il est bon de connaître avant de commencer la surveillance régulière de vos systèmes ONTAP.

Aperçu de la séquence de configuration

Le flux de travail de configuration décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.



Accéder à l'interface Web d'Unified Manager

Après avoir installé Unified Manager, vous pouvez accéder à l'interface utilisateur Web pour configurer Unified Manager afin de pouvoir commencer à surveiller vos systèmes ONTAP.

Avant de commencer

- Si c'est la première fois que vous accédez à l'interface Web, vous devez vous connecter en tant qu'utilisateur de maintenance (ou utilisateur umadmin pour les installations Linux).
- Si vous prévoyez d'autoriser les utilisateurs à accéder à Unified Manager à l'aide du nom court au lieu d'utiliser le nom de domaine complet (FQDN) ou l'adresse IP, votre configuration réseau doit résoudre ce nom court en un FQDN valide.
- Si le serveur utilise un certificat numérique auto-signé, le navigateur peut afficher un avertissement

indiquant que le certificat n'est pas approuvé. Vous pouvez soit reconnaître le risque pour continuer l'accès, soit installer un certificat numérique signé par une autorité de certification (CA) pour l'authentification du serveur.

Étapes

1. Démarrez l'interface Web d'Unified Manager à partir de votre navigateur en utilisant l'URL affichée à la fin de l'installation. L'URL est l'adresse IP ou le nom de domaine complet (FQDN) du serveur Unified Manager.

Le lien est au format suivant : `https://URL` .

2. Connectez-vous à l'interface Web d'Unified Manager à l'aide de vos informations d'identification d'utilisateur de maintenance.



Si vous effectuez trois tentatives infructueuses consécutives pour vous connecter à l'interface Web en une heure, vous serez exclu du système et devrez contacter votre administrateur système. Ceci s'applique uniquement aux utilisateurs locaux.

Effectuer la configuration initiale de l'interface Web d'Unified Manager

Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiales, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, l'hôte du serveur SMTP et l'ajout de clusters ONTAP .

Avant de commencer

Vous devez avoir effectué les opérations suivantes :

- Lancement de l'interface Web d'Unified Manager à l'aide de l'URL fournie après l'installation
- Connecté à l'aide du nom d'utilisateur et du mot de passe de maintenance (utilisateur umadmin pour les installations Linux) créés lors de l'installation

La page de démarrage d' Active IQ Unified Manager s'affiche uniquement lorsque vous accédez pour la première fois à l'interface utilisateur Web. La page ci-dessous provient d'une installation sur VMware.

Active IQ Unified Manager

All

Search All Storage Objects and Actions

Getting Started

1

2

3

4

5

Email

AutoSupport

API Gateway

Add ONTAP Clusters

Finish

Notifications

Configure your email server for assistance in case you forget your password.

Maintenance User Email

Email

mgo@eng.netapp.com

SMTP Server

Host Name or IP Address

email.eng.netapp.com

Port

25

User Name

admin

Password

☐ Use STARTTLS
 [i](#)

☐ Use SSL
 [i](#)

Continue

Si vous souhaitez modifier l'une de ces options ultérieurement, vous pouvez sélectionner votre choix parmi les options générales dans le volet de navigation de gauche d'Unified Manager. Notez que le paramètre NTP est uniquement destiné aux installations VMware et qu'il peut être modifié ultérieurement à l'aide de la console de maintenance Unified Manager.

Étapes

1. Dans la page Configuration initiale Active IQ Unified Manager , saisissez l'adresse e-mail de l'utilisateur de maintenance, le nom d'hôte du serveur SMTP et toutes les options SMTP supplémentaires, ainsi que le serveur NTP (installations VMware uniquement). Cliquez ensuite sur **Continuer**.



Si vous avez sélectionné l'option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Continuer**. Vérifiez les détails du certificat et acceptez le certificat pour continuer avec les paramètres de configuration initiale de l'interface utilisateur Web.

2. Sur la page AutoSupport , cliquez sur **Accepter et continuer** pour activer l'envoi de messages AutoSupport d'Unified Manager à NetAppActive IQ.

Si vous devez désigner un proxy pour fournir un accès Internet afin d'envoyer du contenu AutoSupport , ou

si vous souhaitez désactiver AutoSupport, utilisez l'option **Général** > * AutoSupport* de l'interface utilisateur Web.

3. Sur les systèmes Red Hat, modifiez le mot de passe de l'utilisateur umadmin de la chaîne par défaut « admin » à une chaîne personnalisée.
4. Dans la page Configurer la passerelle API, sélectionnez si vous souhaitez utiliser la fonctionnalité de passerelle API qui permet à Unified Manager de gérer les clusters ONTAP que vous prévoyez de surveiller à l'aide des API REST ONTAP . Cliquez ensuite sur **Continuer**.

Vous pouvez activer ou désactiver ce paramètre ultérieurement dans l'interface utilisateur Web à partir de **Général** > **Paramètres des fonctionnalités** > **Passerelle API**. Pour plus d'informations sur les API, voir "[Prise en main des API REST Active IQ Unified Manager](#)".

5. Ajoutez les clusters que vous souhaitez qu'Unified Manager gère, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez disposer du nom d'hôte ou de l'adresse IP de gestion du cluster (IPv4 ou IPv6) ainsi que des informations d'identification du nom d'utilisateur et du mot de passe - l'utilisateur doit avoir le rôle « admin ».

Cette étape est facultative. Vous pouvez ajouter des clusters ultérieurement dans l'interface utilisateur Web à partir de **Gestion du stockage** > **Configuration du cluster**.

6. Dans la page Résumé, vérifiez que tous les paramètres sont corrects et cliquez sur **Terminer**.

La page de démarrage se ferme et la page du tableau de bord d'Unified Manager s'affiche.

Ajouter des clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir surveiller le cluster. Cela inclut la possibilité d'obtenir des informations sur le cluster telles que l'état, la capacité, les performances et la configuration du cluster afin que vous puissiez trouver et résoudre tous les problèmes qui pourraient survenir.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir les informations suivantes :
 - Unified Manager prend en charge les clusters ONTAP sur site, ONTAP Select et Cloud Volumes ONTAP.
 - Nom d'hôte ou adresse IP de gestion du cluster

Le nom d'hôte est le nom de domaine complet ou le nom court qu'Unified Manager utilise pour se connecter au cluster. Le nom d'hôte doit être résolu en adresse IP de gestion du cluster.

L'adresse IP de gestion de cluster doit être la LIF de gestion de cluster de la machine virtuelle de stockage administratif (SVM). Si vous utilisez un LIF de gestion de nœud, l'opération échoue.

- Le cluster doit exécuter le logiciel ONTAP version 9.1 ou supérieure.
- Nom d'utilisateur et mot de passe de l'administrateur ONTAP

Ce compte doit avoir le rôle *admin* avec l'accès à l'application défini sur *ontapi*, *console* et *http*.

- Le numéro de port pour se connecter au cluster à l'aide du protocole HTTPS (généralement le port

- Vous possédez les certificats requis :

Certificat SSL (HTTPS) : Ce certificat appartient à Unified Manager. Un certificat SSL auto-signé (HTTPS) par défaut est généré avec une nouvelle installation d'Unified Manager. NetApp vous recommande de le mettre à niveau vers un certificat signé par une autorité de certification pour une meilleure sécurité. Si le certificat du serveur expire, vous devez le régénérer et redémarrer Unified Manager pour que les services intègrent le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, voir ["Générer un certificat de sécurité HTTPS"](#) .

Certificat EMS : Ce certificat appartient à Unified Manager. Il est utilisé lors de l'authentification pour les notifications EMS reçues d' ONTAP.

Certificats pour la communication TLS mutuelle : Utilisés lors de la communication TLS mutuelle entre Unified Manager et ONTAP. L'authentification basée sur les certificats est activée pour un cluster, en fonction de la version ONTAP . Si le cluster exécutant la version ONTAP est inférieur à 9.5, l'authentification basée sur les certificats n'est pas activée.

L'authentification basée sur les certificats n'est pas activée automatiquement pour un cluster si vous mettez à jour une ancienne version d'Unified Manager. Cependant, vous pouvez l'activer en modifiant et en enregistrant les détails du cluster. Si le certificat expire, vous devez le régénérer pour incorporer le nouveau certificat. Pour plus d'informations sur l'affichage et la régénération du certificat, voir ["Modification des clusters"](#) .



- Vous pouvez ajouter un cluster à partir de l'interface utilisateur Web et l'authentification basée sur les certificats est automatiquement activée.
- Vous pouvez ajouter un cluster via Unified Manager CLI, l'authentification basée sur un certificat n'est pas activée par défaut. Si vous ajoutez un cluster à l'aide de l'interface de ligne de commande d'Unified Manager, il est nécessaire de modifier le cluster à l'aide de l'interface utilisateur d'Unified Manager. Tu peux voir ["Commandes CLI Unified Manager prises en charge"](#) pour ajouter un cluster à l'aide de Unified Manager CLI.
- Si l'authentification basée sur les certificats est activée pour un cluster et que vous effectuez la sauvegarde d'Unified Manager à partir d'un serveur et la restaurez sur un autre serveur Unified Manager où le nom d'hôte ou l'adresse IP est modifié, la surveillance du cluster peut échouer. Pour éviter l'échec, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, voir ["Modification des clusters"](#) .

+

Certificats de cluster : Ce certificat appartient à ONTAP. Vous ne pouvez pas ajouter un cluster à Unified Manager avec un certificat expiré et si le certificat a déjà expiré, vous devez le régénérer avant d'ajouter le cluster. Pour plus d'informations sur la génération de certificats, consultez l'article de la base de connaissances (KB) ["Comment renouveler un certificat auto-signé ONTAP dans l'interface utilisateur de System Manager"](#) .

- Vous devez disposer d'un espace suffisant sur le serveur Unified Manager. Vous ne pouvez pas ajouter un cluster au serveur lorsque plus de 90 % de l'espace dans le répertoire de base de données est déjà consommé.

Pour une configuration MetroCluster , vous devez ajouter les clusters locaux et distants, et les clusters doivent être configurés correctement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs requises, telles que le nom d'hôte ou l'adresse IP du cluster, le nom d'utilisateur, le mot de passe et le numéro de port.

Vous pouvez modifier l'adresse IP de gestion du cluster d'IPv6 à IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est reflétée dans la grille du cluster et dans la page de configuration du cluster une fois le prochain cycle de surveillance terminé.

4. Cliquez sur **Soumettre**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le cluster.
6. Cliquez sur **Oui**.

Après avoir enregistré les détails du cluster, vous pouvez voir le certificat pour la communication TLS mutuelle pour un cluster.

Si l'authentification basée sur un certificat n'est pas activée, Unified Manager vérifie le certificat uniquement lorsque le cluster est ajouté initialement. Unified Manager ne vérifie pas le certificat pour chaque appel d'API à ONTAP.

Une fois tous les objets d'un nouveau cluster découverts, Unified Manager commence à collecter les données de performances historiques des 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité vous fournit plus de deux semaines d'informations sur les performances d'un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données de performances du cluster en temps réel sont collectées, par défaut, toutes les cinq minutes.



Étant donné que la collecte de 15 jours de données de performances nécessite beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur trop de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte sera interrompue et vous verrez des écarts dans les graphiques de performances pour la période manquante.



Si vous recevez un message d'erreur indiquant que vous ne pouvez pas ajouter le cluster, vérifiez si les horloges des deux systèmes ne sont pas synchronisées et si la date de début du certificat HTTPS d'Unified Manager est postérieure à la date du cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide de NTP ou d'un service similaire.

Informations connexes

["Installation d'un certificat HTTPS signé et renvoyé par une autorité de certification"](#)

Configurer Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour envoyer des notifications qui vous alertent des événements dans votre environnement. Avant de pouvoir envoyer des notifications, vous devez configurer plusieurs autres options d'Unified Manager.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Après avoir déployé Unified Manager et terminé la configuration initiale, vous devez envisager de configurer votre environnement pour déclencher des alertes et générer des e-mails de notification ou des interruptions SNMP en fonction de la réception d'événements.

Étapes

1. "Configurer les paramètres de notification d'événement".

Si vous souhaitez que des notifications d'alerte soient envoyées lorsque certains événements se produisent dans votre environnement, vous devez configurer un serveur SMTP et fournir une adresse e-mail à partir de laquelle la notification d'alerte sera envoyée. Si vous souhaitez utiliser des interruptions SNMP, vous pouvez sélectionner cette option et fournir les informations nécessaires.

2. "Activer l'authentification à distance".

Si vous souhaitez que les utilisateurs LDAP ou Active Directory distants accèdent à l'instance Unified Manager et reçoivent des notifications d'alerte, vous devez activer l'authentification à distance.

3. "Ajouter des serveurs d'authentification".

Vous pouvez ajouter des serveurs d'authentification afin que les utilisateurs distants du serveur d'authentification puissent accéder à Unified Manager.

4. "Ajouter des utilisateurs".

Vous pouvez ajouter plusieurs types différents d'utilisateurs locaux ou distants et attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous attribuez un utilisateur pour recevoir les notifications d'alerte.

5. "Ajouter des alertes".

Après avoir ajouté l'adresse e-mail pour l'envoi de notifications, ajouté des utilisateurs pour recevoir les notifications, configuré vos paramètres réseau et configuré les options SMTP et SNMP nécessaires à votre environnement, vous pouvez attribuer des alertes.

Configurer les paramètres de notification d'événement

Vous pouvez configurer Unified Manager pour envoyer des notifications d'alerte lorsqu'un événement est généré ou lorsqu'un événement est attribué à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour envoyer l'alerte et définir différents mécanismes de notification. Par exemple, les notifications d'alerte peuvent être envoyées sous forme d'e-mails ou d'interruptions SNMP.

Avant de commencer

Vous devez avoir les informations suivantes :

- Adresse e-mail à partir de laquelle la notification d'alerte est envoyée

L'adresse e-mail apparaît dans le champ « De » dans les notifications d'alerte envoyées. Si l'e-mail ne peut pas être délivré pour une raison quelconque, cette adresse e-mail est également utilisée comme destinataire du courrier non distribuable.

- Nom d'hôte du serveur SMTP, ainsi que le nom d'utilisateur et le mot de passe pour accéder au serveur
- Nom d'hôte ou adresse IP de l'hôte de destination de l'interruption qui recevra l'interruption SNMP, ainsi que la version SNMP, le port d'interruption sortant, la communauté et d'autres valeurs de configuration SNMP requises

Pour spécifier plusieurs destinations d'interruption, séparez chaque hôte par une virgule. Dans ce cas, tous les autres paramètres SNMP, tels que la version et le port de trappe sortante, doivent être les mêmes pour tous les hôtes de la liste.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Notifications**.
2. Dans la page Notifications, configurez les paramètres appropriés.

Remarques :

- Si l'adresse de l'expéditeur est pré-remplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la remplacer par une adresse e-mail réelle et fonctionnelle pour vous assurer que toutes les notifications par e-mail sont envoyées avec succès.
 - Si le nom d'hôte du serveur SMTP ne peut pas être résolu, vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) du serveur SMTP au lieu du nom d'hôte.
3. Cliquez sur **Enregistrer**.
 4. Si vous avez sélectionné l'option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Enregistrer**. Vérifiez les détails du certificat et acceptez le certificat pour enregistrer les paramètres de notification.

Vous pouvez cliquer sur le bouton **Afficher les détails du certificat** pour afficher les détails du certificat. Si le certificat existant a expiré, décochez la case **Utiliser STARTTLS** ou **Utiliser SSL**, enregistrez les paramètres de notification, puis cochez à nouveau la case **Utiliser STARTTLS** ou **Utiliser SSL** pour afficher un nouveau certificat.

Activer l'authentification à distance

Vous pouvez activer l'authentification à distance afin que le serveur Unified Manager puisse communiquer avec vos serveurs d'authentification. Les utilisateurs du serveur d'authentification peuvent accéder à l'interface graphique d'Unified Manager pour gérer les objets de stockage et les données.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.



Le serveur Unified Manager doit être connecté directement au serveur d'authentification. Vous devez désactiver tous les clients LDAP locaux tels que SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Vous pouvez activer l'authentification à distance à l'aide d'Open LDAP ou d'Active Directory. Si l'authentification à distance est désactivée, les utilisateurs distants ne peuvent pas accéder à Unified Manager.

L'authentification à distance est prise en charge via LDAP et LDAPS (Secure LDAP). Unified Manager utilise

389 comme port par défaut pour la communication non sécurisée et 636 comme port par défaut pour la communication sécurisée.



Le certificat utilisé pour authentifier les utilisateurs doit être conforme au format X.509.

Étapes

- 1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
- 2. Cochez la case **Activer l’authentification à distance....**
- 3. Dans le champ Service d’authentification, sélectionnez le type de service et configurez le service d’authentification.

Pour le type d’authentification...	Entrez les informations suivantes...
Active Directory	• Nom de l’administrateur du serveur d’authentification dans l’un des formats suivants : ◦ domainname\username ◦ username@domainname ◦ Bind Distinguished Name(en utilisant la notation LDAP appropriée) • Mot de passe administrateur • Nom distinctif de base (en utilisant la notation LDAP appropriée)
Ouvrir le LDAP	• Lier le nom distinctif (dans la notation LDAP appropriée) • Lier le mot de passe • Nom distinctif de base

Si l’authentification d’un utilisateur Active Directory prend beaucoup de temps ou expire, le serveur d’authentification met probablement beaucoup de temps à répondre. La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d’authentification.

Si vous sélectionnez l’option Utiliser une connexion sécurisée pour le serveur d’authentification, Unified Manager communique avec le serveur d’authentification à l’aide du protocole Secure Sockets Layer (SSL).

- 4. **Facultatif** : ajoutez des serveurs d’authentification et testez l’authentification.
- 5. Cliquez sur **Enregistrer**.

Désactiver les groupes imbriqués de l’authentification à distance

Si l’authentification à distance est activée, vous pouvez désactiver l’authentification de groupe imbriquée afin que seuls les utilisateurs individuels, et non les membres du groupe, puissent s’authentifier à distance auprès d’Unified Manager. Vous pouvez désactiver les groupes imbriqués lorsque vous souhaitez améliorer le temps de réponse de l’authentification Active Directory.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application.
- La désactivation des groupes imbriqués s'applique uniquement lors de l'utilisation d'Active Directory.

La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification. Si la prise en charge des groupes imbriqués est désactivée et si un groupe distant est ajouté à Unified Manager, les utilisateurs individuels doivent être membres du groupe distant pour s'authentifier auprès de Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Cochez la case **Désactiver la recherche de groupe imbriqué**.
3. Cliquez sur **Enregistrer**.

Configurer les services d'authentification

Les services d'authentification permettent l'authentification des utilisateurs distants ou des groupes distants dans un serveur d'authentification avant de leur fournir l'accès à Unified Manager. Vous pouvez authentifier les utilisateurs en utilisant des services d'authentification prédéfinis (tels qu'Active Directory ou OpenLDAP) ou en configurant votre propre mécanisme d'authentification.

Avant de commencer

- Vous devez avoir activé l'authentification à distance.
- Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Sélectionnez l'un des services d'authentification suivants :

Si vous sélectionnez...	Alors fais ceci...
Active Directory	a. Entrez le nom et le mot de passe de l'administrateur. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est cn=ou,dc=domain,dc=com.

Si vous sélectionnez...	Alors fais ceci...
OpenLDAP	a. Saisissez le nom distinctif et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est cn=ou,dc=domain,dc=com.
Autres	a. Saisissez le nom distinctif et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est cn=ou,dc=domain,dc=com. c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. d. Saisissez le nom d'utilisateur, l'appartenance au groupe, le groupe d'utilisateurs et les attributs du membre.



Si vous souhaitez modifier le service d'authentification, vous devez supprimer tous les serveurs d'authentification existants, puis ajouter de nouveaux serveurs d'authentification.

3. Cliquez sur **Enregistrer**.

Ajouter des serveurs d'authentification

Vous pouvez ajouter des serveurs d'authentification et activer l'authentification à distance sur le serveur de gestion afin que les utilisateurs distants du serveur d'authentification puissent accéder à Unified Manager.

Avant de commencer

- Les informations suivantes doivent être disponibles :
 - Nom d'hôte ou adresse IP du serveur d'authentification
 - Numéro de port du serveur d'authentification
- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification afin que le serveur de gestion puisse authentifier les utilisateurs ou les groupes distants dans le serveur d'authentification.
- Vous devez disposer du rôle d'administrateur d'application.

Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (HA) (utilisant la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsque l'un des serveurs d'authentification est inaccessible.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Activer ou désactiver l'option **Utiliser une connexion sécurisée** :

Si vous voulez...	Alors fais ceci...
Activez-le	- Sélectionnez l'option Utiliser une connexion sécurisée. - Dans la zone Serveurs d'authentification, cliquez sur Ajouter. - Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. - Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. - Dans la boîte de dialogue Afficher le certificat, vérifiez les informations du certificat, puis cliquez sur Fermer. - Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Oui.  Lorsque vous activez l'option Utiliser l'authentification par connexion sécurisée, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise le port 636 comme port par défaut pour la communication sécurisée et le numéro de port 389 pour la communication non sécurisée.
Désactivez-le	- Désactivez l'option Utiliser une connexion sécurisée. - Dans la zone Serveurs d'authentification, cliquez sur Ajouter. - Dans la boîte de dialogue Ajouter un serveur d'authentification, spécifiez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les détails du port. - Cliquez sur Ajouter.

Le serveur d'authentification que vous avez ajouté s'affiche dans la zone Serveurs.

3. Effectuez un test d'authentification pour confirmer que vous pouvez authentifier les utilisateurs sur le serveur d'authentification que vous avez ajouté.

Tester la configuration des serveurs d'authentification

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion est en mesure de communiquer avec eux. Vous pouvez valider la configuration en recherchant un utilisateur distant ou un groupe distant à partir de vos serveurs d'authentification et en les authentifiant à l'aide des paramètres configurés.

Avant de commencer

- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification afin que le serveur Unified Manager puisse authentifier l'utilisateur distant ou le groupe distant.
- Vous devez avoir ajouté vos serveurs d'authentification afin que le serveur de gestion puisse rechercher l'utilisateur distant ou le groupe distant à partir de ces serveurs et les authentifier.
- Vous devez disposer du rôle d'administrateur d'application.

Si le service d'authentification est défini sur Active Directory et si vous validez l'authentification des utilisateurs distants qui appartiennent au groupe principal du serveur d'authentification, les informations sur le groupe principal ne s'affichent pas dans les résultats d'authentification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Cliquez sur **Tester l'authentification**.
3. Dans la boîte de dialogue Tester l'utilisateur, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom d'utilisateur du groupe distant, puis cliquez sur **Tester**.

Si vous authentifiez un groupe distant, vous ne devez pas saisir le mot de passe.

Ajouter des alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer des alertes pour une seule ressource, pour un groupe de ressources ou pour des événements d'un type de gravité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être notifié et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré les paramètres de notification tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou les adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez qu'un script s'exécute en fonction de l'événement, vous devez avoir ajouté le script à Unified Manager à l'aide de la page Scripts.
- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un événement, en plus de créer une alerte à partir de la page Configuration des alertes, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page Configuration des alertes, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter une alerte, cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et sélectionnez les ressources à inclure ou à exclure de l'alerte.

Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Le nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles affiche uniquement les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

Si une ressource est conforme aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion a priorité sur la règle d'inclusion et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Événements** et sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lesquels vous souhaitez déclencher une alerte.



Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et attribuez un script à exécuter lorsqu'une alerte est générée.



Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur précédemment sélectionné. De plus, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page Utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

Vous pouvez également choisir de notifier les utilisateurs via des interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Cet exemple montre comment créer une alerte qui répond aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz »
- Événements : inclut tous les événements de santé critiques
- Actions : inclut « sample@domain.com », un script « Test », et l'utilisateur doit être notifié toutes les 15 minutes

Effectuez les étapes suivantes dans la boîte de dialogue Ajouter une alerte :

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources** et dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.
 - a. Saisissez **abc** dans le champ **Le nom contient** pour afficher les volumes dont le nom contient « abc ».
 - b. Sélectionnez **+[\[All Volumes whose name contains 'abc'\]](#)+** dans la zone Ressources disponibles et déplacez-le vers la zone Ressources sélectionnées.
 - c. Cliquez sur **Exclure**, saisissez **xyz** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Événements** et sélectionnez **Critique** dans le champ Gravité de l'événement.
4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions** et saisissez **sample@domain.com** dans le champ Alerter ces utilisateurs.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

Vous pouvez configurer une alerte pour envoyer des notifications répétées aux destinataires pendant une durée spécifiée. Vous devez déterminer l'heure à partir de laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Sélectionner le script à exécuter, sélectionnez le script **Tester**.
8. Cliquez sur **Enregistrer**.

Modifier le mot de passe de l'utilisateur local

Vous pouvez modifier votre mot de passe de connexion utilisateur local pour éviter d'éventuels risques de sécurité.

Avant de commencer

Vous devez être connecté en tant qu'utilisateur local.

Les mots de passe de l'utilisateur de maintenance et des utilisateurs distants ne peuvent pas être modifiés à l'aide de ces étapes. Pour modifier le mot de passe d'un utilisateur distant, contactez votre administrateur de mots de passe. Pour modifier le mot de passe de l'utilisateur de maintenance, voir "[Utilisation de la console de maintenance](#)".

Étapes

1. Connectez-vous à Unified Manager.
2. Dans la barre de menu supérieure, cliquez sur l'icône utilisateur, puis sur **Modifier le mot de passe**.

L'option **Modifier le mot de passe** ne s'affiche pas si vous êtes un utilisateur distant.

3. Dans la boîte de dialogue Modifier le mot de passe, entrez le mot de passe actuel et le nouveau mot de passe.
4. Cliquez sur **Enregistrer**.

Si Unified Manager est configuré dans une configuration haute disponibilité, vous devez modifier le mot de passe sur le deuxième nœud de la configuration. Les deux instances doivent avoir le même mot de passe.

Définir le délai d'inactivité de la session

Vous pouvez spécifier la valeur du délai d'inactivité pour Unified Manager afin que la session soit terminée automatiquement après une certaine période d'inactivité. Par défaut, le délai d'expiration est défini sur 4 320 minutes (72 heures).

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Ce paramètre affecte toutes les sessions utilisateur connectées.



Cette option n'est pas disponible si vous avez activé l'authentification SAML (Security Assertion Markup Language).

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Paramètres des fonctionnalités**.
2. Dans la page **Paramètres des fonctionnalités**, spécifiez le délai d'inactivité en choisissant l'une des options suivantes :

Si vous voulez...	Alors fais ceci...
N'avez pas de délai d'expiration défini pour que la session ne soit jamais fermée automatiquement	Dans le panneau Délai d'inactivité , déplacez le bouton du curseur vers la gauche (désactivé) et cliquez sur Appliquer .
Définissez un nombre spécifique de minutes comme valeur de délai d'expiration	Dans le panneau Délai d'inactivité , déplacez le bouton du curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes et cliquez sur Appliquer .

Définir le délai d'expiration de la session via la CLI

Vous pouvez définir une valeur de délai d'expiration de session maximale pour Unified Manager à l'aide de l'interface de ligne de commande afin que la session soit terminée automatiquement après une certaine période de temps. Par défaut, le délai d'expiration de votre session est défini sur la valeur maximale, qui est de 4 320 minutes (72 heures). Cela signifie que votre session se termine automatiquement après 72 heures, même si vous êtes connecté et utilisez activement Unified Manager.

À propos de cette tâche

Vous devez disposer du rôle d'administrateur d'application.

Le paramètre de délai d'expiration de session affecte toutes les sessions utilisateur connectées.

Étapes

1. Connectez-vous à l'interface de ligne de commande Unified Manager en saisissant le `um cli login` commande. Utilisez un nom d'utilisateur et un mot de passe valides pour l'authentification.
2. Entrez le `um option set max.session.timeout.value=<in mins>` commande pour modifier la

valeur du délai d'expiration de la session.

Modifier le nom d'hôte d'Unified Manager

À un moment donné, vous souhaitez peut-être modifier le nom d'hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous souhaitez peut-être renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de cluster surveillé.

Les étapes requises pour modifier le nom d'hôte sont différentes selon qu'Unified Manager s'exécute sur un serveur VMware ESXi, sur un serveur Red Hat Linux ou sur un serveur Microsoft Windows.

Modifier le nom d'hôte de l'appliance virtuelle Unified Manager

Un nom est attribué à l'hôte réseau lors du premier déploiement de l'appliance virtuelle Unified Manager. Vous pouvez modifier le nom de l'hôte après le déploiement. Si vous modifiez le nom d'hôte, vous devez également régénérer le certificat HTTPS.

Avant de commencer

Vous devez être connecté à Unified Manager en tant qu'utilisateur de maintenance ou disposer du rôle d'administrateur d'applications qui vous est attribué pour effectuer ces tâches.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web d'Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous auriez alors désigné un nom pour l'hôte du réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être extrait du DNS. Si DHCP ou DNS n'est pas correctement configuré, le nom d'hôte « Unified Manager » est automatiquement attribué et associé au certificat de sécurité.

Quelle que soit la manière dont le nom d'hôte a été attribué, si vous modifiez le nom d'hôte et que vous avez l'intention d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web en utilisant l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom d'hôte. Cependant, il est recommandé de mettre à jour le certificat afin que le nom d'hôte dans le certificat corresponde au nom d'hôte réel.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans WFA.

Le nouveau certificat ne prend effet qu'une fois la machine virtuelle Unified Manager redémarrée.

Étapes

1. Générer un certificat de sécurité HTTPS

Si vous souhaitez utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez régénérer le certificat HTTPS pour l'associer au nouveau nom d'hôte.

2. Redémarrer la machine virtuelle Unified Manager

Après avoir régénéré le certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Générer un certificat de sécurité HTTPS

Lorsque Active IQ Unified Manager est installé pour la première fois, un certificat HTTPS par défaut est installé. Vous pouvez générer un nouveau certificat de sécurité HTTPS qui remplace le certificat existant.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom distinctif (DN) ou si vous souhaitez une taille de clé plus élevée, une période d'expiration plus longue ou si le certificat actuel a expiré.

Si vous n'avez pas accès à l'interface utilisateur Web d'Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Lors de la régénération des certificats, vous pouvez définir la taille de la clé et la durée de validité de la clé. Si vous utilisez le `Reset Server Certificate` option depuis la console de maintenance, puis un nouveau certificat HTTPS est créé qui est valable 397 jours. Ce certificat aura une clé RSA de taille 2048 bits.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Certificat HTTPS**.
2. Cliquez sur **Régénérer le certificat HTTPS**.

La boîte de dialogue Régénérer le certificat HTTPS s'affiche.

3. Sélectionnez l'une des options suivantes en fonction de la manière dont vous souhaitez générer le certificat :

Si vous voulez...	Fais ceci...
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option Régénérer à l'aide des attributs de certificat actuels .

Si vous voulez...	Fais ceci...
Générer le certificat en utilisant différentes valeurs	Cliquez sur l'option Mettre à jour les attributs du certificat actuel. Les champs Nom commun et Noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le « Nom commun » doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez saisir des valeurs, par exemple, pour l'E-MAIL, l'ENTREPRISE, le SERVICE, la Ville, l'État et le Pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner parmi la TAILLE DE CLÉ disponible (l'algorithme de clé est « RSA ») et la PÉRIODE DE VALIDITÉ.  • Les valeurs autorisées pour la taille de la clé sont 2048 , 3072 et 4096 . • Les périodes de validité sont de minimum 1 jour à maximum 36 500 jours. Même si une période de validité de 36 500 jours est autorisée, il est recommandé d'utiliser une période de validité ne dépassant pas 397 jours ou 13 mois. Car si vous sélectionnez une période de validité de plus de 397 jours et prévoyez d'exporter un CSR pour ce certificat et de le faire signer par une autorité de certification connue, la validité du certificat signé qui vous sera renvoyé par l'autorité de certification sera réduite à 397 jours. • Vous pouvez sélectionner la case à cocher « Exclure les informations d'identification locales (par exemple, localhost) » si vous souhaitez supprimer les informations d'identification locales du champ Noms alternatifs du certificat. Lorsque cette case à cocher est sélectionnée, seul ce que vous saisissez dans le champ est utilisé dans le champ Noms alternatifs. Si ce champ est laissé vide, le certificat résultant n'aura pas du tout de champ Noms alternatifs.

4. Cliquez sur **Oui** pour régénérer le certificat.
5. Redémarrez le serveur Unified Manager pour que le nouveau certificat prenne effet.
6. Vérifiez les nouvelles informations du certificat en affichant le certificat HTTPS.

Redémarrer la machine virtuelle Unified Manager

Vous pouvez redémarrer la machine virtuelle à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou s'il y a un problème avec la machine virtuelle.

Avant de commencer

L'appareil virtuel est sous tension.

Vous êtes connecté à la console de maintenance en tant qu'utilisateur de maintenance.

Vous pouvez également redémarrer la machine virtuelle à partir de vSphere en utilisant l'option **Redémarrer l'invité**. Consultez la documentation VMware pour plus d'informations.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration système > Redémarrer la machine virtuelle**.

Modifier le nom d'hôte d'Unified Manager sur les systèmes Linux

À un moment donné, vous souhaitez peut-être modifier le nom d'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous souhaitez peut-être renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de cluster surveillé lorsque vous répertoriez vos machines Linux.

Avant de commencer

Vous devez disposer d'un accès utilisateur root au système Linux sur lequel Unified Manager est installé.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web d'Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous auriez alors désigné un nom pour l'hôte du réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être extrait du serveur DNS.

Quelle que soit la manière dont le nom d'hôte a été attribué, si vous modifiez le nom d'hôte et avez l'intention d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web en utilisant l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom d'hôte. Cependant, il est recommandé de mettre à jour le certificat afin que le nom d'hôte dans le certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend effet qu'une fois la machine Linux redémarrée.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Unified Manager que vous souhaitez modifier.
2. Arrêtez le logiciel Unified Manager et le logiciel MySQL associé en entrant la commande suivante :

```
systemctl stop ocieau ocie mysqld
```

3. Changer le nom de l'hôte en utilisant Linux `hostnamectl` commande:

```
hostnamectl set-hostname new_FQDN
```

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. Régénérer le certificat HTTPS pour le serveur :

```
/opt/netapp/essentials/bin/cert.sh create
```

5. Redémarrez le service réseau :

```
systemctl restart NetworkManager.service
```

6. Une fois le service redémarré, vérifiez si le nouveau nom d'hôte est capable de se pinger lui-même :

```
ping new_hostname
```

```
ping nuhost
```

Cette commande doit renvoyer la même adresse IP que celle définie précédemment pour le nom d'hôte d'origine.

7. Une fois que vous avez terminé et vérifié le changement de nom d'hôte, redémarrez Unified Manager en entrant la commande suivante :

```
systemctl start mysqld ocie ocieau
```

Activer et désactiver la gestion du stockage basée sur des politiques

À partir d'Unified Manager 9.7, vous pouvez provisionner des charges de travail de stockage (volumes et LUN) sur vos clusters ONTAP et gérer ces charges de travail en fonction des niveaux de service de performances attribués. Cette fonctionnalité est similaire à la création de charges de travail dans ONTAP System Manager et à l'attachement de stratégies QoS, mais lorsqu'elle est appliquée à l'aide d'Unified Manager, vous pouvez provisionner et gérer les charges de travail sur tous les clusters surveillés par votre instance Unified Manager.

Vous devez disposer du rôle d'administrateur d'application.

Cette option est activée par défaut, mais vous pouvez la désactiver si vous ne souhaitez pas provisionner et gérer les charges de travail à l'aide d'Unified Manager.

Lorsqu'elle est activée, cette option fournit de nombreux nouveaux éléments dans l'interface utilisateur :

Nouveau contenu	Pays
Une page pour provisionner de nouvelles charges de travail	Disponible depuis Tâches courantes > Provisionnement
Une page pour créer des politiques de niveau de service de performance	Disponible depuis Paramètres > Politiques > Niveaux de service de performance
Une page pour créer des politiques d'efficacité de stockage des performances	Disponible depuis Paramètres > Politiques > Efficacité du stockage
Panneaux décrivant vos performances de charge de travail actuelles et vos IOPS de charge de travail	Disponible depuis le tableau de bord

Consultez l'aide en ligne du produit pour plus d'informations sur ces pages et sur cette fonctionnalité.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Paramètres des fonctionnalités**.
2. Dans la page **Paramètres des fonctionnalités**, désactivez ou activez la gestion du stockage basée sur des politiques en choisissant l'une des options suivantes :

Si vous voulez...	Alors fais ceci...
Désactiver la gestion du stockage basée sur des politiques	Dans le panneau Gestion du stockage basée sur des politiques , déplacez le bouton du curseur vers la gauche.
Activer la gestion du stockage basée sur des politiques	Dans le panneau Gestion du stockage basée sur des politiques , déplacez le bouton du curseur vers la droite.

Configurer la sauvegarde d'Unified Manager

Vous pouvez configurer la capacité de sauvegarde sur Unified Manager via un ensemble d'étapes de configuration à effectuer sur les systèmes hôtes et via la console de maintenance.

Pour plus d'informations sur les étapes de configuration, voir "[Gestion des opérations de sauvegarde et de restauration](#)".

Gérer les paramètres des fonctionnalités

La page Paramètres des fonctionnalités vous permet d'activer et de désactiver des fonctionnalités spécifiques dans Active IQ Unified Manager. Cela inclut la création et la gestion d'objets de stockage en fonction de politiques, l'activation de la passerelle API et de la bannière de connexion, le téléchargement de scripts pour la gestion des alertes, l'expiration d'une session d'interface utilisateur Web en fonction du temps d'inactivité et la

désactivation de la réception des événements de la plateforme Active IQ .



La page Paramètres des fonctionnalités est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur d'application.

Pour plus d'informations sur le téléchargement de scripts, voir ["Activation et désactivation du téléchargement de scripts"](#) .

Activer la gestion du stockage basée sur des politiques

L'option **Gestion du stockage basée sur des politiques** permet une gestion du stockage basée sur des objectifs de niveau de service (SLO). Cette option est activée par défaut.

En activant cette fonctionnalité, vous pouvez provisionner des charges de travail de stockage sur les clusters ONTAP ajoutés à votre instance Active IQ Unified Manager et gérer ces charges de travail en fonction des niveaux de service de performances et des politiques d'efficacité de stockage attribués.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité depuis **Général > Paramètres des fonctionnalités > Gestion du stockage basée sur des politiques**. En activant cette fonctionnalité, les pages suivantes sont disponibles pour l'exploitation et la surveillance :

- Provisioning (provisionnement de la charge de travail de stockage)
- **Politiques > Niveaux de service de performance**
- **Politiques > Efficacité du stockage**
- Colonne « Charges de travail gérées par niveau de service de performance » sur la page Configuration des clusters
- Panneau Performances de la charge de travail sur le **Tableau de bord**

Vous pouvez utiliser les écrans pour créer des niveaux de service de performances et des politiques d'efficacité de stockage, ainsi que pour provisionner des charges de travail de stockage. Vous pouvez également surveiller les charges de travail de stockage conformes aux niveaux de service de performances attribués, ainsi que celles qui ne sont pas conformes. Le panneau Performances de la charge de travail et IOPS de la charge de travail vous permet également d'évaluer la capacité et les performances totales, disponibles et utilisées (IOPS) des clusters de votre centre de données en fonction des charges de travail de stockage provisionnées sur eux.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST Unified Manager pour exécuter certaines de ces fonctions à partir de **Barre de menus > Bouton Aide > Documentation API > catégorie fournisseur de stockage**. Alternativement, vous pouvez saisir le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page REST API au format `https://<hostname>/docs/api/`

Pour plus d'informations sur les API, voir ["Prise en main des API REST Active IQ Unified Manager"](#) .

Activer la passerelle API

La fonctionnalité API Gateway permet à Active IQ Unified Manager d'être un plan de contrôle unique à partir duquel vous pouvez gérer plusieurs clusters ONTAP , sans vous connecter à eux individuellement.

Vous pouvez activer cette fonctionnalité à partir des pages de configuration qui s'affichent lorsque vous vous

connectez pour la première fois à Unified Manager. Vous pouvez également activer ou désactiver cette fonctionnalité depuis **Général > Paramètres des fonctionnalités > Passerelle API**.

Les API REST d'Unified Manager sont différentes des API REST ONTAP et toutes les fonctionnalités des API REST ONTAP ne peuvent pas être utilisées à l'aide des API REST d'Unified Manager. Toutefois, si vous avez une exigence commerciale spécifique d'accès aux API ONTAP pour gérer des fonctionnalités spécifiques qui ne sont pas exposées à Unified Manager, vous pouvez activer la fonctionnalité API Gateway et exécuter les API ONTAP. La passerelle agit comme un proxy pour tunneliser les requêtes API en conservant l'en-tête et le corps des requêtes dans le même format que dans les API ONTAP. Vous pouvez utiliser vos informations d'identification Unified Manager et exécuter les API spécifiques pour accéder et gérer les clusters ONTAP sans transmettre les informations d'identification de cluster individuelles. Unified Manager fonctionne comme un point de gestion unique pour l'exécution des API sur les clusters ONTAP gérés par votre instance Unified Manager. La réponse renvoyée par les API est la même que la réponse renvoyée par les API REST ONTAP respectives exécutées directement depuis ONTAP.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST Unified Manager à partir de **Barre de menus > Bouton d'aide > Documentation API > catégorie passerelle**. Alternativement, vous pouvez saisir le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page de l'API REST au format

<https://<hostname>/docs/api/>

Pour plus d'informations sur les API, voir "[Prise en main des API REST Active IQ Unified Manager](#)".

Spécifier le délai d'inactivité

Vous pouvez spécifier la valeur du délai d'inactivité pour Active IQ Unified Manager. Après une inactivité du temps spécifié, l'application est automatiquement déconnectée. Cette option est activée par défaut.

Vous pouvez désactiver cette fonctionnalité ou modifier le délai depuis **Général > Paramètres de fonctionnalité > Délai d'inactivité**. Une fois cette fonctionnalité activée, vous devez spécifier la limite de temps d'inactivité (en minutes) dans le champ **DÉCONNEXION APRÈS**, après quoi le système se déconnecte automatiquement. La valeur par défaut est 4320 minutes (72 heures).



Cette option n'est pas disponible si vous avez activé l'authentification SAML (Security Assertion Markup Language).

Activer les événements du portail Active IQ

Vous pouvez spécifier si vous souhaitez activer ou désactiver les événements du portail Active IQ. Ce paramètre permet au portail Active IQ de découvrir et d'afficher des événements supplémentaires concernant la configuration du système, le câblage, etc. Cette option est activée par défaut.

En activant cette fonctionnalité, Active IQ Unified Manager affiche les événements détectés par le portail Active IQ. Ces événements sont créés en exécutant un ensemble de règles sur les messages AutoSupport générés à partir de tous les systèmes de stockage surveillés. Ces événements sont différents des autres événements Unified Manager et ils identifient les incidents ou les risques liés à la configuration du système, au câblage, aux meilleures pratiques et aux problèmes de disponibilité.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité depuis **Général > Paramètres de fonctionnalité > Événements du portail Active IQ ***. Sur les sites sans accès réseau externe, vous devez télécharger les règles manuellement depuis ***Gestion du stockage > Configuration des événements >**

Règles de téléchargement.

Cette fonctionnalité est activée par défaut. La désactivation de cette fonctionnalité empêche la détection ou l'affichage des événements Active IQ sur Unified Manager. Lorsque cette fonctionnalité est désactivée, elle permet à Unified Manager de recevoir les événements Active IQ sur un cluster à une heure prédéfinie de 00:15 pour ce fuseau horaire de cluster.

Activer et désactiver les paramètres de sécurité pour la conformité

En utilisant le bouton **Personnaliser** du panneau **Tableau de bord de sécurité** de la page Paramètres des fonctionnalités, vous pouvez activer ou désactiver les paramètres de sécurité pour la surveillance de la conformité sur Unified Manager.

Les paramètres activés ou désactivés à partir de cette page régissent l'état de conformité global des clusters et des machines virtuelles de stockage sur Unified Manager. En fonction des sélections, les colonnes correspondantes sont visibles dans la vue **Sécurité : tous les clusters** de la page d'inventaire des clusters et dans la vue **Sécurité : toutes les machines virtuelles de stockage** de la page d'inventaire des machines virtuelles de stockage.



Seuls les utilisateurs disposant du rôle d'administrateur peuvent modifier ces paramètres.

Les critères de sécurité de vos clusters ONTAP, machines virtuelles de stockage et volumes sont évalués par rapport aux recommandations définies dans le ["Guide de renforcement de la sécurité pour NetApp ONTAP 9"](#). Le panneau Sécurité du tableau de bord et la page Sécurité affichent l'état de conformité de sécurité par défaut de vos clusters, machines virtuelles de stockage et volumes. Des événements de sécurité sont également générés et des actions de gestion activées pour les clusters et les machines virtuelles de stockage présentant des violations de sécurité.

Personnaliser les paramètres de sécurité

Pour personnaliser les paramètres de surveillance de la conformité applicables à votre environnement ONTAP, procédez comme suit :

Étapes

1. Cliquez sur **Général > Paramètres des fonctionnalités > Tableau de bord de sécurité > Personnaliser**. La fenêtre contextuelle **Personnaliser les paramètres du tableau de bord de sécurité** apparaît.



Les paramètres de conformité de sécurité que vous activez ou désactivez peuvent affecter directement les vues de sécurité par défaut, les rapports et les rapports planifiés sur les écrans Clusters et Machines virtuelles de stockage. Si vous avez téléchargé un rapport Excel à partir de ces écrans avant de modifier les paramètres de sécurité, les rapports Excel téléchargés peuvent être défectueux.

2. Pour activer ou désactiver les paramètres personnalisés de vos clusters ONTAP, sélectionnez le paramètre général requis sous **Cluster**. Pour plus d'informations sur les options de personnalisation de la conformité des clusters, consultez ["Catégories de conformité des clusters"](#).
3. Pour activer ou désactiver les paramètres personnalisés de vos machines virtuelles de stockage, sélectionnez le paramètre général requis sous **VM de stockage**. Pour plus d'informations sur les options de personnalisation de la conformité des machines virtuelles de stockage, consultez ["Catégories de conformité des machines virtuelles de stockage"](#).

Personnaliser les paramètres AutoSupport et d'authentification

Dans la section * Paramètres AutoSupport *, vous pouvez spécifier si le transport HTTPS doit être utilisé pour l'envoi de messages AutoSupport depuis ONTAP.

Dans la section **Paramètres d'authentification**, vous pouvez activer la génération d'alertes Unified Manager pour l'utilisateur administrateur ONTAP par défaut.

Activer et désactiver le téléchargement de scripts

La possibilité de télécharger des scripts sur Unified Manager et de les exécuter est activée par défaut. Si votre organisation ne souhaite pas autoriser cette activité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Paramètres des fonctionnalités**.
2. Dans la page **Paramètres des fonctionnalités**, désactivez ou activez les scripts en choisissant l'une des options suivantes :

Si vous voulez...	Alors fais ceci...
Désactiver les scripts	Dans le panneau Téléchargement de script , déplacez le bouton du curseur vers la gauche.
Activer les scripts	Dans le panneau Téléchargement de script , déplacez le bouton du curseur vers la droite.

Ajouter une bannière de connexion

L'ajout d'une bannière de connexion permet à votre organisation d'afficher toutes les informations, telles que les personnes autorisées à accéder au système et les conditions d'utilisation lors de la connexion et de la déconnexion.

Tout utilisateur, tel que les opérateurs de stockage ou les administrateurs, peut afficher cette bannière de connexion contextuelle lors de la connexion, de la déconnexion et de l'expiration de la session.

Utiliser la console de maintenance

Vous pouvez utiliser la console de maintenance pour configurer les paramètres réseau, configurer et gérer le système sur lequel Unified Manager est installé et effectuer d'autres tâches de maintenance qui vous aident à prévenir et à résoudre d'éventuels problèmes.

Quelles fonctionnalités la console de maintenance fournit-elle ?

La console de maintenance Unified Manager vous permet de gérer les paramètres de votre système Unified Manager et d'apporter les modifications nécessaires pour éviter que des problèmes ne surviennent.

Selon le système d'exploitation sur lequel vous avez installé Unified Manager, la console de maintenance fournit les fonctions suivantes :

- Résolvez tous les problèmes liés à votre appliance virtuelle, en particulier si l'interface Web d'Unified Manager n'est pas disponible
- Mise à niveau vers des versions plus récentes de Unified Manager
- Générer des lots de support à envoyer au support technique
- Configurer les paramètres réseau
- Modifier le mot de passe de l'utilisateur de maintenance
- Connectez-vous à un fournisseur de données externe pour envoyer des statistiques de performances
- Modifier la collecte de données de performance interne
- Restaurez la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

Ce que fait l'utilisateur de maintenance

L'utilisateur de maintenance est créé lors de l'installation d'Unified Manager sur un système Red Hat Enterprise Linux. Le nom d'utilisateur de maintenance est l'utilisateur « umadmin ». L'utilisateur de maintenance dispose du rôle d'administrateur d'application dans l'interface utilisateur Web et peut créer des utilisateurs ultérieurs et leur attribuer des rôles.

L'utilisateur de maintenance, ou utilisateur umadmin, peut également accéder à la console de maintenance Unified Manager.

Capacités de diagnostic utilisateur

L'accès au diagnostic a pour but de permettre au support technique de vous aider à résoudre les problèmes, et vous ne devez l'utiliser que lorsque le support technique vous le demande.

L'utilisateur de diagnostic peut exécuter des commandes au niveau du système d'exploitation lorsque le support technique le lui demande, à des fins de dépannage.

Accéder à la console de maintenance

Si l'interface utilisateur d'Unified Manager n'est pas opérationnelle ou si vous devez exécuter des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour gérer votre système Unified Manager.

Avant de commencer

Vous devez avoir installé et configuré Unified Manager.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.



Lors de l'installation sur VMware, si vous êtes déjà connecté en tant qu'utilisateur de maintenance via la console VMware, vous ne pouvez pas vous connecter simultanément à l'aide de Secure Shell.

Étape

1. Suivez ces étapes pour accéder à la console de maintenance :

Sur ce système d'exploitation...	Suivez ces étapes...
VMware	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. b. Connectez-vous à la console de maintenance en utilisant votre nom d'utilisateur et votre mot de passe de maintenance.
Linux	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager. b. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de maintenance (umadmin). c. Entrez la commande <code>maintenance_console</code> et appuyez sur Entrée.
Windows	a. Connectez-vous au système Unified Manager avec les informations d'identification d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Entrez la commande <code>maintenance_console</code> et appuyez sur Entrée.

Le menu de la console de maintenance d'Unified Manager s'affiche.

Accéder à la console de maintenance à l'aide de la console vSphere VM

Si l'interface utilisateur d'Unified Manager n'est pas opérationnelle ou si vous devez exécuter des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour reconfigurer votre appliance virtuelle.

Avant de commencer

- Vous devez être l'utilisateur de maintenance.

- L'appliance virtuelle doit être sous tension pour accéder à la console de maintenance.

Étapes

1. Dans vSphere Client, recherchez l'appliance virtuelle Unified Manager.
2. Cliquez sur l'onglet **Console**.
3. Cliquez à l'intérieur de la fenêtre de la console pour vous connecter.
4. Connectez-vous à la console de maintenance en utilisant votre nom d'utilisateur et votre mot de passe.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.

Menus de la console de maintenance

La console de maintenance se compose de différents menus qui vous permettent de maintenir et de gérer les fonctionnalités spéciales et les paramètres de configuration du serveur Unified Manager.

Selon le système d'exploitation sur lequel vous avez installé Unified Manager, la console de maintenance se compose des menus suivants :

- Mettre à niveau Unified Manager (VMware uniquement)
- Configuration réseau (VMware uniquement)
- Configuration du système (VMware uniquement)
 - a. Assistance/Diagnostic
 - b. Réinitialiser le certificat du serveur
 - c. Fournisseur de données externe
 - d. Restauration de sauvegarde
 - e. Configuration de l'intervalle d'interrogation des performances
 - f. Désactiver l'authentification SAML
 - g. Afficher/modifier les ports d'application
 - h. Configuration du journal de débogage
 - i. Contrôler l'accès au port MySQL 3306
 - j. Sortie

Vous sélectionnez le numéro dans la liste pour accéder à l'option de menu spécifique. Par exemple, pour la sauvegarde et la restauration, vous sélectionnez 4.

Menu de configuration réseau

Le menu Configuration réseau vous permet de gérer les paramètres réseau. Vous devez utiliser ce menu lorsque l'interface utilisateur d'Unified Manager n'est pas disponible.



Ce menu n'est pas disponible si Unified Manager est installé sur Red Hat Enterprise Linux ou sur Microsoft Windows.

Les choix de menu suivants sont disponibles.

- **Afficher les paramètres d'adresse IP**

Affiche les paramètres réseau actuels de l'apppliance virtuelle, notamment l'adresse IP, le réseau, l'adresse de diffusion, le masque de réseau, la passerelle et les serveurs DNS.

- **Modifier les paramètres d'adresse IP**

Vous permet de modifier n'importe quel paramètre réseau de l'apppliance virtuelle, y compris l'adresse IP, le masque de réseau, la passerelle ou les serveurs DNS. Si vous changez vos paramètres réseau de DHCP à la mise en réseau statique à l'aide de la console de maintenance, vous ne pouvez pas modifier le nom d'hôte. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Afficher les paramètres de recherche de nom de domaine**

Affiche la liste de recherche de noms de domaine utilisée pour résoudre les noms d'hôtes.

- **Modifier les paramètres de recherche de nom de domaine**

Vous permet de modifier les noms de domaine que vous souhaitez rechercher lors de la résolution des noms d'hôtes. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Afficher les itinéraires statiques**

Affiche les itinéraires réseau statiques actuels.

- **Modifier les itinéraires statiques**

Vous permet d'ajouter ou de supprimer des itinéraires réseau statiques. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Ajouter un itinéraire**

Vous permet d'ajouter un itinéraire statique.

- **Supprimer l'itinéraire**

Vous permet de supprimer un itinéraire statique.

- **Dos**

Vous ramène au **Menu principal**.

- **Sortie**

Quitte la console de maintenance.

- **Désactiver l'interface réseau**

Désactive toutes les interfaces réseau disponibles. Si une seule interface réseau est disponible, vous ne pouvez pas la désactiver. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Activer l'interface réseau**

Active les interfaces réseau disponibles. Vous devez sélectionner **Valider les modifications** pour que les

modifications soient appliquées.

- **Valider les modifications**

Applique toutes les modifications apportées aux paramètres réseau de l'appliance virtuelle. Vous devez sélectionner cette option pour appliquer les modifications apportées, sinon les modifications ne se produiront pas.

- **Ping un hôte**

Effectue un ping sur un hôte cible pour confirmer les modifications d'adresse IP ou les configurations DNS.

- **Restaurer les paramètres par défaut**

Réinitialise tous les paramètres aux valeurs par défaut d'usine. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Dos**

Vous ramène au **Menu principal**.

- **Sortie**

Quitte la console de maintenance.

Menu de configuration du système

Le menu Configuration système vous permet de gérer votre appareil virtuel en fournissant diverses options, telles que l'affichage de l'état du serveur, le redémarrage et l'arrêt de la machine virtuelle.



Lorsque Unified Manager est installé sur un système Linux ou Microsoft Windows, seule l'option « Restaurer à partir d'une sauvegarde Unified Manager » est disponible dans ce menu.

Les choix de menu suivants sont disponibles :

- **Afficher l'état du serveur**

Affiche l'état actuel du serveur. Les options d'état incluent En cours d'exécution et Non en cours d'exécution.

Si le serveur ne fonctionne pas, vous devrez peut-être contacter le support technique.

- **Redémarrer la machine virtuelle**

Redémarre la machine virtuelle, arrêtant tous les services. Après le redémarrage, la machine virtuelle et les services redémarrent.

- **Arrêter la machine virtuelle**

Arrête la machine virtuelle, arrêtant tous les services.

Vous ne pouvez sélectionner cette option qu'à partir de la console de la machine virtuelle.

- **Modifier le mot de passe de l'utilisateur <utilisateur connecté>**

Modifie le mot de passe de l'utilisateur actuellement connecté, qui ne peut être que l'utilisateur de maintenance.

- **Augmenter la taille du disque de données**

Augmente la taille du disque de données (disque 3) dans la machine virtuelle.

- **Augmenter la taille du disque d'échange**

Augmente la taille du disque d'échange (disque 2) dans la machine virtuelle.

- **Changer de fuseau horaire**

Modifie le fuseau horaire en fonction de votre emplacement.

- **Changer le serveur NTP**

Modifie les paramètres du serveur NTP, tels que l'adresse IP ou le nom de domaine complet (FQDN).

- **Modifier le service NTP**

Bascule entre les `ntp` et `systemd-timesyncd` services.

- **Restaurer à partir d'une sauvegarde Unified Manager**

Restaure la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

- **Réinitialiser le certificat du serveur**

Réinitialise le certificat de sécurité du serveur.

- **Changer le nom d'hôte**

Modifie le nom de l'hôte sur lequel l'appliance virtuelle est installée.

- **Dos**

Quitte le menu de configuration du système et revient au menu principal.

- **Sortie**

Quitte le menu de la console de maintenance.

Menu Assistance et Diagnostics

Le menu Assistance et diagnostics vous permet de générer un ensemble d'assistance que vous pouvez envoyer au support technique pour obtenir de l'aide en cas de problème.

Les options de menu suivantes sont disponibles :

- **Pack de support Generate Light**

Vous permet de produire un ensemble de support léger qui contient seulement 30 jours de journaux et d'enregistrements de base de données de configuration - il exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

- **Générer un pack de support**

Vous permet de créer un ensemble de support complet (fichier 7-Zip) contenant des informations de diagnostic dans le répertoire personnel de l'utilisateur de diagnostic. Si votre système est connecté à Internet, vous pouvez également télécharger le pack de support sur NetApp.

Le fichier inclut des informations générées par un message AutoSupport , le contenu de la base de données Unified Manager, des données détaillées sur les éléments internes du serveur Unified Manager et des journaux détaillés qui ne sont normalement pas inclus dans les messages AutoSupport ou dans le pack de support léger.

Options de menu supplémentaires

Les options de menu suivantes vous permettent d'effectuer diverses tâches administratives sur le serveur Unified Manager.

Les choix de menu suivants sont disponibles :

- **Réinitialiser le certificat du serveur**

Régénère le certificat du serveur HTTPS.

Vous pouvez régénérer le certificat du serveur dans l'interface graphique d'Unified Manager en cliquant sur **Général > Certificats HTTPS > Régénérer le certificat HTTPS**.

- **Désactiver l'authentification SAML**

Désactive l'authentification SAML afin que le fournisseur d'identité (IdP) ne fournisse plus d'authentification de connexion pour les utilisateurs accédant à l'interface graphique utilisateur d'Unified Manager. Cette option de console est généralement utilisée lorsqu'un problème avec le serveur IdP ou la configuration SAML empêche les utilisateurs d'accéder à l'interface graphique utilisateur d'Unified Manager.

- **Fournisseur de données externe**

Fournit des options pour connecter Unified Manager à un fournisseur de données externe. Une fois la connexion établie, les données de performances sont envoyées à un serveur externe afin que les experts en performances de stockage puissent tracer les mesures de performances à l'aide d'un logiciel tiers. Les options suivantes s'affichent :

- **Afficher la configuration du serveur** – Affiche les paramètres de connexion et de configuration actuels pour un fournisseur de données externe.
- **Ajouter/Modifier la connexion au serveur** – Vous permet de saisir de nouveaux paramètres de connexion pour un fournisseur de données externe ou de modifier les paramètres existants.
- **Modifier la configuration du serveur** – Vous permet de saisir de nouveaux paramètres de configuration pour un fournisseur de données externe ou de modifier les paramètres existants.
- **Supprimer la connexion au serveur**–Supprime la connexion à un fournisseur de données externe.

Une fois la connexion supprimée, Unified Manager perd sa connexion au serveur externe.

- **Restauration de sauvegarde**

Pour plus d'informations, consultez les rubriques sous "[Gestion des opérations de sauvegarde et de restauration](#)".

- **Configuration de l'intervalle d'interrogation des performances**

Fournit une option permettant de configurer la fréquence à laquelle Unified Manager collecte les données statistiques de performances des clusters. L'intervalle de collecte par défaut est de 5 minutes.

Vous pouvez modifier cet intervalle à 10 ou 15 minutes si vous constatez que les collectes de grands clusters ne se terminent pas à temps.

- **Afficher/Modifier les ports d'application**

Fournit une option permettant de modifier les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS, si nécessaire pour des raisons de sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

- **Contrôler l'accès au port MySQL 3306**

Contrôle l'accès de l'hôte au port MySQL par défaut 3306. Pour des raisons de sécurité, l'accès via ce port est limité uniquement à localhost lors d'une nouvelle installation d'Unified Manager sur les systèmes Linux, Windows et VMware vSphere. Cette option vous permet de basculer la visibilité de ce port entre l'hôte local et les hôtes distants, c'est-à-dire que si elle est activée pour l'hôte local uniquement dans votre environnement, vous pouvez également rendre ce port disponible pour les hôtes distants. Alternativement, lorsque cette option est activée pour tous les hôtes, vous pouvez restreindre l'accès de ce port à l'hôte local uniquement. Si l'accès a été activé sur des hôtes distants précédemment, la configuration est conservée dans un scénario de mise à niveau. Vous devez vérifier les paramètres du pare-feu sur les systèmes Windows après avoir activé la visibilité du port et désactiver les paramètres du pare-feu si les paramètres sont configurés pour restreindre l'accès au port MySQL 3306.

- **Sortie**

Quitte le menu de la console de maintenance.

Modifier le mot de passe de l'utilisateur de maintenance sous Windows

Vous pouvez modifier le mot de passe de l'utilisateur de maintenance d'Unified Manager si nécessaire.

Étapes

1. Depuis la page de connexion de l'interface Web d'Unified Manager, cliquez sur **Mot de passe oublié**.

Une page s'affiche et vous demande le nom de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.

2. Saisissez le nom d'utilisateur et cliquez sur **Soumettre**.

Un e-mail contenant un lien pour réinitialiser le mot de passe est envoyé à l'adresse e-mail définie pour ce nom d'utilisateur.

3. Cliquez sur le lien **réinitialiser le mot de passe** dans l'e-mail et définissez le nouveau mot de passe.
4. Revenez à l'interface Web et connectez-vous à Unified Manager à l'aide du nouveau mot de passe.

Modifier le mot de passe umadmin sur les systèmes Linux

Pour des raisons de sécurité, vous devez modifier le mot de passe par défaut de l'utilisateur umadmin d'Unified Manager immédiatement après avoir terminé le processus d'installation. Si nécessaire, vous pouvez modifier à nouveau le mot de passe à tout moment ultérieurement.

Avant de commencer

- Unified Manager doit être installé sur un système Linux Red Hat Enterprise Linux.
- Vous devez disposer des informations d'identification de l'utilisateur root pour le système Linux sur lequel Unified Manager est installé.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Linux sur lequel Unified Manager s'exécute.
2. Changer le mot de passe umadmin :

```
passwd umadmin
```

Le système vous invite à saisir un nouveau mot de passe pour l'utilisateur umadmin.

Modifier les ports utilisés par Unified Manager pour les protocoles HTTP et HTTPS

Les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS peuvent être modifiés après l'installation si nécessaire pour des raisons de sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.



Certains ports sont considérés comme dangereux lors de l'utilisation des navigateurs Mozilla Firefox ou Google Chrome. Vérifiez auprès de votre navigateur avant d'attribuer un nouveau numéro de port pour le trafic HTTP et HTTPS. La sélection d'un port non sécurisé pourrait rendre le système inaccessible, ce qui nécessiterait que vous contactiez le support client pour trouver une solution.

L'instance d'Unified Manager redémarre automatiquement après avoir modifié le port. Assurez-vous donc que c'est le bon moment pour arrêter le système pendant une courte période.

1. Connectez-vous à l'aide de SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

Les invites de la console de maintenance d'Unified Manager s'affichent.

2. Tapez le numéro de l'option de menu intitulée **Afficher/Modifier les ports d'application**, puis appuyez sur Entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe de l'utilisateur de maintenance.

4. Saisissez les nouveaux numéros de port pour les ports HTTP et HTTPS, puis appuyez sur Entrée.

Laisser un numéro de port vide attribue le port par défaut pour le protocole.

Vous êtes invité à indiquer si vous souhaitez modifier les ports et redémarrer Unified Manager maintenant.

5. Tapez **y** pour modifier les ports et redémarrer Unified Manager.
6. Quitter la console de maintenance.

Après cette modification, les utilisateurs doivent inclure le nouveau numéro de port dans l'URL pour accéder à l'interface utilisateur Web d'Unified Manager, par exemple + <https://host.company.com:1234> , <https://12.13.14.15:1122> ou [https://\[2001:db8:0:1\]:2123](https://[2001:db8:0:1]:2123).

Ajouter des interfaces réseau

Vous pouvez ajouter de nouvelles interfaces réseau si vous devez séparer le trafic réseau.

Avant de commencer

Vous devez avoir ajouté l'interface réseau à l'appliance virtuelle à l'aide de vSphere.

L'appareil virtuel doit être sous tension.



Vous ne pouvez pas effectuer cette opération si Unified Manager est installé sur Red Hat Enterprise Linux ou sur Microsoft Windows.

Étapes

1. Dans le menu principal de la console vSphere, sélectionnez **Configuration système > Redémarrer le système d'exploitation**.

Après le redémarrage, la console de maintenance peut détecter la nouvelle interface réseau ajoutée.

2. Accéder à la console de maintenance.
3. Sélectionnez **Configuration réseau > Activer l'interface réseau**.
4. Sélectionnez la nouvelle interface réseau et appuyez sur **Entrée**.

Sélectionnez **eth1** et appuyez sur **Entrée**.

5. Tapez **y** pour activer l'interface réseau.
6. Entrez les paramètres réseau.

Vous êtes invité à saisir les paramètres réseau si vous utilisez une interface statique ou si DHCP n'est pas détecté.

Après avoir entré les paramètres réseau, vous revenez automatiquement au menu **Configuration réseau**.

7. Sélectionnez **Valider les modifications**.

Vous devez valider les modifications pour ajouter l'interface réseau.

Ajouter de l'espace disque au répertoire de la base de données Unified Manager

Le répertoire de la base de données Unified Manager contient toutes les données de santé et de performances collectées à partir des systèmes ONTAP . Certaines circonstances peuvent nécessiter d'augmenter la taille du répertoire de base de données.

Par exemple, le répertoire de base de données peut être plein si Unified Manager collecte des données à partir d'un grand nombre de clusters où chaque cluster comporte de nombreux nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de base de données sera rempli à 90 % et un événement critique lorsque le répertoire sera rempli à 95 %.



Aucune donnée supplémentaire n'est collectée à partir des clusters une fois que le répertoire atteint 95 % de remplissage.

Les étapes requises pour ajouter de la capacité au répertoire de données sont différentes selon qu'Unified Manager s'exécute sur un serveur VMware ESXi, sur un serveur Red Hat ou sur un serveur Microsoft Windows.

Ajouter de l'espace au répertoire de données de l'hôte Linux

Si vous n'avez pas alloué suffisamment d'espace disque au `/opt/netapp/data` répertoire pour prendre en charge Unified Manager lorsque vous avez initialement configuré l'hôte Linux, puis installé Unified Manager, vous pouvez ajouter de l'espace disque après l'installation en augmentant l'espace disque sur le `/opt/netapp/data` annuaire.

Avant de commencer

Vous devez disposer d'un accès utilisateur root à la machine Red Hat Enterprise Linux sur laquelle Unified Manager est installé.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'augmenter la taille du répertoire de données.

Étapes

1. Connectez-vous en tant qu'utilisateur root à la machine Linux sur laquelle vous souhaitez ajouter de l'espace disque.
2. Arrêtez le service Unified Manager et le logiciel MySQL associé dans l'ordre indiqué :

```
systemctl stop ocieau ocie mysqld
```

3. Créez un dossier de sauvegarde temporaire (par exemple, `/backup-data`) avec suffisamment d'espace disque pour contenir les données dans le `/opt/netapp/data` annuaire.
4. Copiez le contenu et la configuration des privilèges de l'existant `/opt/netapp/data` répertoire vers le répertoire des données de sauvegarde :

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Si SE Linux est activé :

- a. Obtenir le type SE Linux pour les dossiers existants `/opt/netapp/data` dossier:

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |  
head -1
```

Le système renvoie une confirmation similaire à la suivante :

```
echo $se_type  
mysqld_db_t
```

a. Exécutez la commande `chcon` pour définir le type SE Linux pour le répertoire de sauvegarde :

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Retirez le contenu du `/opt/netapp/data` annuaire:

a. `cd /opt/netapp/data`

b. `rm -rf *`

7. Augmenter la taille du `/opt/netapp/data` répertoire à un minimum de 150 Go via des commandes LVM ou en ajoutant des disques supplémentaires.



Si vous avez créé `/opt/netapp/data` à partir d'un disque, vous ne devriez pas essayer de monter `/opt/netapp/data` en tant que partage NFS ou CIFS. Car, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` pourrait ne pas fonctionner comme prévu.

8. Confirmez que le `/opt/netapp/data` le propriétaire du répertoire (`mysql`) et le groupe (`root`) restent inchangés :

```
ls -ltr /opt/netapp/ | grep data
```

Le système renvoie une confirmation similaire à la suivante :

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Si SE Linux est activé, confirmez que le contexte du `/opt/netapp/data` le répertoire est toujours défini sur `mysqld_db_t` :

a. `touch /opt/netapp/data/abc`

b. `ls -Z /opt/netapp/data/abc`

Le système renvoie une confirmation similaire à la suivante :

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0  
/opt/netapp/data/abc
```

10. Supprimez le fichier `abc` afin que ce fichier étranger ne provoque pas d'erreur de base de données à l'avenir.

11. Copiez le contenu des données de sauvegarde vers la version étendue /opt/netapp/data annuaire:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Si SE Linux est activé, exécutez la commande suivante :

```
chcon -R --type=mysqlld_db_t /opt/netapp/data
```

13. Démarrez le service MySQL :

```
systemctl start mysqld
```

14. Une fois le service MySQL démarré, démarrez les services ocie et ocieau dans l'ordre indiqué :

```
systemctl start ocie ocieau
```

15. Une fois tous les services démarrés, supprimez le dossier de sauvegarde /backup-data :

```
rm -rf /backup-data
```

Ajouter de l'espace au disque de données de la machine virtuelle VMware

Si vous devez augmenter la quantité d'espace sur le disque de données pour la base de données Unified Manager, vous pouvez ajouter de la capacité après l'installation en augmentant l'espace disque à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez avoir accès au client vSphere.
- La machine virtuelle ne doit avoir aucun snapshot stocké localement.
- Vous devez disposer des informations d'identification de l'utilisateur de maintenance.

Nous vous recommandons de sauvegarder votre machine virtuelle avant d'augmenter la taille des disques virtuels.

Étapes

1. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis ajoutez davantage de capacité de disque aux données `disk 3`. Consultez la documentation VMware pour plus de détails.

Dans certains cas rares, le déploiement d'Unified Manager utilise « Disque dur 2 » pour le disque de données au lieu de « Disque dur 3 ». Si cela se produit lors de votre déploiement, augmentez l'espace du disque le plus grand. Le disque de données aura toujours plus d'espace que l'autre disque.

2. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis sélectionnez l'onglet **Console**.
3. Cliquez dans la fenêtre de la console, puis connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Dans le menu principal, entrez le numéro de l'option **Configuration système**.
5. Dans le menu de configuration système, entrez le numéro de l'option **Augmenter la taille du disque de données**.

Ajouter de l'espace au lecteur logique du serveur Microsoft Windows

Si vous devez augmenter la quantité d'espace disque pour la base de données Unified Manager, vous pouvez ajouter de la capacité au lecteur logique sur lequel Unified Manager est installé.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'ajouter de l'espace disque.

Étapes

1. Connectez-vous en tant qu'administrateur au serveur Windows sur lequel vous souhaitez ajouter de l'espace disque.
2. Suivez l'étape qui correspond à la méthode que vous souhaitez utiliser pour ajouter plus d'espace :

Option	Description
Sur un serveur physique, ajoutez de la capacité au lecteur logique sur lequel le serveur Unified Manager est installé.	Suivez les étapes décrites dans la rubrique Microsoft : "Étendre un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes décrites dans la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes décrites dans la rubrique VMware : "Augmenter la taille d'une partition de disque"

Gérer l'accès des utilisateurs

Vous pouvez créer des rôles et attribuer des fonctionnalités pour contrôler l'accès des utilisateurs à Active IQ Unified Manager. Vous pouvez identifier les utilisateurs qui disposent des capacités requises pour accéder aux objets sélectionnés dans Unified Manager. Seuls les utilisateurs disposant de ces rôles et capacités peuvent gérer les objets dans Unified Manager.

Ajouter des utilisateurs

Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données en utilisant la page Utilisateurs. Vous pouvez également ajouter des utilisateurs ou des groupes distants appartenant à un serveur d'authentification. Vous pouvez attribuer des rôles à ces utilisateurs et, en fonction des privilèges des rôles, les utilisateurs peuvent

gérer les objets de stockage et les données avec Unified Manager ou afficher les données dans une base de données.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application.
- Pour ajouter un utilisateur ou un groupe distant, vous devez avoir activé l'authentification à distance et configuré votre serveur d'authentification.
- Si vous prévoyez de configurer l'authentification SAML afin qu'un fournisseur d'identité (IdP) authentifie les utilisateurs accédant à l'interface graphique, assurez-vous que ces utilisateurs sont définis comme utilisateurs « distants ».

L'accès à l'interface utilisateur n'est pas autorisé pour les utilisateurs de type « local » ou « maintenance » lorsque l'authentification SAML est activée.

Si vous ajoutez un groupe à partir de Windows Active Directory, tous les membres directs et les sous-groupes imbriqués peuvent s'authentifier auprès de Unified Manager, sauf si les sous-groupes imbriqués sont désactivés. Si vous ajoutez un groupe à partir d'OpenLDAP ou d'autres services d'authentification, seuls les membres directs de ce groupe peuvent s'authentifier auprès d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Utilisateurs**.
2. Sur la page Utilisateurs, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un utilisateur, sélectionnez le type d'utilisateur que vous souhaitez ajouter et entrez les informations requises.

Lorsque vous saisissez les informations utilisateur requises, vous devez spécifier une adresse e-mail unique à cet utilisateur. Vous devez éviter de spécifier des adresses e-mail partagées par plusieurs utilisateurs.

4. Cliquez sur **Ajouter**.

Créer un utilisateur de base de données

Pour prendre en charge une connexion entre Workflow Automation et Unified Manager, ou pour accéder aux vues de base de données, vous devez d'abord créer un utilisateur de base de données avec le rôle Schéma d'intégration ou Schéma de rapport dans l'interface utilisateur Web d'Unified Manager.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Les utilisateurs de la base de données fournissent une intégration avec Workflow Automation et un accès aux vues de base de données spécifiques aux rapports. Les utilisateurs de la base de données n'ont pas accès à l'interface utilisateur Web d'Unified Manager ni à la console de maintenance et ne peuvent pas exécuter d'appels API.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Utilisateurs**.
2. Dans la page Utilisateurs, cliquez sur **Ajouter**.

3. Dans la boîte de dialogue Ajouter un utilisateur, sélectionnez **Utilisateur de base de données** dans la liste déroulante **Type**.
4. Saisissez un nom et un mot de passe pour l'utilisateur de la base de données.
5. Dans la liste déroulante **Rôle**, sélectionnez le rôle approprié.

Si vous êtes...	Choisissez ce rôle
Connexion d'Unified Manager à l'automatisation des flux de travail	Schéma d'intégration
Accéder aux rapports et autres vues de base de données	Schéma de rapport

6. Cliquez sur **Ajouter**.

Modifier les paramètres utilisateur

Vous pouvez modifier les paramètres utilisateur, tels que l'adresse e-mail et le rôle, qui sont spécifiés pour chaque utilisateur. Par exemple, vous souhaitez peut-être modifier le rôle d'un utilisateur qui est un opérateur de stockage et attribuer des privilèges d'administrateur de stockage à l'utilisateur.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Lorsque vous modifiez le rôle attribué à un utilisateur, les modifications sont appliquées lorsque l'une des actions suivantes se produit :

- L'utilisateur se déconnecte et se reconnecte à Unified Manager.
- Le délai d'expiration de la session de 24 heures est atteint.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Utilisateurs**.
2. Dans la page Utilisateurs, sélectionnez l'utilisateur pour lequel vous souhaitez modifier les paramètres et cliquez sur **Modifier**.
3. Dans la boîte de dialogue Modifier l'utilisateur, modifiez les paramètres appropriés spécifiés pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

Afficher les utilisateurs

Vous pouvez utiliser la page Utilisateurs pour afficher la liste des utilisateurs qui gèrent les objets de stockage et les données à l'aide d'Unified Manager. Vous pouvez afficher les détails sur les utilisateurs, tels que le nom d'utilisateur, le type d'utilisateur, l'adresse e-mail et le rôle attribué aux utilisateurs.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général > Utilisateurs**.

Supprimer des utilisateurs ou des groupes

Vous pouvez supprimer un ou plusieurs utilisateurs de la base de données du serveur de gestion pour empêcher des utilisateurs spécifiques d'accéder à Unified Manager. Vous pouvez également supprimer des groupes afin que tous les utilisateurs du groupe ne puissent plus accéder au serveur de gestion.

Avant de commencer

- Lorsque vous supprimez des groupes distants, vous devez avoir réaffecté les événements attribués aux utilisateurs des groupes distants.

Si vous supprimez des utilisateurs locaux ou distants, les événements attribués à ces utilisateurs sont automatiquement annulés.

- Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Utilisateurs**.
2. Dans la page Utilisateurs, sélectionnez les utilisateurs ou les groupes que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression.

Qu'est-ce que RBAC

RBAC (contrôle d'accès basé sur les rôles) offre la possibilité de contrôler qui a accès à diverses fonctionnalités et ressources sur le serveur Active IQ Unified Manager .

À quoi sert le contrôle d'accès basé sur les rôles ?

Le contrôle d'accès basé sur les rôles (RBAC) permet aux administrateurs de gérer des groupes d'utilisateurs en définissant des rôles. Si vous devez restreindre l'accès à des fonctionnalités spécifiques à des administrateurs sélectionnés, vous devez configurer des comptes d'administrateur pour eux. Si vous souhaitez restreindre les informations que les administrateurs peuvent afficher et les opérations qu'ils peuvent effectuer, vous devez appliquer des rôles aux comptes d'administrateur que vous créez.

Le serveur de gestion utilise RBAC pour la connexion des utilisateurs et les autorisations de rôle. Si vous n'avez pas modifié les paramètres par défaut du serveur de gestion pour l'accès des utilisateurs administratifs, vous n'avez pas besoin de vous connecter pour les afficher.

Lorsque vous lancez une opération qui nécessite des privilèges spécifiques, le serveur de gestion vous invite à vous connecter. Par exemple, pour créer des comptes d'administrateur, vous devez vous connecter avec l'accès au compte Administrateur d'application.

Définitions des types d'utilisateurs

Un type d'utilisateur spécifie le type de compte détenu par l'utilisateur et inclut les utilisateurs distants, les groupes distants, les utilisateurs locaux, les utilisateurs de base de données et les utilisateurs de maintenance. Chacun de ces types possède son propre rôle, qui est attribué par un utilisateur ayant le rôle d'Administrateur.

Les types d'utilisateurs d'Unified Manager sont les suivants :

- **Utilisateur de maintenance**

Créé lors de la configuration initiale de Unified Manager. L'utilisateur de maintenance crée ensuite des utilisateurs supplémentaires et attribue des rôles. L'utilisateur de maintenance est également le seul utilisateur ayant accès à la console de maintenance. Lorsque Unified Manager est installé sur un système Red Hat Enterprise Linux, l'utilisateur de maintenance reçoit le nom d'utilisateur « umadmin ».

- **Utilisateur local**

Accède à l'interface utilisateur d'Unified Manager et exécute des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou un utilisateur disposant du rôle d'administrateur d'application.

- **Groupe à distance**

Un groupe d'utilisateurs qui accèdent à l'interface utilisateur d'Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Le nom de ce compte doit correspondre au nom d'un groupe stocké sur le serveur d'authentification. Tous les utilisateurs du groupe distant ont accès à l'interface utilisateur d'Unified Manager à l'aide de leurs informations d'identification individuelles. Les groupes distants peuvent exécuter des fonctions en fonction des rôles qui leur sont attribués.

- **Utilisateur distant**

Accède à l'interface utilisateur d'Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Un utilisateur distant exécute des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou un utilisateur disposant du rôle d'administrateur d'application.

- **Utilisateur de la base de données**

Dispose d'un accès en lecture seule aux données de la base de données Unified Manager, n'a pas accès à l'interface Web Unified Manager ni à la console de maintenance et ne peut pas exécuter d'appels API.

Définitions des rôles d'utilisateur

L'utilisateur de maintenance ou l'administrateur d'application attribue un rôle à chaque utilisateur. Chaque rôle contient certains privilèges. L'étendue des activités que vous pouvez effectuer dans Unified Manager dépend du rôle qui vous est attribué et des privilèges qu'il contient.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

Affiche les informations du système de stockage et d'autres données collectées par Unified Manager, y compris les historiques et les tendances de capacité. Ce rôle permet à l'opérateur de stockage d'afficher,

d'attribuer, d'accuser réception, de résoudre et d'ajouter des notes pour les événements.

- **Administrateur de stockage**

Configure les opérations de gestion du stockage dans Unified Manager. Ce rôle permet à l'administrateur de stockage de configurer des seuils et de créer des alertes et d'autres options et politiques spécifiques à la gestion du stockage.

- **Administrateur d'application**

Configure les paramètres non liés à la gestion du stockage. Ce rôle permet la gestion des utilisateurs, des certificats de sécurité, de l'accès à la base de données et des options administratives, notamment l'authentification, SMTP, la mise en réseau et AutoSupport.



Lorsque Unified Manager est installé sur les systèmes Linux, l'utilisateur initial avec le rôle d'administrateur d'application est automatiquement nommé « umadmin ».

- **Schéma d'intégration**

Ce rôle permet l'accès en lecture seule aux vues de base de données Unified Manager pour l'intégration d'Unified Manager avec OnCommand Workflow Automation (WFA).

- **Schéma de rapport**

Ce rôle permet un accès en lecture seule aux rapports et autres vues de base de données directement à partir de la base de données Unified Manager. Les bases de données qui peuvent être consultées comprennent :

- vue_modèle_netapp
- performances_netapp
- ocum
- rapport_ocum
- ocum_report_birt
- opm
- moniteur d'échelle

Rôles et capacités des utilisateurs d'Unified Manager

En fonction du rôle d'utilisateur qui vous est attribué, vous pouvez déterminer les opérations que vous pouvez effectuer dans Unified Manager.

Le tableau suivant affiche les fonctions que chaque rôle d'utilisateur peut exécuter :

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma de rapport
Afficher les informations sur le système de stockage	•	•	•	•	•

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma de rapport
Afficher d'autres données, telles que les historiques et les tendances de capacité	•	•	•	•	•
Afficher, attribuer et résoudre les événements	•	•	•		
Afficher les objets de service de stockage, tels que les associations SVM et les pools de ressources	•	•	•		
Afficher les politiques de seuil	•	•	•		
Gérer les objets de service de stockage, tels que les associations SVM et les pools de ressources		•	•		
Définir les alertes		•	•		
Gérer les options de gestion du stockage		•	•		
Gérer les politiques de gestion du stockage		•	•		
Gérer les utilisateurs			•		

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma de rapport
Gérer les options administratives			•		
Définir des politiques de seuil			•		
Gérer l'accès à la base de données			•		
Gérer l'intégration avec WFA et fournir l'accès aux vues de la base de données				•	
Planifier et enregistrer des rapports		•	•		
Exécuter les opérations « Réparer » à partir des actions de gestion		•	•		
Fournir un accès en lecture seule aux vues de la base de données					•

Gérer les paramètres d'authentification SAML

Après avoir configuré les paramètres d'authentification à distance, vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d'identité sécurisé (IdP) avant de pouvoir accéder à l'interface utilisateur Web d'Unified Manager.

Notez que seuls les utilisateurs distants auront accès à l'interface utilisateur graphique d'Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a pas d'impact sur les utilisateurs qui accèdent à la console de maintenance.

Exigences relatives aux fournisseurs d'identité

Lors de la configuration d'Unified Manager pour utiliser un fournisseur d'identité (IdP) pour effectuer l'authentification SAML pour tous les utilisateurs distants, vous devez connaître certains paramètres de configuration requis pour que la connexion à Unified Manager réussisse.

Vous devez saisir l'URI et les métadonnées d'Unified Manager dans le serveur IdP. Vous pouvez copier ces informations à partir de la page d'authentification SAML d'Unified Manager. Unified Manager est considéré comme le fournisseur de services (SP) dans la norme Security Assertion Markup Language (SAML).

Normes de cryptage prises en charge

- Norme de chiffrement avancée (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Fournisseurs d'identité validés

- Schibboleth
- Services de fédération Active Directory (ADFS)

Exigences de configuration ADFS

- Vous devez définir trois règles de réclamation dans l'ordre suivant qui sont requises pour qu'Unified Manager analyse les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance.

Règle de réclamation	Valeur
nom-du-compte-SAM	Nom d'identification
nom-du-compte-SAM	urn:oid:0.9.2342.19200300.100.1.1
Groupes de jetons – Nom non qualifié	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Vous devez définir la méthode d'authentification sur « Authentification par formulaire » sinon les utilisateurs risquent de recevoir une erreur lors de la déconnexion d'Unified Manager. Suivez ces étapes :
 - a. Ouvrez la console de gestion ADFS.
 - b. Cliquez sur le dossier Stratégies d'authentification dans l'arborescence de gauche.
 - c. Sous Actions sur la droite, cliquez sur Modifier la politique d'authentification principale globale.
 - d. Définissez la méthode d'authentification intranet sur « Authentification par formulaire » au lieu de la valeur par défaut « Authentification Windows ».
- Dans certains cas, la connexion via l'IdP est rejetée lorsque le certificat de sécurité Unified Manager est signé par une autorité de certification. Il existe deux solutions de contournement pour résoudre ce problème :
 - Suivez les instructions identifiées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour la partie de confiance associée au certificat CA chaîné :

["Désactiver la vérification de révocation par approbation de partie de confiance"](#)

- Demandez au serveur CA de résider dans le serveur ADFS pour signer la demande de certificat du serveur Unified Manager.

Autres exigences de configuration

- Le décalage de l'horloge d'Unified Manager est défini sur 5 minutes, de sorte que la différence de temps entre le serveur IdP et le serveur Unified Manager ne peut pas dépasser 5 minutes, sinon l'authentification échouera.

Activer l'authentification SAML

Vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d'identité sécurisé (IdP) avant de pouvoir accéder à l'interface utilisateur Web d'Unified Manager.

Avant de commencer

- Vous devez avoir configuré l'authentification à distance et vérifié qu'elle réussit.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle d'administrateur d'application.
- Le fournisseur d'identité (IdP) doit être pris en charge par Unified Manager et il doit être configuré.
- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès au serveur IdP.

Une fois l'authentification SAML activée à partir d'Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que l'IdP n'a pas été configuré avec les informations de l'hôte du serveur Unified Manager. Vous devez donc être prêt à terminer les deux parties de la connexion avant de commencer le processus de configuration. L'IdP peut être configuré avant ou après la configuration d'Unified Manager.

Seuls les utilisateurs distants auront accès à l'interface utilisateur graphique d'Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a pas d'impact sur les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPI.



Unified Manager redémarre automatiquement une fois la configuration SAML terminée sur cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification SAML**.
2. Cochez la case **Activer l'authentification SAML**.

Les champs requis pour configurer la connexion IdP s'affichent.

3. Saisissez l'URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager au serveur IdP.

Si le serveur IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URI IdP pour remplir automatiquement le champ Métadonnées IdP.

4. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.

Vous pouvez configurer le serveur IdP avec ces informations à ce stade.

5. Cliquez sur **Enregistrer**.

Une boîte de message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **Confirmer et se déconnecter** et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants autorisés tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification sur la page de connexion IdP au lieu de la page de connexion d'Unified Manager.

Si ce n'est pas déjà fait, accédez à votre IdP et saisissez l'URI et les métadonnées du serveur Unified Manager pour terminer la configuration.



Lorsque vous utilisez ADFS comme fournisseur d'identité, l'interface utilisateur graphique d'Unified Manager ne respecte pas le délai d'expiration ADFS et continue de fonctionner jusqu'à ce que le délai d'expiration de la session Unified Manager soit atteint. Vous pouvez modifier le délai d'expiration de la session de l'interface graphique en cliquant sur **Général > Paramètres des fonctionnalités > Délai d'inactivité**.

Modifier le fournisseur d'identité utilisé pour l'authentification SAML

Vous pouvez modifier le fournisseur d'identité (IdP) qu'Unified Manager utilise pour authentifier les utilisateurs distants.

Avant de commencer

- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès à l'IdP.

Le nouvel IdP peut être configuré avant ou après la configuration d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification SAML**.
2. Saisissez le nouvel URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager à l'IdP.

Si l'IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URL de l'IdP pour remplir automatiquement le champ Métadonnées IdP.

3. Copiez l'URI des métadonnées d'Unified Manager ou enregistrez les métadonnées dans un fichier texte XML.
4. Cliquez sur **Enregistrer la configuration**.

Une boîte de message s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouvel IdP et saisissez l'URI et les métadonnées du serveur Unified Manager pour terminer la configuration.

La prochaine fois que les utilisateurs distants autorisés tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la nouvelle page de connexion IdP au lieu de l'ancienne page de connexion IdP.

Mettre à jour les paramètres d'authentification SAML après la modification du certificat de sécurité d'Unified Manager

Toute modification du certificat de sécurité HTTPS installé sur le serveur Unified Manager nécessite la mise à jour des paramètres de configuration de l'authentification SAML. Le certificat est mis à jour si vous renommez le système hôte, attribuez une nouvelle adresse IP au système hôte ou modifiez manuellement le certificat de sécurité du système.

Une fois le certificat de sécurité modifié et le serveur Unified Manager redémarré, l'authentification SAML ne fonctionnera pas et les utilisateurs ne pourront pas accéder à l'interface graphique d'Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IdP et sur le serveur Unified Manager pour réactiver l'accès à l'interface utilisateur.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, saisissez le numéro de l'option **Désactiver l'authentification SAML**.

Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Lancez l'interface utilisateur d'Unified Manager à l'aide du nom de domaine complet ou de l'adresse IP mis à jour, acceptez le certificat de serveur mis à jour dans votre navigateur et connectez-vous à l'aide des informations d'identification de l'utilisateur de maintenance.
4. Dans la page **Configuration/Authentication**, sélectionnez l'onglet **Authentication SAML** et configurez la connexion IdP.
5. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.
6. Cliquez sur **Enregistrer**.

Une boîte de message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

7. Cliquez sur **Confirmer et se déconnecter** et Unified Manager redémarre.
8. Accédez à votre serveur IdP et saisissez l'URI et les métadonnées du serveur Unified Manager pour terminer la configuration.

Fournisseur d'identité	Étapes de configuration
ADFS	- Supprimez l'entrée de confiance de la partie de confiance existante dans l'interface graphique de gestion ADFS. - Ajoutez une nouvelle entrée de confiance de partie de confiance à l'aide de la <code>saml_sp_metadata.xml</code> à partir du serveur Unified Manager mis à jour. - Définissez les trois règles de réclamation requises pour qu'Unified Manager analyse les réponses SAML ADFS pour cette entrée de confiance de partie de confiance. - Redémarrez le service Windows ADFS.
Schibboleth	- Mettez à jour le nouveau FQDN du serveur Unified Manager dans le <code>attribute-filter.xml</code> et <code>relying-party.xml</code> fichiers. - Redémarrez le serveur Web Apache Tomcat et attendez que le port 8005 soit en ligne.

- Connectez-vous à Unified Manager et vérifiez que l'authentification SAML fonctionne comme prévu via votre IdP.

Désactiver l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs distants via un fournisseur d'identité sécurisé (IdP) avant qu'ils puissent se connecter à l'interface utilisateur Web d'Unified Manager. Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, effectuent l'authentification de connexion.

Après avoir désactivé l'authentification SAML, les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à l'aide de la console de maintenance Unified Manager si vous n'avez pas accès à l'interface utilisateur graphique.



Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

- Dans le volet de navigation de gauche, cliquez sur **Général > Authentification SAML**.
- Décochez la case **Activer l'authentification SAML**.
- Cliquez sur **Enregistrer**.

Une boîte de message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

4. Cliquez sur **Confirmer et se déconnecter** et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la page de connexion d'Unified Manager au lieu de la page de connexion IdP.

Accédez à votre IdP et supprimez l'URI et les métadonnées du serveur Unified Manager.

Désactiver l'authentification SAML depuis la console de maintenance

Vous devrez peut-être désactiver l'authentification SAML à partir de la console de maintenance lorsqu'il n'y a pas d'accès à l'interface graphique utilisateur d'Unified Manager. Cela peut se produire en cas de mauvaise configuration ou si l'IdP n'est pas accessible.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu'utilisateur de maintenance.

Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, effectuent l'authentification de connexion. Les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à partir de la page Configuration/Authentification de l'interface utilisateur.



Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, saisissez le numéro de l'option **Désactiver l'authentification SAML**.

Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Tapez **y**, puis appuyez sur Entrée et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la page de connexion d'Unified Manager au lieu de la page de connexion IdP.

Si nécessaire, accédez à votre IdP et supprimez l'URL et les métadonnées du serveur Unified Manager.

Page d'authentification SAML

Vous pouvez utiliser la page Authentification SAML pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identité sécurisé (IdP) avant de pouvoir se connecter à l'interface utilisateur Web d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application pour créer ou modifier la configuration SAML.

- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez sélectionner la case à cocher Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IdP**

L'URI pour accéder à l'IdP à partir du serveur Unified Manager. Des exemples d'URI sont répertoriés ci-dessous.

Exemple d'URI ADFS :

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml
```

Exemple d'URI Shibboleth :

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **Métadonnées IdP**

Les métadonnées IdP au format XML.

Si l'URL IdP est accessible depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** pour remplir ce champ.

- **Système hôte (FQDN)**

Le nom de domaine complet du système hôte Unified Manager tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI de l'hôte**

L'URI pour accéder au système hôte Unified Manager à partir de l'IdP.

- **Métadonnées de l'hôte**

Les métadonnées du système hôte au format XML.

Gérer l'authentification

Vous pouvez activer l'authentification à l'aide de LDAP ou d'Active Directory sur le serveur Unified Manager et le configurer pour qu'il fonctionne avec vos serveurs afin d'authentifier les utilisateurs distants.

Pour activer l'authentification à distance, configurer les services d'authentification et ajouter des serveurs d'authentification, consultez la section précédente sur **Configuration d'Unified Manager pour envoyer des notifications d'alerte**.

Modifier les serveurs d'authentification

Vous pouvez modifier le port que le serveur Unified Manager utilise pour communiquer avec votre serveur d'authentification.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Cochez la case **Désactiver la recherche de groupe imbriqué**.
3. Dans la zone **Serveurs d'authentification**, sélectionnez le serveur d'authentification que vous souhaitez modifier, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Modifier le serveur d'authentification**, modifiez les détails du port.
5. Cliquez sur **Enregistrer**.

Supprimer les serveurs d'authentification

Vous pouvez supprimer un serveur d'authentification si vous souhaitez empêcher le serveur Unified Manager de communiquer avec le serveur d'authentification. Par exemple, si vous souhaitez modifier un serveur d'authentification avec lequel le serveur de gestion communique, vous pouvez supprimer le serveur d'authentification et ajouter un nouveau serveur d'authentification.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Lorsque vous supprimez un serveur d'authentification, les utilisateurs ou groupes distants du serveur d'authentification ne pourront plus accéder à Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Sélectionnez un ou plusieurs serveurs d'authentification que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la demande de suppression.

Si l'option **Utiliser une connexion sécurisée** est activée, les certificats associés au serveur d'authentification sont supprimés avec le serveur d'authentification.

Authentification avec Active Directory ou OpenLDAP

Vous pouvez activer l'authentification à distance sur le serveur de gestion et configurer le serveur de gestion pour communiquer avec vos serveurs d'authentification afin que les utilisateurs des serveurs d'authentification puissent accéder à Unified Manager.

Vous pouvez utiliser l'un des services d'authentification prédéfinis suivants ou spécifier votre propre service d'authentification :

- Microsoft Active Directory



Vous ne pouvez pas utiliser Microsoft Lightweight Directory Services.

- OpenLDAP

Vous pouvez sélectionner le service d'authentification requis et ajouter les serveurs d'authentification appropriés pour permettre aux utilisateurs distants du serveur d'authentification d'accéder à Unified Manager. Les informations d'identification des utilisateurs ou des groupes distants sont conservées par le serveur d'authentification. Le serveur de gestion utilise le protocole LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs distants au sein du serveur d'authentification configuré.

Pour les utilisateurs locaux créés dans Unified Manager, le serveur de gestion conserve sa propre base de données de noms d'utilisateur et de mots de passe. Le serveur de gestion effectue l'authentification et n'utilise pas Active Directory ou OpenLDAP pour l'authentification.

Journalisation d'audit

Vous pouvez détecter si les journaux d'audit ont été compromis à l'aide des journaux d'audit. Toutes les activités effectuées par un utilisateur sont surveillées et enregistrées dans les journaux d'audit. Les audits sont effectués pour toutes les fonctionnalités de l'interface utilisateur et des API exposées publiquement d'Active IQ Unified Manager.

Vous pouvez utiliser **Journal d'audit : Affichage des fichiers** pour afficher et accéder à tous les fichiers journaux d'audit disponibles dans votre Active IQ Unified Manager. Les fichiers dans le journal d'audit : vue Fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux d'audit capturés depuis l'installation ou la mise à niveau jusqu'à ceux présents dans le système. Chaque fois que vous effectuez une action dans Unified Manager, les informations sont mises à jour et sont disponibles dans les journaux. L'état de chaque fichier journal est capturé à l'aide de l'attribut « État d'intégrité du fichier » qui est surveillé activement pour détecter toute falsification ou suppression du fichier journal. Les journaux d'audit peuvent avoir l'un des états suivants lorsque les journaux d'audit sont disponibles dans le système :

État	Description
ACTIF	Fichier dans lequel les journaux sont actuellement enregistrés.
NORMALE	Fichier inactif, compressé et stocké dans le système.
Altéré	Fichier qui a été compromis par un utilisateur qui a modifié manuellement le fichier.
SUPPRESSION_MANUELLE	Fichier qui a été supprimé par un utilisateur autorisé.
SUPPRIMER_PAR_ROULEMENT	Fichier qui a été supprimé en raison d'une mise à l'arrêt basée sur la politique de configuration continue.
SUPPRESSION_INATTENDUE	Fichier qui a été supprimé pour des raisons inconnues.

La page Journal d'audit comprend les boutons de commande suivants :

- Configurer
- Supprimer
- Télécharger

Le bouton **SUPPRIMER** vous permet de supprimer l'un des journaux d'audit répertoriés dans la vue Journaux d'audit. Vous pouvez supprimer un journal d'audit et éventuellement fournir une raison pour supprimer le fichier, ce qui permet à l'avenir de déterminer une suppression valide. La colonne **RAISON** répertorie la raison ainsi que le nom de l'utilisateur qui a effectué l'opération de suppression.



La suppression d'un fichier journal entraînera la suppression du fichier du système, mais l'entrée dans la table de base de données ne sera pas supprimée.

Vous pouvez télécharger les journaux d'audit depuis Active IQ Unified Manager à l'aide du bouton **TÉLÉCHARGER** dans la section Journaux d'audit et exporter les fichiers journaux d'audit. Les fichiers marqués « **NORMAL** » ou « **TAMPERED** » sont téléchargés dans un format compressé. `.gzip` format.

Les fichiers journaux d'audit sont archivés périodiquement et enregistrés dans la base de données pour référence. Avant l'archivage, les journaux d'audit sont signés numériquement pour maintenir la sécurité et l'intégrité.

Lorsqu'un bundle AutoSupport complet est généré, le bundle de support inclut les fichiers journaux d'audit archivés et actifs. Mais lorsqu'un bundle de support léger est généré, il inclut uniquement les journaux d'audit actifs. Les journaux d'audit archivés ne sont pas inclus.

Configurer les journaux d'audit

Vous pouvez utiliser le bouton **Configurer** dans la section Journaux d'audit pour configurer la politique de déploiement pour les fichiers journaux d'audit et pour activer également la journalisation à distance pour les journaux d'audit.

Vous pouvez définir les valeurs dans **TAILLE MAXIMALE DU FICHIER** et **JOURS DE CONSERVATION DU JOURNAL D'AUDIT** en fonction de la quantité et de la fréquence souhaitées des données que vous souhaitez stocker dans le système. La valeur dans le champ **TAILLE TOTALE DU JOURNAL D'AUDIT** correspond à la taille totale des données du journal d'audit présentes dans le système. La politique de renouvellement est déterminée par les valeurs des champs **JOURS DE CONSERVATION DU JOURNAL D'AUDIT**, **TAILLE MAXIMALE DU FICHIER** et **TAILLE TOTALE DU JOURNAL D'AUDIT**. Lorsque la taille de la sauvegarde du journal d'audit atteint la valeur configurée dans **TAILLE TOTALE DU JOURNAL D'AUDIT**, le fichier qui a été archivé en premier est supprimé. Cela signifie que le fichier le plus ancien est supprimé. Mais l'entrée de fichier continue d'être disponible dans la base de données et est marquée comme « Rollover Delete ». La valeur **JOURS DE CONSERVATION DU JOURNAL D'AUDIT** correspond au nombre de jours pendant lesquels les fichiers journaux d'audit sont conservés. Tout fichier plus ancien que la valeur définie dans ce champ est remplacé.

Étapes

1. Cliquez sur **Journaux d'audit > > Configurer**.
2. Saisissez des valeurs dans les champs **TAILLE MAXIMALE DU FICHIER**, **TAILLE TOTALE DU JOURNAL D'AUDIT** et **JOURS DE CONSERVATION DU JOURNAL D'AUDIT**.

Si vous souhaitez activer la journalisation à distance, vous devez sélectionner **Activer la journalisation à distance**. /// 2025-6-11, OTHERDOC-133

Activer la journalisation à distance des journaux d'audit

Vous pouvez sélectionner la case à cocher **Activer la journalisation à distance** dans la boîte de dialogue Configurer les journaux d'audit pour activer la journalisation d'audit à distance. Vous pouvez utiliser cette fonctionnalité pour transférer les journaux d'audit vers un serveur Syslog distant. Cela vous permettra de gérer vos journaux d'audit lorsque des contraintes d'espace sont présentes.

La journalisation à distance des journaux d'audit fournit une sauvegarde inviolable au cas où les fichiers journaux d'audit sur le serveur Active IQ Unified Manager seraient falsifiés.

Étapes

1. Dans la boîte de dialogue **Configurer les journaux d'audit**, cochez la case **Activer la journalisation à distance**.

Des champs supplémentaires pour configurer la journalisation à distance sont affichés.

2. Saisissez le **HOSTNAME** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **CERTIFICAT CA DU SERVEUR**, cliquez sur **PARCOURIR** pour sélectionner un certificat public du serveur cible.

Le certificat doit être téléchargé dans `.pem` format. Ce certificat doit être obtenu auprès du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le « nom d'hôte » sélectionné dans le cadre du SubjectAltName Attribut (SAN).

4. Saisissez les valeurs pour les champs suivants : **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

Les valeurs doivent être en millisecondes pour ces champs.

5. Sélectionnez le format Syslog requis et la version du protocole TLS dans les champs **FORMAT** et **PROTOCOL**.
6. Cochez la case **Activer l'authentification client** si le serveur Syslog cible requiert une authentification basée sur un certificat.

Vous devrez télécharger le certificat d'authentification client et le télécharger sur le serveur Syslog avant d'enregistrer la configuration du journal d'audit, sinon la connexion échouera. Selon le type de serveur Syslog, vous devrez peut-être créer un hachage du certificat d'authentification client.

Exemple : syslog-ng nécessite qu'un <hash> du certificat soit créé à l'aide de la commande `openssl x509 -noout -hash -in cert.pem`, et vous devez ensuite lier symboliquement le certificat d'authentification client à un fichier nommé d'après le <hash> .0.

7. Cliquez sur **Enregistrer** pour configurer la connexion avec votre serveur et activer la journalisation à distance.

Vous serez redirigé vers la page Journaux d'audit.



La valeur **Délai d'expiration de connexion** peut affecter la configuration. Si la configuration prend plus de temps à répondre que la valeur définie, cela peut entraîner un échec de configuration en raison d'une erreur de connexion. Pour établir une connexion réussie, augmentez la valeur **Délai d'expiration de la connexion** et réessayez la configuration.

Page d'authentification à distance

Vous pouvez utiliser la page Authentification à distance pour configurer Unified Manager afin de communiquer avec votre serveur d'authentification pour authentifier les utilisateurs distants qui tentent de se connecter à l'interface utilisateur Web d'Unified Manager.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Après avoir coché la case Activer l'authentification à distance, vous pouvez activer l'authentification à distance à l'aide d'un serveur d'authentification.

- **Service d'authentification**

Vous permet de configurer le serveur de gestion pour authentifier les utilisateurs dans les fournisseurs de services d'annuaire, tels qu'Active Directory, OpenLDAP, ou de spécifier votre propre mécanisme d'authentification. Vous ne pouvez spécifier un service d'authentification que si vous avez activé l'authentification à distance.

- **Active Directory**

- Nom de l'administrateur

Spécifie le nom de l'administrateur du serveur d'authentification.

- Mot de passe

Spécifie le mot de passe pour accéder au serveur d'authentification.

- Nom distinctif de base

Spécifie l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.

- Désactiver la recherche de groupe imbriqué

Spécifie s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Utiliser une connexion sécurisée

Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

- **OpenLDAP**

- Nom distinctif de Bind

Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour rechercher les utilisateurs distants dans le serveur d'authentification.

- Lier le mot de passe

Spécifie le mot de passe pour accéder au serveur d'authentification.

- Nom distinctif de base

Spécifie l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.

- Utiliser une connexion sécurisée

Spécifie que Secure LDAP est utilisé pour communiquer avec les serveurs d'authentification LDAP.

- **Autres**

- Nom distinctif de Bind

Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour rechercher les utilisateurs distants dans le serveur d'authentification que vous avez configuré.

- Lier le mot de passe

Spécifie le mot de passe pour accéder au serveur d'authentification.

- Nom distinctif de base

Spécifie l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.

- Version du protocole

Spécifie la version du protocole LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez spécifier si la version du protocole doit être détectée automatiquement ou définir la version sur 2 ou 3.

- Attribut de nom d'utilisateur

Spécifie le nom de l'attribut dans le serveur d'authentification qui contient les noms de connexion des utilisateurs à authentifier par le serveur de gestion.

- Attribut d'appartenance au groupe

Spécifie une valeur qui attribue l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut et d'une valeur spécifiés dans le serveur d'authentification de l'utilisateur.

- UGID

Si les utilisateurs distants sont inclus en tant que membres d'un objet GroupOfUniqueNames dans le serveur d'authentification, cette option vous permet d'attribuer l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet GroupOfUniqueNames.

- Désactiver la recherche de groupe imbriqué

Spécifie s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Membre

Spécifie le nom d'attribut que votre serveur d'authentification utilise pour stocker des informations sur les membres individuels d'un groupe.

- Classe d'objet utilisateur

Spécifie la classe d'objet d'un utilisateur dans le serveur d'authentification distant.

- Classe d'objet de groupe

Spécifie la classe d'objet de tous les groupes du serveur d'authentification distant.



Les valeurs que vous entrez pour les attributs *Member*, *User Object Class* et *Group Object Class* doivent être les mêmes que celles ajoutées dans vos configurations Active Directory, OpenLDAP et LDAP. Sinon, l'authentification pourrait échouer.

- Utiliser une connexion sécurisée

Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.



Si vous souhaitez modifier le service d'authentification, assurez-vous de supprimer tous les serveurs d'authentification existants et d'ajouter de nouveaux serveurs d'authentification.

Zone des serveurs d'authentification

La zone Serveurs d'authentification affiche les serveurs d'authentification avec lesquels le serveur de gestion communique pour rechercher et authentifier les utilisateurs distants. Les informations d'identification des utilisateurs ou des groupes distants sont conservées par le serveur d'authentification.

- **Boutons de commande**

Vous permet d'ajouter, de modifier ou de supprimer des serveurs d'authentification.

- Ajouter

Vous permet d'ajouter un serveur d'authentification.

Si le serveur d'authentification que vous ajoutez fait partie d'une paire à haute disponibilité (utilisant la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsque l'un des serveurs d'authentification est inaccessible.

- Modifier

Vous permet de modifier les paramètres d'un serveur d'authentification sélectionné.

- Supprimer

Supprime les serveurs d'authentification sélectionnés.

- **Nom ou adresse IP**

Affiche le nom d'hôte ou l'adresse IP du serveur d'authentification utilisé pour authentifier l'utilisateur sur le

serveur de gestion.

- **Port**

Affiche le numéro de port du serveur d'authentification.

- **Tester l'authentification**

Ce bouton valide la configuration de votre serveur d'authentification en authentifiant un utilisateur ou un groupe distant.

Lors du test, si vous spécifiez uniquement le nom d'utilisateur, le serveur de gestion recherche l'utilisateur distant dans le serveur d'authentification, mais n'authentifie pas l'utilisateur. Si vous spécifiez à la fois le nom d'utilisateur et le mot de passe, le serveur de gestion recherche et authentifie l'utilisateur distant.

Vous ne pouvez pas tester l'authentification si l'authentification à distance est désactivée.

Gérer les certificats de sécurité

Vous pouvez configurer HTTPS sur le serveur Unified Manager pour surveiller et gérer vos clusters via une connexion sécurisée.

Afficher le certificat de sécurité HTTPS

Vous pouvez comparer les détails du certificat HTTPS au certificat récupéré dans votre navigateur pour vous assurer que la connexion cryptée de votre navigateur à Unified Manager n'est pas interceptée.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

L'affichage du certificat vous permet de vérifier le contenu d'un certificat régénéré ou d'afficher les noms alternatifs du sujet (SAN) à partir desquels vous pouvez accéder à Unified Manager.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général > Certificat HTTPS**.

Le certificat HTTPS est affiché en haut de la page

Si vous avez besoin d'afficher des informations plus détaillées sur le certificat de sécurité que celles affichées sur la page Certificat HTTPS, vous pouvez afficher le certificat de connexion dans votre navigateur.

Télécharger une demande de signature de certificat HTTPS

Vous pouvez télécharger une demande de signature de certification pour le certificat de sécurité HTTPS actuel afin de pouvoir fournir le fichier à une autorité de certification pour signature. Un certificat signé par une autorité de certification permet d'empêcher les attaques de type « man-in-the-middle » et offre une meilleure protection de sécurité qu'un certificat auto-signé.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Certificat HTTPS**.
2. Cliquez sur **Télécharger la demande de signature de certificat HTTPS**.
3. Sauver le `<hostname>.csr` déposer.

Vous pouvez fournir le fichier à une autorité de certification pour signature, puis installer le certificat signé.

Installer un certificat HTTPS signé et renvoyé par une autorité de certification

Vous pouvez télécharger et installer un certificat de sécurité après qu'une autorité de certification l'a signé et renvoyé. Le fichier que vous téléchargez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification permet d'empêcher les attaques de l'homme du milieu et offre une meilleure protection de sécurité qu'un certificat auto-signé.

*Quoi. Avant de commencer

Vous devez avoir effectué les actions suivantes :

- J'ai téléchargé le fichier de demande de signature de certificat et je l'ai fait signer par une autorité de certification.
- J'ai enregistré la chaîne de certificats au format PEM
- Tous les certificats de la chaîne sont inclus, du certificat du serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

Vous devez disposer du rôle d'administrateur d'application.



Si la validité du certificat pour lequel un CSR a été créé est supérieure à 397 jours, la validité sera réduite à 397 jours par l'AC avant de signer et de renvoyer le certificat

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Certificat HTTPS**.
2. Cliquez sur **Installer le certificat HTTPS**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir un fichier...** pour localiser le fichier à télécharger.
4. Sélectionnez le fichier, puis cliquez sur **Installer** pour installer le fichier.

Pour plus d'informations, voir "[Installation d'un certificat HTTPS généré à l'aide d'outils externes](#)".

Exemple de chaîne de certificats

L'exemple suivant montre à quoi pourrait ressembler le fichier de chaîne de certificats :

```

-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----

```

Installer un certificat HTTPS généré à l'aide d'outils externes

Vous pouvez installer des certificats auto-signés ou signés par une autorité de certification et générés à l'aide d'un outil externe comme OpenSSL, BoringSSL, LetsEncrypt.

Vous devez charger la clé privée avec la chaîne de certificats, car ces certificats sont des paires de clés publiques-privées générées en externe. Les algorithmes de paires de clés autorisés sont « RSA » et « EC ». L'option **Installer le certificat HTTPS** est disponible sur la page Certificats HTTPS sous la section Général. Le fichier que vous téléchargez doit être au format d'entrée suivant.

1. Clé privée du serveur appartenant à l'hôte Active IQ Unified Manager
2. Certificat du serveur correspondant à la clé privée
3. Certificat des CA inversé jusqu'à la racine, qui sont utilisés pour signer le certificat ci-dessus

Format de chargement d'un certificat avec une paire de clés EC

Les courbes autorisées sont « prime256v1 » et « secp384r1 ». Exemple de certificat avec une paire EC générée en externe :

```

-----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----

```

```

-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

Format de chargement d'un certificat avec une paire de clés RSA

Les tailles de clé autorisées pour la paire de clés RSA appartenant au certificat hôte sont 2048, 3072 et 4096. certificat avec une **paire de clés RSA** générée en externe :

```

-----BEGIN RSA PRIVATE KEY-----
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----

```

Une fois le certificat téléchargé, vous devez redémarrer l'instance Active IQ Unified Manager pour que les modifications prennent effet.

Vérifications lors du téléchargement de certificats générés en externe

Le système effectue des vérifications lors du téléchargement d'un certificat généré à l'aide d'outils externes. Si l'une des vérifications échoue, le certificat est rejeté. Des validations sont également incluses pour les certificats générés à partir du CSR au sein du produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée dans l'entrée est validée par rapport au certificat hôte dans l'entrée.
- Le nom commun (CN) dans le certificat de l'hôte est vérifié par rapport au FQDN de l'hôte.

- Le nom commun (CN) du certificat d'hôte ne doit pas être vide ou vide et ne doit pas être défini sur localhost.
- La date de début de validité ne doit pas être dans le futur et la date d'expiration de validité du certificat ne doit pas être dans le passé.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être dans le futur et la date d'expiration de la validité ne doit pas être dans le passé.



La clé privée dans l'entrée ne doit pas être cryptée. S'il existe des clés privées cryptées, elles sont rejetées par le système.

Exemple 1

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemple 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemple 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Si l'installation du certificat échoue, consultez l'article de la base de connaissances (KB) : [https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate\[\"ActiveIQ Unified Manager ne parvient pas à installer un certificat généré en externe\"\]](https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate[\)

Descriptions des pages pour la gestion des certificats

Vous pouvez utiliser la page Certificat HTTPS pour afficher les certificats de sécurité actuels et générer de nouveaux certificats HTTPS.

Page de certificat HTTPS

La page Certificat HTTPS vous permet d'afficher le certificat de sécurité actuel, de télécharger une demande de signature de certificat, de générer un nouveau certificat HTTPS auto-signé ou d'installer un nouveau certificat HTTPS.

Si vous n'avez pas généré de nouveau certificat HTTPS auto-signé, le certificat qui apparaît sur cette page est le certificat qui a été généré lors de l'installation.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les opérations suivantes :

- **Télécharger la demande de signature de certificat HTTPS**

Télécharge une demande de certification pour le certificat HTTPS actuellement installé. Votre navigateur vous invite à enregistrer le fichier <hostname>.csr afin de pouvoir fournir le fichier à une autorité de certification pour signature.

- **Installer le certificat HTTPS**

Vous permet de télécharger et d'installer un certificat de sécurité après qu'une autorité de certification l'a signé et renvoyé. Le nouveau certificat entre en vigueur après le redémarrage du serveur de gestion.

- **Régénérer le certificat HTTPS**

Vous permet de générer un nouveau certificat HTTPS auto-signé, qui remplace le certificat de sécurité actuel. Le nouveau certificat entre en vigueur après le redémarrage d'Unified Manager.

Boîte de dialogue Régénérer le certificat HTTPS

La boîte de dialogue Régénérer le certificat HTTPS vous permet de personnaliser les informations de sécurité, puis de générer un nouveau certificat HTTPS avec ces informations.

Les informations actuelles du certificat apparaissent sur cette page.

Les sélections « Régénérer à l'aide des attributs de certificat actuels » et « Mettre à jour les attributs de certificat actuels » vous permettent de régénérer le certificat avec les informations actuelles ou de générer un certificat avec de nouvelles informations.

- **Nom commun**

Requis. Le nom de domaine entièrement qualifié (FQDN) que vous souhaitez sécuriser.

Dans les configurations haute disponibilité d'Unified Manager, utilisez l'adresse IP virtuelle.

- **E-mail**

Facultatif. Une adresse e-mail pour contacter votre organisation ; généralement l'adresse e-mail de l'administrateur du certificat ou du service informatique.

- **Entreprise**

Facultatif. Généralement le nom incorporé de votre entreprise.

- **Département**

Facultatif. Le nom du département de votre entreprise.

- **Ville**

Facultatif. La ville où se trouve votre entreprise.

- **État**

Facultatif. L'état ou la province où se trouve votre entreprise, sans abréviation.

- **Pays**

Facultatif. Le pays dans lequel se trouve votre entreprise. Il s'agit généralement d'un code ISO à deux lettres du pays.

- **Noms alternatifs**

Requis. Noms de domaine supplémentaires non principaux qui peuvent être utilisés pour accéder à ce serveur en plus de l'hôte local existant ou d'autres adresses réseau. Séparez chaque nom alternatif par une virgule.

Cochez la case « Exclure les informations d'identification locales (par exemple, localhost) » si vous souhaitez supprimer les informations d'identification locales du champ Noms alternatifs du certificat. Lorsque cette case à cocher est sélectionnée, seul ce que vous saisissez dans le champ est utilisé dans le champ Noms alternatifs. Si ce champ est laissé vide, le certificat résultant n'aura pas du tout de champ Noms alternatifs.

- **TAILLE DE LA CLÉ (ALGORITHME DE CLÉ : RSA)**

L'algorithme clé est défini sur RSA. Vous pouvez choisir parmi l'une des tailles de clé : 2 048, 3 072 ou 4 096 bits. La taille de clé par défaut est définie sur 2048 bits.

- **DURÉE DE VALIDITÉ**

La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau à partir d'une version précédente, la validité du certificat précédent peut rester inchangée.

Pour plus d'informations, voir ["Génération de certificats HTTPS"](#).

Surveiller et gérer le stockage

Introduction à Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous permet de surveiller et de gérer l'état et les performances de vos systèmes de stockage ONTAP à partir d'une interface unique.

Unified Manager offre les fonctionnalités suivantes :

- Découverte, surveillance et notifications pour les systèmes installés avec le logiciel ONTAP .
- Tableau de bord pour afficher la capacité, la sécurité et les performances de l'environnement.
- Alertes, événements et infrastructure de seuil améliorés.
- Affiche des graphiques détaillés qui tracent l'activité de la charge de travail au fil du temps ; y compris les IOPS (opérations), les Mbit/s (débit), la latence (temps de réponse), l'utilisation, la capacité de performance et le ratio de cache.
- Identifie les charges de travail qui utilisent de manière excessive les composants du cluster et les charges de travail dont les performances sont affectées par l'activité accrue.
- Fournit des suggestions d'actions correctives qui peuvent être effectuées pour résoudre certains incidents et événements, ainsi qu'un bouton « Réparer » pour certains événements afin que vous puissiez résoudre le problème immédiatement.
- S'intègre à OnCommand Workflow Automation pour exécuter des workflows de protection automatisés.
- Possibilité de créer de nouvelles charges de travail, telles qu'un LUN ou un partage de fichiers, directement à partir d'Unified Manager et d'attribuer un niveau de service de performances pour définir les objectifs de performances et de stockage pour les utilisateurs accédant à l'application à l'aide de cette charge de travail.

Introduction à la surveillance de l'état de santé Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous aide à surveiller un grand nombre de systèmes exécutant le logiciel ONTAP via une interface utilisateur centralisée. L'infrastructure du serveur Unified Manager offre une évolutivité, une capacité de support et des capacités de surveillance et de notification améliorées.

Les principales fonctionnalités d'Unified Manager incluent la surveillance, l'alerte, la gestion de la disponibilité et de la capacité des clusters, la gestion des capacités de protection et le regroupement des données de diagnostic et leur envoi au support technique.

Vous pouvez utiliser Unified Manager pour surveiller vos clusters. Lorsque des problèmes surviennent dans le cluster, Unified Manager vous informe des détails de ces problèmes via des événements. Certains événements vous proposent également une mesure corrective que vous pouvez prendre pour corriger les problèmes. Vous pouvez configurer des alertes pour les événements afin que lorsque des problèmes surviennent, vous soyez averti par e-mail et par des interruptions SNMP.

Vous pouvez utiliser Unified Manager pour gérer les objets de stockage dans votre environnement en les associant à des annotations. Vous pouvez créer des annotations personnalisées et associer dynamiquement des clusters, des machines virtuelles de stockage (SVM) et des volumes aux annotations via des règles.

Vous pouvez également planifier les besoins de stockage de vos objets de cluster à l'aide des informations fournies dans les graphiques de capacité et d'état, pour l'objet de cluster concerné.

Capacité physique et logique

Unified Manager utilise les concepts d'espace physique et logique utilisés pour les objets de stockage ONTAP .

- Capacité physique : l'espace physique fait référence aux blocs physiques de stockage utilisés dans le volume. La « capacité physique utilisée » est généralement inférieure à la capacité logique utilisée en raison de la réduction des données résultant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- Capacité logique : L'espace logique fait référence à l'espace utilisable (les blocs logiques) dans un volume. L'espace logique fait référence à la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats de la déduplication ou de la compression. « L'espace logique utilisé » correspond à l'espace physique utilisé, plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure apparaît souvent plus grande que la capacité physique utilisée car elle ne reflète pas la compression des données et les autres réductions de l'espace physique. Ainsi, la capacité logique totale pourrait être supérieure à l'espace provisionné.

Unités de mesure de capacité

Unified Manager calcule la capacité de stockage en fonction d'unités binaires de 1024 (2¹⁰) octets. Dans ONTAP 9.10.0 et les versions antérieures, ces unités étaient affichées sous la forme Ko, Mo, Go, To et Po. À partir d' ONTAP 9.10.1, ils sont affichés dans Unified Manager sous la forme Kio, Mio, Gio, Tio et Pio.



Les unités utilisées pour le débit continuent d'être les kilooctets par seconde (Kbps), les mégaoctets par seconde (Mbps), les gigaoctets par seconde (Gbps) ou les téraoctets par seconde (Tbps), etc., pour toutes les versions d' ONTAP.

Unité de capacité affichée dans Unified Manager pour ONTAP 9.10.0 et versions antérieures	Unité de capacité affichée dans Unified Manager pour ONTAP 9.10.1	Calcul	Valeur en octets
Ko	KiB	1024	1024 octets
MB	Mio	1024 * 1024	1 048 576 octets
GB	Gio	1024 * 1024 * 1024	1 073 741 824 octets
To	Tio	1024 * 1024 * 1024 * 1024	1 099 511 627 776 octets

Introduction à la surveillance des performances Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) fournit des fonctionnalités de surveillance des performances et d'analyse des causes profondes des événements pour les systèmes exécutant le logiciel NetApp ONTAP .

Unified Manager vous aide à identifier les charges de travail qui utilisent trop les composants du cluster et diminuent les performances des autres charges de travail sur le cluster. En définissant des stratégies de seuil de performances, vous pouvez également spécifier des valeurs maximales pour certains compteurs de performances afin que des événements soient générés lorsque le seuil est dépassé. Unified Manager vous alerte sur ces événements de performance afin que vous puissiez prendre des mesures correctives et ramener les performances à des niveaux de fonctionnement normaux. Vous pouvez afficher et analyser les événements dans l'interface utilisateur d'Unified Manager.

Unified Manager surveille les performances de deux types de charges de travail :

- Charges de travail définies par l'utilisateur

Ces charges de travail se composent de volumes FlexVol et de volumes FlexGroup que vous avez créés dans votre cluster.

- Charges de travail définies par le système

Ces charges de travail sont constituées d'activités internes du système.

Utiliser les API REST d'Unified Manager

Active IQ Unified Manager vous fournit des API REST pour afficher les informations sur la surveillance et la gestion de votre environnement de stockage. Les API permettent également de provisionner et de gérer des objets de stockage en fonction de politiques.

Vous pouvez également exécuter les API ONTAP sur tous les clusters gérés par ONTAP à l'aide de la passerelle API prise en charge par Unified Manager.

Pour plus d'informations sur les API REST d'Unified Manager, consultez ["Prise en main des API REST Active IQ Unified Manager"](#) .

À quoi sert le serveur Unified Manager

L'infrastructure du serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

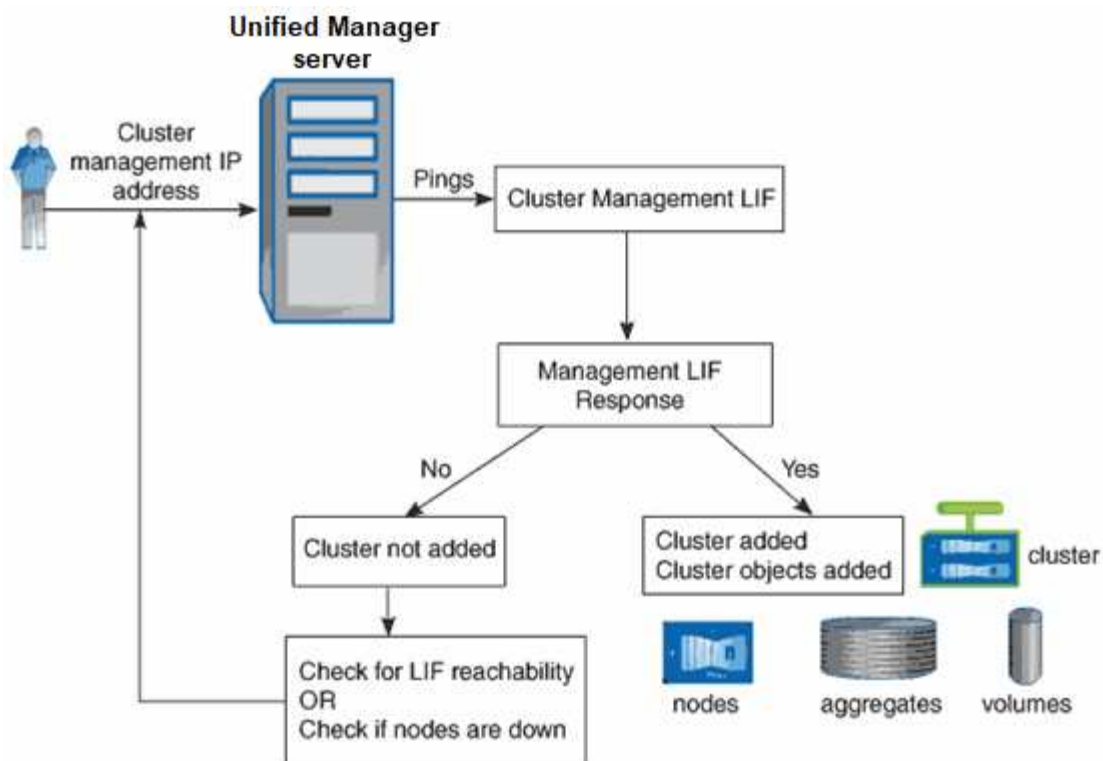
Unified Manager collecte les informations du cluster, stocke les données dans la base de données et analyse les données pour voir s'il existe des problèmes de cluster.

Comment fonctionne le processus de découverte

Une fois le cluster ajouté à Unified Manager, le serveur découvre les objets du cluster et les ajoute à sa base de données. Comprendre le fonctionnement du processus de découverte vous aide à gérer les clusters de votre organisation et leurs objets.

L'intervalle de surveillance par défaut est de 15 minutes : si vous avez ajouté un cluster au serveur Unified Manager, il faut 15 minutes pour afficher les détails du cluster dans l'interface utilisateur d'Unified Manager.

L'image suivante illustre le processus de découverte dans Active IQ Unified Manager:



Comprendre l'interface utilisateur

L'interface utilisateur d'Unified Manager se compose principalement d'un tableau de bord qui fournit une vue d'ensemble des objets surveillés. L'interface utilisateur permet également d'accéder à la visualisation de tous les objets du cluster.

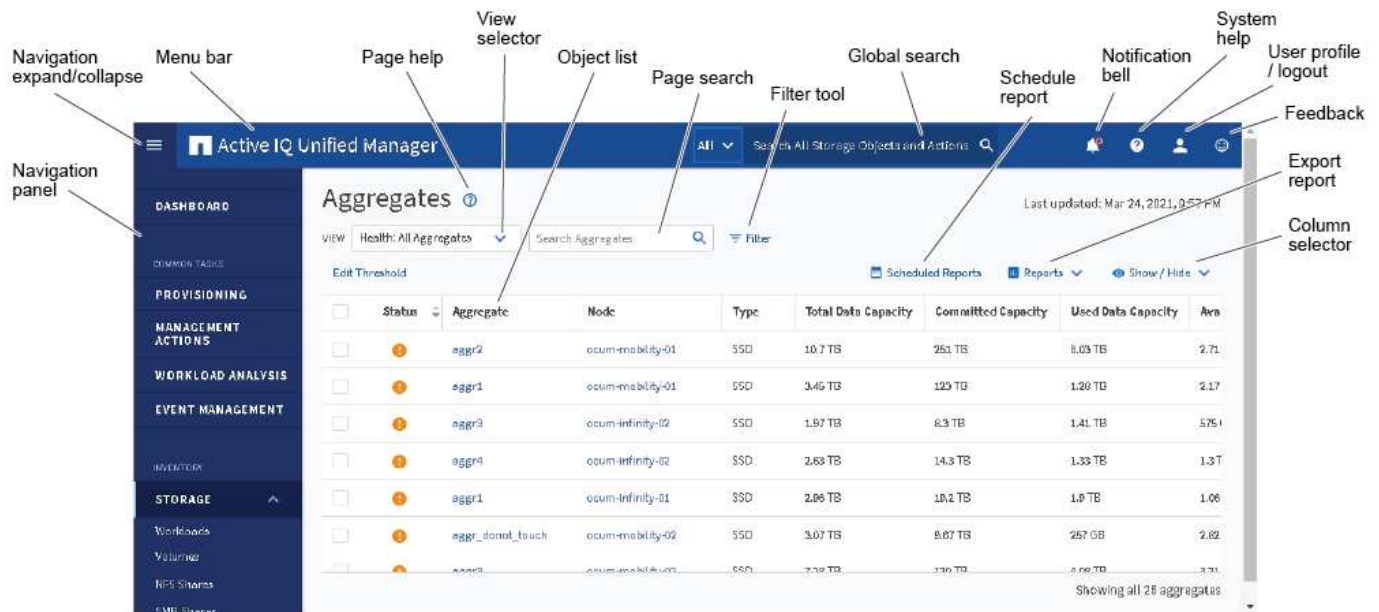
Vous pouvez sélectionner une vue préférée et utiliser les boutons d'action si nécessaire. Votre configuration d'écran est enregistrée dans un espace de travail afin que toutes les fonctionnalités dont vous avez besoin soient disponibles lorsque vous démarrez Unified Manager. Cependant, lorsque vous naviguez d'une vue à une autre, puis revenez en arrière, la vue peut ne pas être la même.

Dispositions de fenêtres typiques

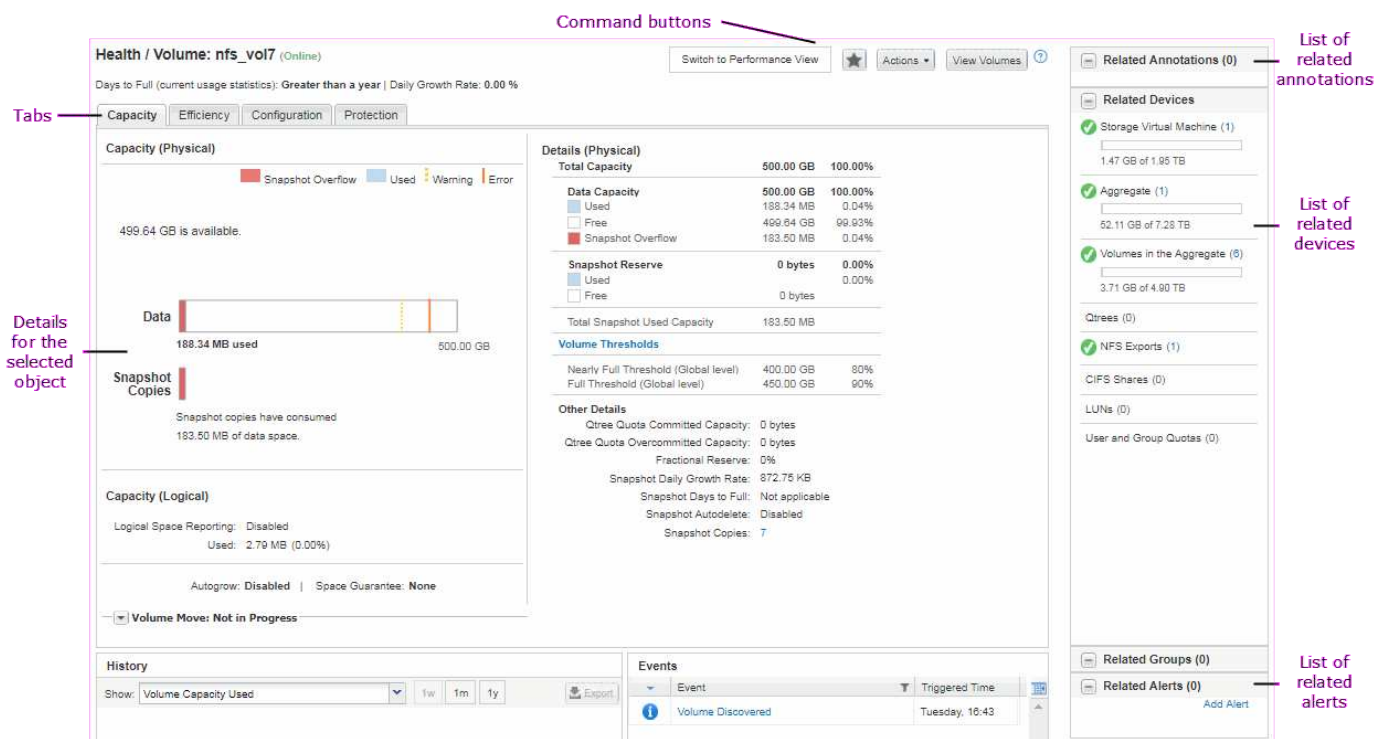
Comprendre les dispositions de fenêtres typiques vous aide à naviguer et à utiliser efficacement Active IQ Unified Manager. La plupart des fenêtres d'Unified Manager sont similaires à l'une des deux présentations générales : liste d'objets ou détails. Le paramètre d'affichage recommandé est d'au moins 1280 x 1024 pixels.

Toutes les fenêtres ne contiennent pas tous les éléments des diagrammes suivants.

Disposition de la fenêtre de liste d'objets



Disposition de la fenêtre des détails de l'objet



Personnalisation de la disposition des fenêtres

Active IQ Unified Manager vous permet de personnaliser la disposition des informations sur les pages d'objets de stockage et de réseau. En personnalisant les fenêtres, vous pouvez contrôler quelles données sont visibles et comment les données sont affichées.

• Tri

Vous pouvez cliquer sur l'en-tête de colonne pour modifier l'ordre de tri des entrées de colonne. Lorsque

vous cliquez sur l'en-tête de colonne, les flèches de tri (▲ et ▼) apparaissent pour cette colonne.

- **Filtration**

Vous pouvez cliquer sur l'icône de filtre () pour appliquer des filtres afin de personnaliser l'affichage des informations sur les pages d'objets de stockage et de réseau afin que seules les entrées correspondant aux conditions fournies soient affichées. Vous appliquez des filtres à partir du volet Filtres.

Le volet Filtres vous permet de filtrer la plupart des colonnes en fonction des options sélectionnées. Par exemple, dans la vue Santé : Tous les volumes, vous pouvez utiliser le volet Filtres pour afficher tous les volumes hors ligne en sélectionnant l'option de filtre appropriée sous État.

Les colonnes relatives à la capacité dans n'importe quelle liste affichent toujours les données de capacité dans des unités appropriées arrondies à deux décimales. Ceci s'applique également lors du filtrage des colonnes de capacité. Par exemple, si vous utilisez le filtre dans la colonne Capacité totale des données dans la vue Intégrité : tous les agrégats pour filtrer les données supérieures à 20,45 Go, la capacité réelle de 20,454 Go s'affiche sous la forme 20,45 Go. De même, si vous filtrez les données inférieures à 20,45 Go, la capacité réelle de 20,449 Go s'affiche comme 20,45 Go.

Si vous utilisez le filtre dans la colonne % de données disponibles dans la vue Santé : tous les agrégats pour filtrer les données supérieures à 20,45 %, la capacité réelle de 20,454 % s'affiche comme 20,45 %. De même, si vous filtrez les données inférieures à 20,45 %, la capacité réelle de 20,449 % s'affiche comme 20,45 %.

- **Masquer ou afficher les colonnes**

Vous pouvez cliquer sur l'icône d'affichage des colonnes (**Afficher/Masquer**) pour sélectionner les colonnes que vous souhaitez afficher. Une fois que vous avez sélectionné les colonnes appropriées, vous pouvez les réorganiser en les faisant glisser à l'aide de votre souris.

- **Recherche**

Vous pouvez utiliser la zone de recherche pour rechercher certains attributs d'objet afin d'affiner la liste des éléments dans la page d'inventaire. Par exemple, vous pouvez saisir « cloud » pour affiner la liste des volumes dans la page d'inventaire des volumes afin de voir tous les volumes contenant le mot « cloud ».

- **Exportation de données**

Vous pouvez cliquer sur le bouton **Rapports** (ou sur le bouton **Exporter** pour exporter les données vers un fichier de valeurs séparées par des virgules) (.csv) déposer, (.pdf) document ou Microsoft Excel (.xlsx) fichier et utiliser les données exportées pour créer des rapports.

Utiliser l'aide du gestionnaire unifié

L'aide comprend des informations sur toutes les fonctionnalités incluses dans Active IQ Unified Manager. Vous pouvez utiliser la table des matières, l'index ou l'outil de recherche pour trouver des informations sur les fonctionnalités et comment les utiliser.

L'aide est disponible à partir de chaque onglet et de la barre de menus de l'interface utilisateur d'Unified Manager.

L'outil de recherche dans l'Aide ne fonctionne pas pour les mots partiels.

- Pour en savoir plus sur des champs ou des paramètres spécifiques, cliquez sur  .
- Pour afficher tout le contenu de l'aide, cliquez sur  * > ***Aide/Documentation** dans la barre de menu.

Vous pouvez trouver des informations plus détaillées en développant n'importe quelle partie de la table des matières dans le volet de navigation.

- Pour rechercher le contenu de l'aide, cliquez sur l'onglet **Rechercher** dans le volet de navigation, saisissez le mot ou la série de mots que vous souhaitez rechercher et cliquez sur **Aller !**
- Pour imprimer les rubriques d'aide, cliquez sur l'icône de l'imprimante.

Ajoutez vos sujets d'aide favoris à vos favoris

Dans l'onglet Favoris d'aide, vous pouvez ajouter à vos favoris les rubriques d'aide que vous utilisez fréquemment. Les signets d'aide fournissent un accès rapide à vos sujets favoris.

Étapes

1. Accédez à la rubrique d'aide que vous souhaitez ajouter comme favori.
2. Cliquez sur **Favoris**, puis sur **Ajouter**.

Rechercher des objets de stockage

Pour accéder rapidement à un objet spécifique, vous pouvez utiliser le champ **Rechercher tous les objets de stockage** en haut de la barre de menu. Cette méthode de recherche globale sur tous les objets vous permet de localiser rapidement des objets spécifiques par type. Les résultats de la recherche sont triés par type d'objet de stockage et vous pouvez les filtrer davantage par objet à l'aide du menu déroulant.

Avant de commencer

- Vous devez disposer de l'un des rôles suivants pour effectuer cette tâche : opérateur, administrateur d'application ou administrateur de stockage.
- Une recherche valide doit contenir au moins trois caractères.

Lorsque vous utilisez la valeur du menu déroulant « Tous », la recherche globale affiche le nombre total de résultats trouvés dans toutes les catégories d'objets ; avec un maximum de 25 résultats de recherche pour chaque catégorie d'objets. Vous pouvez sélectionner un type d'objet spécifique dans le menu déroulant pour affiner la recherche au sein d'un type d'objet spécifique. Dans ce cas, la liste renvoyée n'est pas limitée aux 25 premiers objets.

Les types d'objets que vous pouvez rechercher incluent :

- Groupes
- Nœuds
- Machines virtuelles de stockage
- Agrégats
- Volumes
- Qtrees

- Actions PME
- Actions NFS
- Quotas d'utilisateurs ou de groupes
- LUN
- Espaces de noms NVMe
- Groupes initiateurs
- Initiateurs
- Groupe de cohérence

La saisie d'un nom de charge de travail renvoie la liste des charges de travail sous la catégorie Volumes ou LUN appropriée.

Vous pouvez cliquer sur n'importe quel objet dans les résultats de la recherche pour accéder à la page des détails de santé de cet objet. S'il n'existe pas de page de santé directe pour un objet, la page Santé de l'objet parent s'affiche. Par exemple, lors de la recherche d'un LUN spécifique, la page de détails SVM sur laquelle réside le LUN s'affiche.

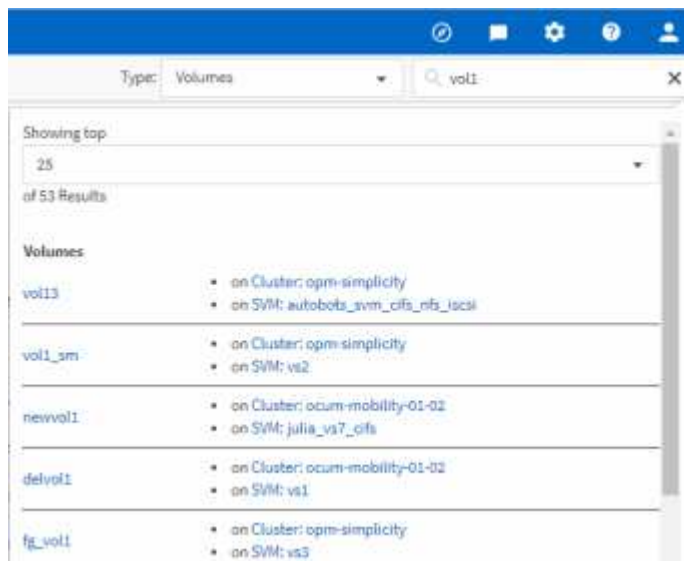


Les ports et les LIF ne sont pas consultables dans la barre de recherche globale.

Étapes

1. Sélectionnez un type d'objet dans le menu pour affiner les résultats de la recherche pour un seul type d'objet.
2. Saisissez au moins trois caractères du nom de l'objet dans le champ **Rechercher tous les objets de stockage**.

Dans cet exemple, la liste déroulante contient le type d'objet Volumes sélectionné. En tapant « vol1 » dans le champ **Rechercher tous les objets de stockage**, vous obtenez une liste de tous les volumes dont les noms contiennent ces caractères.



Exporter les données de stockage sous forme de rapports

Vous pouvez exporter des données de stockage dans divers formats de sortie, puis

utiliser les données exportées pour créer des rapports. Par exemple, s’il y a 10 événements critiques qui n’ont pas été résolus, vous pouvez exporter les données de la page d’inventaire de gestion des événements pour créer un rapport, puis envoyer le rapport aux administrateurs qui peuvent résoudre les problèmes.

Vous pouvez exporter des données vers un `.csv` déposer, `.xlsx` fichier, ou `.pdf` documentez les pages d’inventaire **Stockage** et **Réseau** et utilisez les données exportées pour créer des rapports. Il existe d’autres emplacements dans le produit où seul `.csv` ou `.pdf` des fichiers peuvent être générés.

Étapes

1. Effectuez l’une des actions suivantes :

Si vous souhaitez exporter...	Fais ceci...
Détails de l’inventaire des objets de stockage	Cliquez sur Stockage ou Réseau dans le menu de navigation de gauche, puis sélectionnez un objet de stockage. Choisissez l’une des vues fournies par le système ou toute vue personnalisée que vous avez créée.
Détails du groupe de politiques QoS	Cliquez sur Stockage > Groupes de politiques QoS dans le menu de navigation de gauche.
Détails de la capacité de stockage et de l’historique de protection	Cliquez sur Stockage > Agrégats ou Stockage > Volumes , puis sélectionnez un seul agrégat ou volume.
Détails de l’événement	Cliquez sur Gestion des événements dans le menu de navigation de gauche.
Top 10 des détails sur les performances des objets de stockage	Cliquez sur Stockage > Clusters > Performances : Tous les clusters , puis sélectionnez un cluster et choisissez l’onglet Meilleurs performers . Sélectionnez ensuite un objet de stockage et un compteur de performances.

2. Cliquez sur le bouton **Rapports** (ou sur le bouton **Exporter** dans certaines pages de l’interface utilisateur).
3. Cliquez sur **Télécharger CSV**, **Télécharger PDF** ou **Télécharger Excel** pour confirmer la demande d’exportation.

À partir de l’onglet Meilleurs interprètes, vous pouvez choisir de télécharger un rapport de statistiques pour le cluster unique que vous consultez ou pour tous les clusters du centre de données.

Le fichier est téléchargé.

4. Ouvrez le fichier dans l’application appropriée.

Informations connexes

["Page d’inventaire Santé/Groupes"](#)

Filtrer le contenu de la page d'inventaire

Vous pouvez filtrer les données de la page d'inventaire dans Unified Manager pour localiser rapidement les données en fonction de critères spécifiques. Vous pouvez utiliser le filtrage pour affiner le contenu des pages d'Unified Manager afin d'afficher uniquement les résultats qui vous intéressent. Cela fournit une méthode très efficace pour afficher uniquement les données qui vous intéressent.

Utilisez le **Filtrage** pour personnaliser la vue de la grille en fonction de vos préférences. Les options de filtre disponibles sont basées sur le type d'objet visualisé dans la grille. Si des filtres sont actuellement appliqués, le nombre de filtres appliqués s'affiche à droite du bouton Filtre.

Trois types de paramètres de filtre sont pris en charge.

Paramètre	Validation
Chaîne (texte)	Les opérateurs sont contient , commence par , se termine par et ne contient pas .
Nombre maximum	Les opérateurs sont supérieur à , inférieur à , dans le dernier et entre .
Enum (texte)	Les opérateurs sont is et is not .

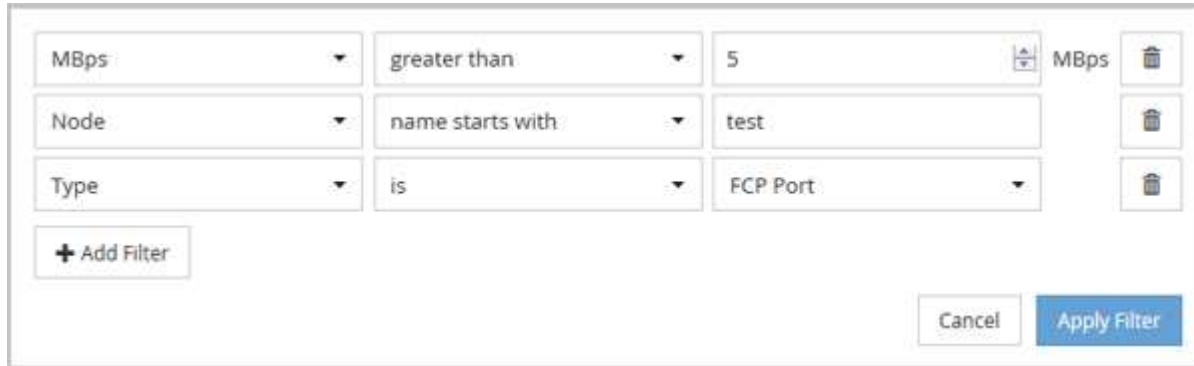
Les champs Colonne, Opérateur et Valeur sont obligatoires pour chaque filtre ; les filtres disponibles reflètent les colonnes filtrables sur la page actuelle. Le nombre maximum de filtres que vous pouvez appliquer est de quatre. Les résultats filtrés sont basés sur des paramètres de filtre combinés. Les résultats filtrés s'appliquent à toutes les pages de votre recherche filtrée, pas seulement à la page actuellement affichée.

Vous pouvez ajouter des filtres à l'aide du panneau Filtrage.

1. En haut de la page, cliquez sur le bouton **Filtre**. Le panneau Filtrage s'affiche.
2. Cliquez sur la liste déroulante de gauche et sélectionnez un objet ; par exemple, *Cluster* ou un compteur de performances.
3. Cliquez sur la liste déroulante centrale et sélectionnez l'opérateur que vous souhaitez utiliser.
4. Dans la dernière liste, sélectionnez ou saisissez une valeur pour compléter le filtre pour cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Ajouter un filtre**. Un champ de filtre supplémentaire s'affiche. Complétez ce filtre en suivant le processus décrit dans les étapes précédentes. Notez qu'après avoir ajouté votre quatrième filtre, le bouton **+Ajouter un filtre** ne s'affiche plus.
6. Cliquez sur **Appliquer le filtre**. Les options de filtre sont appliquées à la grille et le nombre de filtres est affiché à droite du bouton Filtrer.
7. Utilisez le panneau Filtrage pour supprimer des filtres individuels en cliquant sur l'icône de la corbeille à droite du filtre à supprimer.
8. Pour supprimer tous les filtres, cliquez sur **Réinitialiser** en bas du panneau de filtrage.

Exemple de filtrage

L'illustration montre le panneau de filtrage avec trois filtres. Le bouton **+Ajouter un filtre** s'affiche lorsque vous avez moins que le maximum de quatre filtres.



Après avoir cliqué sur **Appliquer le filtre**, le panneau Filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués ( 3).

Afficher les événements actifs depuis la cloche de notification

La cloche de notification () dans la barre de menus fournit un moyen rapide d'afficher les événements actifs les plus importants suivis par Unified Manager.

La liste des événements actifs permet de voir le nombre total d'événements critiques, d'erreur, d'avertissement et de mise à niveau sur tous les clusters. Cette liste comprend les événements des 7 jours précédents et n'inclut pas les événements d'information. Vous pouvez cliquer sur un lien pour afficher la liste des événements qui vous intéressent le plus.

Notez que lorsqu'un cluster n'est pas accessible, Unified Manager affiche ces informations sur cette page. Vous pouvez afficher des informations détaillées sur un cluster inaccessible en cliquant sur le bouton **Détails**. Cette action ouvre la page Détails de l'événement. Les problèmes de surveillance de l'échelle, tels que le manque d'espace ou de RAM sur la station de gestion, sont également affichés sur cette page.

Étapes

1. Dans la barre de menu, cliquez sur .
2. Pour afficher les détails de l'un des événements actifs, cliquez sur le lien texte de l'événement, tel que « 2 Capacité » ou « 4 Performances ».

Surveiller et gérer les clusters depuis le tableau de bord

Le tableau de bord fournit des informations cumulatives en un coup d'œil sur l'état actuel de vos systèmes ONTAP surveillés. Le tableau de bord fournit des « panneaux » qui vous permettent d'évaluer la capacité globale, les performances et l'état de sécurité des clusters que vous surveillez.

De plus, il existe certains problèmes ONTAP que vous pouvez résoudre directement à partir de l'interface utilisateur d'Unified Manager au lieu de devoir utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP.

En haut du tableau de bord, vous pouvez sélectionner si les panneaux affichent des informations pour tous les

clusters surveillés ou pour un cluster individuel. Vous pouvez commencer par afficher l'état de tous les clusters, puis accéder à des clusters individuels lorsque vous souhaitez afficher des informations détaillées.



Certains des panneaux répertoriés ci-dessous peuvent ne pas apparaître sur la page en fonction de votre configuration.

Panneaux	Description
Mesures de gestion	Lorsque Unified Manager peut diagnostiquer et déterminer une résolution unique pour un problème, ces résolutions sont affichées dans ce panneau avec un bouton Réparer .
Capacité	Affiche la capacité totale et utilisée pour le niveau local et le niveau cloud, ainsi que le nombre de jours jusqu'à ce que la capacité locale atteigne la limite supérieure.
Capacité de performance	Affiche la valeur de capacité de performance pour chaque cluster et le nombre de jours jusqu'à ce que la capacité de performance atteigne la limite supérieure.
Charge de travail IOPS	Affiche le nombre total de charges de travail actuellement en cours d'exécution dans une certaine plage d'IOPS.
Performances de la charge de travail	Affiche le nombre total de charges de travail conformes et non conformes attribuées à chaque niveau de service de performances défini.
Sécurité	Affiche le nombre de clusters conformes ou non conformes, le nombre de SVM conformes ou non conformes et le nombre de volumes chiffrés ou non chiffrés.
Protection	Affiche le nombre de machines virtuelles de stockage protégées par la relation SVM-DR, les volumes protégés par la relation SnapMirror, les volumes protégés par Snapshot et les clusters protégés par MetroCluster.
Aperçu de l'utilisation	Affiche les clusters triés par IOPS les plus élevés, débit le plus élevé (Mbit/s) ou capacité physique la plus utilisée.

Page du tableau de bord

La page Tableau de bord comporte des « panneaux » qui affichent la capacité de haut niveau, les performances et l'état de sécurité des clusters que vous surveillez. Cette

page fournit également un panneau Actions de gestion qui répertorie les correctifs qu'Unified Manager peut apporter pour résoudre certains événements.

La plupart des panneaux affichent également le nombre d'événements actifs dans cette catégorie et le nombre de nouveaux événements ajoutés au cours des 24 heures précédentes. Ces informations vous aident à déterminer les clusters que vous devrez peut-être analyser plus en détail pour résoudre les événements. Cliquer sur les événements affiche les principaux événements et fournit un lien vers la page d'inventaire de gestion des événements filtrée pour afficher les événements actifs dans cette catégorie.

En haut du tableau de bord, vous pouvez sélectionner si les panneaux affichent des informations pour tous les clusters surveillés (« Tous les clusters ») ou pour un cluster individuel. Vous pouvez commencer par afficher l'état de tous les clusters, puis accéder à des clusters individuels lorsque vous souhaitez afficher des informations détaillées.



Certains des panneaux répertoriés ci-dessous apparaissent sur le tableau de bord en fonction de votre configuration.

Panneau Actions de gestion

Il existe certains problèmes qu'Unified Manager peut diagnostiquer en profondeur et fournir une résolution unique. Lorsqu'elles sont disponibles, ces résolutions sont affichées dans ce panneau avec un bouton **Réparer** ou **Tout réparer**. Vous pouvez résoudre ces problèmes immédiatement à partir d'Unified Manager au lieu de devoir utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP. Pour consulter tous les numéros, cliquez sur Voir "[Résoudre les problèmes ONTAP directement depuis Unified Manager](#)" pour plus d'informations.

Panneau de capacité

Lors de l'affichage de tous les clusters, ce panneau affiche la capacité physique utilisée (après application des économies d'efficacité de stockage) et la capacité physique disponible (sans compter les économies potentielles d'efficacité de stockage) pour chaque cluster, le nombre de jours jusqu'à ce que les disques soient pleins et le taux de réduction des données (sans copies Snapshot) en fonction des paramètres d'efficacité de stockage ONTAP configurés. Il répertorie également la capacité utilisée pour tous les niveaux de cloud configurés. En cliquant sur le graphique à barres, vous accédez à la page d'inventaire des agrégats pour ce cluster. Cliquer sur le texte « Jours jusqu'à épuisement » affiche un message qui identifie l'agrégat avec le moins de jours de capacité restants ; cliquez sur le nom de l'agrégat pour voir plus de détails.

Lors de l'affichage d'un seul cluster, ce panneau affiche la capacité physique utilisée et la capacité physique disponible pour les agrégats de données triés par chaque type de disque individuel sur le niveau local et pour le niveau cloud. En cliquant sur le graphique à barres d'un type de disque, vous accédez à la page d'inventaire des volumes pour les volumes utilisant ce type de disque.

Panneau de capacité de performance

Lors de l'affichage de tous les clusters, ce panneau affiche la valeur de capacité de performance pour chaque cluster (moyenne sur l'heure précédente) et le nombre de jours jusqu'à ce que la capacité de performance atteigne la limite supérieure (en fonction du taux de croissance quotidien). En cliquant sur le graphique à barres, vous accédez à la page d'inventaire des nœuds pour ce cluster. Notez que la page d'inventaire des nœuds affiche la capacité de performance moyenne sur les 72 heures précédentes. Cliquer sur le texte « Jours avant épuisement » affiche un message qui identifie le nœud avec le moins de jours de capacité de performance restants ; cliquez sur le nom du nœud pour voir plus de détails.

Lors de l'affichage d'un seul cluster, ce panneau affiche le pourcentage de capacité de performances du cluster utilisé, le nombre total d'IOPS et les valeurs de débit total (Mo/s), ainsi que le nombre de jours jusqu'à

ce que chacune de ces trois mesures atteigne sa limite supérieure.

Panneau IOPS de charge de travail

Lorsque vous visualisez un seul cluster, ce panneau affiche le nombre total de charges de travail actuellement en cours d'exécution dans une certaine plage d'IOPS et indique le nombre pour chaque type de disque lorsque vous passez votre curseur sur le graphique.

Panneau de performances de la charge de travail

Ce panneau affiche le nombre total de charges de travail conformes et non conformes attribuées à chaque stratégie de niveau de service de performances (PSL). Il affiche également le nombre de charges de travail auxquelles aucun PSL n'est attribué. Cliquer sur un graphique à barres vous amène aux charges de travail conformes attribuées à cette politique dans la page Charges de travail. En cliquant sur le numéro qui suit le graphique à barres, vous accédez aux charges de travail conformes et non conformes attribuées à cette politique.

Panneau de sécurité

Le panneau Sécurité présente l'état de sécurité de haut niveau pour tous les clusters ou pour un seul cluster, selon votre vue actuelle. Ce panneau affiche :

- une liste des événements de sécurité reçus au cours des dernières 24 heures. Cliquez sur un événement pour afficher les détails sur la page Détails de l'événement
- l'état de sécurité du cluster (nombre de clusters conformes et non conformes)
- l'état de sécurité de la machine virtuelle de stockage (nombre de machines virtuelles de stockage conformes et non conformes)
- l'état de chiffrement du volume (nombre de volumes chiffrés ou non chiffrés)
- l'état anti-ransomware du volume (nombre de volumes avec anti-ransomware activés ou désactivés)

Vous pouvez cliquer sur les graphiques à barres des clusters conformes et non conformes, des machines virtuelles de stockage, des volumes chiffrés et non chiffrés et de l'état anti-ransomware du volume pour accéder aux pages respectives et afficher les détails de sécurité des clusters filtrés, des machines virtuelles de stockage et des volumes.

La conformité est basée sur la "[Guide de renforcement de la sécurité NetApp pour ONTAP 9](#)". Cliquez sur la flèche droite en haut du panneau pour afficher les détails de sécurité de tous les clusters sur la page Sécurité. Pour plus d'informations, voir "[Affichage de l'état de sécurité détaillé des clusters et des machines virtuelles de stockage](#)".

Panneau de protection des données

Ce panneau affiche le résumé de la protection des données pour un ou tous les clusters d'un centre de données. Il affiche le nombre total d'événements de protection des données, d'événements MetroCluster et le nombre d'événements actifs déclenchés au cours des dernières 24 heures dans ONTAP. En cliquant sur le lien de chacun de ces événements, vous accédez à la page des détails de l'événement. Vous pouvez cliquer sur le lien **Afficher tout** pour afficher tous les événements de protection actifs dans la page d'inventaire de gestion des événements. Le panneau affiche :

- Le nombre de volumes dans un cluster ou tous les clusters d'un centre de données protégés par des copies Snapshot.
- Le nombre de volumes dans un cluster ou tous les clusters d'un centre de données protégés par les

relations SnapMirror . Pour les relations SnapMirror , le nombre de volumes au niveau du cluster source est pris en compte.

- Le nombre de clusters ou tous les clusters d'un centre de données protégés par la configuration MetroCluster sur IP ou FC.
- Nombre de relations de volume avec décalage de l'objectif de point de récupération (RPO) de SnapMirror en fonction de l'état du décalage.

Vous pouvez passer votre souris pour afficher les décomptes et légendes respectifs. Vous pouvez cliquer sur la flèche droite en haut du panneau pour afficher les détails d'un seul ou de tous les clusters sur la page Protection des données. Vous pouvez également cliquer sur :

- Les graphiques à barres pour les volumes non protégés et les volumes protégés par des copies Snapshot permettent d'accéder à la page Volumes et d'afficher les détails.
- Les graphiques à barres pour les clusters protégés ou non protégés par la configuration MetroCluster permettent d'accéder à la page Clusters et d'afficher les détails.
- Les graphiques à barres de toutes les relations accèdent à la page Relations, où les détails sont filtrés en fonction du cluster source.

Pour plus d'informations, voir ["Affichage de l'état de protection du volume"](#).

Panneau d'aperçu de l'utilisation

Lors de l'affichage de tous les clusters, vous pouvez choisir d'afficher les clusters triés par IOPS les plus élevées, débit le plus élevé (Mo/s) ou capacité physique la plus utilisée.

Lorsque vous visualisez un seul cluster, vous pouvez choisir d'afficher les charges de travail triées par IOPS les plus élevées, débit le plus élevé (Mo/s) ou capacité logique la plus utilisée.

Informations connexes

["Résolution des problèmes à l'aide des corrections automatiques d'Unified Manager"](#)

["Affichage d'informations sur les événements de performance"](#)

["Gestion des performances à l'aide de la capacité de performance et des informations IOPS disponibles"](#)

["Page de détails sur le volume/la santé"](#)

["Analyse et notification des événements de performance"](#)

["Description des types de gravité des événements"](#)

["Sources d'événements de performance"](#)

["Gérer les objectifs de sécurité du cluster"](#)

["Surveiller les performances du cluster à partir de la page de destination du cluster de performances"](#)

["Surveiller les performances à l'aide des pages d'inventaire des performances"](#)

Gérez les problèmes ou les fonctionnalités ONTAP directement depuis Unified Manager

Vous pouvez résoudre certains problèmes ONTAP ou gérer certaines fonctionnalités ONTAP directement à partir de l'interface utilisateur d'Unified Manager, au lieu de devoir utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP . L'option « Actions de gestion » fournit des correctifs à un certain nombre de problèmes ONTAP qui ont déclenché des événements Unified Manager.

Vous pouvez résoudre les problèmes directement à partir de la page Actions de gestion en sélectionnant l'option **Actions de gestion** dans le volet de navigation de gauche. Les actions de gestion sont également disponibles à partir du panneau Actions de gestion du tableau de bord, de la page Détails de l'événement et de la sélection Analyse de la charge de travail dans le menu de navigation de gauche.

Il existe certains problèmes qu'Unified Manager peut diagnostiquer en profondeur et fournir une résolution unique. Pour certaines fonctionnalités ONTAP , telles que la surveillance anti-ransomware, Unified Manager effectue des contrôles internes et recommande des actions spécifiques. Lorsqu'elles sont disponibles, ces résolutions sont affichées dans les actions de gestion avec un bouton **Corriger**. Cliquez sur le bouton **Réparer** pour résoudre le problème. Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Unified Manager envoie des commandes ONTAP au cluster pour effectuer le correctif demandé. Une fois le correctif terminé, l'événement devient obsolète.

Certaines actions de gestion vous permettent de résoudre le même problème sur plusieurs objets de stockage à l'aide du bouton **Réparer tout**. Par exemple, il peut y avoir 5 volumes qui ont l'événement « Espace volume plein » qui pourrait être résolu en cliquant sur l'action de gestion **Réparer tout** pour « Activer la croissance automatique du volume ». Un clic vous permet de résoudre ce problème sur 5 volumes.

Pour plus d'informations sur les problèmes et les fonctionnalités ONTAP que vous pouvez gérer à l'aide de la correction automatique, consultez "[Quels problèmes Unified Manager peut-il résoudre ?](#)".

Quelles options ai-je lorsque je vois le bouton Réparer ou Tout réparer

La page Actions de gestion vous fournit le bouton **Réparer** ou **Réparer tout** pour résoudre les problèmes dont Unified Manager a été informé via un événement.

Nous vous recommandons de cliquer sur les boutons pour résoudre un problème, si nécessaire. Toutefois, si vous n'êtes pas sûr de vouloir résoudre le problème comme recommandé par Unified Manager, vous pouvez effectuer les actions suivantes :

Qu'est-ce que vous voulez faire?	Action
Demandez à Unified Manager de résoudre le problème sur tous les objets identifiés.	Cliquez sur le bouton Réparer tout .
Ne corrigez pas le problème pour aucun des objets identifiés pour le moment et masquez cette action de gestion jusqu'à ce que l'événement soit à nouveau déclenché.	Cliquez sur la flèche vers le bas et cliquez sur Tout rejeter .

Qu'est-ce que vous voulez faire?	Action
Corrigez le problème sur certains des objets identifiés uniquement.	Cliquez sur le nom de l'action de gestion pour développer la liste et afficher toutes les actions Corriger individuelles. Suivez ensuite les étapes pour corriger ou rejeter les actions de gestion individuelles.
Qu'est-ce que vous voulez faire?	Action
Demandez à Unified Manager de résoudre le problème.	Cliquez sur le bouton Réparer .
Ne résolvez pas le problème pour le moment et masquez cette action de gestion jusqu'à ce que l'événement soit à nouveau déclenché.	Cliquez sur la flèche vers le bas et cliquez sur Ignorer .
Affichez les détails de cet événement afin de mieux comprendre le problème.	• Cliquez sur le bouton Réparer et vérifiez le correctif qui sera appliqué dans la boîte de dialogue qui s'affiche. • Cliquez sur la flèche vers le bas et cliquez sur Afficher les détails de l'événement pour afficher la page des détails de l'événement. Cliquez ensuite sur Réparer sur l'une de ces pages résultantes si vous souhaitez résoudre le problème.
Affichez les détails de cet objet de stockage afin de mieux comprendre le problème.	Cliquez sur le nom de l'objet de stockage pour afficher les détails dans l'Explorateur de performances ou dans la page Détails d'intégrité.

Dans certains cas, le correctif est reflété dans le sondage de configuration suivant de 15 minutes. Dans d'autres cas, il peut falloir plusieurs heures pour que la modification de configuration soit vérifiée et que l'événement devienne obsolète.

Pour voir la liste des actions de gestion terminées ou en cours, cliquez sur l'icône de filtre et sélectionnez **Terminé** ou **En cours**.

Correction Toutes les opérations s'exécutent de manière séquentielle, donc lorsque vous visualisez le panneau **En cours**, certains objets auront le statut **En cours** tandis que d'autres auront le statut **Planifié** ; ce qui signifie qu'ils attendent toujours d'être implémentés.

Afficher l'état des actions de gestion que vous avez choisi de corriger

Vous pouvez afficher l'état de toutes les actions de gestion que vous avez choisi de corriger dans la page Actions de gestion. La plupart des actions sont affichées comme **Terminées** assez rapidement après qu'Unified Manager a envoyé la commande ONTAP au cluster. Cependant, certaines actions, comme le déplacement d'un volume, peuvent prendre plus de temps.

Trois filtres sont disponibles sur la page Actions de gestion :

- **Terminé** indique à la fois les actions de gestion qui ont été terminées avec succès et celles qui ont échoué. Les actions **échouées** fournissent une raison de l'échec afin que vous puissiez résoudre le problème manuellement.
- **En cours** affiche à la fois les actions de gestion en cours de mise en œuvre et celles dont la mise en œuvre est prévue.
- **Recommandé** affiche toutes les actions de gestion actuellement actives pour tous les clusters surveillés.

Étapes

1. Cliquez sur **Actions de gestion** dans le volet de navigation de gauche. Alternativement, cliquez sur  en haut du panneau **Actions de gestion** sur le **Tableau de bord** et sélectionnez la vue que vous souhaitez voir.

La page Actions de gestion s'affiche.
2. Vous pouvez cliquer sur l'icône en forme de curseur à côté de l'action de gestion dans le champ **Description** pour voir les détails sur le problème et la commande utilisée pour résoudre le problème.
3. Pour afficher les actions qui ont **échoué**, triez sur la colonne **Statut** dans la vue **Terminé**. Vous pouvez utiliser l'outil **Filtre** dans le même but.
4. Si vous souhaitez afficher plus d'informations sur une action de gestion ayant échoué ou si vous décidez de corriger une action de gestion recommandée, vous pouvez cliquer sur **Afficher les détails de l'événement** dans la zone développée après avoir cliqué sur l'icône en forme de curseur à côté de l'action de gestion. Un bouton **Réparer** est disponible sur cette page.

Quels problèmes Unified Manager peut-il résoudre ?

En utilisant la fonction de correction automatique d' Active IQ Unified Manager, vous pouvez choisir de résoudre certains problèmes ONTAP ou de gérer efficacement certaines fonctionnalités ONTAP , telles que la surveillance anti-ransomware, via Unified Manager.

Ce tableau décrit les problèmes ou fonctionnalités ONTAP que vous pouvez gérer directement via le bouton **Réparer** ou **Réparer tout** sur l'interface utilisateur Web d'Unified Manager.

Nom et description de l'événement	Mesure de gestion	Opération « Réparer »
Volume Espace Plein Le volume est presque à court d'espace et il a dépassé le seuil de capacité maximale. Ce seuil est fixé par défaut à 90 % de la taille du volume.	Activer la croissance automatique du volume	Unified Manager détermine que la croissance automatique du volume n'est pas configurée pour ce volume. Il active donc cette fonctionnalité afin que la capacité du volume augmente en cas de besoin.
Inodes complets Ce volume n'a plus d'inodes et ne peut accepter aucun nouveau fichier.	Augmenter le nombre d'inodes sur le volume	Augmente le nombre d'inodes sur le volume de 2 pour cent.

Nom et description de l'événement	Mesure de gestion	Opération « Réparer »
Incompatibilité de politique de niveau de stockage détectée Le volume contient beaucoup de données inactives et la politique de hiérarchisation actuelle est définie sur « instantané uniquement » ou « aucun ».	Activer la hiérarchisation automatique du cloud	Étant donné que le volume réside déjà sur un FabricPool, il modifie la stratégie de hiérarchisation sur « auto » afin que les données inactives soient déplacées vers le niveau cloud le moins coûteux.
Incompatibilité de niveau de stockage détectée Le volume contient beaucoup de données inactives, mais elles ne résident pas sur un niveau de stockage compatible cloud (FabricPool).	Modifier le niveau de stockage des volumes	Déplace le volume vers le niveau de stockage compatible cloud et définit la politique de hiérarchisation sur « auto » pour déplacer les données inactives vers le niveau cloud.
Journal d'audit désactivé Le journal d'audit n'est pas activé pour la machine virtuelle de stockage	Activer la journalisation d'audit pour la machine virtuelle de stockage	Active la journalisation d'audit sur la machine virtuelle de stockage. Notez que la machine virtuelle de stockage doit déjà avoir un emplacement de journal d'audit local ou distant configuré.
Bannière de connexion désactivée La bannière de connexion au cluster doit être activée pour augmenter la sécurité en clarifiant les restrictions d'accès.	Définir la bannière de connexion pour le cluster	Définit la bannière de connexion au cluster sur « Accès restreint aux utilisateurs autorisés ».
Bannière de connexion désactivée La bannière de connexion pour la machine virtuelle de stockage doit être activée pour augmenter la sécurité en clarifiant les restrictions d'accès.	Définir la bannière de connexion pour la machine virtuelle de stockage	Définit la bannière de connexion de la machine virtuelle de stockage sur « Accès restreint aux utilisateurs autorisés ».
SSH utilise des chiffrements non sécurisés Les chiffrements avec le suffixe « -cbc » sont considérés comme non sécurisés.	Supprimer les chiffrements non sécurisés du cluster	Supprime les chiffrements non sécurisés, tels que aes192-cbc et aes128-cbc, du cluster.

Nom et description de l'événement	Mesure de gestion	Opération « Réparer »
SSH utilise des chiffrements non sécurisés Les chiffrements avec le suffixe « - cbc » sont considérés comme non sécurisés.	Supprimer les chiffrements non sécurisés de la machine virtuelle de stockage	Supprime les chiffrements non sécurisés (tels que aes192-cbc et aes128-cbc) de la machine virtuelle de stockage.
Transport HTTPS AutoSupport désactivé Le protocole de transport utilisé pour envoyer des messages AutoSupport au support technique doit être crypté.	Définir HTTPS comme protocole de transport pour les messages AutoSupport	Définit HTTPS comme protocole de transport pour les messages AutoSupport sur le cluster.
Dépassement du seuil de déséquilibre de charge du cluster Indique que la charge est déséquilibrée entre les nœuds du cluster. Cet événement est généré lorsque la variation de la capacité de performance utilisée est supérieure à 30 % entre les nœuds.	Équilibrer les charges de travail du cluster	Unified Manager identifie le meilleur volume à déplacer d'un nœud à l'autre pour réduire le déséquilibre, puis déplace le volume.
Dépassement du seuil de déséquilibre des capacités du cluster Indique que la capacité est déséquilibrée parmi les agrégats du cluster. Cet événement est généré lorsque l'écart de capacité utilisée est supérieur à 70 % entre les agrégats.	Équilibrer la capacité du cluster	Unified Manager identifie le meilleur volume à déplacer d'un agrégat à un autre pour réduire le déséquilibre, puis déplace le volume.
Seuil de capacité de performance utilisé dépassé Indique que la charge sur le nœud pourrait devenir surutilisée si vous ne réduisez pas l'utilisation d'une ou plusieurs charges de travail très actives. Cet événement est généré lorsque la valeur de capacité de performance du nœud utilisée est supérieure à 100 % pendant plus de 12 heures.	Limiter la charge élevée sur le nœud	Unified Manager identifie le volume avec les IOPS les plus élevées et applique une politique QoS en utilisant les niveaux d'IOPS historiques attendus et de pointe pour réduire la charge sur le nœud.

Nom et description de l'événement	Mesure de gestion	Opération « Réparer »
Seuil d'avertissement d'événement dynamique dépassé Indique que le nœud fonctionne déjà dans un état de surcharge en raison de la charge anormalement élevée de certaines charges de travail.	Réduire la surcharge dans le nœud	Unified Manager identifie le volume avec les IOPS les plus élevées et applique une politique QoS en utilisant les niveaux d'IOPS historiques attendus et de pointe pour réduire la charge sur le nœud.
La reprise n'est pas possible Le basculement est actuellement désactivé, donc l'accès aux ressources du nœud pendant une panne ou un redémarrage serait perdu jusqu'à ce que le nœud soit à nouveau disponible.	Activer le basculement des nœuds	Unified Manager envoie la commande appropriée pour activer le basculement sur tous les nœuds du cluster.
L'option Cf.takeover.on_panic est configurée sur OFF L'option nodeshell « cf.takeover.on_panic » est définie sur off, ce qui pourrait entraîner un problème sur les systèmes configurés en HA.	Activer la prise de contrôle en cas de panique	Unified Manager envoie la commande appropriée au cluster pour modifier ce paramètre sur on .
Désactiver l'option nodeshell snapmirror.enable L'ancienne option nodeshell « snapmirror.enable » est définie sur on, ce qui pourrait entraîner un problème lors du démarrage après la mise à niveau vers ONTAP 9.3 ou supérieur.	Définissez l'option snapmirror.enable sur désactivé	Unified Manager envoie la commande appropriée au cluster pour modifier ce paramètre sur off .
Telnet activé Indique un problème de sécurité potentiel car Telnet n'est pas sécurisé et transmet les données de manière non chiffrée.	Désactiver Telnet	Unified Manager envoie la commande appropriée au cluster pour désactiver Telnet.

Nom et description de l'événement	Mesure de gestion	Opération « Réparer »
Configurer l'apprentissage anti-ransomware des machines virtuelles de stockage Vérifie périodiquement les clusters avec des licences pour la surveillance anti-ransomware. Valide si une machine virtuelle de stockage prend en charge uniquement les volumes NFS ou SMB dans un tel cluster.	Placez les machines virtuelles de stockage dans un <code>learning mode</code> de surveillance anti-ransomware	Unified Manager définit la surveillance anti-ransomware sur <code>learning</code> état des machines virtuelles de stockage via la console de gestion du cluster. La surveillance anti-ransomware sur tous les nouveaux volumes créés sur la VM de stockage est automatiquement déplacée vers un mode d'apprentissage. Grâce à cette activation, ONTAP peut apprendre le modèle d'activité sur les volumes et détecter les anomalies dues à des attaques malveillantes potentielles.
Configurer l'apprentissage anti-ransomware en volume Vérifie périodiquement les clusters avec des licences pour la surveillance anti-ransomware. Valide si un volume prend en charge uniquement les services NFS ou SMB dans un tel cluster.	Mettre les volumes dans <code>learning mode</code> de surveillance anti-ransomware	Unified Manager définit la surveillance anti-ransomware sur <code>learning</code> état des volumes via la console de gestion du cluster. Grâce à cette activation, ONTAP peut apprendre le modèle d'activité sur les volumes et détecter les anomalies dues à des attaques malveillantes potentielles.
Activer le volume anti-ransomware Vérifie périodiquement les clusters avec des licences pour la surveillance anti-ransomware. Détecte si les volumes sont dans le <code>learning mode</code> de surveillance anti-ransomware depuis plus de 45 jours, et détermine la perspective de les mettre en mode actif.	Mettre les volumes dans <code>active mode</code> de surveillance anti-ransomware	Unified Manager définit la surveillance anti-ransomware sur <code>active</code> sur les volumes via la console de gestion du cluster. Grâce à cette activation, ONTAP peut apprendre le modèle d'activité sur les volumes et détecter les anomalies dues à des attaques malveillantes potentielles, et créer des alertes pour les actions de protection des données.

Nom et description de l'événement	Mesure de gestion	Opération « Réparer »
Désactiver l'anti-ransomware du volume Vérifie périodiquement les clusters avec des licences pour la surveillance anti-ransomware. Détecte les notifications répétitives lors de la surveillance active des ransomwares sur les volumes (par exemple, plusieurs avertissements d'attaques potentielles de ransomwares sont renvoyés sur 30 jours).	Désactiver la surveillance anti-ransomware sur les volumes	Unified Manager désactive la surveillance anti-ransomware sur les volumes via la console de gestion du cluster.

Remplacer les actions de gestion via des scripts

Vous pouvez créer des scripts personnalisés et les associer à des alertes pour effectuer des actions spécifiques pour des événements spécifiques, et ne pas opter pour les actions de gestion par défaut disponibles pour eux sur la page Actions de gestion ou le tableau de bord Unified Manager.

Si vous souhaitez effectuer des actions spécifiques pour un type d'événement et choisissez de ne pas les corriger dans le cadre de la fonctionnalité d'action de gestion fournie par Unified Manager, vous pouvez configurer un script personnalisé pour l'action spécifique. Vous pouvez ensuite associer le script à une alerte pour ce type d'événement et gérer ces événements individuellement. Dans ce cas, les actions de gestion ne sont pas générées pour ce type d'événement spécifique sur la page Actions de gestion ou sur le tableau de bord Unified Manager.

Gérer les clusters

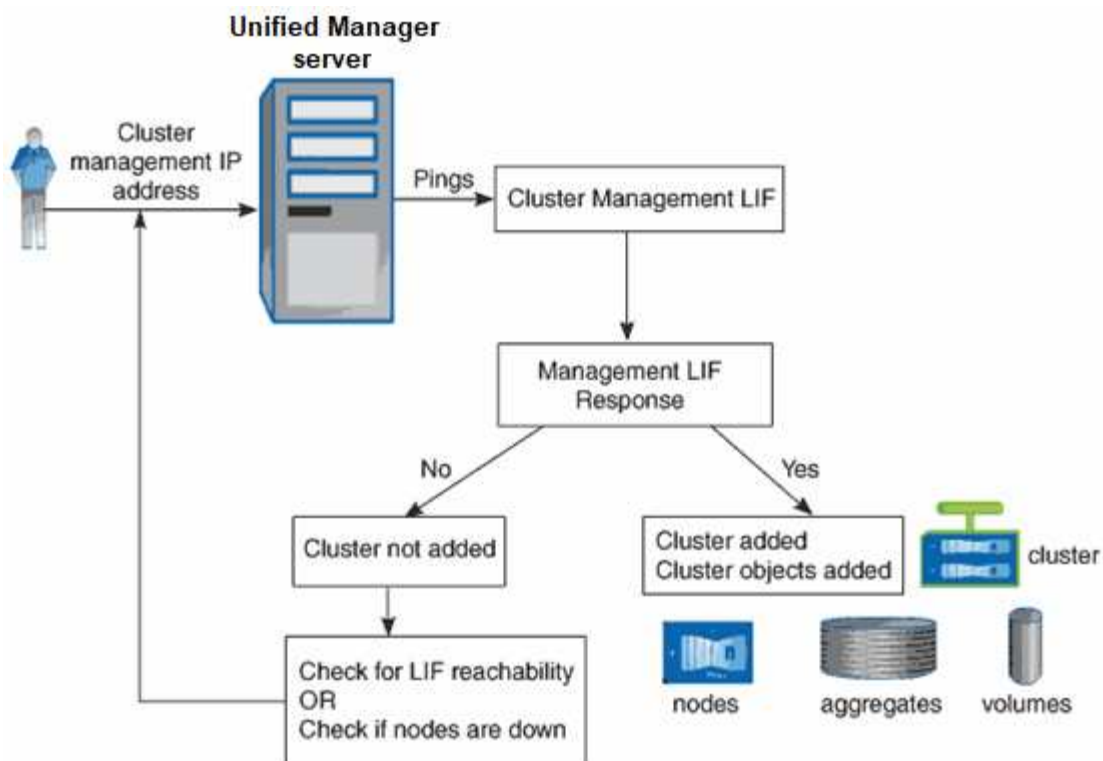
Vous pouvez gérer les clusters ONTAP en utilisant Unified Manager pour surveiller, ajouter, modifier et supprimer des clusters.

Comment fonctionne le processus de découverte de cluster

Une fois que vous avez ajouté un cluster à Unified Manager, le serveur découvre les objets du cluster et les ajoute à sa base de données. Comprendre le fonctionnement du processus de découverte vous aide à gérer les clusters de votre organisation et leurs objets.

L'intervalle de surveillance pour la collecte des informations de configuration du cluster est de 15 minutes. Par exemple, après avoir ajouté un cluster, il faut 15 minutes pour afficher les objets du cluster dans l'interface utilisateur d'Unified Manager. Ce délai est également vrai lors de la modification d'un cluster. Par exemple, si vous ajoutez deux nouveaux volumes à un SVM dans un cluster, vous voyez ces nouveaux objets dans l'interface utilisateur après le prochain intervalle d'interrogation, qui peut durer jusqu'à 15 minutes.

L'image suivante illustre le processus de découverte :



Une fois tous les objets d'un nouveau cluster découverts, Unified Manager commence à collecter les données de performances historiques des 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité vous fournit plus de deux semaines d'informations sur les performances d'un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données de performances du cluster en temps réel sont collectées, par défaut, toutes les cinq minutes.



Étant donné que la collecte de 15 jours de données de performances nécessite beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur trop de clusters en même temps.

Afficher la liste des clusters surveillés

Vous pouvez utiliser la page Configuration du cluster pour afficher votre inventaire de clusters. Vous pouvez afficher les détails des clusters, tels que leur nom ou leur adresse IP et leur état de communication.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.

Tous les clusters de votre environnement de stockage gérés par Unified Manager sont affichés. La liste des clusters est triée par la colonne de niveau de gravité de l'état de la collection. Vous pouvez cliquer sur un en-tête de colonne pour trier les clusters par différentes colonnes.

Ajouter des clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir surveiller le cluster. Cela inclut la possibilité d'obtenir des informations sur le cluster telles que l'état, la capacité, les performances et la configuration du cluster afin que vous puissiez trouver et résoudre tous les problèmes qui pourraient survenir.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou du rôle d'administrateur de stockage.
- Vous devez avoir les informations suivantes :
 - Unified Manager prend en charge les clusters ONTAP sur site, ONTAP Select et Cloud Volumes ONTAP.
 - Vous devez disposer du nom d'hôte ou de l'adresse IP de gestion du cluster (IPv4 ou IPv6) pour le cluster.

Lors de l'utilisation du nom d'hôte, il doit être résolu en adresse IP de gestion de cluster pour le LIF de gestion de cluster. Si vous utilisez un LIF de gestion de nœud, l'opération échoue.

- Vous devez disposer du nom d'utilisateur et du mot de passe pour accéder au cluster.

Ce compte doit avoir le rôle *admin* avec l'accès à l'application défini sur *ontapi*, *console* et *http*.

- Vous devez connaître le numéro de port pour vous connecter au cluster à l'aide du protocole HTTPS (généralement le port 443).
- Le cluster doit exécuter le logiciel ONTAP version 9.9 ou supérieure.
- Vous devez disposer d'un espace suffisant sur le serveur Unified Manager. Vous ne pouvez pas ajouter un cluster au serveur lorsque plus de 90 % de l'espace est déjà consommé.
- Vous possédez les certificats requis :

Certificat SSL (HTTPS) : Ce certificat appartient à Unified Manager. Un certificat SSL auto-signé (HTTPS) par défaut est généré avec une nouvelle installation d'Unified Manager. NetApp vous recommande de le mettre à niveau vers un certificat signé par une autorité de certification pour une meilleure sécurité. Si le certificat du serveur expire, vous devez le régénérer et redémarrer Unified Manager pour que les services intègrent le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, voir ["Générer un certificat de sécurité HTTPS"](#).

Certificat EMS : Ce certificat appartient à Unified Manager. Il est utilisé lors de l'authentification pour les notifications EMS reçues d'ONTAP.

Certificats pour la communication TLS mutuelle : Utilisés lors de la communication TLS mutuelle entre Unified Manager et ONTAP. L'authentification basée sur les certificats est activée pour un cluster, en fonction de la version ONTAP. Si le cluster exécutant la version ONTAP est inférieur à 9.5, l'authentification basée sur les certificats n'est pas activée.

L'authentification basée sur les certificats n'est pas activée automatiquement pour un cluster si vous mettez à jour une ancienne version d'Unified Manager. Cependant, vous pouvez l'activer en modifiant et en enregistrant les détails du cluster. Si le certificat expire, vous devez le régénérer pour incorporer le nouveau certificat. Pour plus d'informations sur l'affichage et la régénération du certificat, voir ["Modification des clusters"](#).



- Vous pouvez ajouter un cluster à partir de l'interface utilisateur Web et l'authentification basée sur les certificats est automatiquement activée.
- Vous pouvez ajouter un cluster via Unified Manager CLI, l'authentification basée sur un certificat n'est pas activée par défaut. Si vous ajoutez un cluster à l'aide de l'interface de ligne de commande d'Unified Manager, il est nécessaire de modifier le cluster à l'aide de l'interface utilisateur d'Unified Manager. Tu peux voir "[Commandes CLI Unified Manager prises en charge](#)" pour ajouter un cluster à l'aide de Unified Manager CLI.
- Si l'authentification basée sur les certificats est activée pour un cluster et que vous effectuez la sauvegarde d'Unified Manager à partir d'un serveur et la restaurez sur un autre serveur Unified Manager où le nom d'hôte ou l'adresse IP est modifié, la surveillance du cluster peut échouer. Pour éviter l'échec, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, voir "[Modification des clusters](#)".
- Au niveau du cluster, l'interface Active IQ ajoute deux nouvelles entrées de groupe d'utilisateurs pour la méthode d'authentification « cert ».

+

Certificats de cluster : Ce certificat appartient à ONTAP. Vous ne pouvez pas ajouter un cluster à Unified Manager avec un certificat expiré et si le certificat a déjà expiré, vous devez le régénérer avant d'ajouter le cluster. Pour plus d'informations sur la génération de certificats, consultez l'article de la base de connaissances (KB) "[Comment renouveler un certificat auto-signé ONTAP dans l'interface utilisateur de System Manager](#)".

- Une seule instance de Unified Manager peut prendre en charge un nombre spécifique de nœuds. Si vous devez surveiller un environnement qui dépasse le nombre de nœuds pris en charge, vous devez installer une instance supplémentaire de Unified Manager pour surveiller certains des clusters. Pour afficher la liste du nombre de nœuds pris en charge, consultez le "[Guide des meilleures pratiques d'Unified Manager](#)".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs selon vos besoins, puis cliquez sur **Soumettre**.
4. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le cluster.
5. Cliquez sur **Oui**.

Après avoir enregistré les détails du cluster, vous pouvez voir le certificat pour la communication TLS mutuelle pour un cluster.

Si l'authentification basée sur un certificat n'est pas activée, Unified Manager vérifie le certificat uniquement lorsque le cluster est ajouté initialement. Unified Manager ne vérifie pas le certificat pour chaque appel d'API à ONTAP.

Une fois tous les objets d'un nouveau cluster découverts, Unified Manager commence à collecter les données de performances historiques des 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité vous fournit plus de deux semaines d'informations sur les performances d'un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données de performances du cluster en temps réel sont collectées, par défaut, toutes les cinq minutes.



- La collecte de 15 jours de données de performances est gourmande en ressources CPU. NetApp vous recommande d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur trop de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte est interrompue et vous verrez des écarts dans les graphiques de performances pour la période manquante.
- Lorsque vous ajoutez un cluster ONTAP avec la version 9.14.1 ou ultérieure, la communication s'effectue via la fonctionnalité d'agent cloud. ONTAP crée automatiquement un utilisateur de compte de service interne avec des privilèges en lecture seule (par exemple, clus-agent-xxxx). Unified Manager arrête de collecter les données de ces clusters si le `clus-agent` l'utilisateur est supprimé.

Si vous recevez un message d'erreur indiquant que vous ne pouvez pas ajouter le cluster, vérifiez si les problèmes suivants existent :



- Si les horloges des deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS d'Unified Manager est postérieure à la date du cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide de NTP ou d'un service similaire.
- Si le cluster a atteint le nombre maximal de destinations de notification EMS, l'adresse Unified Manager ne peut pas être ajoutée. Par défaut, seules 20 destinations de notification EMS peuvent être définies sur le cluster.

Informations connexes

["Ajout d'utilisateurs"](#)

["Affichage de la liste et des détails des clusters"](#)

["Installation d'un certificat HTTPS signé et renvoyé par une autorité de certification"](#)

Modifier les clusters

Vous pouvez modifier les paramètres d'un cluster existant, tels que le nom d'hôte ou l'adresse IP, le nom d'utilisateur, le mot de passe et le port, à l'aide de la boîte de dialogue Modifier le cluster.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou du rôle d'administrateur de stockage.



À partir d'Unified Manager 9.7, les clusters peuvent être ajoutés uniquement via HTTPS.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page **Configuration du cluster**, sélectionnez le cluster que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le cluster**, modifiez les valeurs selon vos besoins. + Si vous avez modifié les détails d'un cluster ajouté à Unified Manager, vous pouvez afficher les détails du certificat pour la communication TLS mutuelle, en fonction de la version ONTAP . Pour plus d'informations sur la version ONTAP , voir "[Certificats pour la communication TLS mutuelle](#)" . + Vous pouvez afficher les détails du certificat en cliquant sur **Détails du certificat**. Si le certificat a expiré, cliquez sur le bouton **Régénérer**

pour incorporer le nouveau certificat.

4. Cliquez sur **Soumettre**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le cluster.
6. Cliquez sur **Oui**.

Informations connexes

["Ajout d'utilisateurs"](#)

["Affichage de la liste et des détails des clusters"](#)

Supprimer les clusters

Vous pouvez supprimer un cluster d'Unified Manager à l'aide de la page Configuration du cluster. Par exemple, vous pouvez supprimer un cluster si la découverte du cluster échoue ou lorsque vous souhaitez mettre hors service un système de stockage.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou du rôle d'administrateur de stockage.

Cette tâche supprime le cluster sélectionné de Unified Manager. Une fois qu'un cluster est supprimé, il n'est plus surveillé. L'instance d'Unified Manager enregistrée auprès du cluster supprimé est également désenregistrée du cluster.

La suppression d'un cluster supprime également tous ses objets de stockage, ses données historiques, ses services de stockage et tous les événements associés d'Unified Manager. Ces modifications sont reflétées sur les pages d'inventaire et les pages de détails après le prochain cycle de collecte de données.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page Configuration du cluster, sélectionnez le cluster que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Supprimer la source de données**, cliquez sur **Supprimer** pour confirmer la demande de suppression.

Informations connexes

["Ajout d'utilisateurs"](#)

["Affichage de la liste et des détails des clusters"](#)

Redécouvrir les clusters

Vous pouvez redécouvrir manuellement un cluster à partir de la page Configuration du cluster afin d'obtenir les dernières informations sur l'état de santé, l'état de surveillance et l'état des performances du cluster.

Vous pouvez redécouvrir manuellement un cluster lorsque vous souhaitez le mettre à jour (par exemple en augmentant la taille d'un agrégat lorsque l'espace est insuffisant) et que vous souhaitez qu'Unified Manager détecte les modifications que vous apportez.

Lorsque Unified Manager est associé à OnCommand Workflow Automation (WFA), l'association déclenche la réacquisition des données mises en cache par WFA.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page **Configuration du cluster**, cliquez sur **Redécouvrir**.

Unified Manager redécouvre le cluster sélectionné et affiche le dernier état de santé et de performances.

Informations connexes

["Affichage de la liste et des détails des clusters"](#)

Surveiller l'infrastructure virtuelle VMware

Active IQ Unified Manager offre une visibilité sur les machines virtuelles (VM) de votre infrastructure virtuelle et permet de surveiller et de résoudre les problèmes de stockage et de performances dans votre environnement virtuel. Vous pouvez utiliser cette fonctionnalité pour déterminer les problèmes de latence dans votre environnement de stockage ou lorsqu'un événement de performances est signalé sur votre vCenter Server.

Un déploiement d'infrastructure virtuelle typique sur ONTAP comporte divers composants répartis sur les couches de calcul, de réseau et de stockage. Tout retard de performance dans une application VM peut se produire en raison d'une combinaison de latences rencontrées par les différents composants au niveau des couches respectives. Cette fonctionnalité est utile pour les administrateurs de stockage et de vCenter Server et les généralistes informatiques qui ont besoin d'analyser un problème de performances dans un environnement virtuel et de comprendre dans quel composant le problème s'est produit.

Vous pouvez désormais accéder au serveur vCenter à partir du menu vCenter de la section VMware. La vue d'ensemble de chaque machine virtuelle répertoriée comporte le lien **VCENTER SERVER** dans la VUE TOPOLOGIE qui lance vCenter Server dans un nouveau navigateur. Vous pouvez également utiliser le bouton **Développer la topologie** pour lancer vCenter Server et cliquer sur le bouton **Afficher dans vCenter** pour afficher les banques de données dans vCenter Server.

Unified Manager présente le sous-système sous-jacent d'un environnement virtuel dans une vue topologique pour déterminer si un problème de latence s'est produit dans le nœud de calcul, le réseau ou le stockage. La vue met également en évidence l'objet spécifique qui provoque le retard de performance pour prendre des mesures correctives et résoudre le problème sous-jacent.

Une infrastructure virtuelle déployée sur le stockage ONTAP comprend les objets suivants :

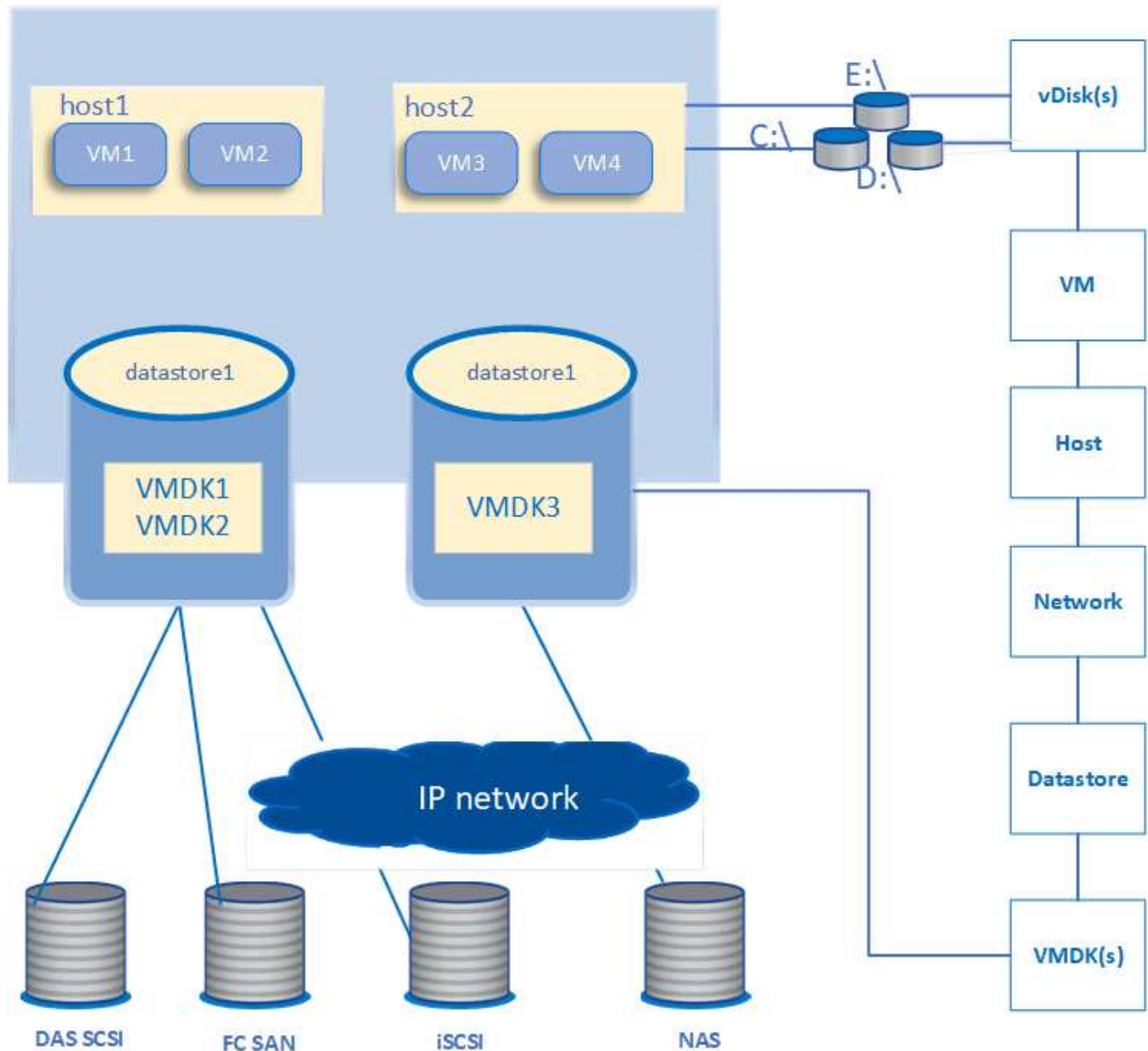
- vCenter Server : un plan de contrôle centralisé pour la gestion des machines virtuelles VMware, des hôtes ESXi et de tous les composants associés dans un environnement virtuel. Pour plus d'informations sur vCenter Server, consultez la documentation VMware.
- Hôte : un système physique ou virtuel qui exécute ESXi, le logiciel de virtualisation de VMware, et héberge la machine virtuelle.
- Banque de données : les banques de données sont des objets de stockage virtuels connectés aux hôtes ESXi. Les magasins de données sont des entités de stockage gérables d'ONTAP, telles que des LUN ou des volumes, utilisées comme référentiel pour les fichiers de machine virtuelle, tels que les fichiers journaux, les scripts, les fichiers de configuration et les disques virtuels. Ils sont connectés aux hôtes de l'environnement via une connexion réseau SAN ou IP. Les banques de données en dehors d'ONTAP qui

sont mappées à vCenter Server ne sont pas prises en charge ou affichées sur Unified Manager.

- VM : une machine virtuelle VMware.
- Disques virtuels : les disques virtuels sur les banques de données appartenant aux machines virtuelles qui ont une extension comme VMDK. Les données d'un disque virtuel sont stockées sur le VMDK correspondant.
- VMDK : un disque de machine virtuelle sur le magasin de données qui fournit un espace de stockage pour les disques virtuels. Pour chaque disque virtuel, il existe un VMDK correspondant.

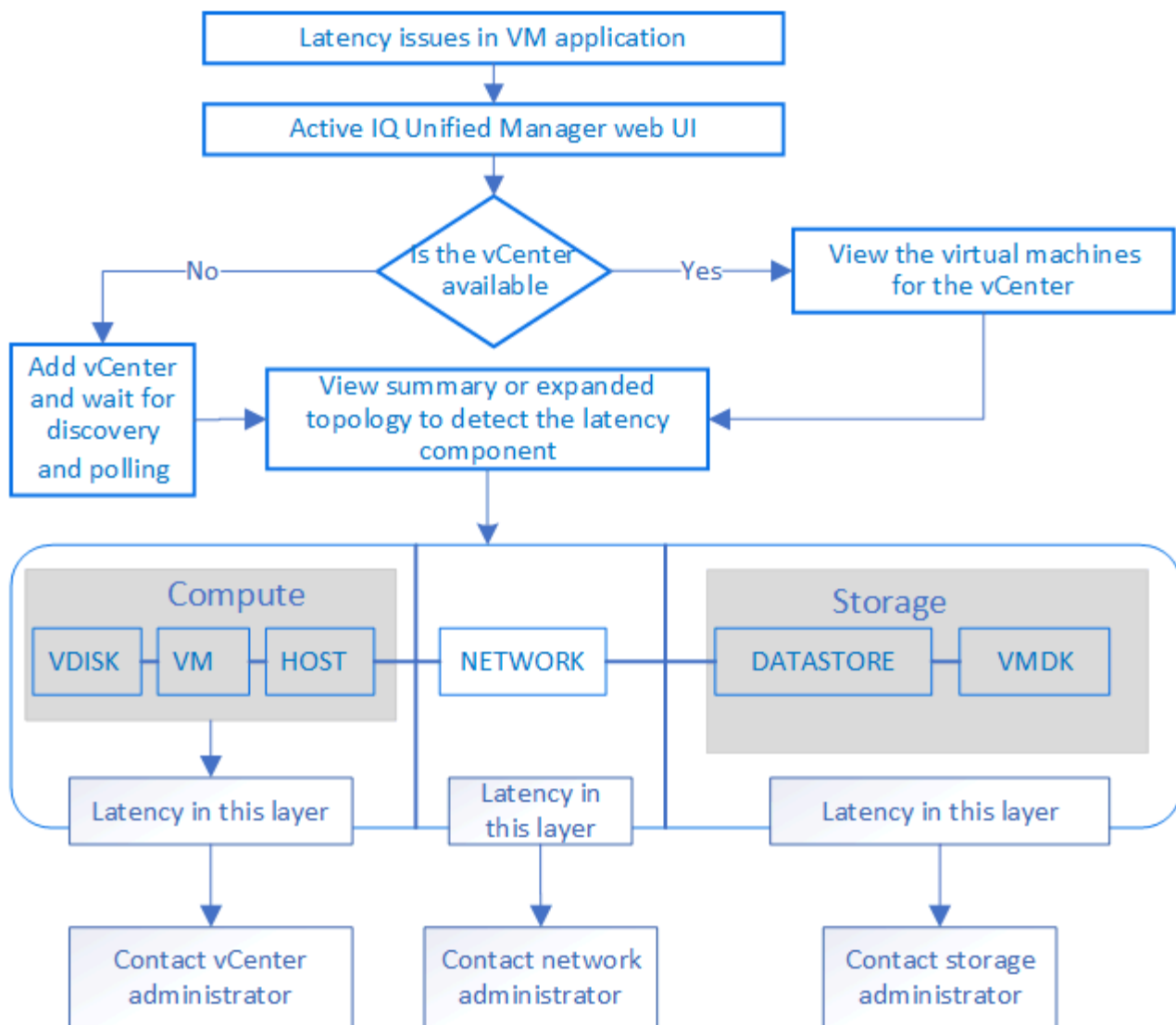
Ces objets sont représentés dans une vue de topologie VM.

Virtualisation VMware sur ONTAP



Flux de travail utilisateur

Le diagramme suivant présente un cas d'utilisation typique de la vue topologique de la machine virtuelle :



Ce qui n'est pas pris en charge

- Les banques de données situées en dehors d' ONTAP et mappées aux instances de vCenter Server ne sont pas prises en charge sur Unified Manager. Les machines virtuelles dotées de disques virtuels sur ces banques de données ne sont pas non plus prises en charge.
- Une banque de données qui s'étend sur plusieurs LUN n'est pas prise en charge.
- Les banques de données utilisant la traduction d'adresses réseau (NAT) pour le mappage des données LIF (point de terminaison d'accès) ne sont pas prises en charge.
- L'exportation de volumes ou de LUN en tant que banques de données sur différents clusters avec les mêmes adresses IP dans une configuration à plusieurs LIF n'est pas prise en charge car Unified Manager n'est pas en mesure d'identifier quelle banque de données appartient à quel cluster.

Exemple : supposons que le cluster A possède un magasin de données A. Le magasin de données A est exporté via le LIF de données avec la même adresse IP xxxx et la VM A est créée sur ce magasin de données. De même, le cluster B possède le datastore B. Le datastore B est exporté via les données LIF avec la même adresse IP xxxx et la VM B est créée sur le datastore B. UM ne pourra ni mapper le datastore A pour la topologie de la VM A au volume/LUN ONTAP correspondant, ni mapper la VM B.

- Seuls les volumes NAS et SAN (iSCSI et FCP pour VMFS) sont pris en charge en tant que banques de données ; les volumes virtuels (vVols) ne sont pas pris en charge.

- Seuls les disques virtuels iSCSI sont pris en charge. Les disques virtuels de types NVMe et SATA ne sont pas pris en charge.
- Les vues ne permettent pas de générer des rapports permettant d'analyser les performances des différents composants.
- Pour la configuration de reprise après sinistre (DR) de la machine virtuelle de stockage (VM de stockage) prise en charge uniquement pour l'infrastructure virtuelle sur Unified Manager, la configuration doit être modifiée manuellement dans vCenter Server pour pointer vers les LUN actifs dans les scénarios de basculement et de retour arrière. Sans intervention manuelle, leurs banques de données deviennent inaccessibles.

Afficher et ajouter vCenter Server

Pour afficher et dépanner les performances des machines virtuelles (VM), les serveurs vCenter associés doivent être ajoutés sur votre instance Active IQ Unified Manager .

Avant de commencer

Avant d'ajouter ou d'afficher des serveurs vCenter, assurez-vous des points suivants :

- Vous connaissez les noms des serveurs vCenter.
- Vous connaissez l'adresse IP de vCenter Server et disposez des informations d'identification requises. Les informations d'identification doivent être celles d'un administrateur vCenter Server ou d'un utilisateur root avec un accès en lecture seule à vCenter Server.
- Le serveur vCenter que vous souhaitez ajouter exécute vSphere 6.5 ou une version ultérieure.



La prise en charge d'Unified Manager pour VMware ESXi et vCenter Server est disponible en anglais et en japonais.

- Le paramètre de collecte de données dans vCenter Server est défini sur le niveau statistique de *Level 3* , garantissant le niveau requis de collecte de métriques pour tous les objets surveillés. La durée de l'intervalle doit être *5 minutes* , et la période de sauvegarde doit être *1 day* .

Pour plus d'informations, consultez la section « Niveaux de collecte de données » du *Guide de surveillance et de performances vSphere* dans la documentation VMware.

- Les valeurs de latence dans vCenter Server sont configurées en millisecondes, et non en microsecondes, pour des calculs réussis des valeurs de latence.
- Lors de l'ajout de la banque de données à vCenter Server, vous pouvez utiliser à la fois l'adresse IP de l'hôte ou le nom de domaine complet (FQDN). Si vous ajoutez un nom de domaine complet, assurez-vous que le nom de domaine peut être résolu par le serveur Unified Manager. Par exemple, pour une installation Linux, assurez-vous que le nom de domaine est ajouté dans le `/etc/resolv.conf` déposer.
- L'heure actuelle de vCenter Server est synchronisée avec le fuseau horaire de vCenter Server.
- vCenter Server est accessible pour une découverte réussie.
- Vous disposez d'un accès en lecture au SDK VMware lors de l'ajout de vCenter Server à Unified Manager. Ceci est nécessaire pour l'interrogation de configuration.

Pour chaque vCenter Server ajouté et découvert, Unified Manager collecte les données de configuration, telles que les détails du vCenter Server et du serveur ESXi, le mappage ONTAP , les détails de la banque de données et le nombre de machines virtuelles hébergées. Il collecte également les mesures de performance des composants.

Étapes

1. Accédez à **VMWARE > vCenter** et vérifiez si votre serveur vCenter est disponible dans la liste.



Si votre vCenter Server n'est pas disponible, vous devez ajouter vCenter Server.

- a. Cliquez sur **Ajouter**.
- b. Ajoutez l'adresse IP correcte pour vCenter Server et assurez-vous que le périphérique est accessible.
- c. Ajoutez le nom d'utilisateur et le mot de passe de l'administrateur ou de l'utilisateur root avec accès en lecture seule à vCenter Server.
- d. Ajoutez le numéro de port personnalisé si vous utilisez un port autre que le port par défaut 443.
- e. Cliquez sur **Enregistrer**.

Une fois la découverte réussie, un certificat de serveur s'affiche pour que vous puissiez l'accepter.

Lorsque vous acceptez le certificat, vCenter Server est ajouté à la liste des vCenter Server disponibles. L'ajout du périphérique n'entraîne pas de collecte de données pour les machines virtuelles associées, et la collecte se produit aux intervalles planifiés.

2. Si votre vCenter Server est disponible sur la page **vCenters**, vérifiez son état en passant votre souris sur le champ **État** pour afficher si votre vCenter Server fonctionne comme prévu ou s'il y a un avertissement ou une erreur.



L'ajout de vCenter Server vous permet d'afficher les statuts suivants. Cependant, les données de performances et de latence des machines virtuelles correspondantes peuvent prendre jusqu'à une heure après l'ajout de vCenter Server pour être reflétées avec précision.

- Vert : « Normal », indiquant que vCenter Server a été découvert et que les mesures de performances ont été collectées avec succès
 - Jaune : « Avertissement » (par exemple, lorsque le niveau de statistiques pour vCenter Server n'a pas été défini sur 3 ou plus pour obtenir des statistiques pour chaque objet)
 - Orange : « Erreur » (indique toute erreur interne, telle qu'une exception, un échec dans la collecte des données de configuration ou l'inaccessibilité de vCenter Server). Vous pouvez cliquer sur l'icône d'affichage de colonne (**Afficher/Masquer**) pour afficher le message d'état d'un état de vCenter Server et résoudre le problème.
3. Si vCenter Server est inaccessible ou si les informations d'identification ont changé, modifiez les détails de vCenter Server en sélectionnant **vCenter > Modifier**.
 4. Apportez les modifications nécessaires sur la page **Modifier VMware vCenter Server**.
 5. Cliquez sur **Enregistrer**.

Début de la collecte des données de vCenter Server

vCenter Server collecte des échantillons de données de performances en temps réel de 20 secondes et les regroupe en échantillons de 5 minutes. La planification de la collecte des données de performances d'Unified Manager est basée sur les paramètres par défaut de vCenter Server. Unified Manager traite les échantillons de 5 minutes obtenus à partir de vCenter Server et calcule une moyenne horaire des IOPS et de la latence pour les disques virtuels, les machines virtuelles et les hôtes. Pour les magasins de données, Unified Manager calcule une moyenne horaire des IOPS et de la latence à partir d'échantillons obtenus à partir d'ONTAP. Ces valeurs sont disponibles en haut de l'heure. Les mesures de performances ne sont pas disponibles

immédiatement après l'ajout de vCenter Server et ne sont disponibles qu'au début de l'heure suivante. L'interrogation des données de performances commence à la fin d'un cycle de collecte de données de configuration.

Pour interroger les données de configuration de vCenter Server, Unified Manager suit le même calendrier que pour la collecte des données de configuration du cluster. Pour plus d'informations sur la configuration de vCenter Server et la planification de la collecte des données de performances, consultez « Activité de configuration du cluster et de collecte des données de performances ».

Informations connexes

["Activité de collecte de données sur la configuration et les performances des clusters"](#)

Supprimer vCenter Server

Vous pouvez supprimer les serveurs vCenter de votre instance Active IQ Unified Manager . Par exemple, vous pouvez supprimer un serveur vCenter Server si la découverte de ce dernier échoue ou lorsqu'il n'est plus nécessaire.

La suppression d'un vCenter Server supprime également toutes les machines virtuelles (VM) hébergées sur ce vCenter et ses données de configuration. Une fois le serveur vCenter supprimé, il ne sera plus surveillé, ainsi que ses objets associés et ses données historiques. Ces modifications seront reflétées sur les pages d'inventaire de vCenter et des machines virtuelles.

Avant de commencer

Avant de supprimer les serveurs vCenter, assurez-vous des points suivants :

- Vous disposez du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez connaître les noms des serveurs vCenter et les adresses IP respectives qui leur sont associées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **VMWARE>vCenter**.
2. Sur la page vCenters, sélectionnez le serveur vCenter que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Supprimer vCenter**, cliquez sur **OK** pour confirmer la demande de suppression.

Surveiller les machines virtuelles

Pour tout problème de latence sur les applications de machine virtuelle (VM), vous devrez peut-être surveiller les VM pour analyser et résoudre la cause. Les machines virtuelles sont disponibles lorsque leur vCenter Server et les clusters ONTAP hébergeant le stockage de la machine virtuelle sont ajoutés à Unified Manager.

Vous voyez les détails des machines virtuelles sur la page **VMWARE > > Machines virtuelles**. Des informations telles que la disponibilité, l'état, la capacité utilisée et allouée, la latence du réseau, ainsi que les IOPS et la latence de la machine virtuelle, de la banque de données et de l'hôte sont affichées. Pour une machine virtuelle prenant en charge plusieurs banques de données, la grille affiche les métriques de la banque de données présentant la pire latence, avec une icône astérisque (*) indiquant des banques de données supplémentaires. Si vous cliquez sur l'icône, les métriques du magasin de données supplémentaire s'affichent. Certaines de ces colonnes ne sont pas disponibles pour le tri et le filtrage.



Pour afficher une machine virtuelle et ses détails, la découverte (interrogation ou collecte de métriques) du cluster ONTAP doit être terminée. Si le cluster est supprimé d'Unified Manager, la machine virtuelle n'est plus disponible après le prochain cycle de découverte.

À partir de cette page, vous pouvez également afficher la topologie détaillée d'une machine virtuelle, en affichant les composants auxquels la machine virtuelle est liée, par exemple, l'hôte, le disque virtuel et la banque de données qui y sont connectés. La vue topologique affiche les composants sous-jacents dans leurs couches spécifiques, dans l'ordre suivant : **Disque virtuel > VM > Hôte > Réseau > Magasin de données > VMDK**.

Vous pouvez déterminer le chemin d'E/S et les latences au niveau des composants à partir d'un aspect topologique et identifier si le stockage est la cause du problème de performances. La vue récapitulative de la topologie affiche le chemin d'E/S et met en évidence le composant qui présente des problèmes d'IOPS et de latence pour que vous puissiez décider des étapes de dépannage. Vous pouvez également avoir une vue étendue de la topologie qui décrit chaque composant séparément ainsi que la latence de ce composant. Vous pouvez sélectionner un composant pour déterminer le chemin d'E/S mis en évidence à travers les calques.

Afficher la topologie récapitulative

Pour déterminer les problèmes de performances en affichant les machines virtuelles dans une topologie récapitulative :

1. Accédez à **VMWARE > Machines virtuelles**.
2. Recherchez votre VM en tapant son nom dans la zone de recherche. Vous pouvez également filtrer vos résultats de recherche en fonction de critères spécifiques en cliquant sur le bouton **Filtre**. Cependant, si vous ne trouvez pas votre machine virtuelle, assurez-vous que le serveur vCenter correspondant a été ajouté et découvert.



Les serveurs vCenter autorisent les caractères spéciaux (tels que %, &, *, \$, #, @, !, \, /, :, *, ?, ", <, >, |, ;, ') dans les noms des entités vSphere, telles que VM, cluster, banque de données, dossier ou fichier. Les serveurs VMware vCenter et ESX/ESXi n'échappent pas aux caractères spéciaux utilisés dans les noms d'affichage. Cependant, lorsque le nom est traité dans Unified Manager, il s'affiche différemment. Par exemple, une machine virtuelle nommée %\$VC_AIQUM_clone_191124% dans vCenter Server s'affiche comme %25\$VC_AIQUM_clone_191124%25 dans Unified Manager. Vous devez garder une note sur ce problème lorsque vous interrogez une machine virtuelle dont le nom contient des caractères spéciaux.

3. Vérifiez l'état de la VM. Les statuts des machines virtuelles sont récupérés à partir de vCenter Server. Les statuts suivants sont disponibles. Pour plus d'informations sur ces statuts, consultez la documentation VMware.
 - Normal
 - Avertissement
 - Alerte
 - Non surveillé
 - Inconnu
4. Cliquez sur la flèche vers le bas à côté de la machine virtuelle pour afficher la vue récapitulative de la topologie des composants sur les couches de calcul, de réseau et de stockage. Le nœud qui présente des problèmes de latence est mis en évidence. La vue récapitulative affiche la pire latence des composants. Par exemple, si une machine virtuelle possède plusieurs disques virtuels, cette vue affiche le disque virtuel

qui présente la pire latence parmi tous les disques virtuels.

5. Pour analyser la latence et le débit du magasin de données sur une période donnée, cliquez sur le bouton **Workload Analyzer** en haut de l'icône de l'objet du magasin de données. Vous accédez à la page Analyse de la charge de travail, où vous pouvez sélectionner une plage horaire et afficher les graphiques de performances du magasin de données. Pour plus d'informations sur l'analyseur de charge de travail, consultez *Dépannage des charges de travail à l'aide de l'analyseur de charge de travail*.

Afficher la topologie développée

Vous pouvez accéder à chaque composant séparément en affichant la topologie développée de la machine virtuelle.

Étapes

1. Dans la vue de topologie récapitulative, cliquez sur **Développer la topologie**. Vous pouvez voir la topologie détaillée de chaque composant séparément avec les numéros de latence pour chaque objet. S'il existe plusieurs nœuds dans une catégorie, par exemple plusieurs nœuds dans la banque de données ou VMDK, le nœud avec la latence la plus élevée est surligné en rouge.
2. Pour vérifier le chemin d'E/S d'un objet spécifique, cliquez sur cet objet pour voir le chemin d'E/S et le mappage correspondant. Par exemple, pour voir le mappage d'un disque virtuel, cliquez sur le disque virtuel pour afficher son mappage en surbrillance sur le VMDK correspondant. En cas de retard de performances de ces composants, vous pouvez collecter davantage de données auprès d'ONTAP et résoudre le problème.



Les métriques ne sont pas signalées pour les VMDK. Dans la topologie, seuls les noms VMDK sont affichés, et non les métriques.

Informations connexes

["Dépannage des charges de travail à l'aide de l'analyseur de charge de travail"](#)

Afficher l'infrastructure virtuelle dans une configuration de reprise après sinistre

Vous pouvez afficher les mesures de configuration et de performances des banques de données hébergées dans une configuration MetroCluster ou une configuration de reprise après sinistre (SVM DR) d'une machine virtuelle de stockage (VM de stockage).

Sur Unified Manager, vous pouvez afficher les volumes NAS ou LUN dans une configuration MetroCluster qui sont attachés en tant que banques de données dans vCenter Server. Les banques de données hébergées dans une configuration MetroCluster sont représentées dans la même vue topologique qu'une banque de données dans un environnement standard.

Vous pouvez également afficher les volumes NAS ou les LUN dans une configuration de récupération après sinistre de machine virtuelle de stockage qui sont mappés aux banques de données dans vCenter Server.

Afficher les banques de données dans la configuration MetroCluster

Notez les conditions préalables suivantes avant d'afficher les banques de données dans une configuration MetroCluster :

- En cas de basculement et de retour en arrière, la découverte des clusters primaire et secondaire de la paire HA et des serveurs vCenter doit être terminée.

- Les clusters principaux et secondaires de la paire HA et les serveurs vCenter doivent être gérés par Unified Manager.
- La configuration requise doit être effectuée sur ONTAP et vCenter Server. Pour plus d'informations, consultez la documentation ONTAP et vCenter.

["Centre de documentation ONTAP 9"](#)

Suivez ces étapes pour afficher les magasins de données :

1. Sur la page **VMWARE > Machines virtuelles**, cliquez sur la machine virtuelle qui héberge la banque de données. Cliquez sur **Workload Analyzer** ou sur le lien de l'objet de la banque de données. Dans le scénario standard, lorsque le site principal hébergeant le volume ou le LUN fonctionne comme prévu, vous pouvez voir les détails du cluster vServer du site principal.
2. En cas de sinistre et de basculement consécutif vers le site secondaire, le lien vers la banque de données pointe vers les mesures de performances du volume ou du LUN dans le cluster secondaire. Cela se reflète une fois le prochain cycle de découverte (acquisition) des clusters et du vServer terminé.
3. Après un basculement réussi, le lien de la banque de données reflète à nouveau les mesures de performances du volume ou du LUN dans le cluster principal. Cela se reflète une fois le prochain cycle de découverte des clusters et du vServer terminé.

Afficher les banques de données dans la configuration de reprise après sinistre de la machine virtuelle de stockage

Notez les conditions préalables suivantes avant d'afficher les banques de données dans une configuration de reprise après sinistre d'une machine virtuelle de stockage :

- En cas de basculement et de retour en arrière, la découverte des clusters primaire et secondaire de la paire HA et des serveurs vCenter doit être terminée.
- Le cluster source et de destination ainsi que les homologues de machines virtuelles de stockage doivent être gérés par Unified Manager.
- La configuration requise doit être effectuée sur ONTAP et vCenter Server.
 - Pour les banques de données NAS (NFS et VMFS), en cas de sinistre, les étapes incluent la mise en service de la machine virtuelle de stockage secondaire, la vérification des LIF et des itinéraires de données, l'établissement des connexions perdues sur vCenter Server et le démarrage des machines virtuelles.

Pour un retour au site principal, les données entre les volumes doivent être synchronisées avant que le site principal ne commence à diffuser les données.

- Pour les banques de données SAN (iSCSI et FC pour VMFS), vCenter Server formate le LUN monté dans un format VMFS. En cas de sinistre, les étapes incluent la mise en service de la machine virtuelle de stockage secondaire, la vérification des LIF et des itinéraires de données. Si les adresses IP cibles iSCSI sont différentes des LIF principales, elles doivent être ajoutées manuellement. Les nouveaux LUN doivent être disponibles en tant que périphériques sous l'adaptateur iSCSI de l'adaptateur de stockage de l'hôte. Par la suite, de nouveaux magasins de données VMFS avec les nouveaux LUN doivent être créés et les anciennes machines virtuelles enregistrées avec de nouveaux noms. Les machines virtuelles doivent être opérationnelles.

En cas de récupération, les données entre les volumes doivent être synchronisées. De nouveaux magasins de données VMFS doivent à nouveau être créés à l'aide des LUN et des anciennes machines virtuelles enregistrées avec de nouveaux noms.

Pour plus d'informations sur la configuration, consultez la documentation ONTAP et de vCenter Server.

["Centre de documentation ONTAP 9"](#)

Suivez ces étapes pour afficher les magasins de données :

1. Sur la page **VMWARE > Machines virtuelles**, cliquez sur l'inventaire de la machine virtuelle qui héberge la banque de données. Cliquez sur le lien de l'objet de la banque de données. Dans le scénario standard, vous pouvez voir les données de performances des volumes et des LUN dans la machine virtuelle de stockage principale.
2. En cas de sinistre et de basculement consécutif vers la machine virtuelle de stockage secondaire, le lien de la banque de données pointe vers les mesures de performances du volume ou du LUN dans la machine virtuelle de stockage secondaire. Cela se reflète une fois le prochain cycle de découverte (acquisition) de clusters et de vServer terminé.
3. Après un basculement réussi, le lien de la banque de données reflète à nouveau les mesures de performances du volume ou du LUN dans la machine virtuelle de stockage principale. Cela se reflète une fois le prochain cycle de découverte des clusters et du vServer terminé.

Scénarios non pris en charge

- Pour une configuration MetroCluster , notez les limitations suivantes :
 - Clusters uniquement dans le NORMAL et SWITCHOVER les états sont occupés. D'autres États, comme PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK , et NOT_REACHABLE ne sont pas pris en charge.
 - À moins que le basculement automatique (ASO) ne soit activé, si le cluster principal tombe en panne, le cluster secondaire ne peut pas être découvert et la topologie continue de pointer vers le volume ou le LUN du cluster principal.
- Pour une configuration de reprise après sinistre d'une machine virtuelle de stockage, notez la limitation suivante :
 - Une configuration avec Site Recovery Manager (SRM) ou Storage Replication Adapter (SRA) activé pour un environnement de stockage SAN n'est pas prise en charge.

Provisionner et gérer les charges de travail

La fonctionnalité de gestion active d' Active IQ Unified Manager fournit des niveaux de service de performances, des politiques d'efficacité du stockage et des API de fournisseur de stockage pour le provisionnement, la surveillance et la gestion des charges de travail de stockage dans un centre de données.



Unified Manager fournit cette fonctionnalité par défaut. Vous pouvez le désactiver depuis **Gestion du stockage > Paramètres des fonctionnalités** si vous ne prévoyez pas d'utiliser cette fonctionnalité.

Lorsque cette option est activée, vous pouvez provisionner des charges de travail sur les clusters ONTAP gérés par votre instance d'Unified Manager. Vous pouvez également attribuer des politiques, telles que les niveaux de service de performances et les politiques d'efficacité du stockage, aux charges de travail et gérer votre environnement de stockage en fonction de ces politiques.

Cette fonctionnalité permet les fonctions suivantes :

- Découverte automatique des charges de travail de stockage sur les clusters ajoutés, permettant une évaluation et un déploiement faciles des charges de travail de stockage
- Provisionnement des charges de travail NAS prenant en charge les protocoles NFS et CIFS
- Provisionnement des charges de travail SAN prenant en charge les protocoles iSCSI et FCP
- Prise en charge des protocoles NFS et CIFS sur le même partage de fichiers
- Gestion des niveaux de service de performance et des politiques d'efficacité du stockage
- Attribution de niveaux de service de performance et de politiques d'efficacité de stockage aux charges de travail de stockage

Les options **Provisioning**, **Stockage > Charges de travail** et **Politiques** dans le volet gauche de l'interface utilisateur vous permettent de modifier diverses configurations.

Vous pouvez exécuter les fonctions suivantes en utilisant ces options :

- Afficher les charges de travail de stockage sur la page **Stockage > Charges de travail**
- Créer des charges de travail de stockage à partir de la page Provisionner la charge de travail
- Créer et gérer les niveaux de service de performance à partir des politiques
- Créer et gérer des politiques d'efficacité de stockage à partir des politiques
- Affecter des politiques aux charges de travail de stockage à partir de la page Charges de travail

Informations connexes

["Gestion du stockage basée sur des politiques"](#)

Aperçu des charges de travail

Une charge de travail représente les opérations d'entrée/sortie (E/S) d'un objet de stockage, tel qu'un volume ou un LUN. La manière dont le stockage est provisionné est basée sur les exigences de charge de travail attendues. Les statistiques de charge de travail sont suivies par Active IQ Unified Manager uniquement après qu'il y a du trafic vers et depuis l'objet de stockage. Par exemple, les valeurs d'IOPS et de latence de la charge de travail sont disponibles une fois que les utilisateurs commencent à utiliser une base de données ou une application de messagerie.

La page Charges de travail affiche un résumé des charges de travail de stockage des clusters ONTAP gérés par Unified Manager. Il fournit des informations cumulatives en un coup d'œil sur les charges de travail de stockage conformes au niveau de service de performances, ainsi que sur les charges de travail de stockage non conformes. Il vous permet également d'évaluer la capacité et les performances totales, disponibles et utilisées (IOPS) des clusters de votre centre de données.



Il est recommandé d'évaluer le nombre de charges de travail de stockage non conformes, indisponibles ou non gérées par un niveau de service de performances et de prendre les mesures nécessaires pour garantir leur conformité, leur utilisation de la capacité et leurs IOPS.

La page Charges de travail comporte les deux sections suivantes :

- Présentation des charges de travail : fournit une vue d'ensemble du nombre de charges de travail de stockage sur les clusters ONTAP gérés par Unified Manager.

- **Présentation du centre de données** : fournit un aperçu de la capacité et des IOPS des charges de travail de stockage dans le centre de données. Les données pertinentes sont affichées au niveau du centre de données et pour chaque individu.

Section de présentation des charges de travail

La section Présentation des charges de travail fournit des informations cumulatives en un coup d'œil sur les charges de travail de stockage. L'état des charges de travail de stockage s'affiche en fonction des niveaux de service de performances attribués et non attribués.

- **Attribué** : les statuts suivants sont signalés pour les charges de travail de stockage sur lesquelles des niveaux de service de performances ont été attribués :
 - **Conformité** : Les performances des charges de travail de stockage sont basées sur les niveaux de service de performances qui leur sont attribués. Si les charges de travail de stockage se situent dans le seuil de latence défini dans les niveaux de service de performance associés, elles sont marquées comme « conformes ». Les charges de travail conformes sont marquées en bleu.
 - **Non conforme** : lors de la surveillance des performances, les charges de travail de stockage sont marquées comme « non conformes » si la latence des charges de travail de stockage dépasse le seuil de latence défini dans le niveau de service de performances associé. Les charges de travail non conformes sont marquées en orange.
 - **Indisponible** : les charges de travail de stockage sont marquées comme « indisponibles » si elles sont hors ligne ou si le cluster correspondant est inaccessible. Les charges de travail indisponibles sont marquées en rouge.
- **Non attribué** : les charges de travail de stockage auxquelles aucun niveau de service de performance n'est attribué sont signalées comme « non attribuées ». Le numéro est transmis par l'icône d'information.

Le nombre total de charges de travail correspond à la somme totale des charges de travail attribuées et non attribuées.

Vous pouvez cliquer sur le nombre total de charges de travail affichées dans cette section et les afficher sur la page Charges de travail.

La sous-section Conformité par niveaux de service de performance affiche le nombre total de charges de travail de stockage disponibles :

- Conforme à chaque type de niveau de service de performance
- Pour lesquels il existe une inadéquation entre les niveaux de service de performance assignés et recommandés

Section de présentation du centre de données

La section Présentation du centre de données représente graphiquement la capacité disponible et utilisée, ainsi que les IOPS pour tous les clusters du centre de données. En utilisant ces données, vous devez gérer la capacité et les IOPS des charges de travail de stockage. La section affiche également les informations suivantes pour les charges de travail de stockage sur tous les clusters :

- La capacité totale, disponible et utilisée pour tous les clusters de votre centre de données
- Les IOPS totales, disponibles et utilisées pour tous les clusters de votre centre de données
- La capacité disponible et utilisée en fonction de chaque niveau de service de performance
- Les IOPS disponibles et utilisés en fonction de chaque niveau de service de performance

- L'espace total et les IOPS utilisés par les charges de travail auxquelles aucun niveau de service de performance n'est attribué

Comment la capacité et les performances du centre de données sont calculées en fonction des niveaux de service de performance

La capacité utilisée et les IOPS sont récupérées en termes de capacité totale utilisée et de performances de toutes les charges de travail de stockage dans les clusters.

Les IOPS disponibles sont calculés en fonction de la latence attendue et des niveaux de service de performances recommandés sur les nœuds. Il inclut les IOPS disponibles pour tous les niveaux de service de performances dont la latence attendue est inférieure ou égale à leur propre latence attendue.

La capacité disponible est calculée en fonction de la latence attendue et des niveaux de service de performance recommandés sur les agrégats. Il inclut la capacité disponible pour tous les niveaux de service de performance dont la latence attendue est inférieure ou égale à leur propre latence attendue.

Afficher les charges de travail

Lorsque vous ajoutez des clusters à Unified Manager, les charges de travail de stockage sur chaque cluster sont automatiquement détectées et affichées sur la page Charges de travail.

Unified Manager commence à analyser les charges de travail pour la recommandation (PSL recommandés) uniquement après le démarrage des opérations d'E/S sur les charges de travail de stockage.

Les volumes de FlexGroup et ses constituants sont exclus.

Aperçu des charges de travail

La page Présentation des charges de travail affiche la présentation des charges de travail dans le centre de données ainsi que la présentation de l'espace et des performances du centre de données.

- Panneau **Aperçu des charges de travail** : affiche le nombre total de charges de travail et le nombre de charges de travail avec ou sans PSL qui leur sont attribuées. La répartition du nombre de charges de travail pour chaque PSL est également affichée. En cliquant sur les comptes, vous accédez à la vue **Toutes les charges de travail** avec les charges de travail filtrées. Vous pouvez également afficher le nombre de charges de travail qui ne sont pas conformes à la recommandation du système et leur attribuer les PSL recommandés par le système en cliquant sur le bouton **Attribuer les PSL recommandés par le système**.
- Panneau **Présentation du centre de données** : affiche l'espace disponible et utilisé (Tio) et les performances (IOPS) du centre de données. Une répartition de l'espace disponible et utilisé (Tio) et des performances (IOPS) de toutes les charges de travail sous chaque PSL est également affichée.

Vue de toutes les charges de travail

La page **Stockage > Charges de travail > Toutes les charges de travail** répertorie les charges de travail de stockage associées aux clusters ONTAP gérés par Unified Manager.

Pour les charges de travail de stockage nouvellement découvertes sur lesquelles aucune opération d'E/S n'a eu lieu, le statut est « En attente d'E/S ». Une fois les opérations d'E/S commencées sur les charges de travail de stockage, Unified Manager commence l'analyse et l'état de la charge de travail passe à « Apprentissage... ». Une fois l'analyse terminée (dans les 24 heures suivant le début des opérations d'E/S), les PSL recommandés sont affichés pour les charges de travail de stockage.

La page vous permet également d'attribuer des politiques d'efficacité de stockage (SEP) et des niveaux de service de performances (PSL) aux charges de travail de stockage. Vous pouvez effectuer plusieurs tâches :

- Ajouter ou provisionner des charges de travail de stockage
- Afficher et filtrer la liste des charges de travail
- Attribuer des PSL aux charges de travail de stockage
- Évaluer les PSL recommandés par le système et les attribuer aux charges de travail
- Affecter des SEP aux charges de travail de stockage

Ajout ou provisionnement de charges de travail de stockage

Vous pouvez ajouter ou provisionner les charges de travail de stockage sur les LUN pris en charge (prenant en charge les protocoles iSCSI et FCP), les partages de fichiers NFS et les partages SMB.

Étapes

1. Cliquez sur **Stockage > Charges de travail > Toutes les charges de travail > Créer**.
2. Créer des charges de travail. Pour plus d'informations, voir "[Provisionnement et gestion des charges de travail](#)".

Affichage et filtrage des charges de travail

Sur l'écran Toutes les charges de travail, vous pouvez afficher toutes les charges de travail de votre centre de données ou rechercher des charges de travail de stockage spécifiques en fonction de leurs PSL ou de leurs noms. Vous pouvez utiliser l'icône de filtre pour saisir des conditions spécifiques pour votre recherche. Vous pouvez effectuer une recherche selon différentes conditions de filtre, par exemple par cluster hôte ou par machine virtuelle de stockage. L'option **Capacité totale** permet de filtrer par la capacité totale des charges de travail (par Mo). Cependant, dans ce cas, le nombre de charges de travail renvoyées peut varier, car la capacité totale est comparée au niveau de l'octet.

Pour chaque charge de travail, des informations telles que le cluster hôte et la machine virtuelle de stockage sont affichées, ainsi que le PSL et le SEP attribués.

La page vous permet également d'afficher les détails des performances d'une charge de travail. Vous pouvez afficher des informations détaillées sur les IOPS, la capacité et la latence de la charge de travail en cliquant sur le bouton **Choisir/Trier les colonnes** et en sélectionnant les colonnes spécifiques à afficher. La colonne Vue des performances affiche les IOPS moyennes et maximales pour une charge de travail, et vous pouvez cliquer sur l'icône de l'analyseur de charge de travail pour afficher l'analyse détaillée des IOPS.

Analyse des critères de performance et de capacité d'une charge de travail

Le bouton **Analyser la charge de travail** de la fenêtre contextuelle **Analyse IOPS** vous amène à la page Analyse de la charge de travail, où vous pouvez sélectionner une plage horaire et afficher les tendances de latence, de débit et de capacité pour la charge de travail sélectionnée. Pour plus d'informations sur l'analyseur de charge de travail, voir "[Dépannage des charges de travail à l'aide de l'analyseur de charge de travail](#)".

Vous pouvez afficher les informations de performances d'une charge de travail pour faciliter le dépannage en cliquant sur l'icône de graphique à barres dans la colonne **Vue des performances**. Pour afficher les graphiques de performances et de capacité sur la page Analyse de la charge de travail afin d'analyser l'objet, cliquez sur le bouton **Analyser la charge de travail**.

Pour plus d'informations, voir "[Quelles données l'analyseur de charge de travail affiche-t-il ?](#)".

Attribuer des politiques aux charges de travail

Vous pouvez attribuer des politiques d'efficacité de stockage (SEP) et des niveaux de service de performances (PSL) aux charges de travail de stockage à partir de la page Toutes les charges de travail en utilisant les différentes options de navigation.

Affecter des politiques à une seule charge de travail

Vous pouvez attribuer un PSL ou un SEP ou les deux à une seule charge de travail. Suivez ces étapes :

1. Sélectionnez la charge de travail.
2. Cliquez sur l'icône de modification à côté de la ligne, puis cliquez sur **Modifier**.

Les champs **Niveau de service de performance attribué** et **Politique d'efficacité du stockage** sont activés.

3. Sélectionnez le PSL ou le SEP requis, ou les deux.
4. Cliquez sur l'icône de vérification pour appliquer les modifications.



Vous pouvez également sélectionner une charge de travail et cliquer sur **Plus d'actions** pour attribuer les politiques.

Attribuer des politiques à plusieurs charges de travail de stockage

Vous pouvez attribuer un PSL ou un SEP à plusieurs charges de travail de stockage ensemble. Suivez ces étapes :

1. Cochez les cases correspondant aux charges de travail auxquelles vous souhaitez attribuer la stratégie ou sélectionnez toutes les charges de travail de votre centre de données.
2. Cliquez sur **Plus d'actions**.
3. Pour attribuer un PSL, sélectionnez **Attribuer un niveau de service de performance**. Pour attribuer un SEP, sélectionnez **Attribuer une politique d'efficacité de stockage**. Une fenêtre contextuelle s'affiche pour vous permettre de sélectionner la politique.
4. Sélectionnez la politique appropriée et cliquez sur **Appliquer**. Le nombre de charges de travail sur lesquelles les politiques sont attribuées est affiché. Les charges de travail sur lesquelles les politiques ne sont pas attribuées sont également répertoriées, avec la cause.



L'application de politiques sur des charges de travail en masse peut prendre un certain temps en fonction du nombre de charges de travail sélectionnées. Vous pouvez cliquer sur le bouton **Exécuter en arrière-plan** et continuer avec d'autres tâches pendant que l'opération s'exécute en arrière-plan. Une fois l'affectation en masse terminée, vous pouvez afficher l'état d'achèvement. Si vous appliquez un PSL sur plusieurs charges de travail, vous ne pouvez pas déclencher une autre demande lorsque la tâche précédente d'affectation en masse est en cours d'exécution.

Attribuer des PSL recommandés par le système aux charges de travail

Vous pouvez attribuer des PSL recommandés par le système aux charges de travail de stockage d'un centre de données auxquelles aucun PSL n'est attribué ou dont les PSL attribués ne correspondent pas à la recommandation du système. Pour utiliser cette fonctionnalité, cliquez sur le bouton **Attribuer les PSL recommandés par le système**. Vous n'avez pas besoin de sélectionner des charges de travail spécifiques.

La recommandation est déterminée en interne par l'analyse du système et est ignorée pour les charges de travail dont les IOPS et autres paramètres ne coïncident pas avec les définitions de tout PSL disponible. Charges de travail de stockage avec `Waiting for I/O` et les statuts d'apprentissage sont également exclus.



Unified Manager recherche des mots-clés spéciaux dans le nom de la charge de travail pour remplacer les analyses du système et recommander un PSL différent pour la charge de travail. Lorsque la charge de travail contient les lettres « ora » dans son nom, le PSL **Extreme Performance** est recommandé. Et lorsque la charge de travail contient les lettres « vm » dans son nom, le PSL **Performance** est recommandé.

Voir également l'article de la base de connaissances (KB) ["La fonction « Attribuer le niveau de service de performance recommandé par le système » d'ActiveIQ Unified Manager ne s'adapte pas à une charge de travail très variable."](#)

Provisionner les volumes de partage de fichiers

Vous pouvez créer des volumes de partage de fichiers prenant en charge les protocoles CIFS/SMB et NFS, sur un cluster existant et une machine virtuelle de stockage (VM de stockage) à partir de la page Provisionner la charge de travail.

Avant de commencer

- La machine virtuelle de stockage doit disposer d'espace pour provisionner le volume de partage de fichiers.
- L'un ou les deux services SMB et NFS doivent être activés sur votre machine virtuelle de stockage.
- Pour sélectionner et attribuer le niveau de service de performances (PSL) et la politique d'efficacité de stockage (SEP) sur la charge de travail, les politiques doivent avoir été créées avant de commencer à créer la charge de travail.

Étapes

1. Sur la page **Provision Workload**, ajoutez le nom de la charge de travail que vous souhaitez créer, puis sélectionnez le cluster dans la liste disponible.
2. En fonction du cluster que vous avez sélectionné, le champ **STORAGE VM** filtre les machines virtuelles de stockage disponibles pour ce cluster. Sélectionnez la machine virtuelle de stockage requise dans la liste.

En fonction des services SMB et NFS pris en charge sur la machine virtuelle de stockage, l'option NAS est activée dans la section Informations sur l'hôte.

3. Dans la section Stockage et optimisation, attribuez la capacité de stockage et le PSL, et éventuellement, un SEP pour la charge de travail.

Les spécifications du SEP sont attribuées au LUN et les définitions du PSL sont appliquées à la charge de travail lors de sa création.

4. Cochez la case **Appliquer les limites de performances** si vous souhaitez appliquer la PSL que vous avez attribuée à la charge de travail.

L'attribution d'un PSL à une charge de travail garantit que l'agrégat sur lequel la charge de travail est créée peut prendre en charge les objectifs de performance et de capacité définis dans la politique respective. Par exemple, si une charge de travail se voit attribuer une politique PSL « Extreme Performance », l'agrégat sur lequel la charge de travail doit être provisionnée doit avoir la capacité de prendre en charge les objectifs de performance et de capacité de la politique « Extreme Performance », comme le stockage SSD.



À moins que vous ne cochiez cette case, le PSL n'est pas appliqué à la charge de travail et le statut de la charge de travail sur le tableau de bord apparaît comme non attribué.

5. Sélectionnez l'option **NAS**.

Si vous ne voyez pas l'option **NAS** activée, vérifiez si la machine virtuelle de stockage que vous avez sélectionnée prend en charge SMB ou NFS, ou les deux.



Si votre machine virtuelle de stockage est activée pour les services SMB et NFS, vous pouvez sélectionner les cases à cocher **Partager par NFS** et **Partager par SMB** et créer un partage de fichiers prenant en charge les protocoles NFS et SMB. Si vous souhaitez créer un partage SMB ou CIFS, cochez uniquement la case correspondante.

6. Pour les volumes de partage de fichiers NFS, spécifiez l'adresse IP de l'hôte ou du réseau pour accéder au volume de partage de fichiers. Vous pouvez saisir des valeurs séparées par des virgules pour plusieurs hôtes.

Lors de l'ajout de l'adresse IP de l'hôte, une vérification interne s'exécute pour faire correspondre les détails de l'hôte avec la machine virtuelle de stockage et la politique d'exportation pour cet hôte est créée, ou s'il existe une politique existante, elle est réutilisée. S'il existe plusieurs partages NFS créés pour le même hôte, une politique d'exportation disponible pour le même hôte avec des règles correspondantes est réutilisée pour tous les partages de fichiers. La fonction de spécification des règles de politiques individuelles ou de réutilisation des politiques en fournissant des clés de politique spécifiques est disponible lorsque vous provisionnez le partage NFS à l'aide d'API.

7. Pour un partage SMB, spécifiez les utilisateurs ou groupes d'utilisateurs qui peuvent accéder au partage SMB et attribuez les autorisations requises. Pour chaque groupe d'utilisateurs, une nouvelle liste de contrôle d'accès (ACL) est générée lors de la création du partage de fichiers.

8. Cliquez sur **Enregistrer**.

La charge de travail est ajoutée à la liste des charges de travail de stockage.

Provisionner les LUN

Vous pouvez créer des LUN prenant en charge les protocoles CIFS/SMB et NFS, sur un cluster existant et une machine virtuelle de stockage (VM de stockage) à partir de la page Provisionner la charge de travail.

Avant de commencer

- La machine virtuelle de stockage doit disposer d'espace pour provisionner le LUN.
- iSCSI et FCP doivent être activés sur la machine virtuelle de stockage sur laquelle vous créez le LUN.
- Pour sélectionner et attribuer le niveau de service de performances (PSL) et la politique d'efficacité de stockage (SEP) sur la charge de travail, les politiques doivent avoir été créées avant de commencer à créer la charge de travail.

Étapes

1. Sur la page **Provision Workload**, ajoutez le nom de la charge de travail que vous souhaitez créer, puis sélectionnez le cluster dans la liste disponible.

En fonction du cluster que vous avez sélectionné, le champ **STORAGE VM** filtre les machines virtuelles de stockage disponibles pour ce cluster.

2. Sélectionnez la machine virtuelle de stockage dans la liste qui prend en charge les services iSCSI et FCP.

En fonction de votre sélection, l'option SAN est activée dans la section Informations sur l'hôte.

3. Dans la section **Stockage et optimisation**, attribuez la capacité de stockage et le PSL, et éventuellement le SEP pour la charge de travail.

Les spécifications du SEP sont attribuées au LUN et les définitions du PSL sont appliquées à la charge de travail lors de sa création.

4. Cochez la case **Appliquer les limites de performances** si vous souhaitez appliquer la PSL attribuée à la charge de travail.

L'attribution d'un PSL à une charge de travail garantit que l'agrégat sur lequel la charge de travail est créée peut prendre en charge les objectifs de performance et de capacité définis dans la politique respective. Par exemple, si une charge de travail se voit attribuer le PSL « Performances extrêmes », l'agrégat sur lequel la charge de travail doit être provisionnée doit avoir la capacité de prendre en charge les objectifs de performances et de capacité de la politique « Performances extrêmes », comme le stockage SSD.



À moins que vous ne cochiez cette case, le PSL n'est pas appliqué à la charge de travail et l'état de la charge de travail sur le tableau de bord apparaît comme suit `unassigned`.

5. Sélectionnez l'option **SAN**. Si vous ne voyez pas l'option **SAN** activée, vérifiez si la machine virtuelle de stockage que vous avez sélectionnée prend en charge iSCSI et FCP.
6. Sélectionnez le système d'exploitation hôte.
7. Spécifiez le mappage d'hôte pour contrôler l'accès des initiateurs au LUN. Vous pouvez affecter des groupes d'initiateurs existants (igroups) ou définir et mapper de nouveaux igroups.



Si vous créez un nouveau groupe d'adresses lors du provisionnement du LUN, vous devez attendre le prochain cycle de découverte (jusqu'à 15 minutes) pour l'utiliser. Il est donc recommandé d'utiliser un igroup existant dans la liste des igroups disponibles.

Si vous souhaitez créer un nouveau groupe i, sélectionnez le bouton **Créer un nouveau groupe initiateur** et saisissez les informations du groupe i.

8. Cliquez sur **Enregistrer**.

Le LUN est ajouté à la liste des charges de travail de stockage.

Niveaux de service de performance

Un niveau de service de performance (PSL) vous permet de définir les objectifs de performances et de stockage pour une charge de travail. Vous pouvez attribuer un PSL à une charge de travail lors de la création initiale de la charge de travail, ou ultérieurement en modifiant la charge de travail.

La gestion et la surveillance des ressources de stockage sont basées sur des objectifs de niveau de service (SLO). Les SLO sont définis par des accords de niveau de service basés sur les performances et la capacité requises. Dans Unified Manager, les SLO font référence aux définitions PSL des applications exécutées sur le stockage NetApp. Les services de stockage sont différenciés en fonction des performances et de l'utilisation des ressources sous-jacentes. Un PSL est une description des objectifs du service de stockage. Un PSL

permet au fournisseur de stockage de spécifier les objectifs de performances et de capacité pour la charge de travail. Lorsque vous attribuez un PSL à une charge de travail, la charge de travail correspondante sur ONTAP est gérée par ses objectifs de performances et de capacité. Chaque PSL est régi par les IOP de pointe, attendus et minimum absolu, ainsi que par la latence attendue.

Unified Manager dispose des types de PSL suivants :

- **Défini par le système** : Unified Manager fournit quelques politiques prédéfinies qui ne peuvent pas être modifiées. Ces PSL prédéfinis sont :
 - Performances extrêmes
 - Performances
 - Valeur

Les PSL Extreme Performance, Performance et Value s'appliquent à la plupart des charges de travail de stockage courantes dans un centre de données.

Unified Manager propose également trois niveaux de service de performance pour les applications de base de données. Il s'agit de PSL extrêmement performants qui prennent en charge les IOPS en rafale et conviennent aux applications de base de données avec la demande de débit la plus élevée.

- Extrême pour les journaux de base de données
- Extrême pour les données partagées de base de données
- Extrême pour les données de base de données
- **Défini par l'utilisateur** : Si les niveaux de service de performance prédéfinis ne répondent pas à vos exigences, vous pouvez créer de nouveaux PSL pour répondre à vos besoins. Pour plus d'informations, voir ["Créer et modifier les niveaux de service de performance"](#) .
- **Au-delà de l'extrême** : les PSL au-delà de l'extrême sont les PSL recommandés par le système et suggérés pour les charges de travail qui exigent des IOP supérieures à Extreme. Les charges de travail sont analysées en interne en fonction de leurs IOPS, de leur capacité et de leur latence, et un PSL Beyond Extreme est recommandé pour chacune de ces charges de travail sur l'écran **Stockage > Charges de travail > Toutes les charges de travail**. Vous pouvez appliquer les PSL aux charges de travail pour garantir des performances optimales.

Les paramètres IOP pour les charges de travail sont générés dynamiquement, en fonction du comportement de la charge de travail, et ajoutés au nom du PSL Beyond Extreme au format `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>` . Par exemple, si le système détermine qu'une charge de travail a les IOP maximales et attendues comme 106345 et 37929 respectivement, le PSL Beyond Extreme qui est généré pour la charge de travail est nommé comme `Beyond Extreme 106345 37929` . Bien que ces PSL soient recommandés par le système, lorsque vous les attribuez à des charges de travail, ces PSL sont étiquetés comme `User-defined` en type.

Gérer les charges de travail en attribuant des PSL

Vous pouvez accéder aux PSL à partir de la page **Politiques > Niveaux de service de performance** et en utilisant les API du fournisseur de stockage. La gestion des charges de travail de stockage en leur attribuant des PSL est pratique car vous n'avez pas à gérer individuellement les charges de travail de stockage. Toutes les modifications peuvent également être gérées en réaffectant un autre PSL plutôt qu'en les gérant individuellement. Unified Manager vous aide à attribuer des PSL à vos charges de travail en fonction d'une évaluation et de recommandations internes.

Pour plus d'informations sur l'attribution des PSL recommandés par le système aux charges de travail,

consultez "[Attribuer des PSL recommandés par le système aux charges de travail](#)"

La page Niveaux de service de performance répertorie les stratégies PSL disponibles et vous permet de les ajouter, de les modifier et de les supprimer.



Vous ne pouvez pas modifier un PSL défini par le système ou actuellement attribué à une charge de travail. Vous ne pouvez pas supprimer un PSL qui est attribué à une charge de travail ou s'il s'agit du seul PSL disponible.

Cette page affiche les informations suivantes :

Champ	Description
Nom	Nom du PSL.
Type	Que la politique soit définie par le système ou par l'utilisateur.
IOPS/TB attendus	Nombre minimum d'IOPS qu'une application est censée effectuer sur un LUN ou un partage de fichiers. Les IOPS attendus spécifient les IOPS minimums attendus alloués, en fonction de la taille allouée de l'objet de stockage.
IOPS/To de pointe	Nombre maximal d'IOPS qu'une application peut effectuer sur un LUN ou un partage de fichiers. Peak IOPS spécifie le nombre maximal d'IOPS possibles alloués, en fonction de la taille allouée de l'objet de stockage ou de la taille utilisée de l'objet de stockage. Les IOPS de pointe sont basés sur une politique d'allocation. La politique d'allocation est soit l'espace alloué, soit l'espace utilisé. Lorsque la stratégie d'allocation est définie sur l'espace alloué, le nombre maximal d'E/S par seconde est calculé en fonction de la taille de l'objet de stockage. Lorsque la politique d'allocation est définie sur l'espace utilisé, le nombre maximal d'E/S par seconde est calculé en fonction de la quantité de données stockées dans l'objet de stockage, en tenant compte de l'efficacité du stockage. Par défaut, la politique d'allocation est définie sur l'espace utilisé.

Champ	Description
IOPS minimum absolu	Le nombre minimum absolu d'IOPS est utilisé comme remplacement lorsque les IOPS attendus sont inférieurs à cette valeur. Les valeurs par défaut des PSL définies par le système sont les suivantes : • Performances extrêmes : si les IOPS attendues sont $\geq 6\,144/T_o$, alors le minimum absolu d'IOPS est de 1 000 • Performances : si les IOPS attendus sont $\geq 2\,048/T_o$ et $< 6\,144/T_o$, alors le minimum absolu d'IOPS est de 500. • Valeur : si les IOPS attendus sont $\geq 128/T_o$ et $< 2\,048/T_o$, alors le minimum absolu d'IOPS est de 75 Les valeurs par défaut des PSL de base de données définies par le système sont les suivantes : • Extrême pour les journaux de base de données : si les IOPS attendus sont $\geq 22\,528$, alors le minimum absolu d'IOPS est de 4 000 • Extrême pour les données partagées de base de données : si les IOPS attendues sont $\geq 16\,384$, alors le minimum absolu d'IOPS est de 2 000 • Extrême pour les données de base de données : si les IOPS attendues sont $\geq 12\,288$, alors le minimum absolu d'IOPS est de 2 000 La valeur la plus élevée du minimum absolu d'IOPS pour les PSL personnalisés peut atteindre un maximum de 75 000. La valeur inférieure est calculée comme suit : $1000/\text{latence attendue}$
Latence attendue	Latence attendue pour les IOPS de stockage en millisecondes par opération (ms/op).
Capacité	Capacité totale disponible et utilisée dans les clusters.
Charges de travail	Nombre de charges de travail de stockage auxquelles le PSL a été attribué.

Pour plus d'informations sur la manière dont les IOPS de pointe et les IOPS attendus contribuent à obtenir des performances différenciées cohérentes sur les clusters ONTAP , consultez l'article de base de connaissances suivant : https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["Qu'est-ce que la budgétisation axée sur la performance ?"]

Événements générés pour les charges de travail dépassant le seuil défini par les PSL

Notez que si les charges de travail dépassent la valeur de latence attendue pendant 30 % du temps au cours de l'heure précédente, Unified Manager génère l'un des événements suivants pour vous informer d'un problème de performances potentiel :

- Dépassement du seuil de latence du volume de charge de travail, tel que défini par la politique de niveau de service des performances
- Le seuil de latence du LUN de charge de travail a été dépassé tel que défini par la politique de niveau de service de performances.

Vous souhaitez peut-être analyser la charge de travail pour voir ce qui peut être à l'origine des valeurs de latence plus élevées.

Pour plus d'informations, consultez les liens suivants :

- ["Événements de volume"](#)
- ["Que se passe-t-il lorsqu'une politique de seuil de performance est violée ?"](#)
- ["Comment Unified Manager utilise la latence de la charge de travail pour identifier les problèmes de performances"](#)
- ["Quels sont les événements de performance"](#)

PSL définis par le système

Le tableau suivant fournit des informations sur les PSL définis par le système :

Niveau de service de performance	Description et cas d'utilisation	Latence attendue (ms/op)	IOPS de pointe	IOPS attendus	IOPS minimum absolu
Performances extrêmes	Fournit un débit extrêmement élevé avec une latence très faible Idéal pour les applications sensibles à la latence	1	12288	6144	1000
Performances	Fournit un débit élevé avec une faible latence Idéal pour les bases de données et les applications virtualisées	2	4096	2048	500

Niveau de service de performance	Description et cas d'utilisation	Latence attendue (ms/op)	IOPS de pointe	IOPS attendus	IOPS minimum absolu
Valeur	Offre une capacité de stockage élevée et une latence modérée Idéal pour les applications à haute capacité telles que la messagerie électronique, le contenu Web, les partages de fichiers et les cibles de sauvegarde	17	512	128	75
Extrême pour les journaux de base de données	Fournit un débit maximal avec la latence la plus faible. Idéal pour les applications de base de données prenant en charge les journaux de base de données. Ce PSL offre le débit le plus élevé car les journaux de base de données sont extrêmement sporadiques et la journalisation est constamment demandée.	1	45056	22528	4000

Niveau de service de performance	Description et cas d'utilisation	Latence attendue (ms/op)	IOPS de pointe	IOPS attendus	IOPS minimum absolu
Extrême pour les données partagées de base de données	Fournit un débit très élevé avec la latence la plus faible. Idéal pour les applications de base de données, les données stockées dans un magasin de données commun, mais partagées entre les bases de données.	1	32768	16384	2000
Extrême pour les données de base de données	Fournit un débit élevé avec la latence la plus faible. Idéal pour les données d'applications de base de données, telles que les informations de table de base de données et les métadonnées.	1	24576	12288	2000

Créer et modifier les niveaux de service de performance

Lorsque les niveaux de service de performances définis par le système ne correspondent pas à vos exigences de charge de travail, vous pouvez créer vos propres niveaux de service de performances optimisés pour vos charges de travail.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application.
- Le nom du niveau de service de performance doit être unique et vous ne pouvez pas utiliser les mots clés réservés suivants :

Prime, Extreme , Performance , Value , Unassigned , Learning , Idle , Default , et None .

Vous créez et modifiez des niveaux de service de performances personnalisés à partir de la page Niveaux de service de performances en définissant les objectifs de niveau de service dont vous avez besoin pour les applications qui accéderont au stockage.



Vous ne pouvez pas modifier un niveau de service de performances s'il est actuellement attribué à une charge de travail.

Étapes

- 1. Dans le volet de navigation de gauche, sous **Paramètres**, sélectionnez **Politiques > Niveaux de service de performance**.
- 2. Dans la page **Niveaux de service de performance**, cliquez sur le bouton approprié selon que vous souhaitez créer un nouveau niveau de service de performance ou modifier un niveau de service de performance existant.

À...	Suivez ces étapes...
Créer un nouveau niveau de service de performance	Cliquez sur Ajouter .
Modifier un niveau de service de performance existant	Sélectionnez un niveau de service de performance existant, puis cliquez sur Modifier .

La page permettant d'ajouter ou de modifier un niveau de service de performance s'affiche.

- 3. Personnalisez le niveau de service de performance en spécifiant les objectifs de performance, puis cliquez sur **Soumettre** pour enregistrer le niveau de service de performance.

Vous pouvez appliquer le niveau de service de performances nouveau ou modifié aux charges de travail (LUN, partages de fichiers NFS, partages CIFS) à partir de la page Charges de travail ou lors du provisionnement d'une nouvelle charge de travail.

Gérer les politiques d'efficacité du stockage

Une politique d'efficacité de stockage (SEP) vous permet de définir les caractéristiques d'efficacité de stockage d'une charge de travail. Vous pouvez attribuer un SEP à une charge de travail lors de la création initiale de la charge de travail, ou ultérieurement en modifiant la charge de travail.

L'efficacité du stockage inclut l'utilisation de technologies telles que le provisionnement léger, la déduplication et la compression des données qui augmentent l'utilisation du stockage et réduisent les coûts de stockage. Lors de la création de SEP, vous pouvez utiliser ces technologies peu encombrantes individuellement ou ensemble pour obtenir une efficacité de stockage maximale. Lorsque vous associez les stratégies à vos charges de travail de stockage, les paramètres de stratégie spécifiés leur sont attribués. Unified Manager vous permet d'attribuer des SEP définis par le système et par l'utilisateur pour optimiser les ressources de stockage dans votre centre de données.

Unified Manager fournit deux SEP définis par le système : haut et bas. Ces SEP s'appliquent à la plupart des charges de travail de stockage dans un centre de données. Toutefois, vous pouvez créer vos propres politiques si les SEP définis par le système ne répondent pas à vos exigences.

Vous ne pouvez pas modifier un SEP défini par le système ou actuellement attribué à une charge de travail.

Vous ne pouvez pas supprimer un SEP qui est attribué à une charge de travail ou s'il s'agit du seul SEP disponible.

La page Stratégies d'efficacité du stockage répertorie les SEP disponibles et vous permet d'ajouter, de modifier et de supprimer des SEP personnalisés. Cette page affiche les informations suivantes :

Champ	Description
Nom	Nom du SEP.
Type	Que la politique soit définie par le système ou par l'utilisateur.
Réserve d'espace	Que le volume soit à provisionnement fin ou à provisionnement épais.
Déduplication	Si la déduplication est activée sur la charge de travail : • En ligne : la déduplication se produit pendant l'écriture sur la charge de travail • Contexte : La déduplication se produit dans la charge de travail • Désactiver : la déduplication est désactivée sur la charge de travail
Compression	Si la compression des données est activée sur la charge de travail : • En ligne : la compression des données se produit lors de l'écriture sur la charge de travail • Contexte : La compression des données se produit dans la charge de travail • Désactiver : la compression des données est désactivée sur la charge de travail
Charges de travail	Nombre de charges de travail de stockage auxquelles le SEP a été attribué

Directives pour la création d'une politique d'efficacité de stockage personnalisée

Si les SEP existants ne répondent pas aux exigences de stratégie pour vos charges de travail de stockage, vous pouvez créer un SEP personnalisé. Cependant, il est recommandé d'essayer d'utiliser les SEP définis par le système pour vos charges de travail de stockage et de créer des SEP personnalisés uniquement si nécessaire.

Vous pouvez afficher le SEP attribué aux charges de travail dans la page Toutes les charges de travail et dans la page Détails du volume/de l'état de santé. Vous pouvez afficher le taux de réduction des données au niveau du cluster (sans copies Snapshot) en fonction de ces efficacités de stockage dans le panneau Capacité du tableau de bord et dans la vue Capacité : Tous les clusters.

Créer et modifier des politiques d'efficacité de stockage

Lorsque les stratégies d'efficacité du stockage définies par le système ne correspondent pas aux exigences de votre charge de travail, vous pouvez créer vos propres stratégies d'efficacité du stockage optimisées pour vos charges de travail.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application.
- Le nom de la politique d'efficacité du stockage doit être unique et vous ne pouvez pas utiliser les mots clés réservés suivants :

High, Low , Unassigned , Learning , Idle , Default , et None .

Vous créez et modifiez des stratégies d'efficacité de stockage personnalisées à partir de la page Stratégies d'efficacité de stockage en définissant les caractéristiques d'efficacité de stockage dont vous avez besoin pour les applications qui accéderont au stockage.



Vous ne pouvez pas modifier une stratégie d'efficacité de stockage si elle est actuellement attribuée à une charge de travail.

Étapes

1. Dans le volet de navigation de gauche, sous **Paramètres**, sélectionnez **Politiques > Efficacité du stockage**.
2. Dans la page **Stratégies d'efficacité du stockage**, cliquez sur le bouton approprié selon que vous souhaitez créer une nouvelle stratégie d'efficacité du stockage ou modifier une stratégie d'efficacité du stockage existante.

À...	Suivez ces étapes...
Créer une nouvelle politique d'efficacité du stockage	Cliquez sur Ajouter
Modifier une politique d'efficacité de stockage existante	Sélectionnez une politique d'efficacité de stockage existante et cliquez sur Modifier

La page permettant d'ajouter ou de modifier une politique d'efficacité de stockage s'affiche.

3. Personnalisez la politique d'efficacité du stockage en spécifiant les caractéristiques d'efficacité du stockage, puis cliquez sur **Soumettre** pour enregistrer la politique d'efficacité du stockage.

Vous pouvez appliquer la nouvelle politique d'efficacité du stockage ou la politique modifiée aux charges de travail (LUN, partages de fichiers NFS, partages CIFS) à partir de la page Charges de travail ou lors du provisionnement d'une nouvelle charge de travail.

Gérer et surveiller les configurations MetroCluster

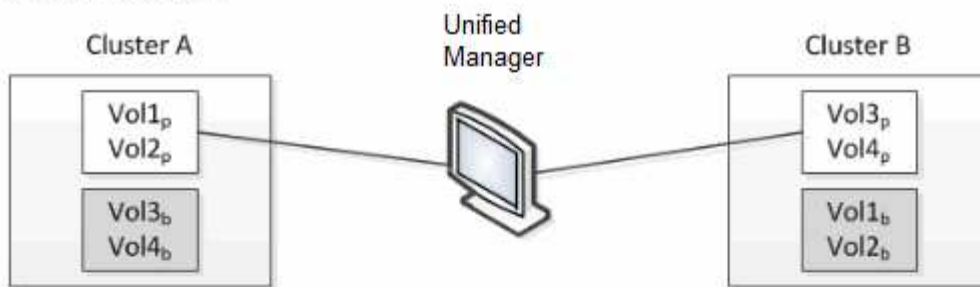
La prise en charge de la surveillance des configurations MetroCluster dans l'interface utilisateur Web d'Unified Manager vous permet de vérifier les éventuels problèmes de connectivité dans vos configurations MetroCluster sur FC et IP. La détection précoce d'un problème de connectivité vous permet de gérer efficacement vos configurations

Comportement du volume lors du basculement et du retour en arrière

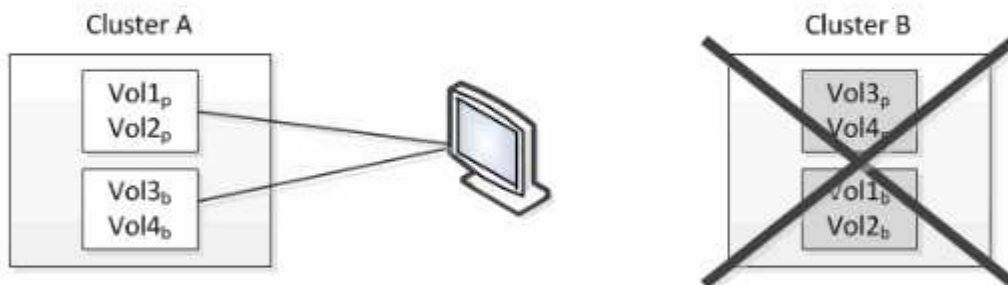
Les événements qui déclenchent un basculement ou un retour en arrière entraînent le déplacement des volumes actifs d'un cluster vers l'autre cluster du groupe de reprise après sinistre. Les volumes du cluster qui étaient actifs et fournissaient des données aux clients sont arrêtés, et les volumes de l'autre cluster sont activés et commencent à fournir des données. Unified Manager surveille uniquement les volumes actifs et en cours d'exécution.

Étant donné que les volumes sont déplacés d'un cluster à un autre, il est recommandé de surveiller les deux clusters. Une seule instance d'Unified Manager peut surveiller les deux clusters dans une configuration MetroCluster , mais parfois la distance entre les deux emplacements nécessite l'utilisation de deux instances d'Unified Manager pour surveiller les deux clusters. La figure suivante montre une seule instance de Unified Manager :

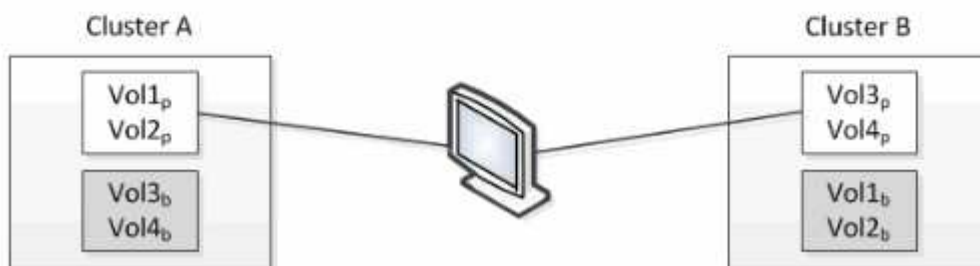
Normal operation



Cluster B fails --- switchover to Cluster A



Cluster B is repaired --- switchback to Cluster B



= active and monitored

= inactive and not monitored

Les volumes avec p dans leurs noms indiquent les volumes principaux et les volumes avec b dans leurs noms

sont des volumes de sauvegarde en miroir créés par SnapMirror.

En fonctionnement normal :

- Le cluster A possède deux volumes actifs : Vol1p et Vol2p.
- Le cluster B possède deux volumes actifs : Vol3p et Vol4p.
- Le cluster A possède deux volumes inactifs : Vol3b et Vol4b.
- Le cluster B possède deux volumes inactifs : Vol1b et Vol2b.

Les informations relatives à chacun des volumes actifs (statistiques, événements, etc.) sont collectées par Unified Manager. Les statistiques Vol1p et Vol2p sont collectées par le cluster A, et les statistiques Vol3p et Vol4p sont collectées par le cluster B.

Après qu'une panne catastrophique provoque un basculement des volumes actifs du cluster B vers le cluster A :

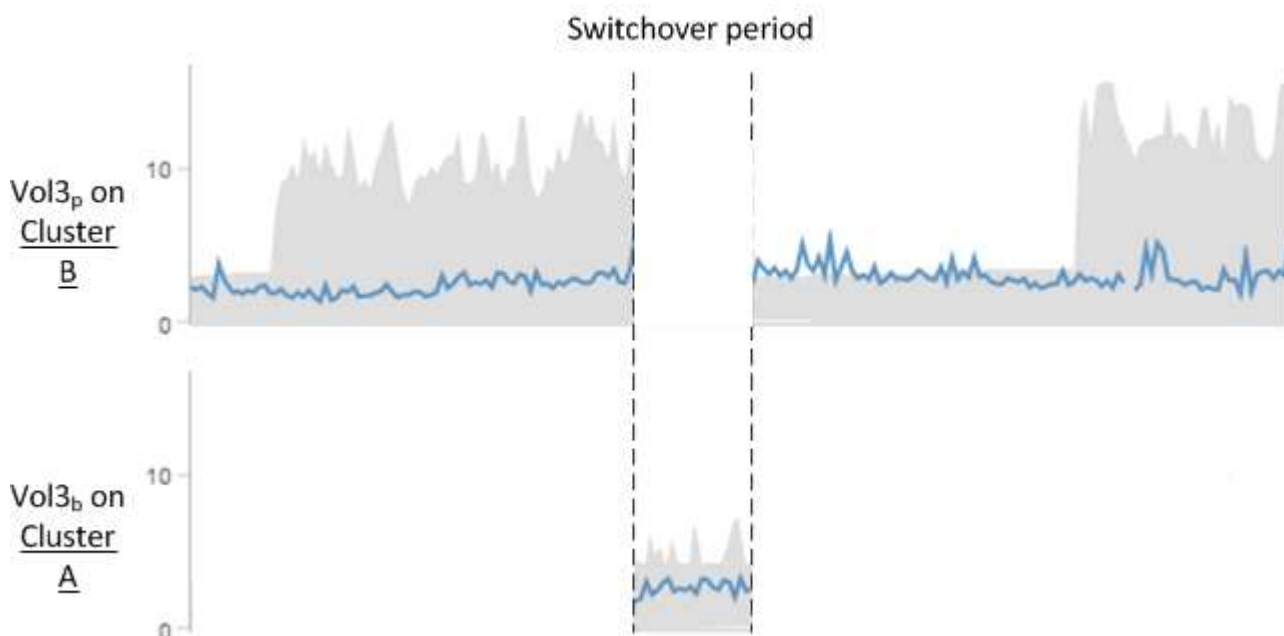
- Le cluster A possède quatre volumes actifs : Vol1p, Vol2p, Vol3b et Vol4b.
- Le cluster B possède quatre volumes inactifs : Vol3p, Vol4p, Vol1b et Vol2b.

Comme lors du fonctionnement normal, les informations relatives à chacun des volumes actifs sont collectées par Unified Manager. Mais dans ce cas, les statistiques Vol1p et Vol2p sont collectées par le cluster A, et les statistiques Vol3b et Vol4b sont également collectées par le cluster A.

Notez que Vol3p et Vol3b ne sont pas les mêmes volumes, car ils se trouvent sur des clusters différents. Les informations dans Unified Manager pour Vol3p ne sont pas les mêmes que celles de Vol3b :

- Lors du passage au cluster A, les statistiques et événements Vol3p ne sont pas visibles.
- Dès le premier basculement, Vol3b ressemble à un nouveau volume sans aucune information historique.

Lorsque le cluster B est réparé et qu'un basculement est effectué, Vol3p est à nouveau actif sur le cluster B, avec les statistiques historiques et un écart de statistiques pour la période pendant le basculement. Vol3b n'est pas visible depuis le cluster A jusqu'à ce qu'un autre basculement se produise :





- Les volumes MetroCluster qui sont inactifs, par exemple Vol3b sur le cluster A après un basculement, sont identifiés par le message « Ce volume a été supprimé ». Le volume n'est pas réellement supprimé, mais il n'est actuellement pas surveillé par Unified Manager car il ne s'agit pas du volume actif.
- Si un seul gestionnaire unifié surveille les deux clusters dans une configuration MetroCluster, la recherche de volume renvoie des informations pour le volume actif à ce moment-là. Par exemple, une recherche pour « Vol3 » renverrait des statistiques et des événements pour Vol3b sur le cluster A si un basculement a eu lieu et que Vol3 est devenu actif sur le cluster A.

Définitions de l'état de connectivité du cluster pour la configuration MetroCluster sur FC

La connectivité entre les clusters d'une configuration MetroCluster sur FC peut avoir l'un des statuts suivants : Optimal, Impacté ou Arrêt. Comprendre les statuts de connectivité vous permet de gérer efficacement vos configurations MetroCluster.

État de connectivité	Description	Icône affichée
Optimal	La connectivité entre les clusters dans la configuration MetroCluster est normale.	
Impacté	Une ou plusieurs erreurs compromettent l'état de disponibilité du basculement ; cependant, les deux clusters de la configuration MetroCluster sont toujours opérationnels. Par exemple, lorsque la liaison ISL est en panne, lorsque la liaison IP intercluster est en panne ou lorsque le cluster partenaire n'est pas accessible.	
Vers le bas	La connectivité entre les clusters dans la configuration MetroCluster est interrompue car l'un ou les deux clusters sont en panne ou les clusters sont en mode de basculement. Par exemple, lorsque le cluster partenaire est hors service en raison d'une catastrophe ou lorsqu'un basculement est prévu à des fins de test.	Basculement avec erreurs :  Basculement réussi : 

Définitions de l'état de mise en miroir des données pour MetroCluster sur FC

Les configurations MetroCluster sur FC fournissent la mise en miroir des données et la capacité supplémentaire de lancer un basculement si un site entier devient indisponible. L'état de la mise en miroir des données entre les clusters d'une configuration MetroCluster sur FC peut être Normal ou Mise en miroir indisponible. Comprendre l'état vous permet de gérer efficacement vos configurations MetroCluster .

État de la mise en miroir des données	Description	Icône affichée
Normal	La mise en miroir des données entre les clusters dans la configuration MetroCluster est normale.	
Mise en miroir indisponible	La mise en miroir des données entre les clusters dans la configuration MetroCluster n'est pas disponible en raison du basculement. Par exemple, lorsque le cluster partenaire est hors service en raison d'une catastrophe ou lorsqu'un basculement est prévu à des fins de test.	Basculement avec erreurs :  Basculement réussi : 

Surveiller les configurations de MetroCluster

Vous pouvez surveiller les problèmes de connectivité dans votre configuration MetroCluster . Les détails incluent l'état des composants et de la connectivité au sein d'un cluster et l'état de la connectivité entre les clusters dans la configuration MetroCluster . Ici, vous apprendrez à surveiller les problèmes de connectivité dans les clusters protégés par les configurations MetroCluster sur FC et MetroCluster sur IP.

Vous pouvez surveiller les configurations MetroCluster à partir des vues suivantes du volet de navigation de gauche d' Active IQ Unified Manager :

- **Stockage > Clusters > Protection : MetroCluster** vue
- **Protection > Relations > Relation : MetroCluster** vue

Unified Manager utilise des alertes d'état du système pour indiquer l'état des composants et de la connectivité dans la configuration MetroCluster .

Avant de commencer

- Les clusters locaux et distants d'une configuration MetroCluster doivent être ajoutés à Active IQ Unified Manager.

- Dans une configuration MetroCluster sur IP, si un médiateur doit être pris en charge, le médiateur doit être configuré et ajouté au cluster par l'API correspondante.
- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Surveiller les problèmes de connectivité dans MetroCluster via la configuration FC

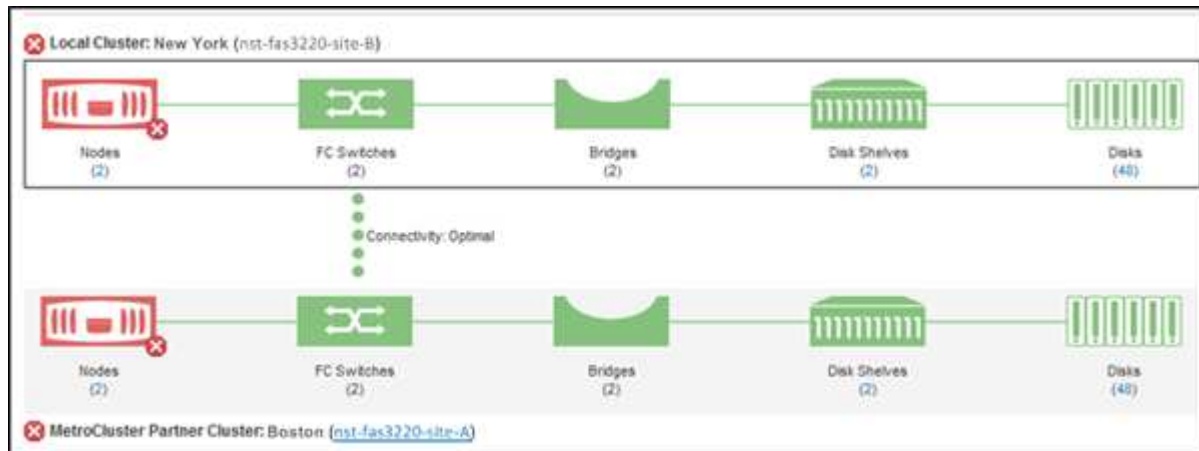
Pour les clusters dans une configuration MetroCluster sur FC, les graphiques de connectivité sont affichés sur la page de détails **Cluster / Santé**. Suivez ces étapes.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.

Une liste de tous les clusters surveillés s'affiche.

2. Dans la vue **Protection : MetroCluster**, cliquez sur le nom du cluster pour lequel vous souhaitez afficher les détails de configuration MetroCluster sur FC. Alternativement, vous pouvez filtrer par clusters dans une configuration MetroCluster .
3. Dans la page de détails **Cluster / Santé**, cliquez sur l'onglet *Connectivité MetroCluster *. L'onglet *Connectivité MetroCluster * est disponible uniquement pour les configurations MetroCluster sur FC.



La topologie de la configuration MetroCluster est affichée dans la zone d'objet de cluster correspondante. Vous pouvez utiliser les informations affichées dans la page Détails du cluster/de la santé pour corriger tout problème de connectivité. Par exemple, si la connectivité entre le nœud et le commutateur d'un cluster est interrompue, l'icône suivante s'affiche :



Si vous déplacez le pointeur sur l'icône, vous pouvez afficher des informations détaillées sur l'événement généré.

Si vous découvrez des problèmes de connectivité dans votre configuration MetroCluster , vous devez vous connecter à System Manager ou accéder à l'interface de ligne de commande ONTAP pour résoudre les problèmes.

Pour plus d'informations sur la détermination de l'état du cluster, consultez ["Déterminer l'état du cluster dans MetroCluster via la configuration FC"](#) .

Surveiller les problèmes de connectivité dans la configuration MetroCluster sur IP

Pour les clusters dans une configuration MetroCluster sur IP, les graphiques de connectivité sont affichés sur la page **Clusters**. Suivez ces étapes.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.

Une liste de tous les clusters surveillés s'affiche.

2. Dans la vue **Protection : MetroClusters**, cliquez sur le nom du cluster pour lequel vous souhaitez afficher les détails de configuration MetroCluster sur IP. Alternativement, vous pouvez filtrer par clusters dans une configuration MetroCluster .
3. Développez la ligne en cliquant sur le signe d'insertion ▾ icône. L'icône en forme de curseur apparaît uniquement pour un cluster protégé par la configuration MetroCluster sur IP.

Vous pouvez afficher la topologie des sites source et miroir, ainsi que le médiateur, le cas échéant, utilisé pour la connexion. Vous pouvez consulter les informations suivantes :

- Connectivité entre les sites
- Problèmes de santé et de disponibilité, le cas échéant, sur les deux sites
- Problèmes liés au médiateur
- Problèmes liés à la réplication.



Les statuts suivants sont signalés : Critique (❌), Erreur (⚠️), ou Normal (✅). Vous pouvez également afficher l'état de réplication des données agrégées des données principales et miroir dans la même topologie.

Dans le diagramme suivant, vous pouvez voir que la connectivité intersite entre les clusters source et de destination n'est pas disponible et que le médiateur entre eux n'est pas configuré.



4. Cliquez sur l'icône d'état. Un message avec la définition de l'erreur s'affiche. Si un événement a été déclenché pour le problème dans votre configuration MetroCluster sur IP, vous pouvez cliquer sur le bouton **Afficher l'événement** dans le message et afficher les détails de l'événement. Lorsque vous avez

résolu le problème et l'événement, l'icône d'état dans cette topologie devient normale (✓).

5. Vous pouvez afficher d'autres détails de configuration dans les sections * Présentation de MetroCluster * et * Protection* de l'onglet * Configuration * de la page de détails * Cluster / Santé *.



Uniquement pour une configuration MetroCluster sur IP, vous pouvez visualiser la topologie du cluster sur la page **Clusters**. Pour les clusters dans une configuration MetroCluster sur FC, la topologie est affichée dans l'onglet * MetroCluster Connectivity* sur la page de détails **Cluster / Health**.

Informations connexes

- ["Page de détails sur les clusters/la santé"](#)
- Pour plus d'informations sur la vue **Relationship: MetroCluster**, voir ["Surveiller les configurations de MetroCluster"](#) .
- Pour plus d'informations sur la vue **Relation : Statut de transfert du dernier mois**, voir ["Relation : Affichage du statut de transfert du dernier mois"](#) .
- Pour plus d'informations sur la vue **Relation : Taux de transfert du dernier mois**, voir ["Relation : Taux de transfert du dernier mois"](#) .
- Pour plus d'informations sur la vue **Relation : Toutes les relations**, voir ["Relation : vue Toutes les relations"](#) .

Surveiller la réplication de MetroCluster

Vous pouvez surveiller et diagnostiquer l'état de santé général des connexions logiques tout en mettant en miroir les données. Vous pouvez identifier les problèmes ou tout risque qui interrompt la mise en miroir des composants du cluster tels que les agrégats, les nœuds et les machines virtuelles de stockage.

Unified Manager utilise des alertes d'état du système pour surveiller l'état des composants et la connectivité dans la configuration MetroCluster .

Avant de commencer

Les clusters locaux et distants de la configuration MetroCluster doivent être ajoutés à Unified Manager

Afficher la réplication pour les configurations MetroCluster sur IP

Pour les configurations MetroCluster sur IP, l'état de réplication des données s'affiche dans la vue d'aperçu de la topologie d'un cluster protégé par MetroCluster sur IP à partir des vues suivantes du volet de navigation gauche d'Unified Manager :

- **Stockage > Clusters > Protection : MetroCluster** vue
- **Protection > Relations > Relation : MetroCluster** vue

Pour plus d'informations, voir ["Surveiller les problèmes de connectivité dans MetroCluster sur IP"](#) .

Afficher la réplication pour les configurations MetroCluster sur FC

Suivez ces étapes pour déterminer les problèmes de réplication des données pour la configuration MetroCluster sur FC.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.

Une liste des clusters surveillés s'affiche.

2. Dans la vue **Santé : tous les clusters**, cliquez sur le nom du cluster pour lequel vous souhaitez afficher les détails de réplication MetroCluster . Sur la page **Détails du cluster / de l'état de santé**, cliquez sur l'onglet ***Réplication MetroCluster ***.

La topologie de la configuration MetroCluster à répliquer est affichée sur le site local dans la zone d'objet de cluster correspondante avec les informations sur le site distant où les données sont mises en miroir. Si vous déplacez le pointeur sur l'icône, vous pouvez afficher des informations détaillées sur l'événement généré.

Vous pouvez utiliser les informations affichées dans la page Détails du cluster/de l'état de santé pour corriger tout problème de réplication. Si vous découvrez des problèmes de mise en miroir dans votre configuration MetroCluster , vous devez vous connecter à System Manager ou accéder à l'interface de ligne de commande ONTAP pour résoudre les problèmes.

Informations connexes

["Page de détails sur les clusters/la santé"](#)

Gérer les quotas

Vous pouvez utiliser des quotas d'utilisateur et de groupe pour limiter la quantité d'espace disque ou le nombre de fichiers qu'un utilisateur ou un groupe d'utilisateurs peut utiliser. Vous pouvez afficher les informations sur les quotas des utilisateurs et des groupes d'utilisateurs, telles que l'utilisation du disque et des fichiers et les différentes limites définies sur les disques.

Quelles sont les limites de quota

Les limites de quota utilisateur sont des valeurs que le serveur Unified Manager utilise pour évaluer si la consommation d'espace par un utilisateur approche de la limite ou a atteint la limite définie par le quota de l'utilisateur. Si la limite souple est dépassée ou si la limite dure est atteinte, le serveur Unified Manager génère des événements de quota utilisateur.

Par défaut, le serveur Unified Manager envoie un e-mail de notification aux utilisateurs qui ont dépassé la limite souple du quota ou ont atteint la limite stricte du quota et pour lesquels des événements de quota utilisateur sont configurés. Les utilisateurs disposant du rôle Administrateur d'applications peuvent configurer des alertes qui notifient les destinataires spécifiés des événements de quota d'utilisateur ou de groupe d'utilisateurs.

Vous pouvez spécifier des limites de quota à l'aide d' ONTAP System Manager ou de l'interface de ligne de commande ONTAP .

Afficher les quotas des utilisateurs et des groupes d'utilisateurs

La page Détails de la machine virtuelle de stockage / Santé affiche des informations sur les quotas d'utilisateur et de groupe d'utilisateurs configurés sur la SVM. Vous pouvez afficher le nom de l'utilisateur ou du groupe d'utilisateurs, les limites définies sur les disques et les fichiers, l'espace disque et l'espace fichier utilisés, ainsi que l'adresse e-mail pour la notification.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.
2. Dans la vue **Santé : toutes les machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, puis cliquez sur l'onglet **Quotas d'utilisateur et de groupe**.

Informations connexes

["Ajout d'utilisateurs"](#)

Créer des règles pour générer des adresses e-mail

Vous pouvez créer des règles pour spécifier l'adresse e-mail en fonction du quota d'utilisateur associé aux clusters, aux machines virtuelles de stockage (SVM), aux volumes, aux qtrees, aux utilisateurs ou aux groupes d'utilisateurs. Une notification est envoyée à l'adresse e-mail spécifiée en cas de dépassement de quota.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir consulté les directives de la page Règles pour générer des adresses e-mail de quota d'utilisateur et de groupe.

Vous devez définir les règles pour les adresses e-mail de quota et les saisir dans l'ordre dans lequel vous souhaitez les exécuter. Par exemple, si vous souhaitez utiliser l'adresse e-mail abc@xyz.com pour recevoir des notifications sur les dépassements de quota pour abc et utiliser l'adresse e-mail `dl-$GROUP@$DOMAIN` pour tous les autres groupes, les règles doivent être répertoriées dans l'ordre suivant :

- si (`$USER == 'abc'`) alors abc@xyz.com
- si (`$GROUP == *`) alors `dl-$GROUP@$DOMAIN`

Si aucun des critères des règles que vous avez spécifiées n'est rempli, la règle par défaut est utilisée :

si (`$USER_OR_GROUP == *`) alors `$USER_OR_GROUP@$DOMAIN`

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Règles de quotas de courrier électronique**.
2. Saisissez la règle en fonction de vos critères.
3. Cliquez sur **Valider** pour valider la syntaxe de la règle.

Un message d'erreur s'affiche si la syntaxe de la règle est incorrecte. Vous devez corriger la syntaxe et cliquer à nouveau sur **Valider**.

4. Cliquez sur **Enregistrer**.
5. Vérifiez que l'adresse e-mail que vous avez créée s'affiche dans l'onglet **Quotas d'utilisateur et de groupe** de la page de détails **VM / Santé** de stockage.

Créer un format de notification par e-mail pour les quotas d'utilisateurs et de groupes d'utilisateurs

Vous pouvez créer un format de notification pour les e-mails envoyés à un utilisateur ou à un groupe d'utilisateurs en cas de problème lié au quota (limite souple dépassée ou limite stricte atteinte).

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Format de courrier électronique de quota**.
2. Saisissez ou modifiez les détails dans les champs **De**, **Objet** et **Détails de l'e-mail**.
3. Cliquez sur **Aperçu** pour prévisualiser la notification par e-mail.
4. Cliquez sur **Fermer** pour fermer la fenêtre d'aperçu.
5. Modifiez le contenu de la notification par e-mail, si nécessaire.
6. Cliquez sur **Enregistrer**.

Modifier les adresses e-mail des quotas d'utilisateur et de groupe

Vous pouvez modifier les adresses e-mail en fonction du quota d'utilisateurs associé aux clusters, aux machines virtuelles de stockage (SVM), aux volumes, aux qtrees, aux utilisateurs ou aux groupes d'utilisateurs. Vous pouvez modifier l'adresse e-mail lorsque vous souhaitez remplacer l'adresse e-mail générée par les règles spécifiées dans la boîte de dialogue Règles pour générer l'adresse e-mail du quota d'utilisateur et de groupe.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir examiné le ["lignes directrices pour la création de règles"](#).

Si vous modifiez une adresse e-mail, les règles de génération des adresses e-mail de quota d'utilisateur et de groupe ne s'appliquent plus au quota. Pour que les notifications soient envoyées à l'adresse e-mail générée par les règles spécifiées, vous devez supprimer l'adresse e-mail et enregistrer la modification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > SVM**.
2. Dans la vue **Santé : toutes les machines virtuelles de stockage**, sélectionnez une SVM, puis cliquez sur l'onglet **Quotas d'utilisateur et de groupe**.
3. Cliquez sur **Modifier l'adresse e-mail** sous la rangée d'onglets.

4. Dans la boîte de dialogue **Modifier l'adresse e-mail**, effectuez l'action appropriée :

Si...	Alors...
Vous souhaitez que les notifications soient envoyées à l'adresse e-mail générée par les règles spécifiées	a. Supprimez l'adresse e-mail dans le champ Adresse e-mail. b. Cliquez sur Enregistrer. c. Actualisez le navigateur en appuyant sur F5 pour recharger la boîte de dialogue Modifier l'adresse e-mail. L'adresse e-mail générée par la règle spécifiée s'affiche dans le champ Adresse e-mail.
Vous souhaitez que les notifications soient envoyées à une adresse e-mail spécifiée	a. Modifiez l'adresse e-mail dans le champ Adresse e-mail. b. Cliquez sur Enregistrer. Les règles de génération des adresses e-mail des quotas d'utilisateurs et de groupes ne sont plus applicables au quota.

En savoir plus sur les quotas

Comprendre les concepts liés aux quotas vous aide à gérer efficacement vos quotas d'utilisateurs et de groupes d'utilisateurs.

Aperçu du processus de quotas

Les quotas peuvent être souples ou stricts. Les quotas souples obligent ONTAP à envoyer une notification lorsque les limites spécifiées sont dépassées, et les quotas stricts empêchent une opération d'écriture de réussir lorsque les limites spécifiées sont dépassées.

Lorsque ONTAP reçoit une demande d'un utilisateur ou d'un groupe d'utilisateurs pour écrire sur un FlexVol volume, il vérifie si les quotas sont activés sur ce volume pour l'utilisateur ou le groupe d'utilisateurs et détermine les éléments suivants :

- La limite stricte sera-t-elle atteinte ?

Si oui, l'opération d'écriture échoue lorsque la limite stricte est atteinte et la notification de quota strict est envoyée.

- La limite souple sera-t-elle dépassée ?

Si oui, l'opération d'écriture réussit lorsque la limite souple est dépassée et la notification de quota souple est envoyée.

- Si une opération d'écriture ne dépassera pas la limite souple

Si oui, l'opération d'écriture réussit et aucune notification n'est envoyée.

À propos des quotas

Les quotas permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree. Vous spécifiez les quotas en utilisant le `/etc/quotas` déposer. Les quotas sont appliqués à un volume ou à un qtree spécifique.

Pourquoi utiliser des quotas

Vous pouvez utiliser des quotas pour limiter l'utilisation des ressources dans les volumes FlexVol , pour fournir une notification lorsque l'utilisation des ressources atteint des niveaux spécifiques ou pour suivre l'utilisation des ressources.

Vous spécifiez un quota pour les raisons suivantes :

- Pour limiter la quantité d'espace disque ou le nombre de fichiers pouvant être utilisés par un utilisateur ou un groupe, ou pouvant être contenus par un qtree
- Pour suivre la quantité d'espace disque ou le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree, sans imposer de limite
- Pour avertir les utilisateurs lorsque leur utilisation du disque ou des fichiers est élevée

Description des boîtes de dialogue des quotas

Vous pouvez utiliser l'option appropriée dans l'onglet Quotas d'utilisateur et de groupe dans la vue Intégrité : toutes les machines virtuelles de stockage pour configurer le format de la notification par e-mail envoyée lorsqu'un problème lié aux quotas se produit et pour configurer des règles afin de spécifier les adresses e-mail en fonction du quota utilisateur.

Page de format de notification par e-mail

La page Format de notification par e-mail affiche les règles de l'e-mail envoyé à un utilisateur ou à un groupe d'utilisateurs en cas de problème lié au quota (limite souple dépassée ou limite stricte atteinte).

La notification par courrier électronique est envoyée uniquement lorsque les événements de quota d'utilisateur ou de groupe d'utilisateurs suivants sont générés : limite logicielle d'espace disque de quota d'utilisateur ou de groupe dépassée, limite logicielle de nombre de fichiers de quota d'utilisateur ou de groupe dépassée, limite stricte d'espace disque de quota d'utilisateur ou de groupe atteinte ou limite stricte de nombre de fichiers de quota d'utilisateur ou de groupe atteinte.

- **Depuis**

Affiche l'adresse e-mail à partir de laquelle l'e-mail est envoyé, que vous pouvez modifier. Par défaut, il s'agit de l'adresse e-mail spécifiée sur la page Notifications.

- **Sujet**

Affiche l'objet de l'e-mail de notification.

- **Détails de l'e-mail**

Affiche le texte de l'e-mail de notification. Vous pouvez modifier le texte en fonction de vos besoins. Par exemple, vous pouvez fournir des informations liées aux attributs de quota et réduire le nombre de mots-clés. Cependant, vous ne devez pas modifier les mots-clés.

Les mots clés valides sont les suivants :

- **\$EVENT_NAME**

Spécifie le nom de l'événement qui a provoqué la notification par e-mail.

- **\$QUOTA_TARGET**

Spécifie le qtree ou le volume sur lequel le quota est applicable.

- **\$QUOTA_USED_PERCENT**

Spécifie le pourcentage de limite matérielle du disque, de limite logicielle du disque, de limite matérielle du fichier ou de limite logicielle du fichier utilisé par l'utilisateur ou le groupe d'utilisateurs.

- **\$QUOTA_LIMIT**

Spécifie la limite matérielle du disque ou la limite matérielle du fichier atteinte par l'utilisateur ou le groupe d'utilisateurs et l'un des événements suivants est généré :

- Limite d'espace disque du quota utilisateur ou groupe atteinte
- Limite logicielle d'espace disque du quota utilisateur ou groupe atteinte
- Limite stricte du nombre de fichiers du quota utilisateur ou groupe atteinte
- Limite logicielle du nombre de fichiers du quota utilisateur ou groupe atteinte

- **\$QUOTA_USED**

Spécifie l'espace disque utilisé ou le nombre de fichiers créés par l'utilisateur ou le groupe d'utilisateurs.

- **\$QUOTA_USER**

Spécifie le nom de l'utilisateur ou du groupe d'utilisateurs.

Boutons de commande

Les boutons de commande vous permettent de prévisualiser, d'enregistrer ou d'annuler les modifications apportées au format de notification par e-mail :

- **Aperçu**

Affiche un aperçu de l'e-mail de notification.

- **Restaurer les paramètres d'usine**

Vous permet de restaurer le format de notification aux valeurs par défaut d'usine.

- **Sauvegarder**

Enregistre les modifications apportées au format de notification.

Page Règles pour générer des adresses e-mail de quota d'utilisateur et de groupe

La page Règles pour générer des adresses e-mail de quota d'utilisateur et de groupe vous permet de créer des règles pour spécifier des adresses e-mail en fonction du quota d'utilisateur associé aux clusters, aux SVM, aux volumes, aux qtrees, aux utilisateurs ou aux groupes d'utilisateurs. Une notification est envoyée à l'adresse e-mail spécifiée lorsqu'un quota est dépassé.

Zone des règles

Vous devez définir les règles pour une adresse e-mail de quota. Vous pouvez également ajouter des commentaires pour expliquer les règles.

Comment vous définissez les règles

Vous devez saisir les règles dans l'ordre dans lequel vous souhaitez les exécuter. Si le critère de la première règle est rempli, l'adresse e-mail est générée sur la base de cette règle. Si le critère n'est pas rempli, le critère de la règle suivante est pris en compte, et ainsi de suite. Chaque ligne répertorie une règle distincte. La règle par défaut est la dernière règle de la liste. Vous pouvez modifier l'ordre de priorité des règles. Cependant, vous ne pouvez pas modifier l'ordre de la règle par défaut.

Par exemple, si vous souhaitez utiliser l'adresse e-mail qtree1@xyz.com pour recevoir des notifications sur les dépassements de quota pour qtree1 et utiliser l'adresse e-mail admin@xyz.com pour tous les autres qtrees, les règles doivent être répertoriées dans l'ordre suivant :

- si (\$QTREE == 'qtree1') alors qtree1@xyz.com
- si (\$QTREE == *) alors admin@xyz.com

Si aucun des critères des règles que vous avez spécifiées n'est rempli, la règle par défaut est utilisée :

```
si ( $USER_OR_GROUP == * ) alors $USER_OR_GROUP@$DOMAIN
```

Si plusieurs utilisateurs ont le même quota, les noms des utilisateurs sont affichés sous forme de valeurs séparées par des virgules et les règles ne sont pas applicables au quota.

Comment ajouter des commentaires

Vous pouvez ajouter des commentaires pour expliquer les règles. Vous devez utiliser # au début de chaque commentaire et chaque ligne répertorie un commentaire distinct.

Syntaxe des règles

La syntaxe de la règle doit être l'une des suivantes :

- si (valid variableoperator *) alors email ID@domain name

if est un mot-clé et est en minuscules. L'opérateur est ==. L'ID de messagerie peut contenir n'importe quel caractère, les variables valides \$USER_OR_GROUP, \$USER ou \$GROUP, ou une combinaison de n'importe quel caractère et des variables valides \$USER_OR_GROUP, \$USER ou \$GROUP. Le nom de domaine peut contenir n'importe quel caractère, la variable valide \$DOMAIN ou une combinaison de n'importe quel caractère et de la variable valide \$DOMAIN. Les variables valides peuvent être en

majuscules ou en minuscules, mais ne doivent pas être une combinaison des deux. Par exemple, \$domain et \$DOMAIN sont valides, mais \$Domain n'est pas une variable valide.

- `si ( valid variableoperator `string` ) alors email ID@domain name`

if est un mot-clé et est en minuscule. L'opérateur peut être contient ou ==. L'ID de messagerie peut contenir n'importe quel caractère, les variables valides \$USER_OR_GROUP, \$USER ou \$GROUP, ou une combinaison de n'importe quel caractère et des variables valides \$USER_OR_GROUP, \$USER ou \$GROUP. Le nom de domaine peut contenir n'importe quel caractère, la variable valide \$DOMAIN ou une combinaison de n'importe quel caractère et de la variable valide \$DOMAIN. Les variables valides peuvent être en majuscules ou en minuscules, mais ne doivent pas être une combinaison des deux. Par exemple, \$domain et \$DOMAIN sont valides, mais \$Domain n'est pas une variable valide.

Boutons de commande

Les boutons de commande permettent de sauvegarder, valider ou annuler les règles créées :

- **Valider**

Valide la syntaxe de la règle créée. S'il y a des erreurs lors de la validation, la règle qui génère l'erreur s'affiche avec un message d'erreur.

- **Restaurer les paramètres d'usine**

Vous permet de restaurer les règles d'adresse aux valeurs par défaut d'usine.

- **Sauvegarder**

Valide la syntaxe de la règle et enregistre la règle s'il n'y a pas d'erreurs. S'il y a des erreurs lors de la validation, la règle qui génère l'erreur s'affiche avec un message d'erreur.

Dépannage

Les informations de dépannage vous aident à identifier et à résoudre les problèmes que vous rencontrez lors de l'utilisation d'Unified Manager.

Ajouter de l'espace disque au répertoire de la base de données Unified Manager

Le répertoire de la base de données Unified Manager contient toutes les données de santé et de performances collectées à partir des systèmes ONTAP . Certaines circonstances peuvent nécessiter d'augmenter la taille du répertoire de base de données.

Par exemple, le répertoire de base de données peut être plein si Unified Manager collecte des données à partir d'un grand nombre de clusters où chaque cluster comporte de nombreux nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de base de données sera rempli à 90 % et un événement critique lorsque le répertoire sera rempli à 95 %.



Aucune donnée supplémentaire n'est collectée à partir des clusters une fois que le répertoire atteint 95 % de remplissage.

Les étapes requises pour ajouter de la capacité au répertoire de données sont différentes selon qu'Unified Manager s'exécute sur un serveur VMware ESXi, sur un serveur Red Hat Linux ou sur un serveur Microsoft

Windows.

Ajouter de l'espace au disque de données de la machine virtuelle VMware

Si vous devez augmenter la quantité d'espace sur le disque de données pour la base de données Unified Manager, vous pouvez ajouter de la capacité après l'installation en augmentant l'espace disque à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez avoir accès au client vSphere.
- La machine virtuelle ne doit avoir aucun snapshot stocké localement.
- Vous devez disposer des informations d'identification de l'utilisateur de maintenance.

Nous vous recommandons de sauvegarder votre machine virtuelle avant d'augmenter la taille des disques virtuels.

Étapes

1. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis ajoutez davantage de capacité de disque aux données `disk 3`. Consultez la documentation VMware pour plus de détails.

Dans certains cas rares, le déploiement d'Unified Manager utilise « Disque dur 2 » pour le disque de données au lieu de « Disque dur 3 ». Si cela se produit lors de votre déploiement, augmentez l'espace du disque le plus grand. Le disque de données aura toujours plus d'espace que l'autre disque.

2. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis sélectionnez l'onglet **Console**.
3. Cliquez dans la fenêtre de la console, puis connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Dans le **Menu principal**, entrez le numéro de l'option **Configuration système**.
5. Dans le **Menu de configuration système**, entrez le numéro de l'option **Augmenter la taille du disque de données**.

Ajouter de l'espace au répertoire de données de l'hôte Linux

Si vous n'avez pas alloué suffisamment d'espace disque au `/opt/netapp/data` répertoire pour prendre en charge Unified Manager lorsque vous avez initialement configuré l'hôte Linux, puis installé Unified Manager, vous pouvez ajouter de l'espace disque après l'installation en augmentant l'espace disque sur le `/opt/netapp/data` annuaire.

Avant de commencer

Vous devez disposer d'un accès utilisateur root à la machine Red Hat Enterprise Linux sur laquelle Unified Manager est installé.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'augmenter la taille du répertoire de données.

Étapes

1. Connectez-vous en tant qu'utilisateur root à la machine Linux sur laquelle vous souhaitez ajouter de l'espace disque.

2. Arrêtez le service Unified Manager et le logiciel MySQL associé dans l'ordre indiqué : `systemctl stop ocieau ocie mysqld`
3. Créez un dossier de sauvegarde temporaire (par exemple, `/backup-data`) avec suffisamment d'espace disque pour contenir les données dans le `/opt/netapp/data` annuaire.
4. Copiez le contenu et la configuration des privilèges de l'existant `/opt/netapp/data` répertoire vers le répertoire des données de sauvegarde :

```
cp -arp /opt/netapp/data/* /backup-data
```

5. Si SE Linux est activé :

- a. Obtenir le type SE Linux pour les dossiers existants `/opt/netapp/data` dossier:

```
se_type=`ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' | head -1
```

Le système renvoie une confirmation similaire à la suivante :

```
echo $se_type
mysqld_db_t
```

- a. Exécutez le `chcon` commande pour définir le type SE Linux pour le répertoire de sauvegarde :

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Retirez le contenu du `/opt/netapp/data` annuaire:

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. Augmenter la taille du `/opt/netapp/data` répertoire à un minimum de 150 Go via des commandes LVM ou en ajoutant des disques supplémentaires.



Si vous avez créé `/opt/netapp/data` à partir d'un disque, vous ne devriez pas essayer de monter `/opt/netapp/data` en tant que partage NFS ou CIFS. Car, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` pourrait ne pas fonctionner comme prévu.

8. Confirmez que le `/opt/netapp/data` le propriétaire du répertoire (`mysql`) et le groupe (`root`) restent inchangés :

```
ls -ltr /opt/netapp/ | grep data
```

Le système renvoie une confirmation similaire à la suivante :

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

9. Si SE Linux est activé, confirmez que le contexte du `/opt/netapp/data` le répertoire est toujours défini

sur `mysqld_db_t` :

- a. `touch /opt/netapp/data/abc`
- b. `ls -Z /opt/netapp/data/abc`

Le système renvoie une confirmation similaire à la suivante :

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Supprimer le fichier `abc` afin que ce fichier étranger ne provoque pas d'erreur de base de données à l'avenir.
11. Copiez le contenu de `backup-data` retour à l'extension `/opt/netapp/data` annuaire:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Si SE Linux est activé, exécutez la commande suivante :

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Démarrez le service MySQL :

```
systemctl start mysqld
```

14. Une fois le service MySQL démarré, démarrez les services `ocie` et `ocieau` dans l'ordre indiqué :

```
systemctl start ocie ocieau
```

15. Une fois tous les services démarrés, supprimez le dossier de sauvegarde `/backup-data` :

```
rm -rf /backup-data
```

Ajouter de l'espace au lecteur logique du serveur Microsoft Windows

Si vous devez augmenter la quantité d'espace disque pour la base de données Unified Manager, vous pouvez ajouter de la capacité au lecteur logique sur lequel Unified Manager est installé.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'ajouter de l'espace disque.

Étapes

1. Connectez-vous en tant qu'administrateur au serveur Windows sur lequel vous souhaitez ajouter de l'espace disque.
2. Suivez l'étape qui correspond à la méthode que vous souhaitez utiliser pour ajouter plus d'espace :

Option	Description
Sur un serveur physique, ajoutez de la capacité au lecteur logique sur lequel le serveur Unified Manager est installé.	Suivez les étapes décrites dans la rubrique Microsoft : "Étendre un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes décrites dans la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes décrites dans la rubrique VMware : "Augmenter la taille d'une partition de disque"

Modifier l'intervalle de collecte des statistiques de performances

L'intervalle de collecte par défaut pour les statistiques de performances est de 5 minutes. Vous pouvez modifier cet intervalle à 10 ou 15 minutes si vous constatez que les collectes de grands clusters ne se terminent pas dans le délai par défaut. Ce paramètre affecte la collecte de statistiques de tous les clusters surveillés par cette instance d'Unified Manager.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

Le problème des collectes de statistiques de performance qui ne se terminent pas à temps est indiqué par les messages de bannière `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

Vous ne devez modifier l'intervalle de collecte que lorsque cela est nécessaire en raison d'un problème de collecte de statistiques. Ne modifiez pas ce paramètre pour une autre raison.



La modification de cette valeur par rapport au paramètre par défaut de 5 minutes peut affecter le nombre et la fréquence des événements de performances signalés par Unified Manager. Par exemple, les seuils de performances définis par le système déclenchent des événements lorsque la politique est dépassée pendant 30 minutes. Lors de l'utilisation de collectes de 5 minutes, la politique doit être dépassée pendant six collectes consécutives. Pour les collectes de 15 minutes, la politique doit être dépassée pendant seulement deux périodes de collecte.

Un message au bas de la page Configuration du cluster indique l'intervalle de collecte de données statistiques actuel.

Étapes

1. Connectez-vous à l'aide de SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

Les invites de la console de maintenance d'Unified Manager s'affichent.

2. Tapez le numéro de l'option de menu intitulée **Configuration de l'intervalle d'interrogation des performances**, puis appuyez sur Entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe de l'utilisateur de maintenance.
4. Tapez le numéro du nouvel intervalle d'interrogation que vous souhaitez définir, puis appuyez sur Entrée.

Si vous avez modifié l'intervalle de collecte d'Unified Manager à 10 ou 15 minutes et que vous disposez d'une connexion actuelle à un fournisseur de données externe (tel que Graphite), vous devez modifier l'intervalle de transmission du fournisseur de données afin qu'il soit égal ou supérieur à l'intervalle de collecte d'Unified Manager.

Modifier la durée pendant laquelle Unified Manager conserve les données d'événements et de performances

Par défaut, Unified Manager stocke les données d'événement et les données de performances pendant 6 mois pour tous les clusters surveillés. Après ce délai, les données plus anciennes sont automatiquement supprimées pour faire place aux nouvelles données. Ce délai par défaut fonctionne bien pour la plupart des configurations, mais les configurations très volumineuses avec de nombreux clusters et nœuds peuvent nécessiter de réduire la période de rétention afin qu'Unified Manager fonctionne de manière optimale.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Vous pouvez modifier les périodes de conservation de ces deux types de données dans la page Conservation des données. Ces paramètres affectent la conservation des données de tous les clusters surveillés par cette instance d'Unified Manager.



Unified Manager collecte des statistiques de performances toutes les 5 minutes. Chaque jour, les statistiques de 5 minutes sont résumées en statistiques de performance horaires. Il conserve 30 jours de données de performances historiques de 5 minutes et 6 mois de données de performances résumées toutes les heures (par défaut).

Vous ne devez réduire la période de conservation que si vous manquez d'espace ou si la sauvegarde et d'autres opérations prennent beaucoup de temps. La réduction de la durée de conservation a les effets suivants :

- Les anciennes données de performances sont supprimées de la base de données Unified Manager après minuit.
- Les anciennes données d'événement sont immédiatement supprimées de la base de données Unified Manager.
- Les événements antérieurs à la période de conservation ne seront plus disponibles à la visualisation dans l'interface utilisateur.
- Les emplacements dans l'interface utilisateur où les statistiques de performances horaires sont affichées seront vides avant la période de conservation.
- Si la période de conservation des événements dépasse la période de conservation des données de performances, un message s'affiche sous le curseur de performances, avertissant que les événements de performances plus anciens peuvent ne pas avoir de données de sauvegarde dans leurs graphiques associés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Politiques > Conservation des données**.
2. Dans la page **Conservation des données**, sélectionnez l'outil curseur dans la zone Conservation des événements ou Conservation des données de performances et déplacez-le sur le nombre de mois pendant lesquels les données doivent être conservées, puis cliquez sur **Enregistrer**.

Erreur d'authentification inconnue

Lorsque vous effectuez une opération liée à l'authentification, telle que l'ajout, la modification, la suppression ou le test d'utilisateurs ou de groupes distants, le message d'erreur suivant peut s'afficher : `Unknown authentication error`.

Cause

Ce problème peut se produire si vous avez défini une valeur incorrecte pour les options suivantes :

- Nom de l'administrateur du service d'authentification Active Directory
- Lier le nom distinctif du service d'authentification OpenLDAP

Mesure corrective

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. En fonction du service d'authentification que vous avez sélectionné, saisissez les informations appropriées pour le nom de l'administrateur ou le nom distinctif de liaison.
3. Cliquez sur **Tester l'authentification** pour tester l'authentification avec les détails que vous avez spécifiés.
4. Cliquez sur **Enregistrer**.

Utilisateur non trouvé

Lorsque vous effectuez une opération liée à l'authentification, telle que l'ajout, la modification, la suppression ou le test d'utilisateurs ou de groupes distants, le message d'erreur suivant s'affiche : `User not found`.

Cause

Ce problème peut se produire si l'utilisateur existe sur le serveur AD ou le serveur LDAP et si vous avez défini le nom distinctif de base sur une valeur incorrecte.

Mesure corrective

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Saisissez les informations appropriées pour le nom distinctif de base.
3. Cliquez sur **Enregistrer**.

Problème lors de l'ajout de LDAP à l'aide d'autres services d'authentification

Lorsque vous sélectionnez Autres comme service d'authentification, la classe d'objet utilisateur et groupe conserve les valeurs du modèle précédemment sélectionné. Si le

serveur LDAP n'utilise pas les mêmes valeurs, l'opération peut échouer.

Cause

Les utilisateurs ne sont pas configurés correctement dans OpenLDAP.

Mesure corrective

Vous pouvez résoudre manuellement ce problème en utilisant l'une des solutions de contournement suivantes.

Si votre classe d'objet utilisateur LDAP et votre classe d'objet groupe sont respectivement utilisateur et groupe, procédez comme suit :

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Dans le menu déroulant **Service d'authentification**, sélectionnez **Active Directory**, puis **Autres**.
3. Remplissez les champs de texte.

Si votre classe d'objet utilisateur LDAP et votre classe d'objet groupe sont respectivement posixAccount et posixGroup, procédez comme suit :

1. Dans le volet de navigation de gauche, cliquez sur **Général > Authentification à distance**.
2. Dans le menu déroulant **Service d'authentification**, sélectionnez **OpenLDAP**, puis sélectionnez **Autres**.
3. Remplissez les champs de texte.

Si les deux premières solutions de contournement ne s'appliquent pas, appelez le `option-set API` et définissez le `auth.ldap.userObjectClass` et `auth.ldap.groupObjectClass` options aux valeurs correctes.

Problème de rotation des journaux du SDK NetApp Manageability sur les systèmes Windows

Après avoir ajouté un cluster basé sur l'API ONTAPI à Unified Manager sur un système d'exploitation Windows, le `nmsdk.log` la taille du fichier augmente et dépasse la limite de 10 Mo.

Cause

Ce problème peut se produire si la rotation des journaux n'a pas lieu.

Mesure corrective

1. Arrêtez Unified Manager.
2. Lorsque vous installez Unified Manager sur Windows, installez Logrotate version 0.0.0.18. Pour plus d'informations, consultez le ["Guide de renforcement de la sécurité pour le rapport technique NetApp Manageability SDK"](#).
3. Démarrez Unified Manager.

Gérer les événements et les alertes

Gérer les événements

Les événements vous aident à identifier les problèmes dans les clusters surveillés.

Quels sont les événements de la plateforme Active IQ

Unified Manager peut afficher les événements qui ont été découverts par la plateforme Active IQ . Ces événements sont créés en exécutant un ensemble de règles sur les messages AutoSupport générés à partir de tous les systèmes de stockage surveillés par Unified Manager.

Pour plus d'informations, voir ["Comment les événements de la plateforme Active IQ sont générés"](#).

Unified Manager recherche automatiquement un nouveau fichier de règles et télécharge un nouveau fichier uniquement lorsqu'il existe des règles plus récentes. Sur les sites sans accès réseau externe, vous devez télécharger les règles manuellement depuis **Gestion du stockage > Configuration des événements > Règles de téléchargement**.

Ces événements Active IQ ne chevauchent pas les événements Unified Manager existants et identifient les incidents ou les risques concernant la configuration du système, le câblage, les meilleures pratiques et les problèmes de disponibilité.

Pour plus d'informations sur l'activation des événements de plateforme, voir ["Activation des événements du portail Active IQ"](#) . Pour plus d'informations sur le téléchargement du fichier de règles, voir ["Téléchargement d'un nouveau fichier de règles Active IQ"](#) .

NetApp Active IQ est un service basé sur le cloud qui fournit des analyses prédictives et un support proactif pour optimiser les opérations du système de stockage dans le cloud hybride NetApp . Voir ["NetApp Active IQ"](#) pour plus d'informations.

Quels sont les événements du système de gestion des événements ?

Le système de gestion des événements (EMS) collecte les données d'événements provenant de différentes parties du noyau ONTAP et fournit des mécanismes de transfert d'événements. Ces événements ONTAP peuvent être signalés comme événements EMS dans Unified Manager. La surveillance et la gestion centralisées facilitent la configuration des événements EMS critiques et des notifications d'alerte basées sur ces événements EMS.

L'adresse Unified Manager est ajoutée comme destination de notification au cluster lorsque vous ajoutez le cluster à Unified Manager. Un événement EMS est signalé dès que l'événement se produit dans le cluster.

Il existe deux méthodes pour recevoir des événements EMS dans Unified Manager :

- Un certain nombre d'événements EMS importants sont signalés automatiquement.
- Vous pouvez vous abonner pour recevoir des événements EMS individuels.

Les événements EMS générés par Unified Manager sont signalés différemment selon la méthode par laquelle

l'événement a été généré :

Fonctionnalité	Messages EMS automatiques	Messages EMS abonnés
Événements EMS disponibles	Sous-ensemble d'événements EMS	Tous les événements EMS
Nom du message EMS lorsqu'il est déclenché	Nom de l'événement Unified Manager (converti à partir du nom de l'événement EMS)	Non spécifique au format « Erreur EMS reçue ». Le message détaillé fournit le format de notation par points de l'événement EMS réel
Messages reçus	Dès que le cluster a été découvert	Après avoir ajouté chaque événement EMS requis à Unified Manager et après le cycle d'interrogation suivant de 15 minutes
Cycle de vie de l'événement	Identique aux autres événements Unified Manager : états Nouveau, Reconnu, Résolu et Obsolète	L'événement EMS devient obsolète après l'actualisation du cluster, après 15 minutes, à compter de la création de l'événement
Capture les événements pendant les temps d'arrêt d'Unified Manager	Oui, lorsque le système démarre, il communique avec chaque cluster pour acquérir les événements manquants	Non
Détails de l'événement	Les actions correctives suggérées sont importées directement depuis ONTAP pour fournir des résolutions cohérentes	Les actions correctives ne sont pas disponibles dans la page Détails de l'événement



Certains des nouveaux événements EMS automatiques sont des événements informatifs qui indiquent qu'un événement précédent a été résolu. Par exemple, l'événement d'information « Statut de l'espace des constituants du FlexGroup : tout est OK » indique que l'événement d'erreur « Les constituants du FlexGroup ont des problèmes d'espace » a été résolu. Les événements d'information ne peuvent pas être gérés à l'aide du même cycle de vie d'événement que les autres types de gravité d'événement. Cependant, l'événement devient automatiquement obsolète si le même volume reçoit un autre événement d'erreur « Problèmes d'espace ».

Événements EMS ajoutés automatiquement à Unified Manager

Les événements ONTAP EMS suivants sont ajoutés automatiquement à Unified Manager. Ces événements seront générés lorsqu'ils seront déclenchés sur n'importe quel cluster surveillé par Unified Manager.

Les événements EMS suivants sont disponibles lors de la surveillance des clusters exécutant le logiciel ONTAP 9.5 ou supérieur :

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité du gestionnaire unifié
Accès au niveau cloud refusé pour la relocalisation d'agrégats	arl.netra.ca.check.failed	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation globale lors du basculement du stockage	gb.netra.ca.check.failed	Agrégat	Erreur
Resynchronisation de la réplication du miroir FabricPool terminée	wafl.ca.resync.complete	Cluster	Erreur
L'espace FabricPool est presque plein	fabricpool.presque.plein	Cluster	Erreur
Début de la période de grâce NVMe-oF	nvmf.graceperiod.start	Cluster	Avertissement
Période de grâce NVMe-oF active	nvmf.graceperiod.active	Cluster	Avertissement
Période de grâce NVMe-oF expirée	nvmf.graceperiod.expiré	Cluster	Avertissement
LUN détruit	lun.détruire	LUN	Information
Cloud AWS MetadataConnFail	cloud.aws.metadataConnFail	Nœud	Erreur
Cloud AWS IAMCredsExpiré	cloud.aws.iamCredsExpiré	Nœud	Erreur
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Nœud	Erreur
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Nœud	Erreur
Cloud AWS IAMCredsNonInitialisé	cloud.aws.iamNonInitialisé	Nœud	Information
Cloud AWS IAMRoleInvalide	cloud.aws.iamRoleInvalid	Nœud	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité du gestionnaire unifié
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Nœud	Erreur
Hôte Cloud Tier non résoluble	objstore.host.insoluble	Nœud	Erreur
Interface réseau intercluster Cloud Tier en panne	objstore.interclusterlifDown	Nœud	Erreur
Signature de niveau cloud non concordante pour les demandes	osc.signatureMismatch	Nœud	Erreur
L'un des pools NFSv4 est épuisé	Nblade.nfsV4PoolExhaust	Nœud	Primordial
Mémoire du moniteur QoS au maximum	qos.monitor.memory.maxed	Nœud	Erreur
Mémoire du moniteur QoS réduite	qos.monitor.memory.abated	Nœud	Information
NVMeNS Détruire	NVMeNS.détruire	Espace de noms	Information
NVMeNS en ligne	NVMeNS.hors ligne	Espace de noms	Information
NVMeNS hors ligne	NVMeNS.online	Espace de noms	Information
NVMeNS hors de l'espace	NVMeNS.hors.espace	Espace de noms	Avertissement
Réplication synchrone désynchronisée	statut sms désynchronisé	Relation SnapMirror	Avertissement
Réplication synchrone restaurée	sms.status.in.sync	Relation SnapMirror	Information
Échec de la resynchronisation automatique de la réplication synchrone	sms.resync.tempt.fail	Relation SnapMirror	Erreur
De nombreuses connexions CIFS	Nblade.cifsManyAuths	SVM	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité du gestionnaire unifié
Connexion CIFS maximale dépassée	Nblade.cifsMaxOpenSam eFile	SVM	Erreur
Nombre maximal de connexions CIFS par utilisateur dépassé	Nblade.cifsMaxSessPerU srConn	SVM	Erreur
Conflit de nom NetBIOS CIFS	Nblade.cifsNbNameConfl ict	SVM	Erreur
Tentatives de connexion à un partage CIFS inexistant	Nblade.cifsNoPrivShare	SVM	Primordial
Échec de l'opération de cliché instantané CIFS	cifs.shadowcopy.échec	SVM	Erreur
Virus détecté par le serveur AV	Nblade.vscanVirusDétect é	SVM	Erreur
Aucune connexion au serveur AV pour l'analyse antivirus	Nblade.vscanNoScanner Conn	SVM	Primordial
Aucun serveur AV enregistré	Nblade.vscanNoRegdSca nner	SVM	Erreur
Aucune connexion au serveur AV réactif	Nblade.vscanConnInactif	SVM	Information
Le serveur AV est trop occupé pour accepter une nouvelle demande d'analyse	Nblade.vscanConnBackPr essure	SVM	Erreur
Tentative d'accès non autorisé d'un utilisateur au serveur AV	Nblade.vscanBadUserPriv Access	SVM	Erreur
Les membres de FlexGroup ont des problèmes d'espace	les constituants du groupe flexible ont des problèmes d'espace	Volume	Erreur
Statut de l'espace des constituants de FlexGroup Tout est OK	flexgroup.constituents.spa ce.status.all.ok	Volume	Information

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité du gestionnaire unifié
Les constituants de FlexGroup ont des problèmes d'inodes	flexgroup.constituents.hav e.inodes.issues	Volume	Erreur
Constituants du FlexGroup Inodes Statut Tout OK	flexgroup.constituents.ino des.status.all.ok	Volume	Information
Espace logique du volume presque plein	moniteur.vol.nearFull.inc.s av	Volume	Avertissement
Volume Espace logique plein	moniteur.vol.full.inc.sav	Volume	Erreur
Volume Espace logique Normal	moniteur.vol.one.ok.inc.sa v	Volume	Information
Échec de la taille automatique du volume WAFL	wafl.vol.autoSize.fail	Volume	Erreur
Dimensionnement automatique du volume WAFL terminé	wafl.vol.autoSize.fait	Volume	Information
Délai d'expiration de l'opération de fichier WAFL READDIR	wafl.readdir.expiré	Volume	Erreur

Abonnez-vous aux événements ONTAP EMS

Vous pouvez vous abonner pour recevoir les événements du système de gestion des événements (EMS) générés par les systèmes installés avec le logiciel ONTAP . Un sous-ensemble d'événements EMS est signalé automatiquement à Unified Manager, mais les événements EMS supplémentaires sont signalés uniquement si vous êtes abonné à ces événements.

Avant de commencer

Ne vous abonnez pas aux événements EMS qui sont déjà ajoutés automatiquement à Unified Manager, car cela peut entraîner une confusion lors de la réception de deux événements pour le même problème.

Vous pouvez vous abonner à n'importe quel nombre d'événements EMS. Tous les événements auxquels vous vous abonnez sont validés et seuls les événements validés sont appliqués aux clusters que vous surveillez dans Unified Manager. Le *Catalogue d'événements EMS ONTAP 9* fournit des informations détaillées sur tous les messages EMS pour la version spécifiée du logiciel ONTAP 9. Recherchez la version appropriée du *Catalogue d'événements EMS* sur la page de documentation du produit ONTAP 9 pour obtenir la liste des

événements applicables.

"Bibliothèque de produits ONTAP 9"

Vous pouvez configurer des alertes pour les événements ONTAP EMS auxquels vous êtes abonné et créer des scripts personnalisés à exécuter pour ces événements.



Si vous ne recevez pas les événements ONTAP EMS auxquels vous êtes abonné, il peut y avoir un problème avec la configuration DNS du cluster qui empêche le cluster d'atteindre le serveur Unified Manager. Pour résoudre ce problème, l'administrateur du cluster doit corriger la configuration DNS du cluster, puis redémarrer Unified Manager. Cela permettra de transférer les événements EMS en attente vers le serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des événements**.
2. Dans la page Configuration de l'événement, cliquez sur le bouton **S'abonner aux événements EMS**.
3. Dans la boîte de dialogue S'abonner aux événements EMS, entrez le nom de l'événement ONTAP EMS auquel vous souhaitez vous abonner.

Pour afficher les noms des événements EMS auxquels vous pouvez vous abonner, à partir du shell du cluster ONTAP, vous pouvez utiliser le `event route show` commande (avant ONTAP 9) ou la `event catalog show` commande (ONTAP 9 ou version ultérieure).

["Comment configurer et recevoir des alertes d'abonnement aux événements ONTAP EMS dans Active IQ Unified Manager"](#)

4. Cliquez sur **Ajouter**.

L'événement EMS est ajouté à la liste des événements EMS abonnés, mais la colonne Applicable au cluster affiche le statut « Inconnu » pour l'événement EMS que vous avez ajouté.

5. Cliquez sur **Enregistrer et fermer** pour enregistrer l'abonnement aux événements EMS auprès du cluster.
6. Cliquez à nouveau sur **S'abonner aux événements EMS**.

Le statut « Oui » apparaît dans la colonne Applicable au cluster pour l'événement EMS que vous avez ajouté.

Si le statut n'est pas « Oui », vérifiez l'orthographe du nom de l'événement ONTAP EMS. Si le nom est saisi de manière incorrecte, vous devez supprimer l'événement incorrect, puis ajouter à nouveau l'événement.

Lorsque l'événement ONTAP EMS se produit, l'événement s'affiche sur la page Événements. Vous pouvez sélectionner l'événement pour afficher les détails de l'événement EMS dans la page Détails de l'événement. Vous pouvez également gérer la disposition de l'événement ou créer des alertes pour l'événement.

Que se passe-t-il lorsqu'un événement est reçu

Lorsqu'Unified Manager reçoit un événement, il s'affiche dans la page Tableau de bord, dans la page d'inventaire Gestion des événements, dans les onglets Résumé et Explorateur de la page Cluster/Performances et dans la page d'inventaire spécifique à

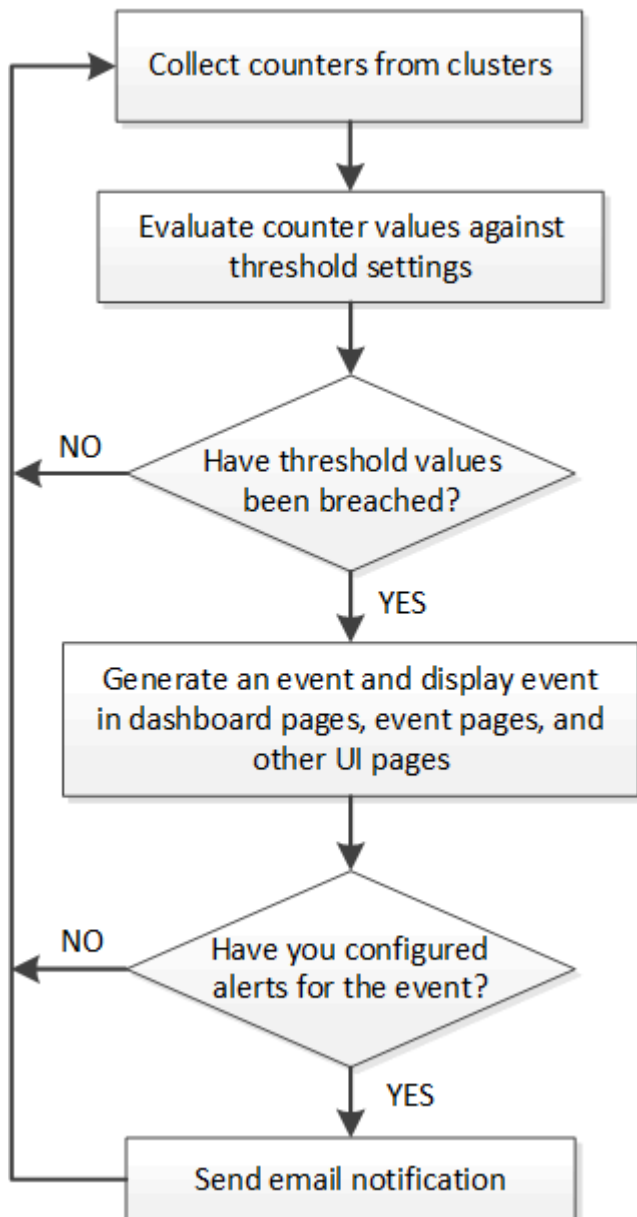
l'objet (par exemple, la page d'inventaire Volumes/Santé).

Lorsque Unified Manager détecte plusieurs occurrences continues de la même condition d'événement pour le même composant de cluster, il traite toutes les occurrences comme un événement unique et non comme des événements distincts. La durée de l'événement est incrémentée pour indiquer que l'événement est toujours actif.

Selon la manière dont vous configurez les paramètres dans la page Configuration des alertes, vous pouvez informer d'autres utilisateurs de ces événements. L'alerte provoque le lancement des actions suivantes :

- Un e-mail concernant l'événement peut être envoyé à tous les utilisateurs administrateurs d'Unified Manager.
- L'événement peut être envoyé à des destinataires de courrier électronique supplémentaires.
- Un piège SNMP peut être envoyé au récepteur du piège.
- Un script personnalisé peut être exécuté pour effectuer une action.

Ce flux de travail est illustré dans le diagramme suivant.



Afficher les événements et les détails des événements

Vous pouvez afficher les détails d'un événement déclenché par Unified Manager pour prendre des mesures correctives. Par exemple, s'il y a un événement de santé Volume Hors ligne, vous pouvez cliquer sur cet événement pour afficher les détails et effectuer des actions correctives.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Les détails de l'événement incluent des informations telles que la source de l'événement, la cause de l'événement et toutes les notes liées à l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

Par défaut, la vue Tous les événements actifs affiche les événements nouveaux et reconnus (actifs) qui ont été générés au cours des 7 derniers jours et qui ont un niveau d'impact d'incident ou de risque.

2. Si vous souhaitez afficher une catégorie particulière d'événements, par exemple, des événements de capacité ou des événements de performance, cliquez sur **Afficher** et sélectionnez-le dans le menu des types d'événements.
3. Cliquez sur le nom de l'événement dont vous souhaitez afficher les détails.

Les détails de l'événement sont affichés sur la page Détails de l'événement.

Afficher les événements non attribués

Vous pouvez afficher les événements non attribués, puis attribuer chacun d'eux à un utilisateur qui peut les résoudre.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

Par défaut, les événements nouveaux et reconnus sont affichés sur la page d'inventaire de gestion des événements.

2. Dans le volet **Filtres**, sélectionnez l'option de filtre **Non attribué** dans la zone **Attribué à**.

Reconnaître et résoudre les événements

Vous devez reconnaître un événement avant de commencer à travailler sur le problème qui a généré l'événement afin de ne pas continuer à recevoir des notifications d'alerte répétées. Après avoir pris des mesures correctives pour un événement particulier, vous devez marquer l'événement comme résolu.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez reconnaître et résoudre plusieurs événements simultanément.



Vous ne pouvez pas reconnaître les événements d'information.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. À partir de la liste des événements, effectuez les actions suivantes pour accuser réception des événements :

Si vous voulez...	Fais ceci...
Reconnaître et marquer un événement unique comme résolu	a. Cliquez sur le nom de l'événement. b. À partir de la page Détails de l'événement, déterminez la cause de l'événement. c. Cliquez sur Reconnaître. d. Prendre les mesures correctives appropriées. e. Cliquez sur Marquer comme résolu.
Reconnaître et marquer plusieurs événements comme résolus	a. Déterminez la cause des événements à partir de la page Détails de l'événement correspondante. b. Sélectionnez les événements. c. Cliquez sur Reconnaître. d. Prendre les mesures correctives appropriées. e. Cliquez sur Marquer comme résolu.

Une fois l'événement marqué comme résolu, l'événement est déplacé vers la liste des événements résolus.

3. **Facultatif** : Dans la zone **Notes et mises à jour**, ajoutez une note sur la manière dont vous avez traité l'événement, puis cliquez sur **Publier**.

Attribuer des événements à des utilisateurs spécifiques

Vous pouvez attribuer des événements non attribués à vous-même ou à d'autres utilisateurs, y compris des utilisateurs distants. Vous pouvez réaffecter les événements attribués à un autre utilisateur, si nécessaire. Par exemple, lorsque des problèmes fréquents surviennent sur un objet de stockage, vous pouvez attribuer les événements de ces problèmes à l'utilisateur qui gère cet objet.

Avant de commencer

- Le nom d'utilisateur et l'identifiant e-mail doivent être configurés correctement.
- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans la page d'inventaire **Gestion des événements**, sélectionnez un ou plusieurs événements que vous souhaitez attribuer.
3. Attribuez l'événement en choisissant l'une des options suivantes :

Si vous souhaitez attribuer l'événement à...	Alors fais ceci...
Toi-même	Cliquez sur Attribuer à > Moi .
Un autre utilisateur	a. Cliquez sur Attribuer à > Un autre utilisateur. b. Dans la boîte de dialogue Attribuer un propriétaire, entrez le nom d'utilisateur ou sélectionnez un utilisateur dans la liste déroulante. c. Cliquez sur Attribuer. Une notification par e-mail est envoyée à l'utilisateur.  Si vous n'entrez pas de nom d'utilisateur ou ne sélectionnez pas d'utilisateur dans la liste déroulante et cliquez sur Attribuer, l'événement reste non attribué.

Désactiver les événements indésirables

Tous les événements sont activés par défaut. Vous pouvez désactiver les événements globalement pour empêcher la génération de notifications pour des événements qui ne sont pas importants dans votre environnement. Vous pouvez activer les événements désactivés lorsque vous souhaitez reprendre la réception des notifications pour eux.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous désactivez les événements, les événements précédemment générés dans le système sont marqués comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications pour ces événements sont générées à partir du prochain cycle de surveillance.

Lorsque vous désactivez un événement pour un objet (par exemple, le `vol offline` (événement), puis vous activez ultérieurement l'événement, Unified Manager ne génère pas de nouveaux événements pour les objets qui sont passés hors ligne lorsque l'événement était à l'état désactivé. Unified Manager génère un nouvel événement uniquement lorsqu'un changement se produit dans l'état de l'objet après la réactivation de l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des événements**.
2. Dans la page **Configuration des événements**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Si vous voulez...	Alors fais ceci...
Désactiver les événements	a. Cliquez sur Désactiver. b. Dans la boîte de dialogue Désactiver les événements, sélectionnez la gravité de l'événement. c. Dans la colonne Événements correspondants, sélectionnez les événements que vous souhaitez désactiver en fonction de la gravité de l'événement, puis cliquez sur la flèche droite pour déplacer ces événements vers la colonne Désactiver les événements. d. Cliquez sur Enregistrer et fermer. e. Vérifiez que les événements que vous avez désactivés s'affichent dans la vue de liste de la page Configuration des événements.
Activer les événements	a. Cochez la case correspondant à l'événement ou aux événements que vous souhaitez activer. b. Cliquez sur Activer.

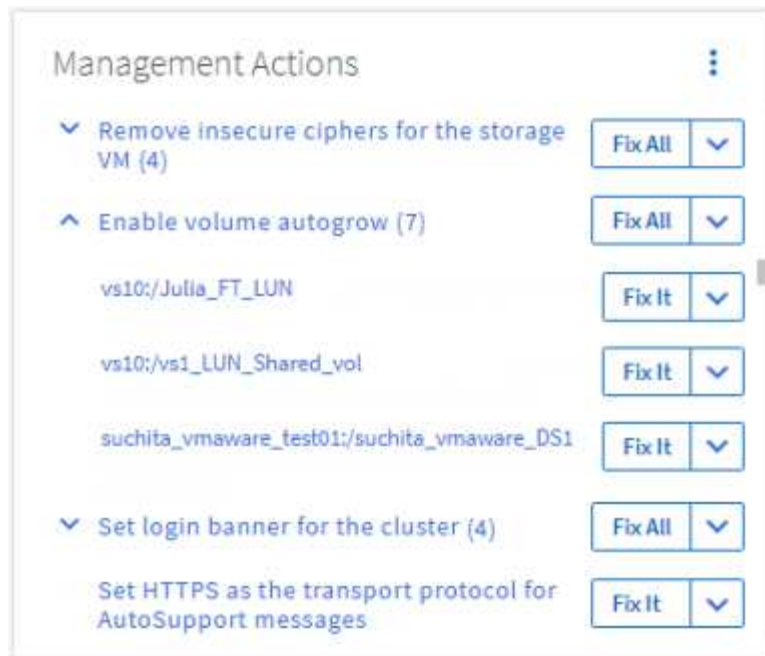
Résoudre les problèmes à l'aide de la correction automatique d'Unified Manager

Il existe certains événements qu'Unified Manager peut diagnostiquer en profondeur et fournir une résolution unique à l'aide du bouton **Réparer**. Lorsqu'elles sont disponibles, ces résolutions sont affichées dans le tableau de bord, à partir de la page Détails de l'événement et à partir de la sélection Analyse de la charge de travail dans le menu de navigation de gauche.

La plupart des événements ont une variété de résolutions possibles qui sont affichées dans la page Détails de l'événement afin que vous puissiez implémenter la meilleure solution à l'aide d'ONTAP System Manager ou de l'ONTAP CLI. Une action **Fix It** est disponible lorsque Unified Manager a déterminé qu'il existe une seule résolution pour résoudre le problème et qu'il peut être résolu à l'aide d'une commande CLI ONTAP .

Étapes

1. Pour afficher les événements qui peuvent être corrigés à partir du **Tableau de bord**, cliquez sur **Tableau de bord**.



2. Pour résoudre l'un des problèmes que Unified Manager peut résoudre, cliquez sur le bouton **Réparer**.
Pour résoudre un problème qui existe sur plusieurs objets, cliquez sur le bouton **Réparer tout**.

Pour plus d'informations sur les problèmes qui peuvent être résolus par la correction automatique, consultez "[Quels problèmes Unified Manager peut-il résoudre ?](#)".

Activer et désactiver les rapports d'événements Active IQ

Les événements de la plateforme Active IQ sont générés et affichés dans l'interface utilisateur d'Unified Manager par défaut. Si vous trouvez que ces événements sont trop « bruyants » ou que vous ne souhaitez pas les afficher dans Unified Manager, vous pouvez désactiver la génération de ces événements. Vous pouvez les activer ultérieurement si vous souhaitez reprendre la réception de ces notifications.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Lorsque vous désactivez cette fonctionnalité, Unified Manager cesse immédiatement de recevoir les événements de la plateforme Active IQ.

Lorsque vous activez cette fonctionnalité, Unified Manager commence à recevoir les événements de la plateforme Active IQ peu après minuit en fonction du fuseau horaire du cluster. L'heure de début est basée sur le moment où Unified Manager reçoit les messages AutoSupport de chaque cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Paramètres des fonctionnalités**.
2. Dans la page **Paramètres des fonctionnalités**, désactivez ou activez les événements de la plateforme Active IQ en choisissant l'une des options suivantes :

Si vous voulez...	Alors fais ceci...
Désactiver les événements de la plateforme Active IQ	Dans le panneau * Événements du portail Active IQ *, déplacez le bouton du curseur vers la gauche.
Activer les événements de la plateforme Active IQ	Dans le panneau * Événements du portail Active IQ *, déplacez le bouton du curseur vers la droite.

Télécharger un nouveau fichier de règles Active IQ

Unified Manager recherche automatiquement un nouveau fichier d'événements Active IQ (règles) et télécharge un nouveau fichier lorsqu'il existe des règles plus récentes. Cependant, sur les sites sans accès réseau externe, vous devez télécharger le fichier de règles manuellement.



Les règles Active IQ sont également appelées règles sécurisées Config Advisor (CA).

Lorsque vous installez ou mettez à niveau Unified Manager vers une version spécifique sur un site sans connectivité réseau, les règles Active IQ groupées sont automatiquement disponibles pour le téléchargement. Cependant, il est recommandé de télécharger un nouveau fichier de règles environ une fois par mois à partir du site de support de NetApp pour vous assurer que les événements mis à jour sont générés et que vos systèmes de stockage continuent de fonctionner de manière optimale.

Avant de commencer

- La création de rapports d'événements sur le portail Active IQ doit être activée. Cette fonctionnalité est activée par défaut. Pour plus d'informations, voir "[Activation des événements du portail Active IQ](#)".
- Vous devez télécharger le fichier de règles à partir du site de support NetApp .

Le fichier des règles se trouve à : https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Étapes

1. Sur un ordinateur disposant d'un accès réseau, accédez au site de support NetApp et téléchargez les règles actuelles .zip déposer.

Le package de règles groupées comprend le référentiel de règles, les sources de données et un article de base de connaissances NetApp .



Sur les systèmes Windows, sur un site sans connectivité réseau, l'article de la base de connaissances NetApp n'est pas fourni par défaut avec le programme d'installation. Vous pouvez télécharger le fichier *secure_rules.zip* depuis le site d'assistance et le télécharger pour afficher l'article de la base de connaissances pour toutes les règles.

2. Transférez le fichier de règles sur un support que vous pouvez apporter dans la zone sécurisée, puis copiez-le sur un système dans la zone sécurisée.
3. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des événements**.
4. Dans la page **Configuration de l'événement**, cliquez sur le bouton **Télécharger les règles**.

5. Dans la boîte de dialogue **Règles de téléchargement**, accédez aux règles et sélectionnez-les .zip le fichier que vous avez téléchargé et cliquez sur **Télécharger**.

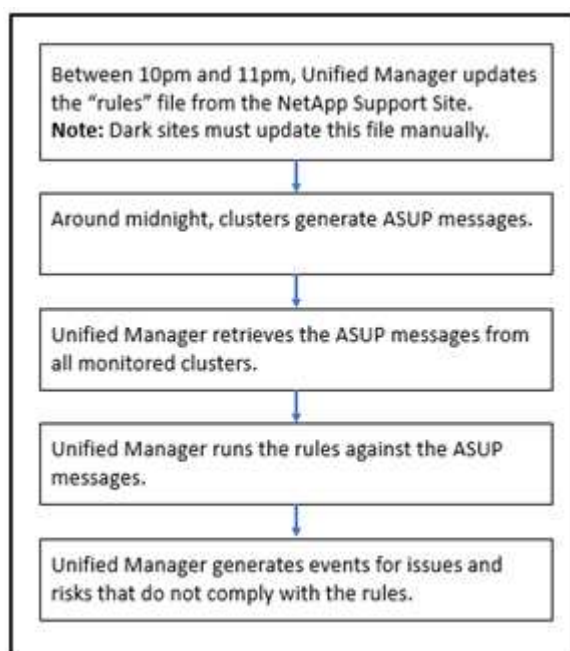
Ce processus peut prendre quelques minutes.

Le fichier de règles est décompressé sur le serveur Unified Manager. Une fois que vos clusters gérés génèrent un fichier AutoSupport après minuit, Unified Manager vérifie les clusters par rapport au fichier de règles et génère de nouveaux événements de risque et d'incident selon les besoins.

Pour plus d'informations, consultez cet article de la base de connaissances (KB) : ["Comment mettre à jour manuellement les règles AIQCA Secure dans Active IQ Unified Manager"](#) .

Comment les événements de la plateforme Active IQ sont générés

Les incidents et les risques de la plateforme Active IQ sont convertis en événements Unified Manager comme indiqué dans le diagramme suivant.

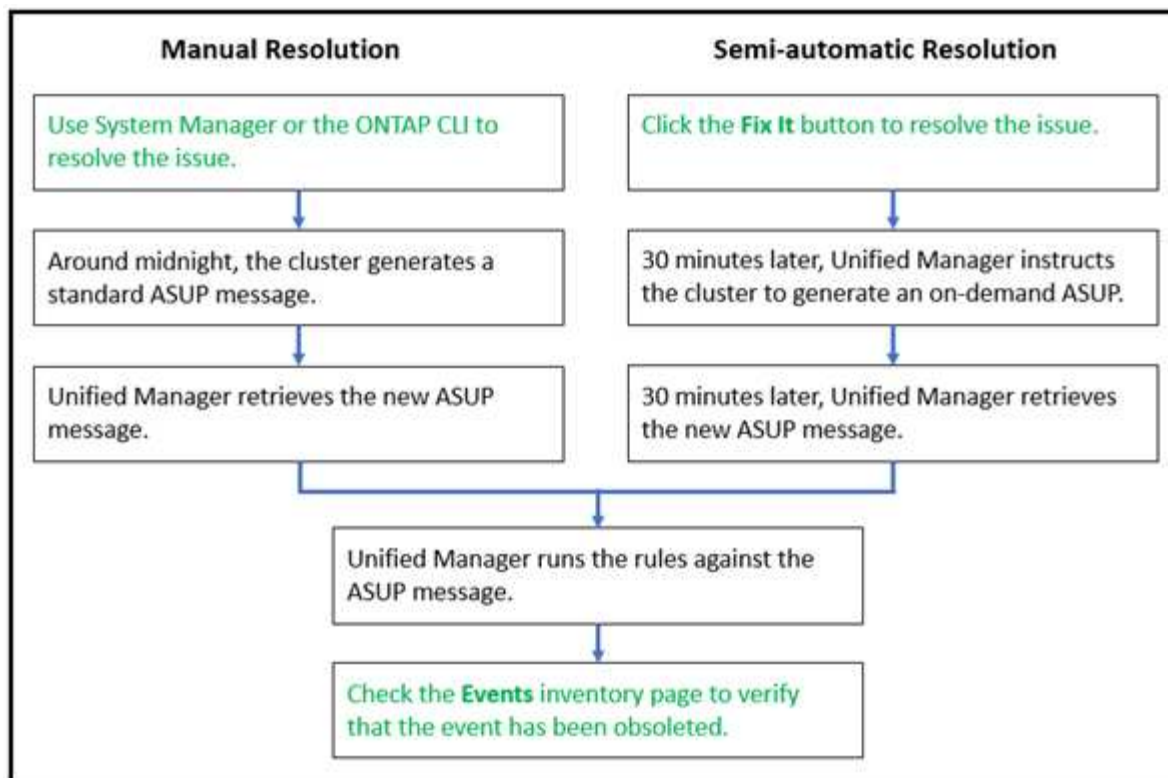


Comme vous pouvez le voir, le fichier de règles compilé sur la plateforme Active IQ est maintenu à jour, les messages AutoSupport du cluster sont générés quotidiennement et Unified Manager met à jour la liste des événements quotidiennement.

Résoudre les événements de la plateforme Active IQ

Les incidents et les risques de la plateforme Active IQ sont similaires aux autres événements Unified Manager car ils peuvent être attribués à d'autres utilisateurs pour résolution et ils ont les mêmes états disponibles. Cependant, lorsque vous résolvez ces types d'événements à l'aide du bouton **Réparer**, vous pouvez vérifier la résolution en quelques heures.

Le diagramme suivant montre les actions que vous devez entreprendre (en vert) et l'action entreprise par Unified Manager (en noir) lors de la résolution des événements générés à partir de la plateforme Active IQ .



Lorsque vous effectuez une résolution manuelle, vous devez vous connecter au Gestionnaire système ou à l'interface de ligne de commande ONTAP pour résoudre le problème. Vous ne pourrez vérifier le problème qu'une fois que le cluster aura généré un nouveau message AutoSupport à minuit.

Lorsque vous effectuez une résolution semi-automatique à l'aide du bouton **Fix It**, vous pouvez vérifier que la correction a réussi en quelques heures.

Configurer les paramètres de conservation des événements

Vous pouvez spécifier le nombre de mois pendant lesquels un événement est conservé sur le serveur Unified Manager avant d'être automatiquement supprimé.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

La conservation des événements pendant plus de 6 mois peut affecter les performances du serveur et n'est pas recommandée.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Conservation des données**.
2. Dans la page **Conservation des données**, sélectionnez le curseur dans la zone Conservation des événements et déplacez-le sur le nombre de mois pendant lesquels les événements doivent être conservés, puis cliquez sur **Enregistrer**.

Qu'est-ce qu'une fenêtre de maintenance Unified Manager

Vous définissez une fenêtre de maintenance Unified Manager pour supprimer les événements et les alertes pendant une période spécifique lorsque vous avez planifié une

maintenance de cluster et que vous ne souhaitez pas recevoir un flot de notifications indésirables.

Lorsque la fenêtre de maintenance démarre, un événement « Fenêtre de maintenance d'objet démarrée » est publié sur la page d'inventaire de gestion des événements. Cet événement devient automatiquement obsolète lorsque la fenêtre de maintenance se termine.

Pendant une fenêtre de maintenance, les événements liés à tous les objets de ce cluster sont toujours générés, mais ils n'apparaissent dans aucune des pages de l'interface utilisateur et aucune alerte ou autre type de notification n'est envoyé pour ces événements. Vous pouvez toutefois afficher les événements qui ont été générés pour tous les objets de stockage au cours d'une fenêtre de maintenance en sélectionnant l'une des options d'affichage sur la page d'inventaire Gestion des événements.

Vous pouvez planifier le lancement d'une fenêtre de maintenance dans le futur, modifier les heures de début et de fin d'une fenêtre de maintenance planifiée et annuler une fenêtre de maintenance planifiée.

Planifier une fenêtre de maintenance pour désactiver les notifications d'événements de cluster

Si vous avez planifié une période d'arrêt pour un cluster, par exemple pour mettre à niveau le cluster ou pour déplacer l'un des nœuds, vous pouvez supprimer les événements et les alertes qui seraient normalement générés pendant cette période en planifiant une fenêtre de maintenance Unified Manager.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Pendant une fenêtre de maintenance, les événements liés à tous les objets de ce cluster sont toujours générés, mais ils n'apparaissent pas dans la page des événements et aucune alerte ou autre type de notification n'est envoyé pour ces événements.

L'heure que vous saisissez pour la fenêtre de maintenance est basée sur l'heure du serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Dans la colonne **Mode de maintenance** du cluster, sélectionnez le bouton du curseur et déplacez-le vers la droite.

La fenêtre du calendrier s'affiche.

3. Sélectionnez la date et l'heure de début et de fin de la fenêtre de maintenance et cliquez sur **Appliquer**.

Le message « Programmé » apparaît à côté du bouton du curseur.

Lorsque l'heure de début est atteinte, le cluster passe en mode maintenance et un événement « Fenêtre de maintenance d'objet démarrée » est généré.

Modifier ou annuler une fenêtre de maintenance planifiée

Si vous avez configuré une fenêtre de maintenance Unified Manager pour qu'elle se produise dans le futur, vous pouvez modifier les heures de début et de fin ou annuler la fenêtre de maintenance.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

L'annulation d'une fenêtre de maintenance en cours d'exécution est utile si vous avez terminé la maintenance du cluster avant l'heure de fin de la fenêtre de maintenance planifiée et que vous souhaitez recommencer à recevoir des événements et des alertes du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Dans la colonne **Mode de maintenance** du cluster :

Si vous voulez...	Effectuez cette étape...
Modifier le délai d'une fenêtre de maintenance planifiée	a. Cliquez sur le texte « Programmé » à côté du bouton du curseur. b. Modifiez la date et l'heure de début et/ou de fin et cliquez sur Appliquer.
Prolonger la durée d'une fenêtre de maintenance active	a. Cliquez sur le texte « Actif » à côté du bouton du curseur. b. Modifiez la date et l'heure de fin et cliquez sur Appliquer.
Annuler une fenêtre de maintenance planifiée	Sélectionnez le bouton du curseur et déplacez-le vers la gauche.
Annuler une fenêtre de maintenance active	Sélectionnez le bouton du curseur et déplacez-le vers la gauche.

Afficher les événements survenus pendant une fenêtre de maintenance

Si nécessaire, vous pouvez afficher les événements qui ont été générés pour tous les objets de stockage pendant une fenêtre de maintenance d'Unified Manager. La plupart des événements apparaîtront dans l'état Obsolète une fois la fenêtre de maintenance terminée et toutes les ressources système seront de nouveau opérationnelles.

Avant de commencer

Au moins une fenêtre de maintenance doit être terminée avant que des événements soient disponibles.

Les événements survenus pendant une fenêtre de maintenance n'apparaissent pas par défaut sur la page d'inventaire de gestion des événements.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Événements**.

Par défaut, tous les événements actifs (nouveaux et reconnus) sont affichés sur la page d'inventaire de gestion des événements.
2. Dans le volet Affichage, sélectionnez l'option **Tous les événements générés pendant la maintenance**.

La liste des événements déclenchés au cours des 7 derniers jours à partir de toutes les sessions de fenêtre de maintenance et de tous les clusters est affichée.

3. S'il y a eu plusieurs fenêtres de maintenance pour un seul cluster, vous pouvez cliquer sur l'icône de calendrier **Heure de déclenchement** et sélectionner la période de temps pour les événements de la fenêtre de maintenance que vous souhaitez afficher.

Gérer les événements des ressources du système hôte

Unified Manager inclut un service qui surveille les problèmes de ressources sur le système hôte sur lequel Unified Manager est installé. Des problèmes tels que le manque d'espace disque disponible ou le manque de mémoire sur le système hôte peuvent déclencher des événements de station de gestion qui s'affichent sous forme de messages de bannière en haut de l'interface utilisateur.

Les événements de la station de gestion indiquent un problème avec le système hôte sur lequel Unified Manager est installé. Les exemples de problèmes de station de gestion incluent un espace disque insuffisant sur le système hôte, l'absence d'un cycle de collecte de données régulier par Unified Manager et l'inachèvement ou l'achèvement tardif de l'analyse des statistiques car l'interrogation de collecte suivante a été lancée.

Contrairement à tous les autres messages d'événement Unified Manager, ces événements d'avertissement et critiques de station de gestion particuliers sont affichés dans des messages de bannière.

Étape

1. Pour afficher les informations sur les événements de la station de gestion, effectuez ces actions :

Si vous voulez...	Fais ceci...
Voir les détails de l'événement	Cliquez sur la bannière de l'événement pour afficher la page des détails de l'événement qui inclut les solutions suggérées au problème.
Voir tous les événements de la station de gestion	a. Dans le volet de navigation de gauche, cliquez sur Gestion des événements. b. Dans le volet Filtres de la page d'inventaire Gestion des événements, cochez la case Station de gestion dans la liste Type de source.

En savoir plus sur les événements

Comprendre les concepts relatifs aux événements vous aide à gérer efficacement vos clusters et objets de cluster et à définir les alertes de manière appropriée.

Définitions de l'état de l'événement

L'état d'un événement vous aide à identifier si une action corrective appropriée est requise. Un événement peut être nouveau, reconnu, résolu ou obsolète. Notez que les événements nouveaux et reconnus sont considérés comme des événements actifs.

Les états de l'événement sont les suivants :

- **Nouveau**

L'état d'un nouvel événement.

- **Reconnu**

L'état d'un événement lorsque vous l'avez reconnu.

- **Résolu**

L'état d'un événement lorsqu'il est marqué comme résolu.

- **Obsolète**

L'état d'un événement lorsqu'il est automatiquement corrigé ou lorsque la cause de l'événement n'est plus valide.



Vous ne pouvez pas reconnaître ou résoudre un événement obsolète.

Exemple de différents états d'un événement

Les exemples suivants illustrent les modifications manuelles et automatiques de l'état des événements.

Lorsque l'événement Cluster Not Reachable est déclenché, l'état de l'événement est Nouveau. Lorsque vous reconnaissez l'événement, l'état de l'événement passe à Reconnu. Lorsque vous avez pris une mesure corrective appropriée, vous devez marquer l'événement comme résolu. L'état de l'événement passe alors à Résolu.

Si l'événement Cluster Not Reachable est généré en raison d'une panne de courant, lorsque l'alimentation est rétablie, le cluster commence à fonctionner sans aucune intervention de l'administrateur. Par conséquent, l'événement Cluster non accessible n'est plus valide et l'état de l'événement passe à Obsolète lors du prochain cycle de surveillance.

Unified Manager envoie une alerte lorsqu'un événement est à l'état Obsolète ou Résolu. L'objet et le contenu de l'e-mail d'une alerte fournissent des informations sur l'état de l'événement. Un piège SNMP inclut également des informations sur l'état de l'événement.

Description des types de gravité des événements

Chaque événement est associé à un type de gravité pour vous aider à hiérarchiser les événements qui nécessitent une action corrective immédiate.

- **Critique**

Un problème est survenu qui pourrait entraîner une interruption de service si des mesures correctives ne sont pas prises immédiatement.

Les événements critiques de performances sont envoyés uniquement à partir de seuils définis par l'utilisateur.

- **Erreur**

La source de l'événement fonctionne toujours ; cependant, une action corrective est nécessaire pour éviter une interruption de service.

- **Avertissement**

La source de l'événement a rencontré un événement dont vous devez être conscient, ou un compteur de performances pour un objet de cluster est hors de portée normale et doit être surveillé pour s'assurer qu'il n'atteint pas la gravité critique. Les événements de cette gravité n'entraînent pas d'interruption de service et aucune mesure corrective immédiate n'est nécessaire.

Les événements d'avertissement de performances sont envoyés à partir de seuils définis par l'utilisateur, définis par le système ou dynamiques.

- **Information**

L'événement se produit lorsqu'un nouvel objet est découvert ou lorsqu'une action utilisateur est effectuée. Par exemple, lorsqu'un objet de stockage est supprimé ou lorsqu'il y a des modifications de configuration, l'événement avec le type de gravité Information est généré.

Les événements d'information sont envoyés directement depuis ONTAP lorsqu'il détecte un changement de configuration.

Description des niveaux d'impact des événements

Chaque événement est associé à un niveau d'impact (incident, risque, événement ou mise à niveau) pour vous aider à hiérarchiser les événements qui nécessitent une action corrective immédiate.

- **Incident**

Un incident est un ensemble d'événements qui peuvent empêcher un cluster de fournir des données au client et de manquer d'espace pour stocker les données. Les événements ayant un niveau d'impact Incident sont les plus graves. Des mesures correctives immédiates doivent être prises pour éviter toute interruption de service.

- **Risque**

Un risque est un ensemble d'événements qui peuvent potentiellement amener un cluster à cesser de fournir des données au client et à manquer d'espace pour stocker les données. Les événements ayant un niveau d'impact de Risque peuvent entraîner une interruption de service. Des mesures correctives pourraient être nécessaires.

- **Événement**

Un événement est un changement d'état ou de statut des objets de stockage et de leurs attributs. Les événements avec un niveau d'impact Événement sont informatifs et ne nécessitent pas de mesure corrective.

- **Mise à niveau**

Les événements de mise à niveau sont un type spécifique d'événement signalé par la plate-forme Active IQ . Ces événements identifient les problèmes pour lesquels la résolution nécessite la mise à niveau du logiciel ONTAP , du micrologiciel du nœud ou du logiciel du système d'exploitation (pour les avis de sécurité). Vous souhaitez peut-être effectuer une action corrective immédiate pour certains de ces

problèmes, tandis que d'autres problèmes pourront attendre votre prochaine maintenance programmée.

Description des zones d'impact de l'événement

Les événements sont classés en six domaines d'impact (disponibilité, capacité, configuration, performances, protection et sécurité) pour vous permettre de vous concentrer sur les types d'événements dont vous êtes responsable.

- **Disponibilité**

Les événements de disponibilité vous avertissent si un objet de stockage est hors ligne, si un service de protocole tombe en panne, si un problème de basculement de stockage se produit ou si un problème matériel se produit.

- **Capacité**

Les événements de capacité vous avertissent si vos agrégats, volumes, LUN ou espaces de noms approchent ou ont atteint un seuil de taille, ou si le taux de croissance est inhabituel pour votre environnement.

- **Configuration**

Les événements de configuration vous informent de la découverte, de la suppression, de l'ajout, de la suppression ou du changement de nom de vos objets de stockage. Les événements de configuration ont un niveau d'impact Événement et un type de gravité Information.

- **Performance**

Les événements de performances vous informent des conditions de ressources, de configuration ou d'activité sur votre cluster qui pourraient affecter négativement la vitesse d'entrée ou de récupération de stockage des données sur vos objets de stockage surveillés.

- **Protection**

Les événements de protection vous informent des incidents ou des risques impliquant les relations SnapMirror, des problèmes de capacité de destination, des problèmes avec les relations SnapVault ou des problèmes avec les tâches de protection. Tout objet ONTAP (en particulier les agrégats, les volumes et les SVM) qui hébergent des volumes secondaires et des relations de protection sont classés dans la zone d'impact de la protection.

- **Sécurité**

Les événements de sécurité vous informent du niveau de sécurité de vos clusters ONTAP, de vos machines virtuelles de stockage (SVM) et de vos volumes en fonction des paramètres définis dans le ["Guide de renforcement de la sécurité NetApp pour ONTAP 9"](#).

De plus, cette zone comprend les événements de mise à niveau signalés par la plateforme Active IQ.

Comment le statut de l'objet est calculé

L'état de l'objet est déterminé par l'événement le plus grave qui détient actuellement un état Nouveau ou Reconnu. Par exemple, si le statut d'un objet est Erreur, l'un des événements de l'objet a un type de gravité Erreur. Une fois l'action corrective entreprise,

l'état de l'événement passe à Résolu.

Détails du graphique des événements de performance dynamique

Pour les événements de performances dynamiques, la section Diagnostic système de la page Détails de l'événement répertorie les principales charges de travail avec la latence ou l'utilisation la plus élevée du composant de cluster en conflit.

Les statistiques de performances sont basées sur le moment où l'événement de performance a été détecté jusqu'à la dernière fois que l'événement a été analysé. Les graphiques affichent également les statistiques de performances historiques du composant de cluster en conflit.

Par exemple, vous pouvez identifier les charges de travail avec une utilisation élevée d'un composant pour déterminer quelle charge de travail déplacer vers un composant moins utilisé. Le déplacement de la charge de travail réduirait la quantité de travail sur le composant actuel, ce qui permettrait éventuellement de sortir le composant de la compétition. En haut de cette section se trouve la plage de dates et d'heures à laquelle un événement a été détecté et analysé pour la dernière fois. Pour les événements actifs (nouveaux ou reconnus), la dernière heure analysée est mise à jour.

Les graphiques de latence et d'activité affichent les noms des principales charges de travail lorsque vous passez votre curseur sur le graphique. Cliquer sur le menu Type de charge de travail à droite du graphique vous permet de trier les charges de travail en fonction de leur rôle dans l'événement, y compris les *requins*, les *intimideurs* ou les *victimes*, et affiche des détails sur leur latence et leur utilisation sur le composant de cluster en conflit. Vous pouvez comparer la valeur réelle à la valeur attendue pour voir quand la charge de travail était en dehors de sa plage de latence ou d'utilisation prévue. Pour plus d'informations, voir ["Types de charges de travail surveillées par Unified Manager"](#).



Lorsque vous triez par écart de pointe en termes de latence, les charges de travail définies par le système ne s'affichent pas dans le tableau, car la latence s'applique uniquement aux charges de travail définies par l'utilisateur. Les charges de travail avec des valeurs de latence très faibles ne sont pas affichées dans le tableau.

Pour plus d'informations sur les seuils de performance dynamiques, voir ["Analyse des événements à partir de seuils de performance dynamiques"](#).

Pour plus d'informations sur la manière dont Unified Manager classe les charges de travail et détermine l'ordre de tri, consultez ["Comment Unified Manager détermine l'impact sur les performances d'un événement"](#).

Les données des graphiques montrent 24 heures de statistiques de performance avant la dernière fois que l'événement a été analysé. Les valeurs réelles et les valeurs attendues pour chaque charge de travail sont basées sur le temps pendant lequel la charge de travail a été impliquée dans l'événement. Par exemple, une charge de travail peut être impliquée dans un événement après sa détection, de sorte que ses statistiques de performances peuvent ne pas correspondre aux valeurs au moment de la détection de l'événement. Par défaut, les charges de travail sont triées par écart maximal (le plus élevé) de latence.



Étant donné qu'Unified Manager conserve un maximum de 30 jours de données historiques de performances et d'événements de 5 minutes, si l'événement a plus de 30 jours, aucune donnée de performances n'est affichée.

- **Colonne de tri de la charge de travail**

- **Tableau de latence**

Affiche l'impact de l'événement sur la latence de la charge de travail lors de la dernière analyse.

- **Colonne Utilisation des composants**

Affiche les détails sur l'utilisation de la charge de travail du composant de cluster en conflit. Dans les graphiques, l'utilisation réelle est une ligne bleue. Une barre rouge met en évidence la durée de l'événement, depuis le moment de détection jusqu'au dernier moment analysé. Pour plus d'informations, voir "[Valeurs de mesure des performances de la charge de travail](#)".



Pour le composant réseau, étant donné que les statistiques de performances réseau proviennent de l'activité hors du cluster, cette colonne n'est pas affichée.

- **Utilisation des composants**

Affiche l'historique d'utilisation, en pourcentage, pour les composants de traitement réseau, de traitement des données et d'agrégation ou l'historique d'activité, en pourcentage, pour le composant de groupe de stratégies QoS. Le graphique n'est pas affiché pour les composants réseau ou d'interconnexion. Vous pouvez pointer vers les statistiques pour afficher les statistiques d'utilisation à un moment précis.

- **Historique total d'écriture en Mo/s**

Pour le composant Ressources MetroCluster uniquement, affiche le débit d'écriture total, en mégaoctets par seconde (Mo/s), pour toutes les charges de travail de volume mises en miroir sur le cluster partenaire dans une configuration MetroCluster .

- **Historique des événements**

Affiche des lignes ombrées en rouge pour indiquer les événements historiques du composant en conflit. Pour les événements obsolètes, le graphique affiche les événements qui se sont produits avant la détection de l'événement sélectionné et après sa résolution.

Modifications de configuration détectées par Unified Manager

Unified Manager surveille vos clusters pour détecter les modifications de configuration afin de vous aider à déterminer si une modification a pu provoquer ou contribuer à un événement de performances. Les pages de l'Explorateur de performances affichent une icône d'événement de modification (●) pour indiquer la date et l'heure à laquelle le changement a été détecté.

Vous pouvez consulter les graphiques de performances dans les pages de l'Explorateur de performances et dans la page Analyse de la charge de travail pour voir si l'événement de modification a eu un impact sur les performances de l'objet de cluster sélectionné. Si le changement a été détecté au même moment ou à peu près au même moment qu'un événement de performance, le changement a peut-être contribué au problème, ce qui a provoqué le déclenchement de l'alerte d'événement.

Unified Manager peut détecter les événements de changement suivants, classés comme événements informatifs :

- Un volume se déplace entre les agrégats.

Unified Manager peut détecter quand le déplacement est en cours, terminé ou échoué. Si Unified Manager est en panne pendant un déplacement de volume, lorsqu'il est de nouveau opérationnel, il détecte le

déplacement de volume et affiche un événement de modification pour celui-ci.

- La limite de débit (Mo/s ou IOPS) d'un groupe de politiques QoS contenant une ou plusieurs charges de travail surveillées change.

La modification d'une limite de groupe de stratégies peut provoquer des pics intermittents de latence (temps de réponse), ce qui peut également déclencher des événements pour le groupe de stratégies. La latence revient progressivement à la normale et tous les événements provoqués par les pics deviennent obsolètes.

- Un nœud d'une paire HA prend en charge ou restitue le stockage de son nœud partenaire.

Unified Manager peut détecter quand l'opération de prise de contrôle, de prise de contrôle partielle ou de restitution a été terminée. Si la prise de contrôle est provoquée par un nœud paniqué, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de restauration ONTAP s'est terminée avec succès.

La version précédente et la nouvelle version sont affichées.

Liste des événements et types de gravité

Vous pouvez utiliser la liste des événements pour vous familiariser davantage avec les catégories d'événements, les noms d'événements et le type de gravité de chaque événement que vous pourriez voir dans Unified Manager. Les événements sont répertoriés par ordre alphabétique par catégorie d'objet.

Événements agrégés

Les événements agrégés vous fournissent des informations sur l'état des agrégats afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Agrégation hors ligne (ocumEvtAggregateState Offline)	Incident	Agrégat	Primordial
Échec de l'agrégation (ocumEvtAggregateState Failed)	Incident	Agrégat	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Agrégat restreint (ocumEvtAggregateStateRestricted)	Risque	Agrégat	Avertissement
Reconstruction d'agrégat (ocumEvtAggregateRaidStateReconstructing)	Risque	Agrégat	Avertissement
Agrégat dégradé (ocumEvtAggregateRaidStateDegraded)	Risque	Agrégat	Avertissement
Niveau de cloud partiellement accessible (ocumEventCloudTierPartiallyReachable)	Risque	Agrégat	Avertissement
Niveau de cloud inaccessible (ocumEventCloudTierUnreachable)	Risque	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation globale (arlNetraCaCheckFailed)	Risque	Agrégat	Erreur
Accès au niveau cloud refusé pour relocalisation d'agrégats lors du basculement du stockage (gbNetraCaCheckFailed)	Risque	Agrégat	Erreur
Agrégat MetroCluster laissé pour compte (ocumEvtMetroClusterAggregateLeftBehind)	Risque	Agrégat	Erreur
Mise en miroir d'agrégat MetroCluster dégradée (ocumEvtMetroClusterAggregateMirrorDegraded)	Risque	Agrégat	Erreur

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Espace agrégé presque plein (ocumEvtAggregateNearlyFull)	Risque	Agrégat	Avertissement
Espace agrégé plein (ocumEvtAggregateFull)	Risque	Agrégat	Erreur
Nombre total de jours avant le plein (ocumEvtAggregateDaysUntilFullSoon)	Risque	Agrégat	Erreur
Agrégat surengagé (ocumEvtAggregateOvercommitted)	Risque	Agrégat	Erreur
Agrégat presque surengagé (ocumEvtAggregateAlmostOvercommitted)	Risque	Agrégat	Avertissement
Réserve d'instantanés agrégés pleine (ocumEvtAggregateSnapshotReserveFull)	Risque	Agrégat	Avertissement
Taux de croissance global anormal (ocumEvtAggregateGrowthRateAbnormal)	Risque	Agrégat	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Agrégat découvert (sans objet)	Événement	Agrégat	Information
Agrégat renommé (sans objet)	Événement	Agrégat	Information
Agrégat supprimé (sans objet)	Événement	Nœud	Information

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'IOPS agrégé (ocumAggregateIopsIncident)	Incident	Agrégat	Primordial
Dépassement du seuil d'avertissement d'IOPS agrégé (ocumAggregateIopsWarning)	Risque	Agrégat	Avertissement
Dépassement du seuil critique de débit agrégé en Mo/s (ocumAggregateMbpsIncident)	Incident	Agrégat	Primordial
Seuil d'avertissement de débit agrégé en Mo/s dépassé (ocumAggregateMbpsWarning)	Risque	Agrégat	Avertissement
Dépassement du seuil critique de latence globale (ocumAggregateLatencyIncident)	Incident	Agrégat	Primordial
Dépassement du seuil d'avertissement de latence globale (ocumAggregateLatencyWarning)	Risque	Agrégat	Avertissement
Seuil critique de capacité de performance globale utilisée dépassé (ocumAggregatePerfCapacityUsedIncident)	Incident	Agrégat	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Avertissement : dépassement du seuil d'avertissement de capacité de performance globale utilisée (ocumAggregatePerfCapa cityUsedWarning)	Risque	Agrégat	Avertissement
Dépassement du seuil critique d'utilisation globale (ocumAggregateUtilizatio nIncident)	Incident	Agrégat	Primordial
Seuil d'avertissement d'utilisation globale dépasse (ocumAggregateUtilizatio nWarning)	Risque	Agrégat	Avertissement
Dépassement du seuil de surutilisation des disques agrégés (ocumAggregateDisksOve rUtilizedWarning)	Risque	Agrégat	Avertissement
Dépassement du seuil dynamique global (ocumAggregateDynamic EventWarning)	Risque	Agrégat	Avertissement

Événements groupés

Les événements de cluster fournissent des informations sur l'état des clusters, ce qui vous permet de surveiller les clusters pour détecter d'éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement, le nom du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Le cluster manque de disques de rechange (ocumEvtDisksNoSpares)	Risque	Cluster	Avertissement
Cluster non accessible (ocumEvtClusterUnreachable)	Risque	Cluster	Erreur
Échec de la surveillance du cluster (ocumEvtClusterMonitoringFailed)	Risque	Cluster	Avertissement
Dépassement des limites de capacité de la licence Cluster FabricPool (ocumEvtExternalCapacityTierSpaceFull)	Risque	Cluster	Avertissement
Début de la période de grâce NVMe-oF *(nvmfGracePeriodStart)	Risque	Cluster	Avertissement
Période de grâce NVMe-oF active *(nvmfGracePeriodActive)	Risque	Cluster	Avertissement
Période de grâce NVMe-oF expirée *(nvmfGracePeriodExpired)	Risque	Cluster	Avertissement
Fenêtre de maintenance d'objet démarrée (objectMaintenanceWindowStarted)	Événement	Cluster	Primordial
Fenêtre de maintenance des objets terminée (objectMaintenanceWindowEnded)	Événement	Cluster	Information
Disques de rechange MetroCluster laissés pour compte (ocumEvtSpareDiskLeftBehind)	Risque	Cluster	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Commutation automatique non planifiée MetroCluster désactivée (ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risque	Cluster	Avertissement
Mot de passe de l'utilisateur du cluster modifié *(cluster.passwd.changed)	Événement	Cluster	Information

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil de déséquilibre de capacité du cluster (ocumConformanceNodeImbalanceWarning)	Risque	Cluster	Avertissement
Planification des niveaux de cluster Cloud (clusterCloudTierPlanningWarning)	Risque	Cluster	Avertissement
Resynchronisation de la réplication du miroir FabricPool terminée *(wafCaResyncComplete)	Événement	Cluster	Avertissement
Espace FabricPool presque plein *(fabricpoolNearlyFull)	Risque	Cluster	Erreur

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Nœud ajouté (non applicable)	Événement	Cluster	Information

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Nœud supprimé (non applicable)	Événement	Cluster	Information
Cluster supprimé (non applicable)	Événement	Cluster	Information
Échec de l'ajout du cluster (non applicable)	Événement	Cluster	Erreur
Nom du cluster modifié (sans objet)	Événement	Cluster	Information
Urgence médicale reçue (sans objet)	Événement	Cluster	Primordial
EMS critique reçu (sans objet)	Événement	Cluster	Primordial
Alerte EMS reçue (sans objet)	Événement	Cluster	Erreur
Erreur EMS reçue (sans objet)	Événement	Cluster	Avertissement
Avertissement EMS reçu (sans objet)	Événement	Cluster	Avertissement
EMS de débogage reçu (sans objet)	Événement	Cluster	Avertissement
Avis EMS reçu (sans objet)	Événement	Cluster	Avertissement
Message d'information EMS reçu (sans objet)	Événement	Cluster	Avertissement

Les événements ONTAP EMS sont classés en trois niveaux de gravité des événements Unified Manager.

Niveau de gravité des événements d'Unified Manager	Niveau de gravité des événements ONTAP EMS
Primordial	Urgence Primordial
Erreur	Alerte

Avertissement	Erreur Avertissement Déboguer Avis Informatif

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil de déséquilibre de charge du cluster()	Risque	Cluster	Avertissement
Dépassement du seuil critique d'IOPS du cluster (ocumClusterIopsIncident)	Incident	Cluster	Primordial
Dépassement du seuil d'avertissement IOPS du cluster (ocumClusterIopsWarning)	Risque	Cluster	Avertissement
Dépassement du seuil critique de débit en Mo/s du cluster (ocumClusterMbpsIncident)	Incident	Cluster	Primordial
Dépassement du seuil d'avertissement de débit en Mo/s du cluster (ocumClusterMbpsWarning)	Risque	Cluster	Avertissement
Dépassement du seuil dynamique du cluster (ocumClusterDynamicEventWarning)	Risque	Cluster	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Transport HTTPS AutoSupport désactivé (ocumClusterASUPHttps ConfiguredDisabled)	Risque	Cluster	Avertissement
Transfert de journaux non chiffré (ocumClusterAuditLogUn encrypted)	Risque	Cluster	Avertissement
Utilisateur administrateur local par défaut activé (ocumClusterDefaultAdmi nEnabled)	Risque	Cluster	Avertissement
Mode FIPS désactivé (ocumClusterFipsDisab led)	Risque	Cluster	Avertissement
Bannière de connexion désactivée (ocumClusterLoginBanner Disabled)	Risque	Cluster	Avertissement
Bannière de connexion modifiée (ocumClusterLoginBanner Changed)	Risque	Cluster	Avertissement
Destinations de transfert de journaux modifiées (ocumLogForwardDestina tionsChanged)	Risque	Cluster	Avertissement
Noms de serveur NTP modifiés (ocumNtpServerNamesC hanged)	Risque	Cluster	Avertissement
Le nombre de serveurs NTP est faible (securityConfigNTPServer CountLowRisk)	Risque	Cluster	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Communication entre homologues du cluster non chiffrée (ocumClusterPeerEncryptionDisabled)	Risque	Cluster	Avertissement
SSH utilise des chiffrements non sécurisés (ocumClusterSSHInsecure)	Risque	Cluster	Avertissement
Protocole Telnet activé (ocumClusterTelnetEnabled)	Risque	Cluster	Avertissement
Les mots de passe de certains comptes d'utilisateur ONTAP utilisent la fonction de hachage MD5 moins sécurisée (ocumClusterMD5PasswordHashUsed)	Risque	Cluster	Avertissement
Le cluster utilise un certificat auto-signé (ocumClusterSelfSignedCertificate)	Risque	Cluster	Avertissement
Le shell distant du cluster est activé (ocumClusterRshDisabled)	Risque	Cluster	Avertissement
Certificat de cluster sur le point d'expirer (ocumEvtClusterCertificateAboutToExpire)	Risque	Cluster	Avertissement
Certificat de cluster expiré (ocumEvtClusterCertificateExpired)	Risque	Cluster	Erreur

Événements sur les disques

Les événements de disques vous fournissent des informations sur l'état des disques afin

que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Disques Flash - Blocs de réserve presque épuisés (ocumEvtClusterFlashDiskFewerSpareBlockError)	Risque	Cluster	Erreur
Disques Flash - Aucun bloc de rechange (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incident	Cluster	Primordial
Certains disques non attribués (ocumEvtClusterUnassignedDisksSome)	Risque	Cluster	Avertissement
Certains disques défaillants (ocumEvtDisksSomeFailed)	Incident	Cluster	Primordial

Événements liés aux enceintes

Les événements de boîtiers vous fournissent des informations sur l'état des boîtiers d'étagères de disques dans votre centre de données afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Échec des ventilateurs du plateau de disque (ocumEvtShelfFanFailed)	Incident	Étagère de rangement	Primordial
Échec des alimentations du plateau de disque (ocumEvtShelfPowerSupplyFailed)	Incident	Étagère de rangement	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Chemin d'accès multiple de l'étagère de disques non configuré (ocumDiskShelfConnectivityNotInMultiPath) Cet événement ne s'applique pas à : - Clusters qui sont dans une configuration MetroCluster - Les plateformes suivantes : FAS2554, FAS2552, FAS2520 et FAS2240	Risque	Nœud	Avertissement
Échec du chemin d'accès au disque dur (ocumDiskShelfConnectivityPathFailure)	Risque	Étagère de rangement	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Étagère de disque découverte (sans objet)	Événement	Nœud	Information
Étagères de disques supprimées (sans objet)	Événement	Nœud	Information

Événements pour les fans

Les événements de ventilateurs vous fournissent des informations sur l'état des ventilateurs sur les nœuds de votre centre de données afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Un ou plusieurs ventilateurs en panne (ocumEvtFansOneOrMoreFailed)	Incident	Nœud	Primordial

Événements de cartes flash

Les événements de cartes flash vous fournissent des informations sur l'état des cartes flash installées sur les nœuds de votre centre de données afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Cartes Flash hors ligne (ocumEvtFlashCardOffline)	Incident	Nœud	Primordial

Événements d'inodes

Les événements d'inode fournissent des informations lorsque l'inode est plein ou presque plein afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Inodes presque pleins (ocumEvtInodesAlmostFull)	Risque	Volume	Avertissement
Inodes complets (ocumEvtInodesFull)	Risque	Volume	Erreur

Événements d'interface réseau (LIF)

Les événements d'interface réseau fournissent des informations sur l'état de votre interface réseau (LIF), afin que vous puissiez surveiller les problèmes potentiels. Les

événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
État de l'interface réseau en panne (ocumEvtLifStatusDown)	Risque	Interface	Erreur
État de l'interface réseau FC/FCoE en panne (ocumEvtFCLifStatusDown)	Risque	Interface	Erreur
Basculement de l'interface réseau impossible (ocumEvtLifFailoverNotPossible)	Risque	Interface	Avertissement
Interface réseau non présente sur le port d'origine (ocumEvtLifNotAtHomePort)	Risque	Interface	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Route d'interface réseau non configurée (non applicable)	Événement	Interface	Information

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique de débit en Mo/s de l'interface réseau (ocumNetworkLifMbpsIncident)	Incident	Interface	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement de débit en Mo/s de l'interface réseau (ocumNetworkLifMbpsWarning)	Risque	Interface	Avertissement
Dépassement du seuil critique de débit en Mo/s de l'interface réseau FC (ocumFcpLifMbpsIncident)	Incident	Interface	Primordial
Dépassement du seuil d'avertissement de débit en Mo/s de l'interface réseau FC (ocumFcpLifMbpsWarning)	Risque	Interface	Avertissement
Dépassement du seuil critique de débit en Mo/s de l'interface réseau FC NVMf (ocumNvmfFcLifMbpsIncident)	Incident	Interface	Primordial
Dépassement du seuil d'avertissement de débit en Mo/s de l'interface réseau FC NVMf (ocumNvmfFcLifMbpsWarning)	Risque	Interface	Avertissement

Événements LUN

Les événements LUN vous fournissent des informations sur l'état de vos LUN, afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
LUN hors ligne (ocumEvtLunOffline)	Incident	LUN	Primordial
LUN détruit *(lunDestroy)	Événement	LUN	Information
LUN mappé avec un système d'exploitation non pris en charge dans igroup (igroupUnsupportedOsType)	Incident	LUN	Avertissement
Chemin actif unique pour accéder au LUN (ocumEvtLunSingleActivePath)	Risque	LUN	Avertissement
Aucun chemin actif pour accéder au LUN (ocumEvtLunNotReachable)	Incident	LUN	Primordial
Aucun chemin optimisé pour accéder au LUN (ocumEvtLunOptimizedPathInactive)	Risque	LUN	Avertissement
Aucun chemin d'accès au LUN depuis le partenaire HA (ocumEvtLunHaPathInactive)	Risque	LUN	Avertissement
Aucun chemin d'accès au LUN à partir d'un nœud dans une paire HA (ocumEvtLunNodePathStatusDown)	Risque	LUN	Erreur

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Espace insuffisant pour la copie d'instantané LUN (ocumEvtLunSnapshotNotPossible)	Risque	Volume	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
LUN mappé avec un système d'exploitation non pris en charge dans igroup (igroupUnsupportedOsType)	Risque	LUN	Avertissement

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'IOPS LUN (ocumLunIopsIncident)	Incident	LUN	Primordial
Seuil d'avertissement IOPS LUN dépassé (ocumLunIopsWarning)	Risque	LUN	Avertissement
Dépassement du seuil critique de débit en Mo/s du LUN (ocumLunMbpsIncident)	Incident	LUN	Primordial
Seuil d'avertissement LUN MB/s dépassé (ocumLunMbpsWarning)	Risque	LUN	Avertissement
Dépassement du seuil critique de latence LUN (ms/op) (ocumLunLatencyIncident)	Incident	LUN	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement ms/op de latence LUN (ocumLunLatencyWarning)	Risque	LUN	Avertissement
Dépassement du seuil critique de latence LUN et d'IOPS (ocumLunLatencylopsIncident)	Incident	LUN	Primordial
Dépassement du seuil d'avertissement de latence LUN et d'IOPS (ocumLunLatencylopsWarning)	Risque	LUN	Avertissement
Latence LUN et seuil critique en Mo/s dépassés (ocumLunLatencyMbpsIncident)	Incident	LUN	Primordial
Dépassement du seuil d'avertissement de latence LUN et de débit en Mo/s (ocumLunLatencyMbpsWarning)	Risque	LUN	Avertissement
Seuil critique de latence LUN et de capacité de performance globale utilisée dépassé (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incident	LUN	Primordial
Avertissement concernant le seuil de latence LUN et la capacité de performance globale utilisée (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risque	LUN	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique de latence et d'utilisation globale des LUN (ocumLunLatencyAggregateUtilizationIncident)	Incident	LUN	Primordial
Dépassement du seuil d'avertissement de latence et d'utilisation globale des LUN (ocumLunLatencyAggregateUtilizationWarning)	Risque	LUN	Avertissement
Seuil critique de latence LUN et de capacité de performance des nœuds utilisé dépassé (ocumLunLatencyNodePerfCapacityUsedIncident)	Incident	LUN	Primordial
Avertissement concernant le seuil de latence LUN et la capacité de performance des nœuds utilisés (ocumLunLatencyNodePerfCapacityUsedWarning)	Risque	LUN	Avertissement
Latence LUN et capacité de performance des nœuds utilisée - Seuil critique de reprise dépassé (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	LUN	Primordial
Latence LUN et capacité de performance des nœuds utilisés - Seuil d'avertissement de reprise dépassé (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risque	LUN	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique de latence LUN et d'utilisation des nœuds (ocumLunLatencyNodeUtilizationIncident)	Incident	LUN	Primordial
Dépassement du seuil d'avertissement de latence LUN et d'utilisation des nœuds (ocumLunLatencyNodeUtilizationWarning)	Risque	LUN	Avertissement
Dépassement du seuil d'avertissement QoS LUN Max IOPS (ocumQosLunMaxIopsWarning)	Risque	LUN	Avertissement
Dépassement du seuil d'avertissement QoS LUN Max MB/s (ocumQosLunMaxMbpsWarning)	Risque	LUN	Avertissement
Dépassement du seuil de latence du LUN de charge de travail, tel que défini par la politique de niveau de service de performance (ocumConformanceLatencyWarning)	Risque	LUN	Avertissement

Événements de la station de gestion

Les événements de la station de gestion vous fournissent des informations sur l'état du serveur sur lequel Unified Manager est installé afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Espace disque du serveur de gestion presque plein (ocumEvtUnifiedManager DiskSpaceNearlyFull)	Risque	Poste de gestion	Avertissement
Espace disque du serveur de gestion plein (ocumEvtUnifiedManager DiskSpaceFull)	Incident	Poste de gestion	Primordial
Serveur de gestion à faible niveau de mémoire (ocumEvtUnifiedManager MemoryLow)	Risque	Poste de gestion	Avertissement
Serveur de gestion presque à court de mémoire (ocumEvtUnifiedManager MemoryAlmostOut)	Incident	Poste de gestion	Primordial
Augmentation de la taille du fichier journal MySQL ; redémarrage requis (ocumEvtMysqlLogFileSiz eWarning)	Incident	Poste de gestion	Avertissement
La taille totale allouée au journal d'audit est sur le point d'être saturée	Risque	Poste de gestion	Avertissement
Le certificat du serveur Syslog est sur le point d'expirer	Risque	Poste de gestion	Avertissement
Certificat du serveur Syslog expiré	Risque	Poste de gestion	Erreur
Fichier journal d'audit falsifié	Risque	Poste de gestion	Avertissement
Fichier journal d'audit supprimé	Risque	Poste de gestion	Avertissement
Erreur de connexion au serveur Syslog	Risque	Poste de gestion	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Configuration du serveur Syslog modifiée	Événement	Poste de gestion	Avertissement

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
L'analyse des données de performance est affectée (ocumEvtUnifiedManagerDataMissingAnalyze)	Risque	Poste de gestion	Avertissement
La collecte des données de performances est affectée (ocumEvtUnifiedManagerDataMissingCollection)	Incident	Poste de gestion	Primordial



Ces deux derniers événements de performance n'étaient disponibles que pour Unified Manager 7.2. Si l'un de ces événements existe dans l'état Nouveau, puis que vous effectuez une mise à niveau vers une version plus récente du logiciel Unified Manager, les événements ne seront pas purgés automatiquement. Vous devrez déplacer les événements vers l'état Résolu manuellement.

Événements du MetroCluster Bridge

Les événements MetroCluster Bridge vous fournissent des informations sur l'état des ponts afin que vous puissiez surveiller les problèmes potentiels dans une configuration MetroCluster sur FC. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Pont inaccessible (ocumEvtBridgeUnreachable)	Incident	Pont MetroCluster	Primordial
Température anormale du pont (ocumEvtBridgeTemperatureAbnormal)	Incident	Pont MetroCluster	Primordial

Événements de connectivité MetroCluster

Les événements de connectivité vous fournissent des informations sur la connectivité entre les composants d'un cluster et entre les clusters dans les configurations MetroCluster sur FC et MetroCluster sur IP, afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Événements communs aux deux configurations

Ces événements de connectivité sont communs aux configurations MetroCluster sur FC et MetroCluster sur IP.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Tous les liens entre les partenaires MetroCluster sont interrompus (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incident	Relation MetroCluster	Primordial
Partenaires MetroCluster inaccessibles via le réseau de peering (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incident	Relation MetroCluster	Primordial
Capacité de reprise après sinistre de MetroCluster impactée (ocumEvtMetroClusterDRStatusImpacted)	Risque	Relation MetroCluster	Primordial
Configuration du MetroCluster commutée (ocumEvtMetroClusterDRStatusImpacted)	Risque	Relation MetroCluster	Avertissement

Configuration MetroCluster sur FC

Ces événements concernent les configurations MetroCluster sur FC.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Toutes les liaisons inter-commutateurs sont interrompues (ocumEvtMetroClusterAllSLBetweenSwitchesDown)	Incident	Connexion inter-commutateurs MetroCluster	Primordial
Liaison pont FC-SAS vers pile de stockage interrompue (ocumEvtBridgeSasPortDown)	Incident	Connexion de pile de pont MetroCluster	Primordial
Configuration de MetroCluster partiellement basculée (ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risque	Relation MetroCluster	Erreur
Nœud vers commutateur FC : toutes les liaisons d'interconnexion FC-VI sont désactivées (ocumEvtMccNodeSwitchFcviLinksDown)	Incident	Connexion du commutateur de nœud MetroCluster	Primordial
Nœud vers commutateur FC : une ou plusieurs liaisons d'initiateur FC désactivées (ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risque	Connexion du commutateur de nœud MetroCluster	Avertissement
Nœud vers commutateur FC : toutes les liaisons d'initiateur FC sont désactivées (ocumEvtMccNodeSwitchFcLinksDown)	Incident	Connexion du commutateur de nœud MetroCluster	Primordial
Passer au pont FC-SAS, liaison FC interrompue (ocumEvtMccSwitchBridgeFcLinksDown)	Incident	Connexion au pont de commutation MetroCluster	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Tous les liens d'interconnexion FC VI entre nœuds sont hors service (ocumEvtMccInterNodeLinksDown)	Incident	Connexion inter-nœuds	Primordial
Interconnexions FC VI entre nœuds : une ou plusieurs liaisons sont interrompues (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risque	Connexion inter-nœuds	Avertissement
Liaison nœud-pont interrompue (ocumEvtMccNodeBridgeLinksDown)	Incident	Connexion de pont de nœud	Primordial
Nœud vers pile de stockage : tous les liens SAS sont désactivés (ocumEvtMccNodeStackLinksDown)	Incident	Connexion à la pile de nœuds	Primordial
Nœud vers pile de stockage : une ou plusieurs liaisons SAS sont interrompues (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risque	Connexion à la pile de nœuds	Avertissement

Configuration de MetroCluster sur IP

Ces événements concernent les configurations MetroCluster sur IP.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
L'état de connectivité intersite IP de MetroCluster est en panne (mccIntersiteconnectivityStatusDown)	Risque	Relation MetroCluster	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
MetroCluster- Nœud IP pour commuter la connexion hors ligne (mcclpPortStatusOffline)	Risque	Nœud	Erreur

Événements de commutation MetroCluster

Les événements de commutation MetroCluster pour les configurations MetroCluster sur FC vous fournissent des informations sur l'état des commutateurs MetroCluster afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Température de commutation anormale (ocumEvtSwitchTemperatureAbnormal)	Incident	Commutateur MetroCluster	Primordial
Commutateur inaccessible (ocumEvtSwitchUnreachable)	Incident	Commutateur MetroCluster	Primordial
Échec du commutateur de ventilateurs (ocumEvtSwitchFansOneOrMoreFailed)	Incident	Commutateur MetroCluster	Primordial
Échec des alimentations de commutation (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incident	Commutateur MetroCluster	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Échec du commutateur de capteurs de température (ocumEvtSwitchTemperatureSensorFailed)  Cet événement s'applique uniquement aux commutateurs Cisco .	Incident	Commutateur MetroCluster	Primordial

Événements de l'espace de noms NVMe

Les événements d'espace de noms NVMe vous fournissent des informations sur l'état de vos espaces de noms, afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
NVMeNS hors ligne *(nvmeNamespaceStatusOffline)	Événement	Espace de noms	Information
NVMeNS en ligne *(nvmeNamespaceStatusOnline)	Événement	Espace de noms	Information
NVMeNS manque d'espace *(nvmeNamespaceSpaceOutOfSpace)	Risque	Espace de noms	Avertissement
NVMeNS Détruire *(nvmeNamespaceDestroy)	Événement	Espace de noms	Information

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'IOPS de l'espace de noms NVMe (ocumNvmeNamespacesIopsIncident)	Incident	Espace de noms	Primordial
Dépassement du seuil d'avertissement IOPS de l'espace de noms NVMe (ocumNvmeNamespacesIopsWarning)	Risque	Espace de noms	Avertissement
Dépassement du seuil critique de débit en Mo/s de l'espace de noms NVMe (ocumNvmeNamespacesMbpsIncident)	Incident	Espace de noms	Primordial
Seuil d'avertissement de débit en Mo/s de l'espace de noms NVMe dépassé (ocumNvmeNamespacesMbpsWarning)	Risque	Espace de noms	Avertissement
Dépassement du seuil critique de latence ms/op de l'espace de noms NVMe (ocumNvmeNamespacesLatencyIncident)	Incident	Espace de noms	Primordial
Seuil d'avertissement ms/op de latence de l'espace de noms NVMe dépassé (ocumNvmeNamespacesLatencyWarning)	Risque	Espace de noms	Avertissement
Dépassement du seuil critique de latence et d'IOPS de l'espace de noms NVMe (ocumNvmeNamespacesLatencyIopsIncident)	Incident	Espace de noms	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil d'avertissement de latence et d'IOPS de l'espace de noms NVMe dépassé (ocumNvmeNamespaceLatencyIopsWarning)	Risque	Espace de noms	Avertissement
Latence de l'espace de noms NVMe et seuil critique en Mo/s dépassé (ocumNvmeNamespaceLatencyMbpsIncident)	Incident	Espace de noms	Primordial
Latence de l'espace de noms NVMe et seuil d'avertissement de débit en Mo/s dépassé (ocumNvmeNamespaceLatencyMbpsWarning)	Risque	Espace de noms	Avertissement

Événements de nœud

Les événements de nœud vous fournissent des informations sur l'état du nœud afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Espace du volume racine du nœud presque plein (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risque	Nœud	Avertissement
Cloud AWS MetadataConnFail *(ocumCloudAwsMetadataConnFail)	Risque	Nœud	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Cloud AWS IAMCredsExpiré *(ocumCloudAwsIamCredsExpiré)	Risque	Nœud	Erreur
Cloud AWS IAMCredsInvalide *(ocumCloudAwsIamCredsInvalid)	Risque	Nœud	Erreur
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risque	Nœud	Erreur
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Événement	Nœud	Information
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Risque	Nœud	Erreur
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risque	Nœud	Erreur
Hôte de niveau cloud non résoluble *(ocumObjstoreHostUnresolvable)	Risque	Nœud	Erreur
Interface réseau intercluster de niveau cloud en panne *(ocumObjstoreInterClusterLifDown)	Risque	Nœud	Erreur
L'un des pools NFSv4 épuisé *(nbladeNfsv4PoolExhaust)	Incident	Nœud	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Demande de non-concordance de signature Cloud Tier *(oscSignatureMismatch)	Risque	Nœud	Erreur

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Mémoire du moniteur QoS au maximum *(ocumQosMonitorMemoryMaxed)	Risque	Nœud	Erreur
Mémoire du moniteur QoS réduite *(ocumQosMonitorMemoryAbated)	Événement	Nœud	Information

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Nœud renommé (sans objet)	Événement	Nœud	Information

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'IOPS du nœud (ocumNodeIopsIncident)	Incident	Nœud	Primordial
Dépassement du seuil d'avertissement IOPS du nœud (ocumNodeIopsWarning)	Risque	Nœud	Avertissement
Dépassement du seuil critique de débit en Mo/s du nœud (ocumNodeMbpsIncident)	Incident	Nœud	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement de débit en Mo/s du nœud (ocumNodeMbpsWarning)	Risque	Nœud	Avertissement
Dépassement du seuil critique de latence du nœud (ms/op) (ocumNodeLatencyIncident)	Incident	Nœud	Primordial
Dépassement du seuil d'avertissement ms/op de latence du nœud (ocumNodeLatencyWarning)	Risque	Nœud	Avertissement
Dépassement du seuil critique de capacité de performance du nœud (ocumNodePerfCapacityUsedIncident)	Incident	Nœud	Primordial
Avertissement : dépassement du seuil d'avertissement de capacité de performance du nœud (ocumNodePerfCapacityUsedWarning)	Risque	Nœud	Avertissement
Capacité de performance du nœud utilisée - Seuil critique de reprise dépassé (ocumNodePerfCapacityUsedTakeoverIncident)	Incident	Nœud	Primordial
Capacité de performance du nœud utilisée - Seuil d'avertissement de reprise dépassé (ocumNodePerfCapacityUsedTakeoverWarning)	Risque	Nœud	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'utilisation des nœuds (ocumNodeUtilizationIncident)	Incident	Nœud	Primordial
Seuil d'avertissement d'utilisation des nœuds dépassé (ocumNodeUtilizationWarning)	Risque	Nœud	Avertissement
Dépassement du seuil de surutilisation de la paire de nœuds HA (ocumNodeHaPairOverUtilizedInformation)	Événement	Nœud	Information
Dépassement du seuil de fragmentation du disque du nœud (ocumNodeDiskFragmentationWarning)	Risque	Nœud	Avertissement
Seuil de capacité de performance utilisé dépassé (ocumNodeOverUtilizedWarning)	Risque	Nœud	Avertissement
Dépassement du seuil dynamique du nœud (ocumNodeDynamicEventWarning)	Risque	Nœud	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
ID d'avis : NTAP- <i><ID d'avis></i> (ocumx)	Risque	Nœud	Primordial

Événements de batterie NVRAM

Les événements de batterie NVRAM vous fournissent des informations sur l'état de vos batteries afin que vous puissiez surveiller les problèmes potentiels. Les événements sont

regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Batterie NVRAM faible (ocumEvtNvramBatteryLow)	Risque	Nœud	Avertissement
Batterie NVRAM déchargée (ocumEvtNvramBatteryDischarged)	Risque	Nœud	Erreur
Batterie NVRAM trop chargée (ocumEvtNvramBatteryOverCharged)	Incident	Nœud	Primordial

Événements portuaires

Les événements de port vous fournissent l'état des ports du cluster afin que vous puissiez surveiller les changements ou les problèmes sur le port, par exemple si le port est en panne.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
État du port en panne (ocumEvtPortStatusDown)	Incident	Nœud	Primordial

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique de débit en Mo/s du port réseau (ocumNetworkPortMbpsIncident)	Incident	Port	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement de débit en Mo/s du port réseau (ocumNetworkPortMbpsWarning)	Risque	Port	Avertissement
Dépassement du seuil critique de débit en MB/s du port FCP (ocumFcpPortMbpsIncident)	Incident	Port	Primordial
Dépassement du seuil d'avertissement de débit en MB/s du port FCP (ocumFcpPortMbpsWarning)	Risque	Port	Avertissement
Dépassement du seuil critique d'utilisation des ports réseau (ocumNetworkPortUtilizationIncident)	Incident	Port	Primordial
Seuil d'avertissement d'utilisation du port réseau dépassé (ocumNetworkPortUtilizationWarning)	Risque	Port	Avertissement
Dépassement du seuil critique d'utilisation du port FCP (ocumFcpPortUtilizationIncident)	Incident	Port	Primordial
Seuil d'avertissement d'utilisation du port FCP dépassé (ocumFcpPortUtilizationWarning)	Risque	Port	Avertissement

Événements liés aux alimentations électriques

Les événements d'alimentation vous fournissent des informations sur l'état de votre matériel afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau

d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Une ou plusieurs alimentations défectueuses (ocumEvtPowerSupplyOneOrMoreFailed)	Incident	Nœud	Primordial

Événements de protection

Les événements de protection vous indiquent si une tâche a échoué ou a été abandonnée afin que vous puissiez surveiller les problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Échec de la tâche de protection (ocumEvtProtectionJobTaskFailed)	Incident	Volume ou service de stockage	Primordial
Tâche de protection abandonnée (ocumEvtProtectionJobAborted)	Risque	Volume ou service de stockage	Avertissement

Événements Qtree

Les événements Qtree vous fournissent des informations sur la capacité de Qtree et les limites des fichiers et du disque afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Espace Qtree presque plein (ocumEvtQtreeSpaceNearlyFull)	Risque	Qtree	Avertissement
Espace Qtree plein (ocumEvtQtreeSpaceFull)	Risque	Qtree	Erreur
Espace Qtree normal (ocumEvtQtreeSpaceThresholdOk)	Événement	Qtree	Information
Limite stricte des fichiers Qtree atteinte (ocumEvtQtreeFilesHardLimitReached)	Incident	Qtree	Primordial
Dépassement de la limite logicielle des fichiers Qtree (ocumEvtQtreeFilesSoftLimitBreached)	Risque	Qtree	Avertissement
Limite stricte d'espace Qtree atteinte (ocumEvtQtreeSpaceHardLimitReached)	Incident	Qtree	Primordial
Dépassement de la limite souple de l'espace Qtree (ocumEvtQtreeSpaceSoftLimitBreached)	Risque	Qtree	Avertissement

Événements du processeur de service

Les événements du processeur de service vous fournissent des informations sur l'état de votre processeur afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Processeur de service non configuré (ocumEvtServiceProcessorNotConfigured)	Risque	Nœud	Avertissement
Processeur de service hors ligne (ocumEvtServiceProcessorOffline)	Risque	Nœud	Erreur

Événements relationnels SnapMirror

Les événements de relation SnapMirror vous fournissent des informations sur l'état de vos relations SnapMirror asynchrones et synchrones afin que vous puissiez surveiller les problèmes potentiels. Les événements de relation SnapMirror asynchrones sont générés pour les machines virtuelles de stockage et les volumes, mais les événements de relation SnapMirror synchrones sont générés uniquement pour les relations de volume. Aucun événement n'est généré pour les volumes constitutifs qui font partie des relations de reprise après sinistre de la machine virtuelle de stockage. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.



Les événements de relations SnapMirror sont générés pour les machines virtuelles de stockage protégées par la récupération après sinistre des machines virtuelles de stockage, mais pas pour les relations d'objets constitutifs.

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Réplication miroir défectueuse (ocumEvtSnapmirrorRelationshipUnhealthy)	Risque	Relation SnapMirror	Avertissement
Réplication miroir interrompue (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risque	Relation SnapMirror	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Échec de l'initialisation de la réplication miroir (ocumEvtSnapmirrorRelationshipInitializeFailed)	Risque	Relation SnapMirror	Erreur
Échec de la mise à jour de la réplication miroir (ocumEvtSnapmirrorRelationshipUpdateFailed)	Risque	Relation SnapMirror	Erreur
Erreur de décalage de réplication miroir (ocumEvtSnapMirrorRelationshipLagError)	Risque	Relation SnapMirror	Erreur
Avertissement de décalage de réplication miroir (ocumEvtSnapMirrorRelationshipLagWarning)	Risque	Relation SnapMirror	Avertissement
Échec de la resynchronisation de la réplication miroir (ocumEvtSnapmirrorRelationshipResyncFailed)	Risque	Relation SnapMirror	Erreur
Réplication synchrone désynchronisée *(syncSnapmirrorRelationshipOutofsync)	Risque	Relation SnapMirror	Avertissement
Réplication synchrone restaurée *(syncSnapmirrorRelationshipInSync)	Événement	Relation SnapMirror	Information
Échec de la resynchronisation automatique de la réplication synchrone *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risque	Relation SnapMirror	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Ontap Mediator est ajouté sur le cluster (snapmirrorMediatorAdded)	Événement	Cluster	Information
Ontap Mediator est supprimé du cluster (snapmirrorMediatorRemoved)	Événement	Cluster	Information
Ontap Mediator est inaccessible depuis le cluster (snapmirrorMediatorUnreachable)	Risque	Médiateur	Avertissement
Ontap Mediator n'est pas accessible depuis le cluster (snapmirrorMediatorMisconfigured)	Risque	Médiateur	Erreur
La connectivité d'Ontap Mediator a été rétablie et est resynchronisée et prête pour la synchronisation active de SnapMirror (snapmirrorMediatorInQuorum)	Événement	Médiateur	Information

Événements de relation miroir et coffre-fort asynchrones

Les événements de relation miroir asynchrone et coffre-fort vous fournissent des informations sur l'état de vos relations SnapMirror asynchrone et coffre-fort afin que vous puissiez surveiller les problèmes potentiels. Les événements de relation miroir et coffre asynchrones sont pris en charge pour les relations de protection de volume et de machine virtuelle de stockage. Mais seules les relations Vault ne sont pas prises en charge pour la reprise après sinistre de la machine virtuelle de stockage. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection



Les événements de relations SnapMirror et Vault sont également générés pour les machines virtuelles de stockage protégées par la récupération après sinistre des machines virtuelles de stockage, mais pas pour les relations d'objets constitutifs.

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Miroir asynchrone et coffre-fort défectueux (ocumEvtMirrorVaultRelationshipUnhealthy)	Risque	Relation SnapMirror	Avertissement
Miroir asynchrone et coffre-fort interrompus (ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risque	Relation SnapMirror	Erreur
Échec de l'initialisation du miroir asynchrone et du coffre-fort (ocumEvtMirrorVaultRelationshipInitializeFailed)	Risque	Relation SnapMirror	Erreur
Échec de la mise à jour asynchrone du miroir et du coffre-fort (ocumEvtMirrorVaultRelationshipUpdateFailed)	Risque	Relation SnapMirror	Erreur
Erreur de décalage du miroir asynchrone et du coffre-fort (ocumEvtMirrorVaultRelationshipLagError)	Risque	Relation SnapMirror	Erreur
Avertissement de décalage entre miroir asynchrone et coffre-fort (ocumEvtMirrorVaultRelationshipLagWarning)	Risque	Relation SnapMirror	Avertissement
Échec de la resynchronisation asynchrone du miroir et du coffre-fort (ocumEvtMirrorVaultRelationshipResyncFailed)	Risque	Relation SnapMirror	Erreur



L'événement « Échec de la mise à jour de SnapMirror » est déclenché par le portail Active IQ (Config Advisor).

Instantanés d'événements

Les événements d'instantanés fournissent des informations sur l'état des instantanés, ce qui vous permet de surveiller les instantanés pour détecter d'éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement, le nom du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Suppression automatique des instantanés désactivée (non applicable)	Événement	Volume	Information
Suppression automatique des instantanés activée (non applicable)	Événement	Volume	Information
Configuration de suppression automatique des instantanés modifiée (non applicable)	Événement	Volume	Information

Événements relationnels SnapVault

Les événements de relation SnapVault vous fournissent des informations sur l'état de vos relations SnapVault afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Coffre-fort asynchrone défectueux (ocumEvtSnapVaultRelationshipUnhealthy)	Risque	Relation SnapMirror	Avertissement
Coffre-fort asynchrone interrompu (ocumEvtSnapVaultRelationshipStateBrokenoff)	Risque	Relation SnapMirror	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Échec de l'initialisation du coffre-fort asynchrone (ocumEvtSnapVaultRelationshipInitializeFailed)	Risque	Relation SnapMirror	Erreur
Échec de la mise à jour asynchrone du coffre-fort (ocumEvtSnapVaultRelationshipUpdateFailed)	Risque	Relation SnapMirror	Erreur
Erreur de décalage du coffre-fort asynchrone (ocumEvtSnapVaultRelationshipLagError)	Risque	Relation SnapMirror	Erreur
Avertissement de décalage du coffre-fort asynchrone (ocumEvtSnapVaultRelationshipLagWarning)	Risque	Relation SnapMirror	Avertissement
Échec de la resynchronisation asynchrone du coffre-fort (ocumEvtSnapvaultRelationshipResyncFailed)	Risque	Relation SnapMirror	Erreur

Événements des paramètres de basculement de stockage

Les événements de paramètres de basculement de stockage (SFO) vous fournissent des informations indiquant si votre basculement de stockage est désactivé ou non configuré afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Interconnexion de basculement de stockage : une ou plusieurs liaisons sont interrompues (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risque	Nœud	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Basculement de stockage désactivé (ocumEvtSfoSettingsDisabled)	Risque	Nœud	Erreur
Basculement de stockage non configuré (ocumEvtSfoSettingsNotConfigured)	Risque	Nœud	Erreur
État de basculement du stockage - Reprise (ocumEvtSfoStateTakeover)	Risque	Nœud	Avertissement
État de basculement du stockage - Retour partiel (ocumEvtSfoStatePartialGiveback)	Risque	Nœud	Erreur
État du nœud de basculement de stockage désactivé (ocumEvtSfoNodeStatusDown)	Risque	Nœud	Erreur
Basculement de stockage impossible (ocumEvtSfoTakeoverNotPossible)	Risque	Nœud	Erreur

Événements liés aux services de stockage

Les événements des services de stockage vous fournissent des informations sur la création et l'abonnement aux services de stockage afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Service de stockage créé (sans objet)	Événement	Service de stockage	Information

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Service de stockage souscrit (sans objet)	Événement	Service de stockage	Information
Service de stockage désabonné (non applicable)	Événement	Service de stockage	Information

Zone d'impact : protection

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Suppression inattendue de la relation SnapMirror géréeocumEvtStorageServiceUnsupportedRelationshipDeletion	Risque	Service de stockage	Avertissement
Suppression inattendue du volume membre du service de stockage (ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incident	Service de stockage	Primordial

Événements sur les étagères de stockage

Les événements d'étagère de stockage vous indiquent si votre étagère de stockage présente une anomalie afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Plage de tension anormale (ocumEvtShelfVoltageAbnormal)	Risque	Étagère de rangement	Avertissement
Plage de courant anormale (ocumEvtShelfCurrentAbnormal)	Risque	Étagère de rangement	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Température anormale (ocumEvtShelfTemperatureAbnormal)	Risque	Étagère de rangement	Avertissement

Événements de la machine virtuelle de stockage

Les événements de machine virtuelle de stockage (SVM, également appelés SVM) vous fournissent des informations sur l'état de vos machines virtuelles de stockage (SVM) afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Service CIFS de la machine virtuelle de stockage arrêté (ocumEvtVserverCifsServiceStatusDown)	Incident	SVM	Primordial
Service SVM CIFS non configuré (non applicable)	Événement	SVM	Information
Tentatives de connexion à un partage CIFS inexistant (nbladeCifsNoPrivShare)	Incident	SVM	Primordial
Conflit de nom NetBIOS CIFS (nbladeCifsNbNameConflict)	Risque	SVM	Erreur
Échec de l'opération de cliché instantané CIFS (cifsShadowCopyFailure)	Risque	SVM	Erreur
Plusieurs connexions CIFS (nbladeCifsManyAuths)	Risque	SVM	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Connexion CIFS maximale dépassée *(nbladeCifsMaxOpenSameFile)	Risque	SVM	Erreur
Nombre maximal de connexions CIFS par utilisateur dépassé *(nbladeCifsMaxSessPerUsrConn)	Risque	SVM	Erreur
Service FC/FCoE SVM hors service (ocumEvtVserverFcServiceStatusDown)	Incident	SVM	Primordial
Service iSCSI SVM arrêté (ocumEvtVserverIscsiServiceStatusDown)	Incident	SVM	Primordial
Service NFS de la machine virtuelle de stockage hors service (ocumEvtVserverNfsServiceStatusDown)	Incident	SVM	Primordial
Service SVM FC/FCoE non configuré (non applicable)	Événement	SVM	Information
Service iSCSI SVM non configuré (non applicable)	Événement	SVM	Information
Service NFS SVM non configuré (non applicable)	Événement	SVM	Information
Machine virtuelle de stockage arrêtée (ocumEvtVserverDown)	Risque	SVM	Avertissement
Le serveur AV est trop occupé pour accepter une nouvelle demande d'analyse *(nbladeVscanConnBackPressure)	Risque	SVM	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Aucune connexion au serveur AV pour l'analyse antivirus *(nbladeVscanNoScannerConn)	Incident	SVM	Primordial
Aucun serveur AV enregistré *(nbladeVscanNoRegdScanner)	Risque	SVM	Erreur
Aucune connexion au serveur AV réactif *(nbladeVscanConnInactive)	Événement	SVM	Information
Tentative d'accès non autorisé d'un utilisateur au serveur AV *(nbladeVscanBadUserPrivAccess)	Risque	SVM	Erreur
Virus détecté par le serveur AV *(nbladeVscanVirusDetected)	Risque	SVM	Erreur

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
SVM découvert (sans objet)	Événement	SVM	Information
SVM supprimé (non applicable)	Événement	Cluster	Information
SVM renommé (sans objet)	Événement	SVM	Information

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'IOPS SVM (ocumSvmIopsIncident)	Incident	SVM	Primordial
Seuil d'avertissement IOPS SVM dépassé (ocumSvmIopsWarning)	Risque	SVM	Avertissement
Dépassement du seuil critique de débit en Mo/s de la SVM (ocumSvmMbpsIncident)	Incident	SVM	Primordial
Seuil d'avertissement SVM MB/s dépassé (ocumSvmMbpsWarning)	Risque	SVM	Avertissement
Dépassement du seuil critique de latence SVM (ocumSvmLatencyIncident)	Incident	SVM	Primordial
Seuil d'avertissement de latence SVM dépassé (ocumSvmLatencyWarning)	Risque	SVM	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Journal d'audit désactivé (ocumVserverAuditLogDisabled)	Risque	SVM	Avertissement
Bannière de connexion désactivée (ocumVserverLoginBannerDisabled)	Risque	SVM	Avertissement
SSH utilise des chiffrements non sécurisés (ocumVserverSSHInsecure)	Risque	SVM	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Bannière de connexion modifiée (ocumVserverLoginBannerChanged)	Risque	SVM	Avertissement
La surveillance anti-ransomware des machines virtuelles de stockage est désactivée (antiRansomwareSvmStateDisabled)	Risque	SVM	Avertissement
La surveillance anti-ransomware des machines virtuelles de stockage est activée (mode d'apprentissage) (antiRansomwareSvmStateDryrun)	Événement	SVM	Information
Machine virtuelle de stockage adaptée à la surveillance anti-ransomware (mode d'apprentissage) (ocumEvtSvmArwCandidate)	Événement	SVM	Information

Événements de quotas d'utilisateurs et de groupes

Les événements de quota d'utilisateur et de groupe vous fournissent des informations sur la capacité du quota d'utilisateur et de groupe d'utilisateurs ainsi que sur les limites de fichier et de disque afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Limite logicielle d'espace disque du quota utilisateur ou groupe dépassée (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risque	Quota d'utilisateur ou de groupe	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Limite d'espace disque du quota utilisateur ou groupe atteinte (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incident	Quota d'utilisateur ou de groupe	Primordial
Dépassement de la limite logicielle du nombre de fichiers de quota d'utilisateur ou de groupe (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreach)	Risque	Quota d'utilisateur ou de groupe	Avertissement
Limite stricte du nombre de fichiers de quota d'utilisateur ou de groupe atteinte (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incident	Quota d'utilisateur ou de groupe	Primordial

Événements de volume

Les événements de volume fournissent des informations sur l'état des volumes, ce qui vous permet de surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement, le nom du piège, le niveau d'impact, le type de source et la gravité.

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Zone d'impact : disponibilité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Volume restreint (ocumEvtVolumeRestricted)	Risque	Volume	Avertissement
Volume hors ligne (ocumEvtVolumeOffline)	Incident	Volume	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Volume partiellement disponible (ocumEvtVolumePartially Available)	Risque	Volume	Erreur
Volume non monté (sans objet)	Événement	Volume	Information
Volume monté (sans objet)	Événement	Volume	Information
Volume remonté (sans objet)	Événement	Volume	Information
Chemin de jonction de volume inactif (ocumEvtVolumeJunction PathInactive)	Risque	Volume	Avertissement
Dimensionnement automatique du volume activé (non applicable)	Événement	Volume	Information
Dimensionnement automatique du volume - Désactivé (non applicable)	Événement	Volume	Information
Volume Autosize Capacité maximale modifiée (sans objet)	Événement	Volume	Information
Augmentation automatique du volume Taille modifiée (sans objet)	Événement	Volume	Information

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Espace de volume à provisionnement fin à risque (ocumThinProvisionVolumeSpaceAtRisk)	Risque	Volume	Avertissement
Erreur d'opération d'efficacité volumique (ocumEvtVolumeEfficiencyOperationError)	Risque	Volume	Erreur
Espace de volume plein (ocumEvtVolumeFull)	Risque	Volume	Erreur
Espace de volume presque plein (ocumEvtVolumeNearlyFull)	Risque	Volume	Avertissement
Espace logique du volume plein (volumeLogicalSpaceFull)	Risque	Volume	Erreur
Espace logique du volume presque plein (volumeLogicalSpaceNearlyFull)	Risque	Volume	Avertissement
Volume Espace logique Normal (volumeLogicalSpaceAllOK)	Événement	Volume	Information
Espace de réserve de snapshot de volume plein (ocumEvtSnapshotFull)	Risque	Volume	Avertissement
Trop de copies d'instantanés (ocumEvtSnapshotTooMany)	Risque	Volume	Erreur
Volume Qtree Quota surchargé (ocumEvtVolumeQtreeQuotaOvercommitted)	Risque	Volume	Erreur

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Volume Qtree Quota presque surchargé (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risque	Volume	Avertissement
Taux de croissance du volume anormal (ocumEvtVolumeGrowthRateAbnormal)	Risque	Volume	Avertissement
Volume en jours jusqu'à la pleine capacité (ocumEvtVolumeDaysUntilFullSoon)	Risque	Volume	Erreur
Garantie d'espace de volume désactivée (non applicable)	Événement	Volume	Information
Garantie d'espace de volume activée (non applicable)	Événement	Volume	Information
Garantie d'espace de volume modifiée (sans objet)	Événement	Volume	Information
Jours de réserve d'instantané de volume jusqu'à saturation (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risque	Volume	Erreur
Les constituants de FlexGroup ont des problèmes d'espace (flexGroupConstituentsHaveSpaceIssues)	Risque	Volume	Erreur
Statut de l'espace des constituants FlexGroup : tout est OK (flexGroupConstituentsSpaceStatusAllOK)	Événement	Volume	Information

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Les constituants de FlexGroup ont des problèmes d'inodes *(flexGroupConstituentsHaveInodesIssues)	Risque	Volume	Erreur
Statut des inodes des constituants du FlexGroup : tout est OK *(flexGroupConstituentsInodesStatusAllOK)	Événement	Volume	Information
Échec de la taille automatique du volume WAFL *(wafVolAutoSizeFail)	Risque	Volume	Erreur
Dimensionnement automatique du volume WAFL terminé *(wafVolAutoSizeDone)	Événement	Volume	Information
Le volume de FlexGroup est utilisé à plus de 80 %*	Incident	Volume	Erreur
Le volume de FlexGroup est utilisé à plus de 90 %*	Incident	Volume	Primordial
Anomalie d'efficacité de stockage du volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risque	Volume	Avertissement
Réserve d'instantanés de volume sous-utilisée (volumeSnapshotReserveUnderutilizedWarning)	Événement	Volume	Avertissement
Réserve d'instantanés de volume sous-utilisée (volumeSnapshotReserveUnderutilizedCleared)	Événement	Volume	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Volume renommé (sans objet)	Événement	Volume	Information
Volume découvert (sans objet)	Événement	Volume	Information
Volume supprimé (sans objet)	Événement	Volume	Information

Domaine d'impact : performance

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement d'IOPS maximal du volume QoS (ocumQosVolumeMaxIopsWarning)	Risque	Volume	Avertissement
Dépassement du seuil d'avertissement de volume QoS maximal en Mo/s (ocumQosVolumeMaxMbpsWarning)	Risque	Volume	Avertissement
Dépassement du seuil d'avertissement de volume QoS max. IOPS/To (ocumQosVolumeMaxIopsPerTbWarning)	Risque	Volume	Avertissement
Dépassement du seuil de latence du volume de charge de travail, tel que défini par la politique de niveau de service de performance (ocumConformanceLatencyWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique d'IOPS de volume (ocumVolumeIopsIncident)	Incident	Volume	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil d'avertissement de volume IOPS dépassé (ocumVolumelopsWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique de volume en Mo/s (ocumVolumeMbpsIncident)	Incident	Volume	Primordial
Seuil d'avertissement de volume en Mo/s dépassé (ocumVolumeMbpsWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique de latence du volume (ocumVolumeLatencyIncident)	Incident	Volume	Primordial
Seuil d'avertissement de latence du volume dépassé (ocumVolumeLatencyWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique du taux d'échec du cache de volume (ocumVolumeCacheMissRatioIncident)	Incident	Volume	Primordial
Seuil d'avertissement de taux d'échec du cache de volume dépassé (ocumVolumeCacheMissRatioWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique de latence du volume et d'IOPS (ocumVolumeLatencyIopsIncident)	Incident	Volume	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement de latence du volume et d'IOPS (ocumVolumeLatencyIopsWarning)	Risque	Volume	Avertissement
Latence du volume et seuil critique en Mo/s dépassés (ocumVolumeLatencyMbpsIncident)	Incident	Volume	Primordial
Dépassement du seuil d'avertissement de latence de volume et de débit en Mo/s (ocumVolumeLatencyMbpsWarning)	Risque	Volume	Avertissement
Seuil critique de latence du volume et de capacité de performance globale utilisée dépassé (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incident	Volume	Primordial
Avertissement concernant le seuil de latence du volume et la capacité de performance globale utilisée (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique de latence du volume et d'utilisation globale (ocumVolumeLatencyAggregateUtilizationIncident)	Incident	Volume	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement de latence du volume et d'utilisation globale (ocumVolumeLatencyAggregateUtilizationWarning)	Risque	Volume	Avertissement
Seuil critique de latence du volume et de capacité de performance des nœuds utilisé dépassé (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incident	Volume	Primordial
Avertissement : seuil de latence du volume et de capacité de performance des nœuds utilisé dépassé (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risque	Volume	Avertissement
Latence du volume et capacité de performance du nœud utilisée - Seuil critique de reprise dépassé (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	Volume	Primordial
Latence du volume et capacité de performance du nœud utilisée - Seuil d'avertissement de reprise dépassé (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risque	Volume	Avertissement
Dépassement du seuil critique de latence du volume et d'utilisation des nœuds (ocumVolumeLatencyNodeUtilizationIncident)	Incident	Volume	Primordial

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil d'avertissement de latence du volume et d'utilisation des nœuds (ocumVolumeLatencyNodeUtilizationWarning)	Risque	Volume	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
La surveillance anti-ransomware du volume est activée (mode actif) (antiRansomwareVolumeStateEnabled)	Événement	Volume	Information
La surveillance anti-ransomware du volume est désactivée (antiRansomwareVolumeStateDisabled)	Risque	Volume	Avertissement
La surveillance anti-ransomware du volume est activée (mode d'apprentissage) (antiRansomwareVolumeStateDryrun)	Événement	Volume	Information
La surveillance anti-ransomware du volume est suspendue (mode d'apprentissage) (antiRansomwareVolumeStateDryrunPaused)	Risque	Volume	Avertissement
La surveillance anti-ransomware du volume est suspendue (mode actif) (antiRansomwareVolumeStateEnablePaused)	Risque	Volume	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
La surveillance anti-ransomware du volume est désactivée (antiRansomwareVolumeStateDisableInProgress)	Risque	Volume	Avertissement
Activité de rançongiciel observée (callHomeRansomwareActivitySeen)	Incident	Volume	Primordial
Volume adapté à la surveillance anti-ransomware (mode d'apprentissage) (ocumEvtVolumeArwCandidate)	Événement	Volume	Information
Volume adapté à la surveillance anti-ransomware (mode actif) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risque	Volume	Avertissement
Le volume présente des alertes anti-ransomware bruyantes (antiRansomwareFeatureNoisyVolume)	Risque	Volume	Avertissement

Domaine d'impact : protection des données

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Le volume ne dispose pas d'une protection suffisante contre les snapshots locaux (volumeLacksLocalProtectionWarning)	Risque	Volume	Avertissement

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Le volume ne dispose pas d'une protection suffisante contre les snapshots locaux (volumeLacksLocalProtectionCleared)	Risque	Volume	Avertissement

Événements d'état de déplacement de volume

Les événements d'état de déplacement de volume vous informent de l'état de votre déplacement de volume afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom du piège)	Niveau d'impact	Type de source	Gravité
Statut du déplacement du volume : En cours (sans objet)	Événement	Volume	Information
État du déplacement du volume - Échec (ocumEvtVolumeMoveFailed)	Risque	Volume	Erreur
Statut du déplacement du volume : Terminé (sans objet)	Événement	Volume	Information
Déplacement de volume - Coupure différée (ocumEvtVolumeMoveCutoverDeferred)	Risque	Volume	Avertissement

Description des fenêtres d'événements et des boîtes de dialogue

Les événements vous informent de tout problème dans votre environnement. Vous pouvez utiliser la page d'inventaire de gestion des événements et la page de détails des événements pour surveiller tous les événements. Vous pouvez utiliser la boîte de dialogue Options de configuration des notifications pour configurer les notifications. Vous pouvez utiliser la page Configuration des événements pour désactiver ou activer les événements.

Page de notifications

Vous pouvez configurer le serveur Unified Manager pour envoyer des notifications lorsqu'un événement est généré ou lorsqu'il est attribué à un utilisateur. Vous pouvez également configurer les mécanismes de notification. Par exemple, les notifications peuvent être envoyées sous forme d'e-mails ou d'interruptions SNMP.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Messagerie électronique

Cette zone vous permet de configurer les paramètres de courrier électronique suivants pour la notification d'alerte :

- **Adresse de l'expéditeur**

Spécifie l'adresse e-mail à partir de laquelle la notification d'alerte est envoyée. Cette valeur est également utilisée comme adresse d'expéditeur pour un rapport lorsqu'il est partagé. Si l'adresse de l'expéditeur est pré-remplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la remplacer par une adresse e-mail réelle et fonctionnelle pour vous assurer que toutes les notifications par e-mail sont envoyées avec succès.

Serveur SMTP

Cette zone vous permet de configurer les paramètres du serveur SMTP suivants :

- **Nom d'hôte ou adresse IP**

Spécifie le nom d'hôte de votre serveur hôte SMTP, qui est utilisé pour envoyer la notification d'alerte aux destinataires spécifiés.

- **Nom d'utilisateur**

Spécifie le nom d'utilisateur SMTP. Le nom d'utilisateur SMTP est requis uniquement lorsque SMTPAUTH est activé sur le serveur SMTP.

- **Mot de passe**

Spécifie le mot de passe SMTP. Le nom d'utilisateur SMTP est requis uniquement lorsque SMTPAUTH est activé sur le serveur SMTP.

- **Port**

Spécifie le port utilisé par le serveur hôte SMTP pour envoyer une notification d'alerte.

La valeur par défaut est 25.

- **Utilisez START/TLS**

Cocher cette case permet une communication sécurisée entre le serveur SMTP et le serveur de gestion en utilisant les protocoles TLS/SSL (également appelés start_tls et StartTLS).

- **Utiliser SSL**

Cocher cette case permet une communication sécurisée entre le serveur SMTP et le serveur de gestion en

utilisant le protocole SSL.

SNMP

Cette zone vous permet de configurer les paramètres de trap SNMP suivants :

- **Version**

Spécifie la version SNMP que vous souhaitez utiliser en fonction du type de sécurité dont vous avez besoin. Les options incluent la version 1, la version 3, la version 3 avec authentification et la version 3 avec authentification et chiffrement. La valeur par défaut est la version 1.

- **Hôte de destination du piège**

Spécifie le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) qui reçoit les interruptions SNMP envoyées par le serveur de gestion. Pour spécifier plusieurs destinations d'interruption, séparez chaque hôte par une virgule.



Tous les autres paramètres SNMP, tels que « Version » et « Port de sortie », doivent être les mêmes pour tous les hôtes de la liste.

- **Port de piège sortant**

Spécifie le port via lequel le serveur SNMP reçoit les interruptions envoyées par le serveur de gestion.

La valeur par défaut est 162.

- **Communauté**

La chaîne de communauté pour accéder à l'hôte.

- **ID du moteur**

Spécifie l'identifiant unique de l'agent SNMP et est généré automatiquement par le serveur de gestion. L'ID du moteur est disponible avec SNMP version 3, SNMP version 3 avec authentification et SNMP version 3 avec authentification et chiffrement.

- **Nom d'utilisateur**

Spécifie le nom d'utilisateur SNMP. Le nom d'utilisateur est disponible avec SNMP version 3, SNMP version 3 avec authentification et SNMP version 3 avec authentification et chiffrement.

- **Protocole d'authentification**

Spécifie le protocole utilisé pour authentifier un utilisateur. Les options de protocole incluent MD5 et SHA. MD5 est la valeur par défaut. Le protocole d'authentification est disponible avec SNMP version 3 avec authentification et SNMP version 3 avec authentification et chiffrement.

- **Mot de passe d'authentification**

Spécifie le mot de passe utilisé lors de l'authentification d'un utilisateur. Le mot de passe d'authentification est disponible avec SNMP version 3 avec authentification et SNMP version 3 avec authentification et chiffrement.

- **Protocole de confidentialité**

Spécifie le protocole de confidentialité utilisé pour crypter les messages SNMP. Les options de protocole incluent AES 128 et DES. La valeur par défaut est AES 128. Le protocole de confidentialité est disponible avec SNMP version 3 avec authentification et cryptage.

- **Mot de passe de confidentialité**

Spécifie le mot de passe lors de l'utilisation du protocole de confidentialité. Le mot de passe de confidentialité est disponible avec SNMP version 3 avec authentification et cryptage.

Pour plus d'informations sur les objets et les interruptions SNMP, vous pouvez télécharger le "[Active IQ Unified Manager MIB](#)" à partir du site de support NetApp .

Page d'inventaire de gestion des événements

La page d'inventaire de gestion des événements vous permet d'afficher une liste des événements actuels et de leurs propriétés. Vous pouvez effectuer des tâches telles que la reconnaissance, la résolution et l'attribution d'événements. Vous pouvez également ajouter une alerte pour des événements spécifiques.

Les informations sur cette page sont actualisées automatiquement toutes les 5 minutes pour garantir que les nouveaux événements les plus récents sont affichés.

Composants du filtre

Vous permet de personnaliser les informations affichées dans la liste des événements. Vous pouvez affiner la liste des événements affichés à l'aide des composants suivants :

- Menu d'affichage pour sélectionner parmi une liste prédéfinie de sélections de filtres.

Cela inclut des éléments tels que tous les événements actifs (nouveaux et reconnus), les événements de performance actifs, les événements qui me sont attribués (l'utilisateur connecté) et tous les événements générés pendant toutes les fenêtres de maintenance.

- Volet de recherche pour affiner la liste des événements en saisissant des termes complets ou partiels.
- Bouton Filtrer qui lance le volet Filtres afin que vous puissiez sélectionner parmi tous les champs et attributs de champ disponibles pour affiner la liste des événements.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Attribuer à**

Vous permet de sélectionner l'utilisateur à qui l'événement est attribué. Lorsque vous attribuez un événement à un utilisateur, le nom d'utilisateur et l'heure à laquelle vous avez attribué l'événement sont ajoutés dans la liste des événements pour les événements sélectionnés.

- Moi

Affecte l'événement à l'utilisateur actuellement connecté.

- Un autre utilisateur

Affiche la boîte de dialogue Attribuer un propriétaire, qui vous permet d'attribuer ou de réattribuer

l'événement à d'autres utilisateurs. Vous pouvez également annuler l'attribution d'événements en laissant le champ de propriété vide.

- **Reconnaître**

Reconnaît les événements sélectionnés.

Lorsque vous reconnaissez un événement, votre nom d'utilisateur et l'heure à laquelle vous avez reconnu l'événement sont ajoutés dans la liste des événements pour les événements sélectionnés. Lorsque vous reconnaissez un événement, vous êtes responsable de la gestion de cet événement.



Vous ne pouvez pas reconnaître les événements d'information.

- **Marquer comme résolu**

Vous permet de modifier l'état de l'événement sur résolu.

Lorsque vous résolvez un événement, votre nom d'utilisateur et l'heure à laquelle vous avez résolu l'événement sont ajoutés dans la liste des événements pour les événements sélectionnés. Après avoir pris des mesures correctives pour l'événement, vous devez marquer l'événement comme résolu.

- **Ajouter une alerte**

Affiche la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter des alertes pour les événements sélectionnés.

- **Rapports**

Vous permet d'exporter les détails de la vue de l'événement actuel vers un fichier de valeurs séparées par des virgules (.csv) ou un document PDF.

- **Afficher/Masquer le sélecteur de colonnes**

Vous permet de choisir les colonnes à afficher sur la page et de sélectionner l'ordre dans lequel elles sont affichées.

Liste des événements

Affiche les détails de tous les événements classés par heure de déclenchement.

Par défaut, la vue Tous les événements actifs s'affiche pour afficher les événements nouveaux et reconnus des sept jours précédents qui ont un niveau d'impact d'incident ou de risque.

- **Heure déclenchée**

L'heure à laquelle l'événement a été généré.

- **Gravité**

La gravité de l'événement : Critique (❌), Erreur (⚠️), Avertissement (⚠️), et Informations (ℹ️).

- **État**

L'état de l'événement : Nouveau, Reconnu, Résolu ou Obsolète.

- **Niveau d'impact**

Le niveau d'impact de l'événement : incident, risque, événement ou mise à niveau.

- **Zone d'impact**

Le domaine d'impact de l'événement : Disponibilité, Capacité, Performances, Protection, Configuration ou Sécurité.

- **Nom**

Le nom de l'événement. Vous pouvez sélectionner le nom pour afficher la page des détails de l'événement pour cet événement.

- **Source**

Le nom de l'objet sur lequel l'événement s'est produit. Vous pouvez sélectionner le nom pour afficher la page de détails sur l'état ou les performances de cet objet.

Lorsqu'une violation de la politique QoS partagée se produit, seul l'objet de charge de travail qui consomme le plus d'IOPS ou de Mo/s est affiché dans ce champ. Les charges de travail supplémentaires qui utilisent cette politique sont affichées dans la page Détails de l'événement.

- **Type de source**

Le type d'objet (par exemple, machine virtuelle de stockage, volume ou Qtree) auquel l'événement est associé.

- **Attribué à**

Le nom de l'utilisateur à qui l'événement est attribué.

- **Origine de l'événement**

Que l'événement provienne du « Portail Active IQ » ou directement du « Active IQ Unified Manager ».

- **Nom de l'annotation**

Le nom de l'annotation attribuée à l'objet de stockage.

- **Remarques**

Le nombre de notes ajoutées pour un événement.

- **Jours en suspens**

Le nombre de jours depuis que l'événement a été initialement généré.

- **Heure assignée**

Le temps écoulé depuis que l'événement a été attribué à un utilisateur. Si le temps écoulé dépasse une semaine, l'horodatage auquel l'événement a été attribué à un utilisateur s'affiche.

- **Reconnu par**

Le nom de l'utilisateur qui a reconnu l'événement. Le champ est vide si l'événement n'est pas reconnu.

- **Heure reconnue**

Le temps écoulé depuis que l'événement a été reconnu. Si le temps écoulé dépasse une semaine, l'horodatage auquel l'événement a été reconnu est affiché.

- **Résolu par**

Le nom de l'utilisateur qui a résolu l'événement. Le champ est vide si l'événement n'est pas résolu.

- **Temps résolu**

Le temps écoulé depuis que l'événement a été résolu. Si le temps écoulé dépasse une semaine, l'horodatage auquel l'événement a été résolu est affiché.

- **Temps obsolète**

Le moment où l'état de l'événement est devenu obsolète.

Page de détails de l'événement

À partir de la page Détails de l'événement, vous pouvez afficher les détails d'un événement sélectionné, tels que la gravité de l'événement, le niveau d'impact, la zone d'impact et la source de l'événement. Vous pouvez également consulter des informations supplémentaires sur les solutions possibles pour résoudre le problème.

- **Nom de l'événement**

Le nom de l'événement et l'heure à laquelle l'événement a été vu pour la dernière fois.

Pour les événements sans performance, lorsque l'événement est dans l'état Nouveau ou Reconnu, les dernières informations vues ne sont pas connues et sont donc masquées.

- **Description de l'événement**

Une brève description de l'événement.

Dans certains cas, la raison du déclenchement de l'événement est fournie dans la description de l'événement.

- **Composant en conflit**

Pour les événements de performances dynamiques, cette section affiche des icônes qui représentent les composants logiques et physiques du cluster. Si un composant est en conflit, son icône est entourée et surlignée en rouge.

Voir *Composants de cluster et pourquoi ils peuvent être en conflit* pour une description des composants affichés ici.

Les sections Informations sur l'événement, Diagnostic système et Actions suggérées sont décrites dans d'autres rubriques.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Icône Notes**

Vous permet d'ajouter ou de mettre à jour une note sur l'événement et de consulter toutes les notes laissées par d'autres utilisateurs.

Menu Actions

- **Attribuez-moi**

Vous attribue l'événement.

- **Attribuer à d'autres**

Ouvre la boîte de dialogue Attribuer un propriétaire, qui vous permet d'attribuer ou de réattribuer l'événement à d'autres utilisateurs.

Lorsque vous attribuez un événement à un utilisateur, le nom de l'utilisateur et l'heure à laquelle l'événement a été attribué sont ajoutés dans la liste des événements pour les événements sélectionnés.

Vous pouvez également annuler l'attribution d'événements en laissant le champ de propriété vide.

- **Reconnaître**

Reconnaît les événements sélectionnés afin que vous ne continuiez pas à recevoir des notifications d'alerte répétées.

Lorsque vous reconnaissez un événement, votre nom d'utilisateur et l'heure à laquelle vous avez reconnu l'événement sont ajoutés dans la liste des événements (Reconnu par) pour les événements sélectionnés. Lorsque vous reconnaissez un événement, vous assumez la responsabilité de la gestion de cet événement.

- **Marquer comme résolu**

Vous permet de modifier l'état de l'événement sur Résolu.

Lorsque vous résolvez un événement, votre nom d'utilisateur et l'heure à laquelle vous avez résolu l'événement sont ajoutés dans la liste des événements (Résolu par) pour les événements sélectionnés. Après avoir pris des mesures correctives pour l'événement, vous devez marquer l'événement comme résolu.

- **Ajouter une alerte**

Affiche la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter une alerte pour l'événement sélectionné.

Ce que la section Informations sur l'événement affiche

Vous utilisez la section Informations sur l'événement sur la page Détails de l'événement pour afficher les détails d'un événement sélectionné, tels que la gravité de l'événement, le niveau d'impact, la zone d'impact et la source de l'événement.

Les champs qui ne s'appliquent pas au type d'événement sont masqués. Vous pouvez consulter les détails de l'événement suivants :

- **Heure de déclenchement de l'événement**

L'heure à laquelle l'événement a été généré.

- **État**

L'état de l'événement : Nouveau, Reconnu, Résolu ou Obsolète.

- **Cause obsolète**

Les actions qui ont rendu l'événement obsolète, par exemple, le problème a été résolu.

- **Durée de l'événement**

Pour les événements actifs (nouveaux et reconnus), il s'agit du temps entre la détection et le moment où l'événement a été analysé pour la dernière fois. Pour les événements obsolètes, il s'agit du temps écoulé entre la détection et le moment où l'événement a été résolu.

Ce champ s'affiche pour tous les événements de performance et pour les autres types d'événements uniquement après qu'ils ont été résolus ou obsolètes.

- **Vu pour la dernière fois**

La date et l'heure à laquelle l'événement a été vu pour la dernière fois comme actif.

Pour les événements de performance, cette valeur peut être plus récente que l'heure de déclenchement de l'événement, car ce champ est mis à jour après chaque nouvelle collecte de données de performance tant que l'événement est actif. Pour les autres types d'événements, lorsqu'ils sont dans l'état Nouveau ou Reconnu, ce contenu n'est pas mis à jour et le champ est donc masqué.

- **Gravité**

La gravité de l'événement : Critique (❌), Erreur (⚠️), Avertissement (⚠️), et Informations (ℹ️).

- **Niveau d'impact**

Le niveau d'impact de l'événement : incident, risque, événement ou mise à niveau.

- **Zone d'impact**

Le domaine d'impact de l'événement : Disponibilité, Capacité, Performances, Protection, Configuration ou Sécurité.

- **Source**

Le nom de l'objet sur lequel l'événement s'est produit.

Lors de l'affichage des détails d'un événement de stratégie QoS partagé, jusqu'à trois des objets de charge de travail qui consomment le plus d'IOPS ou de MBps sont répertoriés dans ce champ.

Vous pouvez cliquer sur le lien du nom de la source pour afficher la page des détails de santé ou de performances de cet objet.

- **Annotations de la source**

Affiche le nom et la valeur de l'annotation pour l'objet auquel l'événement est associé.

Ce champ s'affiche uniquement pour les événements d'intégrité sur les clusters, les SVM et les volumes.

- **Groupes sources**

Affiche les noms de tous les groupes dont l'objet impacté est membre.

Ce champ s'affiche uniquement pour les événements d'intégrité sur les clusters, les SVM et les volumes.

- **Type de source**

Le type d'objet (par exemple, SVM, Volume ou Qtree) auquel l'événement est associé.

- **Sur Cluster**

Le nom du cluster sur lequel l'événement s'est produit.

Vous pouvez cliquer sur le lien du nom du cluster pour afficher la page des détails d'intégrité ou de performances de ce cluster.

- **Nombre d'objets affectés**

Le nombre d'objets affectés par l'événement.

Vous pouvez cliquer sur le lien de l'objet pour afficher la page d'inventaire remplie avec les objets actuellement affectés par cet événement.

Ce champ s'affiche uniquement pour les événements de performance.

- **Volumes affectés**

Le nombre de volumes affectés par cet événement.

Ce champ s'affiche uniquement pour les événements de performances sur les nœuds ou les agrégats.

- **Politique déclenchée**

Le nom de la politique de seuil qui a émis l'événement.

Vous pouvez passer votre curseur sur le nom de la politique pour voir les détails de la politique de seuil. Pour les politiques QoS adaptatives, la politique définie, la taille du bloc et le type d'allocation (espace alloué ou espace utilisé) sont également affichés.

Ce champ s'affiche uniquement pour les événements de performance.

- **Identifiant de règle**

Pour les événements de la plateforme Active IQ , il s'agit du numéro de la règle qui a été déclenchée pour générer l'événement.

- **Reconnu par**

Le nom de la personne qui a reconnu l'événement et l'heure à laquelle l'événement a été reconnu.

- **Résolu par**

Le nom de la personne qui a résolu l'événement et l'heure à laquelle l'événement a été résolu.

- **Attribué à**

Le nom de la personne chargée de travailler sur l'événement.

- **Paramètres d'alerte**

Les informations suivantes sur les alertes sont affichées :

- S'il n'y a aucune alerte associée à l'événement sélectionné, un lien **Ajouter une alerte** s'affiche.

Vous pouvez ouvrir la boîte de dialogue Ajouter une alerte en cliquant sur le lien.

- S'il existe une alerte associée à l'événement sélectionné, le nom de l'alerte s'affiche.

Vous pouvez ouvrir la boîte de dialogue Modifier l'alerte en cliquant sur le lien.

- S'il existe plusieurs alertes associées à l'événement sélectionné, le nombre d'alertes s'affiche.

Vous pouvez ouvrir la page de configuration des alertes en cliquant sur le lien pour afficher plus de détails sur ces alertes.

Les alertes désactivées ne sont pas affichées.

- **Dernière notification envoyée**

La date et l'heure à laquelle la notification d'alerte la plus récente a été envoyée.

- **Envoyer par**

Le mécanisme utilisé pour envoyer la notification d'alerte : e-mail ou trap SNMP.

- **Exécution du script précédent**

Le nom du script qui a été exécuté lorsque l'alerte a été générée.

Ce que la section Actions suggérées affiche

La section Actions suggérées de la page Détails de l'événement fournit les raisons possibles de l'événement et suggère quelques actions afin que vous puissiez essayer de résoudre l'événement par vous-même. Les actions suggérées sont personnalisées en fonction du type d'événement ou du type de seuil dépassé.

Cette zone s'affiche uniquement pour certains types d'événements.

Dans certains cas, des liens **Aide** sont fournis sur la page qui font référence à des informations supplémentaires pour de nombreuses actions suggérées, y compris des instructions pour effectuer une action spécifique. Certaines actions peuvent impliquer l'utilisation d'Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP CLI ou d'une combinaison de ces outils.

Vous devez considérer les actions suggérées ici uniquement comme un guide pour résoudre cet événement. L'action que vous entreprenez pour résoudre cet événement doit être basée sur le contexte de votre

environnement.

Si vous souhaitez analyser l'objet et l'événement plus en détail, cliquez sur le bouton **Analyser la charge de travail** pour afficher la page Analyse de la charge de travail.

Il existe certains événements qu'Unified Manager peut diagnostiquer en profondeur et fournir une résolution unique. Lorsqu'elles sont disponibles, ces résolutions sont affichées avec un bouton **Réparer**. Cliquez sur ce bouton pour que Unified Manager résolve le problème à l'origine de l'événement.

Pour les événements de la plateforme Active IQ, cette section peut contenir un lien vers un article de la base de connaissances NetApp, lorsqu'il est disponible, qui décrit le problème et les résolutions possibles. Sur les sites sans accès réseau externe, un PDF de l'article de la base de connaissances est ouvert localement ; le PDF fait partie du fichier de règles que vous téléchargez manuellement sur l'instance Unified Manager.

Ce qu'affiche la section Diagnostic du système

La section Diagnostic système de la page Détails de l'événement fournit des informations qui peuvent vous aider à diagnostiquer les problèmes qui peuvent être responsables de l'événement.

Cette zone s'affiche uniquement pour certains événements.

Certains événements de performance fournissent des graphiques pertinents pour l'événement particulier qui a été déclenché. Cela comprend généralement un graphique IOPS ou MBps et un graphique de latence pour les dix jours précédents. En organisant les éléments de cette manière, vous pouvez voir quels composants de stockage affectent le plus la latence, ou sont affectés par la latence, lorsque l'événement est actif.

Pour les événements de performance dynamiques, les graphiques suivants sont affichés :

- Latence de la charge de travail - Affiche l'historique de la latence des principales charges de travail de victime, d'intimidateur ou de requin au niveau du composant en conflit.
- Activité de charge de travail - Affiche les détails sur l'utilisation de la charge de travail du composant de cluster en conflit.
- Activité des ressources - Affiche les statistiques de performances historiques pour le composant de cluster en conflit.

D'autres graphiques sont affichés lorsque certains composants du cluster sont en conflit.

D'autres événements fournissent une brève description du type d'analyse que le système effectue sur l'objet de stockage. Dans certains cas, il y aura une ou plusieurs lignes ; une pour chaque composant qui a été analysé, pour les stratégies de performances définies par le système qui analysent plusieurs compteurs de performances. Dans ce scénario, une icône verte ou rouge s'affiche à côté du diagnostic pour indiquer si un problème a été détecté ou non dans ce diagnostic particulier.

Page de configuration de l'événement

La page Configuration des événements affiche la liste des événements désactivés et fournit des informations telles que le type d'objet associé et la gravité de l'événement. Vous pouvez également effectuer des tâches telles que la désactivation ou l'activation d'événements à l'échelle mondiale.

Vous ne pouvez accéder à cette page que si vous disposez du rôle d'administrateur d'application ou d'administrateur de stockage.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour les événements sélectionnés :

- **Désactiver**

Lance la boîte de dialogue Désactiver les événements, que vous pouvez utiliser pour désactiver les événements.

- **Activer**

Active les événements sélectionnés que vous aviez choisi de désactiver précédemment.

- **Règles de téléchargement**

Lance la boîte de dialogue Règles de téléchargement, qui permet aux sites sans accès réseau externe de télécharger manuellement le fichier de règles Active IQ vers Unified Manager. Les règles sont exécutées sur les messages AutoSupport du cluster pour générer des événements pour la configuration du système, le câblage, les meilleures pratiques et la disponibilité tels que définis par la plate-forme Active IQ .

- **Abonnez-vous aux événements EMS**

Lance la boîte de dialogue S'abonner aux événements EMS, qui vous permet de vous abonner pour recevoir des événements spécifiques du système de gestion des événements (EMS) des clusters que vous surveillez. L'EMS collecte des informations sur les événements qui se produisent sur le cluster. Lorsqu'une notification est reçue pour un événement EMS souscrit, un événement Unified Manager est généré avec la gravité appropriée.

Vue de liste

La vue Liste affiche (sous forme de tableau) des informations sur les événements désactivés. Vous pouvez utiliser les filtres de colonnes pour personnaliser les données affichées.

- **Événement**

Affiche le nom de l'événement désactivé.

- **Gravité**

Affiche la gravité de l'événement. La gravité peut être Critique, Erreur, Avertissement ou Information.

- **Type de source**

Affiche le type de source pour lequel l'événement est généré.

Boîte de dialogue Désactiver les événements

La boîte de dialogue Désactiver les événements affiche la liste des types d'événements pour lesquels vous pouvez désactiver les événements. Vous pouvez désactiver les événements pour un type d'événement en fonction d'une gravité particulière ou pour un ensemble d'événements.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Zone Propriétés de l'événement

La zone Propriétés de l'événement spécifie les propriétés d'événement suivantes :

- **Gravité de l'événement**

Vous permet de sélectionner des événements en fonction du type de gravité, qui peut être Critique, Erreur, Avertissement ou Information.

- **Le nom de l'événement contient**

Vous permet de filtrer les événements dont le nom contient les caractères spécifiés.

- **Événements correspondants**

Affiche la liste des événements correspondant au type de gravité de l'événement et à la chaîne de texte que vous spécifiez.

- **Désactiver les événements**

Affiche la liste des événements que vous avez sélectionnés pour la désactivation.

La gravité de l'événement est également affichée avec le nom de l'événement.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour les événements sélectionnés :

- **Enregistrer et fermer**

Désactive le type d'événement et ferme la boîte de dialogue.

- **Annuler**

Annule les modifications et ferme la boîte de dialogue.

Gérer les alertes

Vous pouvez configurer des alertes pour envoyer automatiquement une notification lorsque des événements spécifiques ou des événements de certains types de gravité se produisent. Vous pouvez également associer une alerte à un script qui est exécuté lorsqu'une alerte est déclenchée.

Que sont les alertes

Alors que les événements se produisent en continu, Unified Manager génère une alerte uniquement lorsqu'un événement répond aux critères de filtre spécifiés. Vous pouvez choisir les événements pour lesquels des alertes doivent être générées, par exemple lorsqu'un seuil d'espace est dépassé ou lorsqu'un objet est mis hors ligne. Vous pouvez également associer une alerte à un script qui est exécuté lorsqu'une alerte est déclenchée.

Les critères de filtrage incluent la classe d'objet, le nom ou la gravité de l'événement.

Quelles informations sont contenues dans un e-mail d'alerte

Les e-mails d'alerte d'Unified Manager fournissent le type d'événement, la gravité de l'événement, le nom de la politique ou du seuil qui a été violé pour provoquer l'événement et une description de l'événement. Le message électronique fournit également un lien hypertexte pour chaque événement qui vous permet d'afficher la page de détails de l'événement dans l'interface utilisateur.

Des e-mails d'alerte sont envoyés à tous les utilisateurs qui se sont abonnés pour recevoir des alertes.

Si un compteur de performances ou une valeur de capacité subit un changement important au cours d'une période de collecte, cela peut entraîner le déclenchement simultané d'un événement critique et d'un événement d'avertissement pour la même stratégie de seuil. Dans ce cas, vous pouvez recevoir un e-mail pour l'événement d'avertissement et un pour l'événement critique. Cela est dû au fait qu'Unified Manager vous permet de vous abonner séparément pour recevoir des alertes en cas de dépassement des seuils d'avertissement et de seuil critique.

Un exemple d'e-mail d'alerte est présenté ci-dessous :

From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
<https://10.11.12.13:443/events/94>

Source details:
<https://10.11.12.13:443/health/volumes/106>

Alert details:
<https://10.11.12.13:443/alerting/1>

Ajouter des alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer des alertes pour une seule ressource, pour un groupe de

ressources ou pour des événements d'un type de gravité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être notifié et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré les paramètres de notification tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou les adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez qu'un script s'exécute en fonction de l'événement, vous devez avoir ajouté le script à Unified Manager à l'aide de la page Scripts.
- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un événement, en plus de créer une alerte à partir de la page Configuration des alertes, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et sélectionnez les ressources à inclure ou à exclure de l'alerte.

Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Le nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles affiche uniquement les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

Si une ressource est conforme aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion a priorité sur la règle d'inclusion et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Événements** et sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lesquels vous souhaitez déclencher une alerte.



Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et attribuez un script à exécuter lorsqu'une alerte est générée.



Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur précédemment sélectionné. De plus, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page Utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

Vous pouvez également choisir de notifier les utilisateurs via des interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Cet exemple montre comment créer une alerte qui répond aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz »
- Événements : inclut tous les événements de santé critiques
- Actions : inclut « sample@domain.com », un script « Test », et l'utilisateur doit être notifié toutes les 15 minutes

Effectuez les étapes suivantes dans la boîte de dialogue Ajouter une alerte :

1. Cliquez sur **Nom** et saisissez `*HealthTest *` dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources** et dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.
 - a. Entrer `*abc *` dans le champ **Le nom contient** pour afficher les volumes dont le nom contient « abc ».
 - b. Sélectionnez **+[\[All Volumes whose name contains 'abc'\]](#)+** dans la zone Ressources disponibles et déplacez-le vers la zone Ressources sélectionnées.
 - c. Cliquez sur **Exclure** et saisissez `*xyz *` dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Événements** et sélectionnez **Critique** dans le champ Gravité de l'événement.
4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions** et entrez `*sample@domain.com *` dans le champ Alerter ces utilisateurs.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

Vous pouvez configurer une alerte pour envoyer des notifications répétées aux destinataires pendant une durée spécifiée. Vous devez déterminer l'heure à partir de laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Sélectionner le script à exécuter, sélectionnez le script **Tester**.
8. Cliquez sur **Enregistrer**.

Directives pour l'ajout d'alertes

Vous pouvez ajouter des alertes en fonction d'une ressource, telle qu'un cluster, un nœud, un agrégat ou un volume, et des événements d'un type de gravité particulier. En tant que meilleure pratique, vous pouvez ajouter une alerte pour n'importe lequel de vos objets critiques après avoir ajouté le cluster auquel appartient l'objet.

Vous pouvez utiliser les directives et considérations suivantes pour créer des alertes afin de gérer efficacement vos systèmes :

- Description de l'alerte

Vous devez fournir une description de l'alerte afin qu'elle vous aide à suivre efficacement vos alertes.

- Ressources

Vous devez décider quelle ressource physique ou logique nécessite une alerte. Vous pouvez inclure et exclure des ressources, selon vos besoins. Par exemple, si vous souhaitez surveiller de près vos agrégats en configurant une alerte, vous devez sélectionner les agrégats requis dans la liste des ressources.

Si vous sélectionnez une catégorie de ressources, par exemple, **+[\[All User or Group Quotas\]](#) +**, vous recevrez alors des alertes pour tous les objets de cette catégorie.



La sélection d'un cluster comme ressource ne sélectionne pas automatiquement les objets de stockage au sein de ce cluster. Par exemple, si vous créez une alerte pour tous les événements critiques de tous les clusters, vous recevrez des alertes uniquement pour les événements critiques du cluster. Vous ne recevrez pas d'alertes pour les événements critiques sur les nœuds, les agrégats, etc.

- Gravité de l'événement

Vous devez décider si un événement d'un type de gravité spécifié (Critique, Erreur, Avertissement) doit déclencher l'alerte et, si oui, quel type de gravité.

- Événements sélectionnés

Si vous ajoutez une alerte en fonction du type d'événement généré, vous devez décider quels événements nécessitent une alerte.

Si vous sélectionnez une gravité d'événement, mais ne sélectionnez aucun événement individuel (si vous laissez la colonne « Événements sélectionnés » vide), vous recevrez des alertes pour tous les événements de la catégorie.

- Actions

Vous devez fournir les noms d'utilisateur et les adresses e-mail des utilisateurs qui reçoivent la notification. Vous pouvez également spécifier une interruption SNMP comme mode de notification. Vous pouvez associer vos scripts à une alerte afin qu'ils soient exécutés lorsqu'une alerte est générée.

- Fréquence des notifications

Vous pouvez configurer une alerte pour envoyer une notification de manière répétée aux destinataires pendant une durée spécifiée. Vous devez déterminer l'heure à partir de laquelle la notification d'événement est active pour l'alerte. Si vous souhaitez que la notification d'événement soit répétée jusqu'à ce que l'événement soit reconnu, vous devez déterminer la fréquence à laquelle vous souhaitez que la notification soit répétée.

- Exécuter le script

Vous pouvez associer votre script à une alerte. Votre script est exécuté lorsque l'alerte est générée.

Ajouter des alertes pour les événements de performance

Vous pouvez configurer des alertes pour des événements de performance individuels, comme pour tout autre événement reçu par Unified Manager. De plus, si vous souhaitez traiter tous les événements de performance de la même manière et envoyer un e-mail à la même personne, vous pouvez créer une alerte unique pour vous avertir lorsque des

événements de performance critiques ou d'avertissement sont déclenchés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

L'exemple ci-dessous montre comment créer un événement pour tous les événements critiques de latence, d'IOPS et de MBps. Vous pouvez utiliser cette même méthodologie pour sélectionner des événements parmi tous les compteurs de performances et pour tous les événements d'avertissement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
4. Ne sélectionnez aucune ressource sur la page **Ressources**.

Étant donné qu'aucune ressource n'est sélectionnée, l'alerte est appliquée à tous les clusters, agrégats, volumes, etc., pour lesquels ces événements sont reçus.

5. Cliquez sur **Événements** et effectuez les actions suivantes :
 - a. Dans la liste Gravité de l'événement, sélectionnez **Critique**.
 - b. Dans le champ Le nom de l'événement contient, saisissez `*latency *` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
 - c. Dans le champ Le nom de l'événement contient, saisissez `*iops *` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
 - d. Dans le champ Le nom de l'événement contient, saisissez `*mbps *` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
6. Cliquez sur **Actions** puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
7. Configurez toutes les autres options sur cette page pour émettre des interruptions SNMP et exécuter un script.
8. Cliquez sur **Enregistrer**.

Alertes de test

Vous pouvez tester une alerte pour vérifier que vous l'avez configurée correctement. Lorsqu'un événement est déclenché, une alerte est générée et un e-mail d'alerte est envoyé aux destinataires configurés. Vous pouvez vérifier si la notification est envoyée et si votre script est exécuté en utilisant l'alerte de test.

Avant de commencer

- Vous devez avoir configuré les paramètres de notification tels que l'adresse e-mail des destinataires, le serveur SMTP et l'interruption SNMP.

Le serveur Unified Manager peut utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.

- Vous devez avoir attribué un script et configuré le script pour qu'il s'exécute lorsque l'alerte est générée.

- Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page **Configuration des alertes**, sélectionnez l'alerte que vous souhaitez tester, puis cliquez sur **Tester**.

Un e-mail d'alerte de test est envoyé aux adresses e-mail que vous avez spécifiées lors de la création de l'alerte.

Activer et désactiver les alertes pour les événements résolus et obsolètes

Pour tous les événements pour lesquels vous avez configuré l'envoi d'alertes, un message d'alerte est envoyé lorsque ces événements passent par tous les états disponibles : Nouveau, Reconnu, Résolu et Obsolète. Si vous ne souhaitez pas recevoir d'alertes pour les événements lorsqu'ils passent aux états Résolu et Obsolète, vous pouvez configurer un paramètre global pour supprimer ces alertes.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Par défaut, les alertes ne sont pas envoyées pour les événements lorsqu'ils passent aux états Résolu et Obsolète.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page **Configuration des alertes**, effectuez l'une des actions suivantes à l'aide du curseur en regard de l'élément **Alertes pour les événements résolus et obsolètes** :

À...	Fais ceci...
Arrêtez d'envoyer des alertes lorsque les événements sont résolus ou obsolètes	Déplacez le curseur vers la gauche
Commencez à envoyer des alertes lorsque les événements sont résolus ou obsolètes	Déplacez le curseur vers la droite

Exclure les volumes de destination de reprise après sinistre de la génération d'alertes

Lors de la configuration des alertes de volume, vous pouvez spécifier une chaîne dans la boîte de dialogue Alerte qui identifie un volume ou un groupe de volumes. Toutefois, si vous avez configuré la récupération après sinistre pour les SVM, les volumes source et de destination ont le même nom. Vous recevrez donc des alertes pour les deux volumes.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez désactiver les alertes pour les volumes de destination de reprise après sinistre en excluant les volumes portant le nom du SVM de destination. Cela est possible car l'identifiant des événements de volume contient à la fois le nom de la SVM et le nom du volume au format « <svm_name>:/<volume_name> ».

L'exemple ci-dessous montre comment créer des alertes pour le volume « vol1 » sur le SVM principal « vs1 », mais exclure la génération de l'alerte sur un volume portant le même nom sur le SVM « vs1-dr ».

Effectuez les étapes suivantes dans la boîte de dialogue Ajouter une alerte :

Étapes

1. Cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
2. Cliquez sur **Ressources**, puis sélectionnez l'onglet **Inclure**.
 - a. Sélectionnez **Volume** dans la liste déroulante, puis entrez `*vol1 *` dans le champ **Le nom contient** pour afficher les volumes dont le nom contient « vol1 ».
 - b. Sélectionnez **+ [All Volumes whose name contains 'vol1'] +** dans la zone **Ressources disponibles** et déplacez-le vers la zone **Ressources sélectionnées**.
3. Sélectionnez l'onglet **Exclure**, sélectionnez **Volume**, entrez `*vs1-dr *` dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.

Cela exclut la génération de l'alerte pour le volume « vol1 » sur SVM « vs1-dr ».

4. Cliquez sur **Événements** et sélectionnez l'événement ou les événements que vous souhaitez appliquer au ou aux volumes.
5. Cliquez sur **Actions** puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
6. Configurez toutes les autres options sur cette page pour émettre des interruptions SNMP et exécuter un script, puis cliquez sur **Enregistrer**.

Afficher les alertes

Vous pouvez afficher la liste des alertes créées pour divers événements à partir de la page Configuration des alertes. Vous pouvez également afficher les propriétés d'alerte telles que la description de l'alerte, la méthode et la fréquence de notification, les événements qui déclenchent l'alerte, les destinataires de courrier électronique des alertes et les ressources affectées telles que les clusters, les agrégats et les volumes.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.

La liste des alertes s'affiche dans la page Configuration des alertes.

Modifier les alertes

Vous pouvez modifier les propriétés d'alerte telles que la ressource à laquelle l'alerte est associée, les événements, les destinataires, les options de notification, la fréquence de notification et les scripts associés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page **Configuration des alertes**, sélectionnez l'alerte que vous souhaitez modifier et cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier l'alerte**, modifiez les sections nom, ressources, événements et actions, selon vos besoins.

Vous pouvez modifier ou supprimer le script associé à l'alerte.

4. Cliquez sur **Enregistrer**.

Supprimer les alertes

Vous pouvez supprimer une alerte lorsqu'elle n'est plus nécessaire. Par exemple, vous pouvez supprimer une alerte créée pour une ressource particulière lorsque cette ressource n'est plus surveillée par Unified Manager.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Sur la page **Configuration des alertes**, sélectionnez les alertes que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la demande de suppression.

Description des fenêtres d'alerte et des boîtes de dialogue

Vous devez configurer des alertes pour recevoir des notifications sur les événements à l'aide de la boîte de dialogue Ajouter une alerte. Vous pouvez également afficher la liste des alertes à partir de la page Configuration des alertes.

Page de configuration des alertes

La page Configuration des alertes affiche une liste d'alertes et fournit des informations sur le nom de l'alerte, l'état, la méthode de notification et la fréquence de notification. Vous pouvez également ajouter, modifier, supprimer, activer ou désactiver des alertes à partir de cette page.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Boutons de commande

- **Ajouter**

Affiche la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter de nouvelles alertes.

- **Modifier**

Affiche la boîte de dialogue Modifier l'alerte, qui vous permet de modifier les alertes sélectionnées.

- **Supprimer**

Supprime les alertes sélectionnées.

- **Activer**

Permet aux alertes sélectionnées d'envoyer des notifications.

- **Désactiver**

Désactive les alertes sélectionnées lorsque vous souhaitez arrêter temporairement l'envoi de notifications.

- **Test**

Teste les alertes sélectionnées pour vérifier leur configuration après avoir été ajoutées ou modifiées.

- **Alertes pour les événements résolus et obsolètes**

Permet d'activer ou de désactiver l'envoi d'alertes lorsque les événements sont déplacés vers les états Résolu ou Obsolète. Cela peut aider les utilisateurs à ne pas recevoir de notifications inutiles.

Vue de liste

La vue de liste affiche, sous forme de tableau, des informations sur les alertes créées. Vous pouvez utiliser les filtres de colonnes pour personnaliser les données affichées. Vous pouvez également sélectionner une alerte pour afficher plus d'informations à son sujet dans la zone de détails.

- **Statut**

Spécifie si une alerte est activée () ou désactivée () .

- **Alerte**

Affiche le nom de l'alerte.

- **Description**

Affiche une description de l'alerte.

- **Méthode de notification**

Affiche la méthode de notification sélectionnée pour l'alerte. Vous pouvez avertir les utilisateurs par e-mail ou par traps SNMP.

- **Fréquence de notification**

Spécifie la fréquence (en minutes) à laquelle le serveur de gestion continue d'envoyer des notifications jusqu'à ce que l'événement soit reconnu, résolu ou déplacé vers l'état Obsolète.

Zone de détails

La zone de détails fournit plus d'informations sur l'alerte sélectionnée.

- **Nom de l'alerte**

Affiche le nom de l'alerte.

- **Description de l'alerte**

Affiche une description de l'alerte.

- **Événements**

Affiche les événements pour lesquels vous souhaitez déclencher l'alerte.

- **Ressources**

Affiche les ressources pour lesquelles vous souhaitez déclencher l'alerte.

- **Comprend**

Affiche le groupe de ressources pour lequel vous souhaitez déclencher l'alerte.

- **Exclut**

Affiche le groupe de ressources pour lesquelles vous ne souhaitez pas déclencher l'alerte.

- **Méthode de notification**

Affiche la méthode de notification de l'alerte.

- **Fréquence de notification**

Affiche la fréquence à laquelle le serveur de gestion continue d'envoyer des notifications d'alerte jusqu'à ce que l'événement soit reconnu, résolu ou déplacé vers l'état Obsolète.

- **Nom du script**

Affiche le nom du script associé à l'alerte sélectionnée. Ce script est exécuté lorsqu'une alerte est générée.

- **Destinataires du courrier électronique**

Affiche les adresses e-mail des utilisateurs qui reçoivent la notification d'alerte.

Boîte de dialogue Ajouter une alerte

Vous pouvez créer des alertes pour vous avertir lorsqu'un événement particulier est généré, afin de pouvoir résoudre le problème rapidement et ainsi minimiser l'impact sur votre environnement. Vous pouvez créer des alertes pour une ressource unique ou un ensemble de ressources, ainsi que pour des événements d'un type de gravité particulier. Vous pouvez également spécifier la méthode de notification et la fréquence des alertes.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Nom

Cette zone vous permet de spécifier un nom et une description pour l'alerte :

- **Nom de l'alerte**

Vous permet de spécifier un nom d'alerte.

- **Description de l'alerte**

Vous permet de spécifier une description pour l'alerte.

Ressources

Cette zone vous permet de sélectionner une ressource individuelle ou de regrouper les ressources en fonction d'une règle dynamique pour laquelle vous souhaitez déclencher l'alerte. Une *règle dynamique* est l'ensemble des ressources filtrées en fonction de la chaîne de texte que vous spécifiez. Vous pouvez rechercher des ressources en sélectionnant un type de ressource dans la liste déroulante ou vous pouvez spécifier le nom exact de la ressource pour afficher une ressource spécifique.

Si vous créez une alerte à partir de l'une des pages de détails de l'objet de stockage, l'objet de stockage est automatiquement inclus dans l'alerte.

- **Inclure**

Vous permet d'inclure les ressources pour lesquelles vous souhaitez déclencher des alertes. Vous pouvez spécifier une chaîne de texte pour regrouper les ressources qui correspondent à la chaîne et sélectionner ce groupe à inclure dans l'alerte. Par exemple, vous pouvez regrouper tous les volumes dont le nom contient la chaîne « abc ».

- **Exclure**

Vous permet d'exclure les ressources pour lesquelles vous ne souhaitez pas déclencher d'alertes. Par exemple, vous pouvez exclure tous les volumes dont le nom contient la chaîne « xyz ».

L'onglet Exclure s'affiche uniquement lorsque vous sélectionnez toutes les ressources d'un type de ressource particulier : par exemple, +[All Volumes] ou [All Volumes whose name contains 'xyz'] +.

Si une ressource est conforme aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion a la priorité sur la règle d'inclusion et l'alerte n'est pas générée pour l'événement.

Événements

Cette zone vous permet de sélectionner les événements pour lesquels vous souhaitez créer les alertes. Vous pouvez créer des alertes pour des événements en fonction d'une gravité particulière ou pour un ensemble d'événements.

Pour sélectionner plusieurs événements, maintenez la touche Ctrl enfoncée pendant que vous effectuez vos sélections.

- **Gravité de l'événement**

Vous permet de sélectionner des événements en fonction du type de gravité, qui peut être Critique, Erreur ou Avertissement.

- **Le nom de l'événement contient**

Vous permet de sélectionner des événements dont le nom contient des caractères spécifiés.

Actions

Cette zone vous permet de spécifier les utilisateurs que vous souhaitez notifier lorsqu'une alerte est déclenchée. Vous pouvez également spécifier la méthode de notification et la fréquence de notification.

- **Alerter ces utilisateurs**

Vous permet de spécifier l'adresse e-mail ou le nom d'utilisateur de l'utilisateur pour recevoir des notifications.

Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur précédemment sélectionné. De plus, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page Utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

- **Fréquence de notification**

Vous permet de spécifier la fréquence à laquelle le serveur de gestion envoie des notifications jusqu'à ce que l'événement soit reconnu, résolu ou déplacé vers l'état obsolète.

Vous pouvez choisir les méthodes de notification suivantes :

- Notifier une seule fois
- Notifier à une fréquence spécifiée
- Notifier à une fréquence spécifiée dans la plage horaire spécifiée

- **Problème d'interruption SNMP**

La sélection de cette case vous permet de spécifier si les interruptions SNMP doivent être envoyées à l'hôte SNMP configuré globalement.

- **Exécuter le script**

Vous permet d'ajouter votre script personnalisé à l'alerte. Ce script est exécuté lorsqu'une alerte est générée.



Si vous ne voyez pas cette fonctionnalité disponible dans l'interface utilisateur, c'est parce que la fonctionnalité a été désactivée par votre administrateur. Si nécessaire, vous pouvez activer cette fonctionnalité depuis **Gestion du stockage > Paramètres des fonctionnalités**.

Boutons de commande

- **Sauvegarder**

Crée une alerte et ferme la boîte de dialogue.

- **Annuler**

Annule les modifications et ferme la boîte de dialogue.

Boîte de dialogue Modifier l'alerte

Vous pouvez modifier les propriétés d'alerte telles que la ressource à laquelle l'alerte est associée, les événements, le script et les options de notification.

Nom

Cette zone vous permet de modifier le nom et la description de l'alerte.

- **Nom de l'alerte**

Vous permet de modifier le nom de l'alerte.

- **Description de l'alerte**

Vous permet de spécifier une description pour l'alerte.

- **État d'alerte**

Vous permet d'activer ou de désactiver l'alerte.

Ressources

Cette zone vous permet de sélectionner une ressource individuelle ou de regrouper les ressources en fonction d'une règle dynamique pour laquelle vous souhaitez déclencher l'alerte. Vous pouvez rechercher des ressources en sélectionnant un type de ressource dans la liste déroulante ou vous pouvez spécifier le nom exact de la ressource pour afficher une ressource spécifique.

- **Inclure**

Vous permet d'inclure les ressources pour lesquelles vous souhaitez déclencher des alertes. Vous pouvez spécifier une chaîne de texte pour regrouper les ressources qui correspondent à la chaîne et sélectionner ce groupe à inclure dans l'alerte. Par exemple, vous pouvez regrouper tous les volumes dont le nom contient la chaîne « vol0 ».

- **Exclure**

Vous permet d'exclure les ressources pour lesquelles vous ne souhaitez pas déclencher d'alertes. Par exemple, vous pouvez exclure tous les volumes dont le nom contient la chaîne « xyz ».



L'onglet Exclure s'affiche uniquement lorsque vous sélectionnez toutes les ressources d'un type de ressource particulier, par exemple, +[All Volumes] + ou +[All Volumes whose name contains 'xyz'] +.

Événements

Cette zone vous permet de sélectionner les événements pour lesquels vous souhaitez déclencher les alertes. Vous pouvez déclencher une alerte pour des événements en fonction d'une gravité particulière ou pour un ensemble d'événements.

- **Gravité de l'événement**

Vous permet de sélectionner des événements en fonction du type de gravité, qui peut être Critique, Erreur ou Avertissement.

- **Le nom de l'événement contient**

Vous permet de sélectionner les événements dont le nom contient les caractères spécifiés.

Actions

Cette zone vous permet de spécifier la méthode de notification et la fréquence de notification.

- **Alerter ces utilisateurs**

Vous permet de modifier l'adresse e-mail ou le nom d'utilisateur, ou de spécifier une nouvelle adresse e-mail ou un nouveau nom d'utilisateur pour recevoir des notifications.

- **Fréquence de notification**

Vous permet de modifier la fréquence à laquelle le serveur de gestion envoie des notifications jusqu'à ce que l'événement soit reconnu, résolu ou déplacé vers l'état obsolète.

Vous pouvez choisir les méthodes de notification suivantes :

- Notifier une seule fois
- Notifier à une fréquence spécifiée
- Notifier à une fréquence spécifiée dans la plage horaire spécifiée

- **Problème d'interruption SNMP**

Vous permet de spécifier si les interruptions SNMP doivent être envoyées à l'hôte SNMP configuré globalement.

- **Exécuter le script**

Vous permet d'associer un script à l'alerte. Ce script est exécuté lorsqu'une alerte est générée.

Boutons de commande

- **Sauvegarder**

Enregistre les modifications et ferme la boîte de dialogue.

- **Annuler**

Annule les modifications et ferme la boîte de dialogue.

Gérer les scripts

Vous pouvez utiliser des scripts pour modifier ou mettre à jour automatiquement plusieurs objets de stockage dans Unified Manager. Le script est associé à une alerte. Lorsqu'un événement déclenche une alerte, le script est exécuté. Vous pouvez télécharger des scripts personnalisés et tester leur exécution lorsqu'une alerte est générée.

La possibilité de télécharger des scripts sur Unified Manager et de les exécuter est activée par défaut. Si votre organisation ne souhaite pas autoriser cette fonctionnalité pour des raisons de sécurité, vous pouvez la

désactiver depuis **Gestion du stockage > Paramètres des fonctionnalités**.

Informations connexes

["Activation et désactivation de la possibilité de télécharger des scripts"](#)

Comment fonctionnent les scripts avec les alertes

Vous pouvez associer une alerte à votre script afin que le script soit exécuté lorsqu'une alerte est déclenchée pour un événement dans Unified Manager. Vous pouvez utiliser les scripts pour résoudre les problèmes liés aux objets de stockage ou identifier les objets de stockage qui génèrent les événements.

Lorsqu'une alerte est générée pour un événement dans Unified Manager, un e-mail d'alerte est envoyé aux destinataires spécifiés. Si vous avez associé une alerte à un script, le script est exécuté. Vous pouvez obtenir les détails des arguments transmis au script à partir de l'e-mail d'alerte.



Si vous avez créé un script personnalisé et l'avez associé à une alerte pour un type d'événement spécifique, les actions sont effectuées en fonction de votre script personnalisé pour ce type d'événement, et les actions **Corriger** ne sont pas disponibles par défaut sur la page Actions de gestion ou sur le tableau de bord Unified Manager.

Le script utilise les arguments suivants pour l'exécution :

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType
- -eventState
- -eventArgs

Vous pouvez utiliser les arguments dans vos scripts et collecter des informations sur les événements associés ou modifier les objets de stockage.

Exemple d'obtention d'arguments à partir de scripts

```
`print "$ARGV[0] : $ARGV[1]\n"`  
`print "$ARGV[7] : $ARGV[8]\n"`
```

Lorsqu'une alerte est générée, ce script est exécuté et la sortie suivante s'affiche :

```
-`eventID : 290`  
-`eventSourceID : 4138`
```

Ajouter des scripts

Vous pouvez ajouter des scripts dans Unified Manager et associer les scripts à des alertes. Ces scripts sont exécutés automatiquement lorsqu'une alerte est générée et vous permettent d'obtenir des informations sur les objets de stockage pour lesquels l'événement est généré.

Avant de commencer

- Vous devez avoir créé et enregistré les scripts que vous souhaitez ajouter au serveur Unified Manager.
- Les formats de fichiers pris en charge pour les scripts sont Perl, Shell, PowerShell, Python et .bat fichiers.

Plateforme sur laquelle Unified Manager est installé	Langues prises en charge
VMware	Scripts Perl et Shell
Linux	Scripts Perl, Python et Shell
Windows	Scripts PowerShell, Perl, Python et .bat

- Pour les scripts Perl, Perl doit être installé sur le serveur Unified Manager. Pour les installations VMware, Perl 5 est installé par défaut et les scripts prendront en charge uniquement ce que Perl 5 prend en charge. Si Perl a été installé après Unified Manager, vous devez redémarrer le serveur Unified Manager.
- Pour les scripts PowerShell, la stratégie d'exécution PowerShell appropriée doit être définie sur le serveur Windows afin que les scripts puissent être exécutés.



Si votre script crée des fichiers journaux pour suivre la progression du script d'alerte, vous devez vous assurer que les fichiers journaux ne sont créés nulle part dans le dossier d'installation d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez télécharger des scripts personnalisés et collecter des détails sur l'événement concernant l'alerte.



Si vous ne voyez pas cette fonctionnalité disponible dans l'interface utilisateur, c'est parce que la fonctionnalité a été désactivée par votre administrateur. Si nécessaire, vous pouvez activer cette fonctionnalité depuis **Gestion du stockage > Paramètres des fonctionnalités**.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Scripts**.
2. Dans la page **Scripts**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un script**, cliquez sur **Parcourir** pour sélectionner votre fichier de script.
4. Saisissez une description pour le script que vous sélectionnez.
5. Cliquez sur **Ajouter**.

Informations connexes

Supprimer les scripts

Vous pouvez supprimer un script d'Unified Manager lorsque le script n'est plus nécessaire ou valide.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Le script ne doit pas être associé à une alerte.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Scripts**.
2. Dans la page **Scripts**, sélectionnez le script que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Exécution du script de test

Vous pouvez vérifier que votre script est exécuté correctement lorsqu'une alerte est générée pour un objet de stockage.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir téléchargé un script dans le format de fichier pris en charge sur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Scripts**.
2. Dans la page **Scripts**, ajoutez votre script de test.
3. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
4. Dans la page **Configuration des alertes**, effectuez l'une des actions suivantes :

À...	Fais ceci...
Ajouter une alerte	a. Cliquez sur Ajouter. b. Dans la section Actions, associez l'alerte à votre script de test.
Modifier une alerte	a. Sélectionnez une alerte, puis cliquez sur Modifier. b. Dans la section Actions, associez l'alerte à votre script de test.

5. Cliquez sur **Enregistrer**.
6. Dans la page **Configuration des alertes**, sélectionnez l'alerte que vous avez ajoutée ou modifiée, puis cliquez sur **Tester**.

Le script est exécuté avec l'argument « -test » et une alerte de notification est envoyée aux adresses e-mail spécifiées lors de la création de l'alerte.

Commandes CLI Unified Manager prises en charge

En tant qu'administrateur de stockage, vous pouvez utiliser les commandes CLI pour effectuer des requêtes sur les objets de stockage ; par exemple, sur les clusters, les agrégats, les volumes, les qtrees et les LUN. Vous pouvez utiliser les commandes CLI pour interroger la base de données interne d'Unified Manager et la base de données ONTAP . Vous pouvez également utiliser des commandes CLI dans des scripts qui sont exécutés au début ou à la fin d'une opération ou qui sont exécutés lorsqu'une alerte est déclenchée.

Toutes les commandes doivent être précédées de la commande `um cli login` et un nom d'utilisateur et un mot de passe valides pour l'authentification.



Pour exécuter la commande `um run`, assurez-vous que votre compte dispose de l'accès à l'application *console*.

Commande CLI	Description	Sortir
<code>um cli login -u <username> [-p <password>]</code>	Se connecte à la CLI. Pour des raisons de sécurité, vous devez saisir uniquement le nom d'utilisateur suivant l'option « -u ». Lorsque vous l'utilisez de cette manière, vous serez invité à saisir le mot de passe, et celui-ci ne sera pas enregistré dans l'historique ou dans la table des processus. La session expire trois heures après la connexion, après quoi l'utilisateur doit se reconnecter.	Affiche le message correspondant.
<code>um cli logout</code>	Se déconnecte de la CLI.	Affiche le message correspondant.
<code>um help</code>	Affiche toutes les sous-commandes de premier niveau.	Affiche toutes les sous-commandes de premier niveau.

Commande CLI	Description	Sortir
um run cmd [-t <timeout>] <cluster> <command>	La manière la plus simple d'exécuter une commande sur un ou plusieurs hôtes. Principalement utilisé pour les scripts d'alerte pour obtenir ou effectuer une opération sur ONTAP. L'argument de délai d'expiration facultatif définit une limite de temps maximale (en secondes) pour que la commande s'exécute sur le client. La valeur par défaut est 0 (attendre indéfiniment).	Tel que reçu de ONTAP.
um run query <sql command>	Exécute une requête SQL. Seules les requêtes lisant à partir de la base de données sont autorisées. Aucune opération de mise à jour, d'insertion ou de suppression n'est prise en charge.	Les résultats sont affichés sous forme de tableau. Si un ensemble vide est renvoyé, ou s'il y a une erreur de syntaxe ou une mauvaise demande, il affiche le message d'erreur approprié.
um datasource add -u <username> -P <password> [-t <protocol>] [-p <port>] <hostname-or-ip>	Ajoute une source de données à la liste des systèmes de stockage gérés. Une source de données décrit comment les connexions aux systèmes de stockage sont établies. Les options -u (nom d'utilisateur) et -P (mot de passe) doivent être spécifiées lors de l'ajout d'une source de données. L'option -t (protocole) spécifie le protocole utilisé pour communiquer avec le cluster (http ou https). Si le protocole n'est pas spécifié, les deux protocoles seront tentés. L'option -p (port) spécifie le port utilisé pour communiquer avec le cluster. Si le port n'est pas spécifié, la valeur par défaut du protocole approprié sera tentée. Cette commande ne peut être exécutée que par l'administrateur de stockage.	Invite l'utilisateur à accepter le certificat et imprime le message correspondant.
um datasource list [<datasource-id>]	Affiche les sources de données pour les systèmes de stockage gérés.	Affiche les valeurs suivantes sous forme de tableau : ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.

Commande CLI	Description	Sortir
um datasource modify [-h <hostname-or-ip>] [-u <username>] [-P <password>] [-t <protocol>] [-p <port>] <datasource-id>	Modifie une ou plusieurs options de source de données. Ne peut être exécuté que par l'administrateur de stockage.	Affiche le message correspondant.
um datasource remove <datasource-id>	Supprime la source de données (cluster) de Unified Manager.	Affiche le message correspondant.
um option list [<option> ..]	Répertorie toutes les options que vous pouvez configurer à l'aide de la commande set.	Affiche les valeurs suivantes sous forme de tableau : Name, Value, Default Value, and Requires Restart.
um option set <option-name>=<option-value> [<option-name>=<option-value> ...]	Définit une ou plusieurs options. La commande ne peut être exécutée que par l'administrateur de stockage.	Affiche le message correspondant.
um version	Affiche la version du logiciel Unified Manager.	Version ("9.6")
um lun list [-q] [-ObjectType <object-id>]	Répertorie les LUN après filtrage sur l'objet spécifié. -q s'applique à toutes les commandes pour n'afficher aucun en-tête. ObjectType peut être lun, qtree, cluster, volume, quota ou svm. Par exemple: um lun list -cluster 1 Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les LUN du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : ID and LUN path.

Commande CLI	Description	Sortir
<pre>um svm list [-q] [-ObjectType <object-id>]</pre>	Répertorie les machines virtuelles de stockage après filtrage sur l'objet spécifié. ObjectType peut être lun, qtree, cluster, volume, quota ou svm. Par exemple: <pre>um svm list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie toutes les machines virtuelles de stockage au sein du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : Name and Cluster ID.
<pre>um qtree list [-q] [-ObjectType <object-id>]</pre>	Répertorie les qtrees après filtrage sur l'objet spécifié. -q s'applique à toutes les commandes pour n'afficher aucun en-tête. ObjectType peut être lun, qtree, cluster, volume, quota ou svm. Par exemple: <pre>um qtree list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les qtrees du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : Qtree ID and Qtree Name.
<pre>um disk list [-q] [-ObjectType <object-id>]</pre>	Répertorie les disques après filtrage sur l'objet spécifié. ObjectType peut être un disque, un aggr, un nœud ou un cluster. Par exemple: <pre>um disk list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les disques du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau ObjectType and object-id.

Commande CLI	Description	Sortir
<pre>um cluster list [-q] [-ObjectType <object-id>]</pre>	Répertorie les clusters après filtrage sur l'objet spécifié. ObjectType peut être un disque, un aggr, un nœud, un cluster, un lun, un qtree, un volume, un quota ou un svm. Par exemple: <pre>um cluster list -aggr 1</pre> Dans cet exemple, « -aggr » est l'objectType et « 1 » est l'objectId. La commande répertorie le cluster auquel appartient l'agrégat avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key .
<pre>um cluster node list [-q] [-ObjectType <object-id>]</pre>	Répertorie les nœuds du cluster après filtrage sur l'objet spécifié. ObjectType peut être un disque, un aggr, un nœud ou un cluster. Par exemple: <pre>um cluster node list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les nœuds du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau Name and Cluster ID .
<pre>um volume list [-q] [-ObjectType <object-id>]</pre>	Répertorie les volumes après filtrage sur l'objet spécifié. ObjectType peut être lun, qtree, cluster, volume, quota, svm ou agrégat. Par exemple: <pre>um volume list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les volumes du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau Volume ID and Volume Name .

Commande CLI	Description	Sortir
um quota user list [-q] [-ObjectType <object-id>]	Répertorie les utilisateurs de quota après filtrage sur l'objet spécifié. ObjectType peut être qtree, cluster, volume, quota ou svm. Par exemple: <pre>um quota user list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les utilisateurs de quota au sein du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau ID, Name, SID and Email .
um aggr list [-q] [-ObjectType <object-id>]	Répertorie les agrégats après filtrage sur l'objet spécifié. ObjectType peut être un disque, un aggr, un nœud, un cluster ou un volume. Par exemple: <pre>um aggr list -cluster 1</pre> Dans cet exemple, « -cluster » est l'objectType et « 1 » est l'objectId. La commande répertorie tous les agrégats du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau Aggr ID, and Aggr Name .
um event ack <event-ids>	Reconnaît un ou plusieurs événements.	Affiche le message correspondant.
um event resolve <event-ids>	Résout un ou plusieurs événements.	Affiche le message correspondant.
um event assign -u <username> <event-id>	Affecte un événement à un utilisateur.	Affiche le message correspondant.
um event list [-s <source>] [-S <event-state-filter-list>..] [<event-id> ..]	Répertorie les événements générés par le système ou l'utilisateur. Filtre les événements en fonction de la source, de l'état et des identifiants.	Affiche les valeurs suivantes sous forme de tableau Source, Source type, Name, Severity, State, User and Timestamp .

Commande CLI	Description	Sortir
um backup restore -f <backup_file_path_and_name>	Restaure une sauvegarde de base de données MySQL à l'aide de fichiers .7z.	Affiche le message correspondant.

Description des fenêtres de script et des boîtes de dialogue

La page Scripts vous permet d'ajouter des scripts à Unified Manager.

Page de scripts

La page Scripts vous permet d'ajouter vos scripts personnalisés à Unified Manager. Vous pouvez associer ces scripts à des alertes pour permettre la reconfiguration automatique des objets de stockage.

La page Scripts vous permet d'ajouter ou de supprimer des scripts depuis Unified Manager.

Boutons de commande

- **Ajouter**

Affiche la boîte de dialogue Ajouter un script, qui vous permet d'ajouter des scripts.

- **Supprimer**

Supprime le script sélectionné.

Vue de liste

La vue de liste affiche, sous forme de tableau, les scripts que vous avez ajoutés à Unified Manager.

- **Nom**

Affiche le nom du script.

- **Description**

Affiche la description du script.

Boîte de dialogue Ajouter un script

La boîte de dialogue Ajouter un script vous permet d'ajouter des scripts à Unified Manager. Vous pouvez configurer des alertes avec vos scripts pour résoudre automatiquement les événements générés pour les objets de stockage.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

- **Sélectionnez le fichier de script**

Vous permet de sélectionner un script pour l'alerte.

- **Description**

Vous permet de spécifier une description pour le script.

Surveiller et gérer les performances du cluster

Introduction à la surveillance des performances Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) fournit des fonctionnalités de surveillance des performances et d'analyse des causes profondes des événements pour les systèmes exécutant le logiciel NetApp ONTAP .

Unified Manager vous aide à identifier les charges de travail qui utilisent trop les composants du cluster et diminuent les performances des autres charges de travail sur le cluster. En définissant des stratégies de seuil de performances, vous pouvez également spécifier des valeurs maximales pour certains compteurs de performances afin que des événements soient générés lorsque le seuil est dépassé. Unified Manager vous alerte sur ces événements de performance afin que vous puissiez prendre des mesures correctives et ramener les performances à des niveaux de fonctionnement normaux. Vous pouvez afficher et analyser les événements dans l'interface utilisateur d'Unified Manager.

Unified Manager surveille les performances de deux types de charges de travail :

- Charges de travail définies par l'utilisateur

Ces charges de travail se composent de volumes FlexVol et de volumes FlexGroup que vous avez créés dans votre cluster.

- Charges de travail définies par le système

Ces charges de travail sont constituées d'activités internes du système.

Fonctionnalités de surveillance des performances d'Unified Manager

Unified Manager collecte et analyse les statistiques de performances des systèmes exécutant le logiciel ONTAP . Il utilise des seuils de performances dynamiques et des seuils de performances définis par l'utilisateur pour surveiller une variété de compteurs de performances sur de nombreux composants de cluster.

Un temps de réponse élevé (latence) indique que l'objet de stockage, par exemple un volume, fonctionne plus lentement que la normale. Ce problème indique également que les performances ont diminué pour les applications clientes qui utilisent le volume. Unified Manager identifie le composant de stockage où se situe le problème de performances et fournit une liste d'actions suggérées que vous pouvez entreprendre pour résoudre le problème de performances.

Unified Manager comprend les fonctionnalités suivantes :

- Surveille et analyse les statistiques de performances de la charge de travail d'un système exécutant le logiciel ONTAP .
- Suivi des compteurs de performances pour les clusters, les nœuds, les agrégats, les ports, les SVM, les volumes, les LUN, les espaces de noms NVMe et les interfaces réseau (LIF).
- Affiche des graphiques détaillés qui tracent l'activité de la charge de travail au fil du temps ; y compris les IOPS (opérations), les Mo/s (débit), la latence (temps de réponse), l'utilisation, la capacité de performance et le ratio de cache.

- Vous permet de créer des stratégies de seuil de performances définies par l'utilisateur qui déclenchent des événements et envoient des alertes par e-mail lorsque les seuils sont dépassés.
- Utilise des seuils définis par le système et des seuils de performances dynamiques qui en apprennent davantage sur votre activité de charge de travail pour identifier et vous alerter des problèmes de performances.
- Identifie les politiques de qualité de service (QoS) et les politiques de niveau de service de performance (PSL) qui sont appliquées à vos volumes et LUN.
- Identifie clairement le composant du cluster qui est en conflit.
- Identifie les charges de travail qui utilisent de manière excessive les composants du cluster et les charges de travail dont les performances sont affectées par l'activité accrue.

Interfaces Unified Manager utilisées pour gérer les performances du système de stockage

Ces sections contiennent des informations sur les deux interfaces utilisateur fournies par Active IQ Unified Manager pour résoudre les problèmes de capacité de stockage, de disponibilité et de protection des données. Les deux interfaces utilisateur sont l'interface Web Unified Manager et la console de maintenance.

Si vous souhaitez utiliser les fonctionnalités de protection dans Unified Manager, vous devez également installer et configurer OnCommand Workflow Automation (WFA).

Interface utilisateur Web d'Unified Manager

L'interface utilisateur Web d'Unified Manager permet à un administrateur de surveiller et de résoudre les problèmes de cluster liés à la capacité de stockage, à la disponibilité et à la protection des données.

Ces sections décrivent certains flux de travail courants qu'un administrateur peut suivre pour résoudre les problèmes de capacité de stockage, de disponibilité des données ou de protection affichés dans l'interface utilisateur Web d'Unified Manager.

Console de maintenance

La console de maintenance Unified Manager permet à un administrateur de surveiller, de diagnostiquer et de résoudre les problèmes de système d'exploitation, les problèmes de mise à niveau de version, les problèmes d'accès utilisateur et les problèmes de réseau liés au serveur Unified Manager lui-même. Si l'interface Web d'Unified Manager n'est pas disponible, la console de maintenance est la seule forme d'accès à Unified Manager.

Vous pouvez utiliser ces informations pour accéder à la console de maintenance et l'utiliser pour résoudre les problèmes liés au fonctionnement du serveur Unified Manager.

Activité de collecte de données sur la configuration et les performances des clusters

L'intervalle de collecte des *données de configuration du cluster* est de 15 minutes. Par exemple, après avoir ajouté un cluster, il faut 15 minutes pour afficher les détails du cluster dans l'interface utilisateur d'Unified Manager. Cet intervalle s'applique également lors des modifications apportées à un cluster.

Par exemple, si vous ajoutez deux nouveaux volumes à un SVM dans un cluster, vous voyez ces nouveaux objets dans l'interface utilisateur après le prochain intervalle d'interrogation, qui peut aller jusqu'à 15 minutes.

Unified Manager collecte les *statistiques de performances* actuelles de tous les clusters surveillés toutes les cinq minutes. Il analyse ces données pour identifier les événements de performance et les problèmes potentiels. Il conserve 30 jours de données de performances historiques de cinq minutes et 180 jours de données de performances historiques d'une heure. Cela vous permet d'afficher des détails de performances très précis pour le mois en cours et des tendances générales de performances jusqu'à un an.

Les sondages de collecte sont décalés de quelques minutes afin que les données de chaque cluster ne soient pas envoyées en même temps, ce qui pourrait affecter les performances.

Le tableau suivant décrit les activités de collecte effectuées par Unified Manager :

Activité	Intervalle de temps	Description
Sondage sur les statistiques de performance	Toutes les 5 minutes	Collecte les données de performances en temps réel de chaque cluster.
Analyse statistique	Toutes les 5 minutes	Après chaque interrogation statistique, Unified Manager compare les données collectées aux seuils définis par l'utilisateur, définis par le système et dynamiques. Si des seuils de performances ont été dépassés, Unified Manager génère des événements et envoie des e-mails aux utilisateurs spécifiés, s'il est configuré pour le faire.
Sondage de configuration	Toutes les 15 minutes	Collecte des informations d'inventaire détaillées de chaque cluster pour identifier tous les objets de stockage (nœuds, SVM, volumes, etc.).
Récapitulation	Toutes les heures	Résume les 12 dernières collectes de données de performance de cinq minutes en moyennes horaires. Les valeurs moyennes horaires sont utilisées dans certaines pages de l'interface utilisateur et sont conservées pendant 180 jours.

Activité	Intervalle de temps	Description
Analyse des prévisions et élagage des données	Tous les jours après minuit	Analyse les données du cluster pour établir des seuils dynamiques pour la latence du volume et les IOPS pour les 24 heures suivantes. Supprime de la base de données toutes les données de performance de cinq minutes datant de plus de 30 jours.
Élagage des données	Tous les jours après 2 heures du matin	Supprime de la base de données tous les événements datant de plus de 180 jours et les seuils dynamiques datant de plus de 180 jours.
Élagage des données	Tous les jours après 3h30 du matin	Supprime de la base de données toutes les données de performance d'une heure datant de plus de 180 jours.

Qu'est-ce qu'un cycle de collecte de continuité des données

Un cycle de collecte de continuité des données récupère les données de performances en dehors du cycle de collecte des performances du cluster en temps réel qui s'exécute, par défaut, toutes les cinq minutes. Les collectes de continuité des données permettent à Unified Manager de combler les lacunes de données statistiques qui se produisent lorsqu'il n'a pas pu collecter de données en temps réel.

Unified Manager effectue des interrogations de collecte de continuité des données sur les données de performances historiques lorsque les événements suivants se produisent :

- Un cluster est initialement ajouté à Unified Manager.

Unified Manager collecte les données de performances historiques des 15 jours précédents. Cela vous permet d'afficher deux semaines d'informations sur les performances historiques d'un cluster quelques heures après son ajout.

De plus, les événements de seuil définis par le système sont signalés pour la période précédente, le cas échéant.

- Le cycle actuel de collecte des données de performance ne se termine pas à temps.

Si l'enquête de performance en temps réel dépasse la période de collecte de cinq minutes, un cycle de collecte de continuité des données est lancé pour recueillir les informations manquantes. Sans la collecte de continuité des données, la période de collecte suivante est ignorée.

- Unified Manager a été inaccessible pendant un certain temps, puis il revient en ligne, comme dans les situations suivantes :

- Il a été redémarré.
- Il a été arrêté lors d'une mise à niveau du logiciel ou lors de la création d'un fichier de sauvegarde.
- Une panne de réseau est réparée.
- Un cluster a été inaccessible pendant un certain temps, puis il revient en ligne, comme dans les situations suivantes :
 - Une panne de réseau est réparée.
 - Une connexion réseau longue distance lente a retardé la collecte normale des données de performances.

Un cycle de collecte de continuité des données peut collecter un maximum de 24 heures de données historiques. Si Unified Manager est en panne pendant plus de 24 heures, un écart dans les données de performances apparaît dans les pages de l'interface utilisateur.

Un cycle de collecte de données en continuité et un cycle de collecte de données en temps réel ne peuvent pas s'exécuter en même temps. Le cycle de collecte de continuité des données doit se terminer avant que la collecte des données de performances en temps réel ne soit lancée. Lorsque la collecte de continuité des données doit collecter plus d'une heure de données historiques, un message de bannière pour ce cluster s'affiche en haut du volet Notifications.

Ce que signifie l'horodatage dans les données et événements collectés

L'horodatage qui apparaît dans les données de santé et de performances collectées, ou qui apparaît comme heure de détection d'un événement, est basé sur l'heure du cluster ONTAP, ajustée au fuseau horaire défini sur le navigateur Web.

Il est fortement recommandé d'utiliser un serveur NTP (Network Time Protocol) pour synchroniser l'heure sur vos serveurs Unified Manager, vos clusters ONTAP et vos navigateurs Web.



Si vous voyez des horodatages qui semblent incorrects pour un cluster particulier, vous souhaitez peut-être vérifier que l'heure du cluster a été correctement définie.

Naviguer dans les flux de travail de performance dans l'interface graphique d'Unified Manager

L'interface Unified Manager fournit de nombreuses pages pour la collecte et l'affichage des informations sur les performances. Vous utilisez le panneau de navigation de gauche pour accéder aux pages de l'interface graphique, et vous utilisez les onglets et les liens sur les pages pour afficher et configurer les informations.

Vous utilisez toutes les pages suivantes pour surveiller et dépanner les informations sur les performances du cluster :

- page du tableau de bord
- pages d'inventaire des objets de stockage et de réseau
- pages de détails des objets de stockage (y compris l'explorateur de performances)
- pages de configuration et d'installation
- pages d'événements

Connectez-vous à l'interface utilisateur

Vous pouvez vous connecter à l'interface utilisateur d'Unified Manager à l'aide d'un navigateur Web pris en charge.

Avant de commencer

- Le navigateur Web doit répondre aux exigences minimales.

Consultez la matrice d'interopérabilité sur "mysupport.netapp.com/matrix" pour la liste complète des versions de navigateur prises en charge.

- Vous devez disposer de l'adresse IP ou de l'URL du serveur Unified Manager.

Vous êtes automatiquement déconnecté de la session après 1 heure d'inactivité. Ce délai peut être configuré sous **Général > Paramètres des fonctionnalités**.

Étapes

1. Saisissez l'URL dans votre navigateur Web, où URL est l'adresse IP ou le nom de domaine complet (FQDN) du serveur Unified Manager :
 - Pour IPv4 : `https://URL/`
 - Pour IPv6 : `https://[URL]/`

Si le serveur utilise un certificat numérique auto-signé, le navigateur peut afficher un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez soit reconnaître le risque pour continuer l'accès, soit installer un certificat numérique signé par une autorité de certification (CA) pour l'authentification du serveur. Sur l'écran de connexion, entrez votre nom d'utilisateur et votre mot de passe.

Si la connexion à l'interface utilisateur d'Unified Manager est protégée à l'aide de l'authentification SAML, vous saisissez vos informations d'identification sur la page de connexion du fournisseur d'identité (IdP) au lieu de la page de connexion d'Unified Manager.

La page Tableau de bord s'affiche.



Si le serveur Unified Manager n'est pas initialisé, une nouvelle fenêtre de navigateur affiche l'assistant de première expérience. Vous devez saisir un destinataire de courrier électronique initial auquel les alertes par courrier électronique seront envoyées, le serveur SMTP qui gèrera les communications par courrier électronique et si AutoSupport est activé pour envoyer des informations sur votre installation d'Unified Manager au support technique. L'interface utilisateur du gestionnaire unifié s'affiche une fois ces informations complétées.

Interface graphique et chemins de navigation

Unified Manager offre une grande flexibilité et vous permet d'accomplir plusieurs tâches de différentes manières. Vous découvrirez de nombreux chemins de navigation lorsque vous travaillerez dans Unified Manager. Bien que toutes les combinaisons possibles de navigations ne puissent pas être affichées, vous devez être familiarisé avec quelques-uns des scénarios les plus courants.

Surveiller la navigation des objets du cluster

Vous pouvez surveiller les performances de tous les objets de n'importe quel cluster géré par Unified Manager. La surveillance de vos objets de stockage vous offre un aperçu des performances du cluster et des objets, et inclut la surveillance des événements de performances. Vous pouvez afficher les performances et les événements à un niveau élevé, ou vous pouvez examiner plus en détail les performances des objets et les événements de performances.

Voici un exemple parmi tant d'autres de navigations possibles dans les objets de cluster :

1. À partir de la page Tableau de bord, examinez les détails du panneau Capacité de performance pour identifier le cluster qui utilise la plus grande capacité de performance et cliquez sur le graphique à barres pour accéder à la liste des nœuds de ce cluster.
2. Identifiez le nœud avec la valeur de capacité de performance utilisée la plus élevée et cliquez sur ce nœud.
3. Depuis la page Explorateur de nœuds/performances, cliquez sur **Agrégats sur ce nœud** dans le menu Afficher et comparer.
4. Identifiez l'agrégat qui utilise la plus grande capacité de performance et cliquez sur cet agrégat.
5. À partir de la page Explorateur d'agrégats/performances, cliquez sur **Volumes sur cet agrégat** dans le menu Afficher et comparer.
6. Identifiez les volumes qui utilisent le plus d'IOPS.

Vous devez examiner ces volumes pour voir si vous devez appliquer une politique de qualité de service (QoS) ou une politique de niveau de service de performances, ou modifier les paramètres de politique, afin que ces volumes n'utilisent pas un pourcentage aussi élevé d'IOPS sur le cluster.

Dashboard All Clusters

Management Actions

- Enable takeover on panic (2)
- Disable telnet (2)
- Enable volume autogrow (9)

Capacity

31 events (No new in past 24 hours)

CLUSTER	USED	DAYS TO FULL	REDUCTION
opm-sl...llicity	40.5 TB	< 1 month	13.0 : 1
umeng...1-02	83.6 TB	51 days	8.0 : 1
symgr...0-1-8	33 TB	149 days	8.3 : 1

Performance Capacity

No new events

CLUSTER	USED	DAYS TO FULL
umeng-aff220-01-02	83%	< 1 month
symgr-fas8060-1-8	49%	< 1 month
fas8040-206-21	46%	77 days

Nodes

Last updated: Nov 15, 2019, 10:48 AM

VIEW Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show / Hide

Status	Node	Latency	IOPS	MB/s	Performance Capacity Used	Utilization	Fr
✖	umeng-aff220-01	21.7 ms/op	27,333 IOPS	211 MB/s	73%	50%	3.1
✖	umeng-aff220-02	8.33 ms/op	83.4 IOPS	102 MB/s	53%	42%	6.1

Node / Performance : umeng-aff220-01

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

Aggregate	Latency	IOPS	MB/s	Perf
NSLM12_002	12.4 ...	47.51 ...	5.8 M...	11%
NSLM12_001	11.4 ...	216 L...	4.33 ...	5%

Aggregate / Performance : NSLM12_002

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

Volume	Latency	IOPS	MB/s
suchita_vmaware_d...	6.38 ms...	76.8 IOPS	2.55 MB/s
suchita_vmaware_d...	5.82 ms...	4,775 L...	18.7 MB/s
aiqum_scale_do_no...	0.114 m...	< 1 IOPS	< 1 MB/s

Surveiller la navigation des performances du cluster

Vous pouvez surveiller les performances de tous les clusters gérés par Unified Manager. La surveillance de vos clusters vous offre un aperçu des performances des clusters et des objets et inclut la surveillance des événements de performances. Vous pouvez afficher les performances et les événements à un niveau élevé, ou vous pouvez examiner plus en détail les performances et les événements de performances du cluster et de l'objet.

Voici un exemple parmi de nombreux chemins de navigation possibles en matière de performances de cluster :

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Pour afficher des informations sur les performances de ces agrégats, sélectionnez la vue Performances : Tous les agrégats.
3. Identifiez l'agrégat que vous souhaitez étudier et cliquez sur le nom de cet agrégat pour accéder à la page Explorateur d'agrégats/performances.
4. Vous pouvez également sélectionner d'autres objets à comparer avec cet agrégat dans le menu Afficher et comparer, puis ajouter l'un des objets au volet de comparaison.

Les statistiques des deux objets apparaîtront dans les graphiques de compteurs à des fins de comparaison.

5. Dans le volet Comparaison à droite de la page Explorateur, cliquez sur **Zoom View** dans l'un des graphiques de compteurs pour afficher les détails de l'historique des performances de cet agrégat.

Aggregates ?

Last updated: Nov 15, 2019, 1:18 PM

VIEW Performance: All Aggregates Search Aggregates Filter

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Scheduled Reports



Show / Hide ▼

☐	Status	Aggregate	Type	Latency	IOPS	MB/s	Performance Capacity Used	Utilization
☐	!	aggr_evt	SSD	0.29 ms/op	3.79 IOPS	< 1 MB/s	< 1%	< 1%
☐	!	aggr4	HDD	5.74 ms/op	14.4 IOPS	1.31 MB/s	6%	5%
☐	!	aggr3	HDD	5.06 ms/op	3.06 IOPS	< 1 MB/s	6%	5%
☐	!	meg_aggr2	HDD	10.4 ms/op	52.9 IOPS	7.28 MB/s	3%	2%

Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM ?

Summary

Explorer

Information

Compare the performance of associated objects and display detailed charts ?

TIME RANGE Last 72 Hours

VIEW AND COMPARE

Aggregates on same Node ▼

Filter

Aggregate	Latency	IOPS	MB/s	Perf...	
aggr3	5.06 ...	3.06 ...	< 1 M...	6%	
aggr_evt	0.29 ...	3.79 ...	< 1 M...	< 1%	Add
aggr_automation	0.27 ...	6.35 ...	< 1 M...	< 1%	Add

Comparing

1 Additional Object



aggr4

aggr3

CHOOSE CHARTS 7 Charts Selected ▼

Events for Aggregate: aggr4



No data to display

Latency

VIEW Total ▼

Zoom View

Latency - Total view (ms/op)



Latency for Aggregate: aggr4 ?

Last updated: Nov 15, 2019, 1:23 PM ?

Event Timeline: aggr4

TIME RANGE Last 72 Hours

- × Critical Events
- ! Error Events
- ! Warning Events
- i Information Events

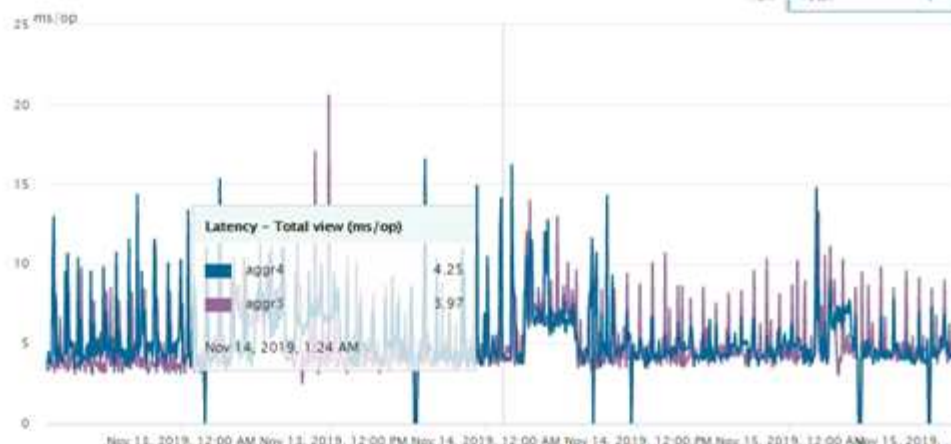


No data to display

Comparing Objects

aggr4

aggr3



Navigation dans l'enquête sur les événements

Les pages de détails des événements d'Unified Manager vous offrent un aperçu détaillé de tout événement de performance. Cela est utile lors de l'enquête sur les événements de performances, lors du dépannage et lors du réglage précis des performances du système.

Selon le type d'événement de performance, vous pouvez voir l'un des deux types de pages de détails de l'événement :

- Page de détails des événements pour les événements de politique de seuil définis par l'utilisateur et par le système
- Page de détails des événements pour les événements de politique de seuil dynamique

Ceci est un exemple de navigation d'enquête d'événement.

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans le menu Affichage, cliquez sur **Événements de performance actifs**.
3. Cliquez sur le nom de l'événement que vous souhaitez étudier et la page Détails de l'événement s'affiche.
4. Consultez la description de l'événement et examinez les actions suggérées (le cas échéant) pour afficher plus de détails sur l'événement qui peuvent vous aider à résoudre le problème. Vous pouvez cliquer sur le bouton **Analyser la charge de travail** pour afficher des graphiques de performances détaillés afin de vous aider à analyser plus en détail le problème.

Event Management

Last updated: Nov 15, 2019, 11:23 AM

VIEW **Active performance events** Search Events Filter +

Assign To Acknowledge Mark as Resolved Add Alert

Show / Hide

Triggered Time	Severity	State	Impact Lev	Impact Area	Name	Source	Source Ty
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_feb12_vol3	Volume
Nov 14, 2019, 11:39 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	vs7:/julia_non_shared_3	Volume
Nov 15, 2019, 5:04 AM	Warning	New	Risk	Performance	QoS Volume Peak IOP... Threshold Breached	suchita_vmwvar...nt_delete_01	Volume
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-01	LUN
Nov 15, 2019, 10:39 AM	Warning	New	Risk	Performance	Workload LUN Latency...Service Level Policy	iscsi_boot/ia.../ocum-c220-07	LUN

Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM_vs7_Performance_2_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.



Actions

Suggested Actions to Fix The Issue

Troubleshoot

Analyze Workload

Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput

- Leave the QoS configuration setting as it is.

Event Information

EVENT TRIGGER TIME	SEVERITY	SOURCE
Nov 14, 2019, 11:39 AM	Warning	vs7:/julia_non_shared_3
STATE	IMPACT LEVEL	SOURCE TYPE
New	Risk	Volume
EVENT DURATION	IMPACT AREA	ION CLUSTER
1 day 40 minutes	Performance	ocum-mobility-01-02
LAST SEEN		AFFECTED OBJECTS COUNT
Nov 15, 2019, 11:19 AM		1
		TRIGGERED POLICY
		QoS Peak IOPS/TB threshold

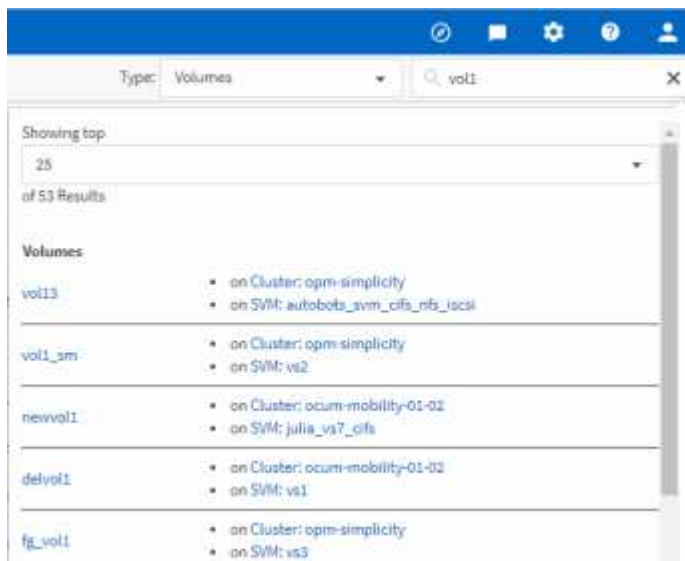
Rechercher des objets de stockage

Pour accéder rapidement à un objet spécifique, vous pouvez utiliser le champ **Rechercher tous les objets de stockage** en haut de la barre de menu. Cette méthode de recherche globale sur tous les objets vous permet de localiser rapidement des objets spécifiques par type. Les résultats de la recherche sont triés par type d'objet de stockage et vous pouvez les filtrer à l'aide du menu déroulant. Une recherche valide doit contenir au moins trois caractères.

La recherche globale affiche le nombre total de résultats, mais seuls les 25 premiers résultats de recherche sont accessibles. De ce fait, la fonctionnalité de recherche globale peut être considérée comme un outil de raccourci pour trouver des éléments spécifiques si vous connaissez les éléments que vous souhaitez localiser rapidement. Pour des résultats de recherche complets, vous pouvez utiliser la recherche dans les pages d'inventaire d'objets et sa fonctionnalité de filtrage associée.

Vous pouvez cliquer sur la liste déroulante et sélectionner **Tous** pour rechercher simultanément tous les objets et événements. Vous pouvez également cliquer sur la liste déroulante pour spécifier le type d'objet. Saisissez au moins trois caractères du nom de l'objet ou de l'événement dans le champ **Rechercher tous les objets de stockage**, puis appuyez sur **Entrée** pour afficher les résultats de la recherche, tels que :

- Clusters : noms de clusters
- Nœuds : noms de nœuds
- Agrégats : noms d'agrégats
- SVM : noms de SVM
- Volumes : noms des volumes
- LUN : chemins LUN



Les LIF et les ports ne sont pas consultables dans la barre de recherche globale.

Dans cet exemple, la liste déroulante contient le type d'objet Volume sélectionné. En tapant « vol » dans le champ **Rechercher tous les objets de stockage**, vous obtenez une liste de tous les volumes dont les noms contiennent ces caractères. Pour les recherches d'objets, vous pouvez cliquer sur n'importe quel résultat de recherche pour accéder à la page Explorateur de performances de cet objet. Pour les recherches d'événements, cliquer sur un élément dans le résultat de la recherche permet d'accéder à la page Détails de l'événement.

Filtrer le contenu de la page d'inventaire

Vous pouvez filtrer les données de la page d'inventaire dans Unified Manager pour localiser rapidement les données en fonction de critères spécifiques. Vous pouvez utiliser le filtrage pour affiner le contenu des pages d'Unified Manager afin d'afficher uniquement les résultats qui vous intéressent. Cela fournit une méthode très efficace pour afficher

uniquement les données qui vous intéressent.

Utilisez le **Filtrage** pour personnaliser la vue de la grille en fonction de vos préférences. Les options de filtre disponibles sont basées sur le type d'objet visualisé dans la grille. Si des filtres sont actuellement appliqués, le nombre de filtres appliqués s'affiche à droite du bouton Filtre.

Trois types de paramètres de filtre sont pris en charge.

Paramètre	Validation
Chaîne (texte)	Les opérateurs sont contient , commence par , se termine par et ne contient pas .
Nombre maximum	Les opérateurs sont supérieur à , inférieur à , dans le dernier et entre .
Enum (texte)	Les opérateurs sont is et is not .

Les champs Colonne, Opérateur et Valeur sont obligatoires pour chaque filtre ; les filtres disponibles reflètent les colonnes filtrables sur la page actuelle. Le nombre maximum de filtres que vous pouvez appliquer est de quatre. Les résultats filtrés sont basés sur des paramètres de filtre combinés. Les résultats filtrés s'appliquent à toutes les pages de votre recherche filtrée, pas seulement à la page actuellement affichée.

Vous pouvez ajouter des filtres à l'aide du panneau Filtrage.

1. En haut de la page, cliquez sur le bouton **Filtre**. Le panneau Filtrage s'affiche.
2. Cliquez sur la liste déroulante de gauche et sélectionnez un objet ; par exemple, *Cluster* ou un compteur de performances.
3. Cliquez sur la liste déroulante centrale et sélectionnez l'opérateur que vous souhaitez utiliser.
4. Dans la dernière liste, sélectionnez ou saisissez une valeur pour compléter le filtre pour cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Ajouter un filtre**. Un champ de filtre supplémentaire s'affiche. Complétez ce filtre en suivant le processus décrit dans les étapes précédentes. Notez qu'après avoir ajouté votre quatrième filtre, le bouton **+Ajouter un filtre** ne s'affiche plus.
6. Cliquez sur **Appliquer le filtre**. Les options de filtre sont appliquées à la grille et le nombre de filtres est affiché à droite du bouton Filtrer.
7. Utilisez le panneau Filtrage pour supprimer des filtres individuels en cliquant sur l'icône de la corbeille à droite du filtre à supprimer.
8. Pour supprimer tous les filtres, cliquez sur **Réinitialiser** en bas du panneau de filtrage.

Exemple de filtrage

L'illustration montre le panneau de filtrage avec trois filtres. Le bouton **+Ajouter un filtre** s'affiche lorsque vous avez moins que le maximum de quatre filtres.

MBps	greater than	5	MBps	
Node	name starts with	test		
Type	is	FCP Port		

[+ Add Filter](#)

[Cancel](#) [Apply Filter](#)

Après avoir cliqué sur **Appliquer le filtre**, le panneau Filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Surveiller les performances du cluster à partir du tableau de bord

Le tableau de bord d'Unified Manager fournit quelques panneaux qui affichent l'état des performances de haut niveau de tous les clusters surveillés par cette instance d'Unified Manager. Il vous permet d'évaluer les performances globales des clusters gérés et de noter, localiser ou attribuer rapidement la résolution à tout événement spécifique identifié.

Comprendre les panneaux de performances sur le tableau de bord

Le tableau de bord Unified Manager fournit quelques panneaux qui affichent l'état des performances de haut niveau pour tous les clusters surveillés dans votre environnement. Vous pouvez choisir d'afficher l'état de tous les clusters ou d'un cluster individuel.

En plus d'afficher des informations sur les performances, la plupart des panneaux affichent également le nombre d'événements actifs dans cette catégorie et le nombre de nouveaux événements ajoutés au cours des 24 heures précédentes. Ces informations vous aident à déterminer les clusters que vous devrez peut-être analyser plus en détail pour résoudre les événements signalés. Cliquer sur les événements affiche les quelques événements les plus importants et fournit un lien vers la page d'inventaire de gestion des événements filtrée pour afficher les événements de cette catégorie.

Les panneaux suivants fournissent l'état des performances.

- **Panneau Capacité de performance**

Lors de l'affichage de tous les clusters, ce panneau affiche la valeur de capacité de performance pour chaque cluster (moyenne sur l'heure précédente) et le nombre de jours jusqu'à ce que la capacité de performance atteigne la limite supérieure (en fonction du taux de croissance quotidien). En cliquant sur le graphique à barres, vous accédez à la page d'inventaire des nœuds pour ce cluster. Notez que la page d'inventaire des nœuds affiche la capacité de performance moyenne sur les 72 heures précédentes. Cette valeur peut donc ne pas correspondre à la valeur du tableau de bord.

Lors de l'affichage d'un seul cluster, ce panneau affiche la capacité de performance du cluster, le nombre total d'IOPS et les valeurs de débit total.

- **Panneau IOPS de charge de travail**

Lorsque la gestion active de la charge de travail est activée et lors de l’affichage d’un seul cluster, ce panneau affiche le nombre total de charges de travail actuellement en cours d’exécution dans une certaine plage d’IOPS.

- **Panneau de performance de la charge de travail**

Lorsque la gestion active de la charge de travail est activée, ce panneau affiche le nombre total de charges de travail conformes et non conformes attribuées à chaque niveau de service de performances défini. Cliquer sur un graphique à barres vous amène aux charges de travail attribuées à cette politique dans la page Charges de travail.

- **Panneau d’aperçu de l’utilisation**

Lors de l’affichage de tous les clusters, vous pouvez choisir d’afficher les clusters triés par IOPS ou débit (Mo/s) le plus élevé.

Lorsque vous visualisez un seul cluster, vous pouvez choisir d’afficher les charges de travail sur ce cluster triées par IOPS ou débit (Mo/s) le plus élevé.

Messages et descriptions des bannières de performance

Unified Manager peut afficher des messages de bannière sur la page Notifications (à partir de la cloche de notification) pour vous alerter des problèmes d’état d’un cluster particulier.

Message de la bannière	Description	Résolution
No performance data is being collected from cluster <i>cluster_name</i> . Restart Unified Manager to correct this issue.	Le service de collecte Unified Manager s’est arrêté et aucune donnée de performances n’est collectée à partir d’aucun cluster.	Redémarrez Unified Manager pour corriger ce problème. Si cela ne résout pas le problème, contactez le support technique.
More than x hour(s) of historical data is being collected from cluster <i>cluster_name</i> . Current data collections will start after all historical data is collected.	Un cycle de collecte de continuité des données est actuellement en cours d’exécution pour récupérer les données de performances en dehors du cycle de collecte des performances du cluster en temps réel.	Aucune action n’est requise. Les données de performance actuelles seront collectées une fois le cycle de collecte de continuité des données terminé. Un cycle de collecte de continuité des données s’exécute lorsqu’un nouveau cluster est ajouté ou lorsque Unified Manager n’a pas pu collecter les données de performances actuelles pour une raison quelconque.

Modifier l’intervalle de collecte des statistiques de performances

L’intervalle de collecte par défaut pour les statistiques de performances est de 5 minutes. Vous pouvez modifier cet intervalle à 10 ou 15 minutes si vous constatez que les

collectes de grands clusters ne se terminent pas dans le délai par défaut. Ce paramètre affecte la collecte de statistiques de tous les clusters surveillés par cette instance d'Unified Manager.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

Le problème des collectes de statistiques de performance qui ne se terminent pas à temps est indiqué par les messages de bannière `Unable to consistently collect from cluster <cluster_name>` ou `Data collection is taking too long on cluster <cluster_name>`.

Vous ne devez modifier l'intervalle de collecte que lorsque cela est nécessaire en raison d'un problème de collecte de statistiques. Ne modifiez pas ce paramètre pour une autre raison.



La modification de cette valeur par rapport au paramètre par défaut de 5 minutes peut affecter le nombre et la fréquence des événements de performances signalés par Unified Manager. Par exemple, les seuils de performances définis par le système déclenchent des événements lorsque la politique est dépassée pendant 30 minutes. Lors de l'utilisation de collectes de 5 minutes, la politique doit être dépassée pendant six collectes consécutives. Pour les collectes de 15 minutes, la politique doit être dépassée pendant seulement deux périodes de collecte.

Un message au bas de la page Configuration du cluster indique l'intervalle de collecte de données statistiques actuel.

Étapes

1. Connectez-vous à l'aide de SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

Les invites de la console de maintenance d'Unified Manager s'affichent.

2. Tapez le numéro de l'option de menu intitulée **Configuration de l'intervalle d'interrogation des performances**, puis appuyez sur Entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe de l'utilisateur de maintenance.
4. Tapez le numéro du nouvel intervalle d'interrogation que vous souhaitez définir, puis appuyez sur Entrée.

Si vous avez modifié l'intervalle de collecte d'Unified Manager à 10 ou 15 minutes et que vous disposez d'une connexion actuelle à un fournisseur de données externe (tel que Graphite), vous devez modifier l'intervalle de transmission du fournisseur de données afin qu'il soit égal ou supérieur à l'intervalle de collecte d'Unified Manager.

Dépanner les charges de travail à l'aide de l'analyseur de charge de travail

L'analyseur de charge de travail permet d'afficher des critères importants de santé et de performances pour une charge de travail unique sur une seule page afin de faciliter le dépannage. En visualisant tous les événements actuels et passés d'une charge de travail, vous pouvez avoir une meilleure idée des raisons pour lesquelles la charge de travail peut rencontrer un problème de performances ou de capacité actuellement.

L'utilisation de cet outil peut également vous aider à déterminer si le stockage est la cause de problèmes de

performances d'une application ou si le problème est causé par un problème de réseau ou autre problème connexe.

Vous pouvez lancer cette fonctionnalité à partir de différents emplacements dans l'interface utilisateur :

- À partir de la sélection Analyse de la charge de travail dans le menu de navigation de gauche
- Depuis la page Détails de l'événement en cliquant sur le bouton **Analyser la charge de travail**
- Depuis n'importe quelle page d'inventaire de charge de travail (volume, LUN, charge de travail, partage NFS ou partage SMB/CIFS), en cliquant sur l'icône Plus  , puis **Analyser la charge de travail**
- Depuis la page Machines virtuelles en cliquant sur le bouton **Analyser la charge de travail** à partir de n'importe quel objet Datastore

Lorsque vous lancez l'outil à partir du menu de navigation de gauche, vous pouvez saisir le nom de n'importe quelle charge de travail que vous souhaitez analyser et sélectionner la plage horaire pour laquelle vous souhaitez effectuer le dépannage. Lorsque vous lancez l'outil à partir de l'une des pages d'inventaire de charge de travail ou de machine virtuelle, le nom de la charge de travail est renseigné automatiquement et les données de la charge de travail sont présentées avec la plage horaire par défaut de 2 heures. Lorsque vous lancez l'outil à partir de la page Détails de l'événement, le nom de la charge de travail est renseigné automatiquement et les données de 10 jours s'affichent.

Quelles données l'analyseur de charge de travail affiche-t-il ?

La page de l'analyseur de charge de travail affiche des informations sur les événements actuels susceptibles d'affecter la charge de travail, des recommandations pour résoudre potentiellement le problème à l'origine de l'événement et des graphiques pour analyser l'historique des performances et de la capacité.

En haut de la page, vous spécifiez le nom de la charge de travail (volume ou LUN) que vous souhaitez analyser et la période sur laquelle vous souhaitez voir les statistiques. Vous pouvez modifier la période à tout moment si vous souhaitez afficher une période plus courte ou plus longue.

Les autres zones de la page affichent les résultats de l'analyse et les graphiques de performances et de capacité.



Les graphiques de charge de travail pour les LUN ne fournissent pas le même niveau de statistiques que ceux pour les volumes. Vous remarquerez donc des différences lors de l'analyse de ces deux types de charges de travail.

• Zone de résumé des événements

Affiche un bref aperçu du nombre et des types d'événements qui se sont produits au cours de la période. Lorsqu'il y a des événements provenant de différents domaines d'impact (par exemple, performances et capacité), ces informations s'affichent afin que vous puissiez sélectionner les détails du type d'événement qui vous intéresse. Cliquez sur le type d'événement pour afficher la liste des noms d'événements.

S'il n'y a qu'un seul événement pendant la période, une liste de recommandations pour résoudre le problème est répertoriée pour certains événements.

• Chronologie de l'événement

Affiche toutes les occurrences d'événements pendant la période spécifiée. Passez votre curseur sur chaque événement pour afficher le nom de l'événement.

Si vous êtes arrivé sur cette page en cliquant sur le bouton **Analyser la charge de travail** de la page Détails de l'événement, l'icône de l'événement sélectionné apparaît plus grande afin que vous puissiez identifier l'événement.

• Zone des graphiques de performances

Affiche des graphiques pour la latence, le débit (IOPS et Mo/s) et l'utilisation (pour le nœud et l'agrégat) en fonction de la période sélectionnée. Vous pouvez cliquer sur le lien [Afficher les détails des performances](#) pour afficher la page Explorateur de performances de la charge de travail au cas où vous souhaiteriez effectuer une analyse plus approfondie.

- **Latence** affiche la latence de la charge de travail sur la période sélectionnée. Le graphique comporte trois vues qui vous permettent de voir :
 - **Latence totale**
 - **Décomposition** de la latence (décomposée par lectures, écritures et autres processus)
 - **Composants du cluster** latence (décomposée par composant du cluster)

Voir "[Composants de cluster et pourquoi ils peuvent être en conflit](#)" pour une description des composants du cluster qui sont affichés ici. **Débit** affiche à la fois le débit IOPS et Mo/s pour la charge de travail sur la période sélectionnée. Le graphique comporte quatre vues qui vous permettent de voir : * **Débit total** * **Répartition du débit (décomposé par lectures, écritures et autres processus)** * **Débit du cloud** (les Mo/s utilisés pour écrire et lire des données dans le cloud ; pour les charges de travail qui hiérarchisent la capacité vers le cloud) * **IOPS avec prévision (une prédiction des valeurs de débit IOPS supérieures et inférieures attendues sur la période)** Ce graphique affiche également les paramètres de seuil de débit maximum et minimum de qualité de service (QoS), s'ils sont configurés, afin que vous puissiez voir où le système peut limiter intentionnellement le débit avec des politiques de QoS. **Utilisation** affiche l'utilisation de l'agrégat et du nœud sur lesquels la charge de travail s'exécute sur la période sélectionnée. À partir de là, vous pouvez voir si votre agrégat ou votre nœud est surutilisé, ce qui peut entraîner une latence élevée. Lors de l'analyse des volumes FlexGroup, plusieurs nœuds et plusieurs agrégats sont répertoriés dans les graphiques d'utilisation.

• Zone du tableau des capacités

Affiche des graphiques sur la capacité des données et la capacité des instantanés pour le mois dernier pour la charge de travail.

Pour les volumes, vous pouvez cliquer sur le lien [Afficher les détails de la capacité](#) pour afficher la page Détails d'intégrité de la charge de travail au cas où vous souhaiteriez effectuer une analyse plus approfondie. Les LUN ne fournissent pas ce lien car il n'existe pas de page Détails de santé pour les LUN.

- **Vue de la capacité** affiche l'espace total disponible alloué à la charge de travail et l'espace logique utilisé (après toutes les optimisations NetApp).
- **Vue instantanée** affiche l'espace total réservé aux copies instantanées et la quantité d'espace actuellement utilisée. Notez que les LUN ne fournissent pas de vue instantanée.
- **Cloud Tier View** affiche la quantité de capacité utilisée dans le niveau de performance local et la quantité utilisée dans le niveau cloud. Ces graphiques incluent une estimation du temps restant avant que la capacité soit pleine pour cette charge de travail. Ces informations sont basées sur l'utilisation historique et nécessitent un minimum de 10 jours de données. Lorsqu'il reste moins de 30 jours de capacité, Unified Manager identifie le stockage comme « presque plein ».

Quand dois-je utiliser l'analyseur de charge de travail

Vous utiliserez généralement l'analyseur de charge de travail pour résoudre un problème de latence signalé par un utilisateur, pour analyser plus en détail un événement ou une alerte signalé, ou pour explorer une charge de travail qui, selon vous, fonctionne de manière anormale.

Dans le cas où des utilisateurs vous ont contacté pour vous dire que l'application qu'ils utilisent s'exécute très lentement, vous pouvez vérifier les graphiques de latence, de débit et d'utilisation de la charge de travail sur laquelle l'application s'exécute pour voir si le stockage est la cause du problème de performances. Vous pouvez également utiliser le tableau de capacité pour voir si la capacité est faible, car un système ONTAP dans lequel la capacité est utilisée à plus de 85 % peut entraîner des problèmes de performances. Ces graphiques vous aideront à déterminer si le problème est causé par le stockage ou par un problème de réseau ou autre problème connexe.

Dans le cas où Unified Manager a généré un événement de performance et que vous souhaitez examiner la cause du problème plus en détail, vous pouvez lancer l'analyseur de charge de travail à partir de la page Détails de l'événement en cliquant sur le bouton **Analyser la charge de travail** pour rechercher certaines des tendances de latence, de débit et de capacité de la charge de travail.

Dans le cas où vous remarquez une charge de travail qui semble fonctionner anormalement lorsque vous consultez une page d'inventaire de charge de travail (volume, LUN, charge de travail, partage NFS ou partage SMB/CIFS), vous pouvez cliquer sur l'icône Plus , puis **Analyser la charge de travail** pour ouvrir la page Analyse de la charge de travail afin d'examiner la charge de travail plus en détail.

Utiliser l'analyseur de charge de travail

Il existe de nombreuses façons de démarrer l'analyseur de charge de travail à partir de l'interface utilisateur. Nous décrivons ici le lancement de l'outil à partir du volet de navigation de gauche.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Analyse de la charge de travail**.

La page Analyse de la charge de travail s'affiche.

2. Si vous connaissez le nom de la charge de travail, saisissez-le. Si vous n'êtes pas sûr du nom complet, entrez au moins 3 caractères et le système affiche une liste de charges de travail correspondant à la chaîne.
3. Sélectionnez la plage horaire si vous souhaitez afficher les statistiques sur une période supérieure à la durée par défaut de 2 heures et cliquez sur **Appliquer**.
4. Consultez la zone Résumé pour voir les événements qui se sont produits au cours de la période.
5. Consultez les graphiques de performances et de capacité pour voir quand l'une des mesures est anormale et voir si des événements correspondent à l'entrée anormale.

Surveiller les performances du cluster à partir de la page de destination du cluster de performances

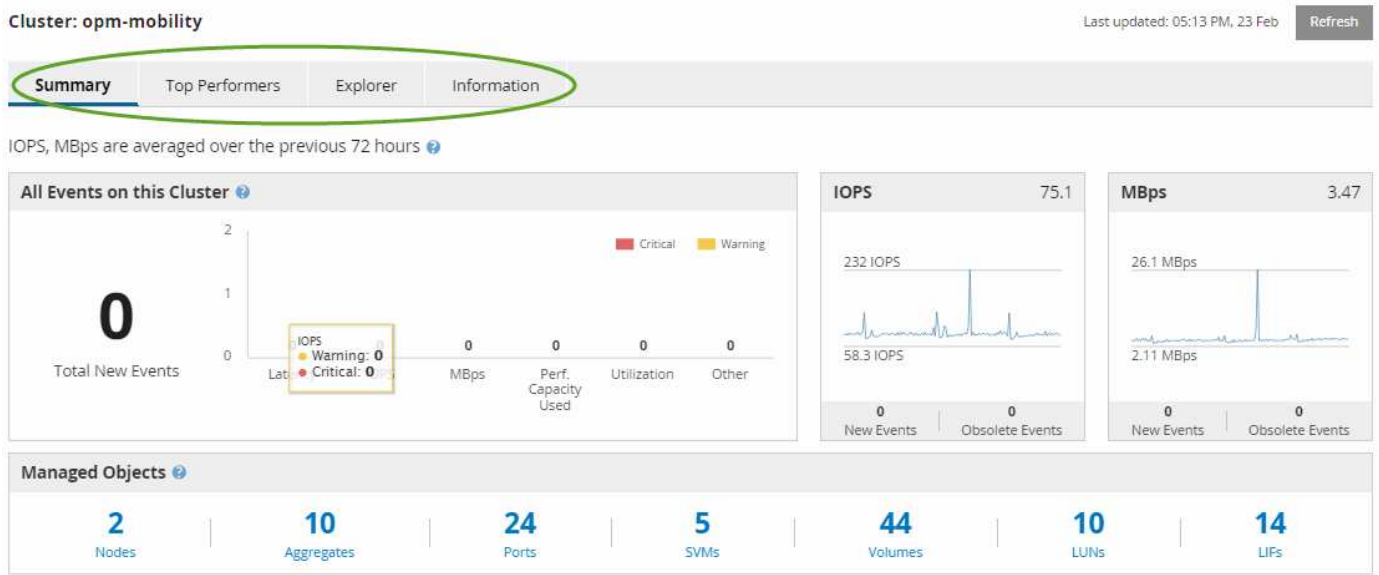
La page d'accueil du cluster de performances affiche l'état des performances de haut

niveau d'un cluster sélectionné qui est surveillé par une instance d'Unified Manager. Cette page vous permet d'évaluer les performances globales d'un cluster spécifique et de noter, localiser ou attribuer rapidement la résolution à tout événement spécifique au cluster identifié.

Comprendre la page de destination du cluster de performance

La page d'accueil du cluster de performances fournit un aperçu des performances de haut niveau d'un cluster sélectionné, en mettant l'accent sur l'état des performances des 10 principaux objets du cluster. Les problèmes de performances sont affichés en haut de la page, dans le panneau Tous les événements de ce cluster.

La page de destination du cluster de performances fournit un aperçu de haut niveau de chaque cluster géré par une instance d'Unified Manager. Cette page vous fournit des informations sur les événements et les performances, et vous permet de surveiller et de dépanner les clusters. L'image suivante montre un exemple de la page de destination du cluster de performances pour le cluster appelé opm-mobility :



Le nombre d'événements sur la page Résumé du cluster peut ne pas correspondre au nombre d'événements sur la page Inventaire des événements de performances. Cela est dû au fait que la page Résumé du cluster peut afficher un événement dans chacune des barres Latence et Utilisation lorsque les stratégies de seuil de combinaison ont été violées, tandis que la page Inventaire des événements de performances n'affiche qu'un seul événement lorsqu'une stratégie de combinaison a été violée.



Si un cluster a été supprimé de la gestion d'Unified Manager, le statut **Supprimé** s'affiche à droite du nom du cluster en haut de la page.

Page de destination du cluster de performance

La page de destination du cluster de performances affiche l'état des performances de haut niveau d'un cluster sélectionné. La page vous permet d'accéder aux détails complets de chaque compteur de performances pour les objets de stockage sur le cluster sélectionné.

La page de destination du cluster de performances comprend quatre onglets qui séparent les détails du cluster en quatre zones d'informations :

- Page de résumé
 - Volet Événements de cluster
 - Graphiques de performances MB/s et IOPS
 - Volet Objets gérés
- Page des meilleurs interprètes
- Page de l'explorateur
- Page d'information

Page de résumé du cluster de performance

La page Résumé du cluster de performances fournit un résumé des événements actifs, des performances IOPS et des performances Mo/s pour un cluster. Cette page inclut également le nombre total d'objets de stockage dans le cluster.

Volet des événements de performances du cluster

Le volet Événements de performances du cluster affiche les statistiques de performances et tous les événements actifs du cluster. Ceci est très utile lors de la surveillance de vos clusters et de toutes les performances et événements liés aux clusters.

Tous les événements sur ce volet de cluster

Le volet Tous les événements de ce cluster affiche tous les événements de performances du cluster actifs au cours des 72 heures précédentes. Le nombre total d'événements actifs s'affiche à l'extrême gauche ; ce nombre représente le total de tous les événements nouveaux et reconnus pour tous les objets de stockage de ce cluster. Vous pouvez cliquer sur le lien Total des événements actifs pour accéder à la page Inventaire des événements, qui est filtrée pour afficher ces événements.

Le graphique à barres Total des événements actifs pour le cluster affiche le nombre total d'événements critiques et d'avertissement actifs :

- Latence (total pour les nœuds, les agrégats, les SVM, les volumes, les LUN et les espaces de noms)
- IOPS (total pour les clusters, les nœuds, les agrégats, les SVM, les volumes, les LUN et les espaces de noms)
- Mo/s (total pour les clusters, les nœuds, les agrégats, les SVM, les volumes, les LUN, les espaces de noms, les ports et les LIF)
- Capacité de performance utilisée (total pour les nœuds et les agrégats)
- Utilisation (total pour les nœuds, les agrégats et les ports)
- Autre (taux d'échec de cache pour les volumes)

La liste contient des événements de performances actifs déclenchés à partir de stratégies de seuil définies par l'utilisateur, de stratégies de seuil définies par le système et de seuils dynamiques.

Les données du graphique (barres verticales du compteur) sont affichées en rouge (■) pour les événements critiques, et jaune (■) pour les événements d'avertissement. Placez votre curseur sur chaque barre de

compteur verticale pour afficher le type et le nombre réels d'événements. Vous pouvez cliquer sur **Actualiser** pour mettre à jour les données du panneau de compteur.

Vous pouvez afficher ou masquer les événements critiques et d'avertissement dans le graphique de performances Total des événements actifs en cliquant sur les icônes **Critique** et **Avertissement** dans la légende. Si vous masquez certains types d'événements, les icônes de légende s'affichent en gris.

Panneaux de comptoir

Les panneaux de compteurs affichent l'activité du cluster et les événements de performance pour les 72 heures précédentes et incluent les compteurs suivants :

- **Panneau de compteur IOPS**

IOPS indique la vitesse de fonctionnement du cluster en nombre d'opérations d'entrée/sortie par seconde. Ce panneau de compteur fournit un aperçu de haut niveau de l'état des IOPS du cluster pour la période de 72 heures précédente. Vous pouvez positionner votre curseur sur la ligne de tendance du graphique pour afficher la valeur IOPS pour une période spécifique.

- **Panneau de compteur MB/s**

MB/s indique la quantité de données transférées vers et depuis le cluster en mégaoctets par seconde. Ce panneau de compteur fournit un aperçu de haut niveau de l'état de santé du cluster en Mo/s pour la période de 72 heures précédente. Vous pouvez positionner votre curseur sur la ligne de tendance du graphique pour afficher la valeur MB/s pour une période spécifique.

Le nombre en haut à droite du graphique dans la barre grise est la valeur moyenne de la dernière période de 72 heures. Les chiffres affichés en bas et en haut du graphique de tendance sont les valeurs minimales et maximales pour la dernière période de 72 heures. La barre grise sous le graphique contient le nombre d'événements actifs (nouveaux et reconnus) et d'événements obsolètes de la dernière période de 72 heures.

Les panneaux de compteurs contiennent deux types d'événements :

- **Actif**

Indique que l'événement de performance est actuellement actif (nouveau ou reconnu). Le problème à l'origine de l'événement ne s'est pas corrigé ou n'a pas été résolu. Le compteur de performances de l'objet de stockage reste au-dessus du seuil de performances.

- **Obsolète**

Indique que l'événement n'est plus actif. Le problème à l'origine de l'événement s'est corrigé ou a été résolu. Le compteur de performances de l'objet de stockage n'est plus au-dessus du seuil de performances.

Pour les **événements actifs**, s'il y a un événement, vous pouvez positionner votre curseur sur l'icône de l'événement et cliquer sur le numéro de l'événement pour accéder à la page Détails de l'événement appropriée. S'il y a plusieurs événements, vous pouvez cliquer sur **Afficher tous les événements** pour afficher la page Inventaire des événements, qui est filtrée pour afficher tous les événements pour le type de compteur d'objet sélectionné.

Volet Objets gérés

Le volet Objets gérés de l'onglet Résumé des performances fournit un aperçu de niveau

supérieur des types et des nombres d'objets de stockage pour le cluster. Ce volet vous permet de suivre l'état des objets dans chaque cluster.

Le nombre d'objets gérés correspond à des données ponctuelles à partir de la dernière période de collecte. De nouveaux objets sont découverts à des intervalles de 15 minutes.

Cliquer sur le numéro lié à n'importe quel type d'objet affiche la page d'inventaire des performances de l'objet pour ce type d'objet. La page d'inventaire des objets est filtrée pour afficher uniquement les objets de ce cluster.

Les objets gérés sont :

- **Nœuds**

Un système physique dans un cluster.

- **Agrégats**

Un ensemble de plusieurs groupes de disques redondants indépendants (RAID) qui peuvent être gérés comme une seule unité à des fins de protection et de provisionnement.

- **Ports**

Un point de connexion physique sur les nœuds utilisé pour se connecter à d'autres périphériques sur un réseau.

- **VM de stockage**

Une machine virtuelle fournissant un accès au réseau via des adresses réseau uniques. Un SVM peut fournir des données à partir d'un espace de noms distinct et est administrable séparément du reste du cluster.

- **Volumes**

Une entité logique contenant des données utilisateur accessibles via un ou plusieurs des protocoles d'accès pris en charge. Le décompte inclut à la fois les volumes FlexVol et les volumes FlexGroup ; il n'inclut pas les constituants FlexGroup .

- **LUN**

L'identifiant d'une unité logique Fibre Channel (FC) ou d'une unité logique iSCSI. Une unité logique correspond généralement à un volume de stockage et est représentée dans un système d'exploitation informatique comme un périphérique.

- **Interfaces réseau**

Une interface réseau logique représentant un point d'accès réseau à un nœud. Le décompte inclut tous les types d'interface.

Page des meilleurs interprètes

La page Meilleurs interprètes affiche les objets de stockage qui ont les performances les plus élevées ou les performances les plus faibles, en fonction du compteur de performances que vous sélectionnez. Par exemple, dans la catégorie Machines virtuelles

de stockage, vous pouvez afficher les SVM qui ont les IOPS les plus élevées, la latence la plus élevée ou le débit en Mo/s le plus bas. Cette page indique également si l'un des meilleurs artistes a des événements de performance actifs (nouveaux ou reconnus).

La page Meilleurs interprètes affiche un maximum de 10 exemplaires de chaque objet. Notez que l'objet Volume inclut à la fois les volumes FlexVol et les volumes FlexGroup .

- **Plage horaire**

Vous pouvez sélectionner une plage horaire pour afficher les éléments les plus performants ; la plage horaire sélectionnée s'applique à tous les objets de stockage. Plages horaires disponibles :

- Dernière heure
- Les 24 dernières heures
- Dernières 72 heures (par défaut)
- Les 7 derniers jours

- **Métrique**

Cliquez sur le menu **Métrique** pour sélectionner un autre compteur. Les options de compteur sont uniques au type d'objet. Par exemple, les compteurs disponibles pour l'objet **Volumes** sont **Latency**, **IOPS** et **MB/s**. La modification du compteur recharge les données du panel avec les éléments les plus performants en fonction du compteur sélectionné.

Compteurs disponibles :

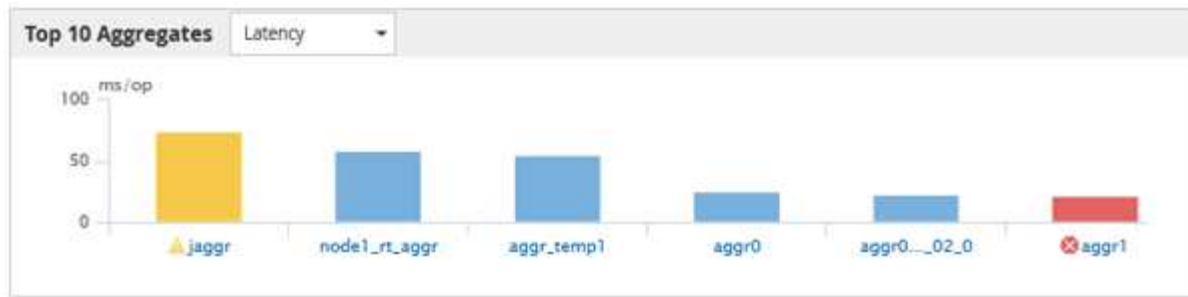
- Latence
- Op E/S par sec
- Mo/s
- Capacité de performance utilisée (pour les nœuds et les agrégats)
- Utilisation (pour les nœuds et les agrégats)

- **Trier**

Cliquez sur le menu **Trier** pour sélectionner un tri croissant ou décroissant pour l'objet et le compteur sélectionnés. Les options sont **Du plus élevé au plus bas** et **Du plus bas au plus élevé**. Ces options vous permettent de visualiser les objets ayant les performances les plus élevées ou les performances les plus faibles.

- **Comptoir-bar**

La barre de compteur dans le graphique affiche les statistiques de performance pour chaque objet, représentées sous forme de barre pour cet élément. Les graphiques à barres sont codés par couleur. Si le compteur ne dépasse pas un seuil de performance, la barre du compteur s'affiche en bleu. Si un dépassement de seuil est actif (un événement nouveau ou reconnu), la barre s'affiche dans la couleur de l'événement : les événements d'avertissement sont affichés en jaune (■), et les événements critiques sont affichés en rouge (■). Les violations de seuil sont également indiquées par des icônes d'indicateur d'événement de gravité pour les événements d'avertissement et critiques.



Pour chaque graphique, l'axe X affiche les meilleurs éléments pour le type d'objet sélectionné. L'axe Y affiche les unités applicables au compteur sélectionné. En cliquant sur le lien du nom de l'objet sous chaque élément du graphique à barres verticales, vous accédez à la page de destination des performances de l'objet sélectionné.

• Indicateur de gravité de l'événement

L'icône de l'indicateur **Événement de gravité** s'affiche à gauche du nom d'un objet pour un événement critique actif (❌) ou avertissement (⚠️) événements dans les graphiques des meilleurs interprètes. Cliquez sur l'icône de l'indicateur **Événement de gravité** pour afficher :

◦ Un événement

Accède à la page des détails de l'événement pour cet événement.

◦ Deux événements ou plus

Accède à la page d'inventaire des événements, qui est filtrée pour afficher tous les événements de l'objet sélectionné.

• Bouton Exporter

Crée un .csv fichier qui contient les données qui apparaissent dans la barre du compteur. Vous pouvez choisir de créer le fichier pour le cluster unique que vous visualisez ou pour tous les clusters du centre de données.

Surveiller les performances à l'aide des pages d'inventaire des performances

Les pages de performances de l'inventaire des objets affichent des informations sur les performances, les événements de performances et l'état des objets pour tous les objets d'une catégorie de type d'objet. Cela vous fournit un aperçu rapide de l'état des performances de chaque objet au sein d'un cluster, par exemple, pour tous les nœuds ou tous les volumes.

Les pages de performances de l'inventaire des objets fournissent un aperçu de haut niveau de l'état des objets, vous permettant d'évaluer les performances globales de tous les objets et de comparer les données de performances des objets. Vous pouvez affiner le contenu des pages d'inventaire d'objets en recherchant, en triant et en filtrant. Cela est utile lors de la surveillance et de la gestion des performances des objets, car cela vous permet de localiser rapidement les objets présentant des problèmes de performances et de commencer le processus de dépannage.

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

View

All Nodes

Search Nodes

Assign Performance Threshold Policy

Clear Performance Threshold Policy

Schedule Report

☐	Status	Node	Latency	IOPS	MBps	Flash Cache Reads	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster
☐		ocum-mobility-02	10.2 ms/op	18,884 IOPS	156 MBps	N/A	81%	35%	16.6 TB	23.2 TB	ocum-mobility-01-02
☒		opm-simplicity-01	2.01 ms/op	39,358 IOPS	153 MBps	< 1%	119%	88%	4.88 TB	18.3 TB	opm-simplicity
☐		ocum-mobility-01	0.018 ms/op	< 1 IOPS	18.2 MBps	N/A	23%	18%	8.69 TB	15.7 TB	ocum-mobility-01-02
☐		opm-simplicity-02	17 ms/op	14,627 IOPS	124 MBps	< 1%	29%	20%	212 GB	5.88 TB	opm-simplicity

Par défaut, les objets sur les pages d'inventaire des performances sont triés en fonction de la criticité des performances de l'objet. Les objets avec de nouveaux événements de performances critiques sont répertoriés en premier, et les objets avec des événements d'avertissement sont répertoriés en second. Cela fournit une indication visuelle immédiate des problèmes qui doivent être résolus. Toutes les données de performance sont basées sur une moyenne sur 72 heures.

Vous pouvez facilement naviguer de la page de performances de l'inventaire des objets vers une page de détails d'objet en cliquant sur le nom de l'objet dans la colonne du nom de l'objet. Par exemple, sur la page d'inventaire Performances/Tous les nœuds, vous devez cliquer sur un objet nœud dans la colonne **Nœuds**. La page des détails de l'objet fournit des informations détaillées sur l'objet sélectionné, y compris une comparaison côte à côte des événements actifs.

Afficher les pages d'inventaire des performances pour tous les objets de stockage

Vous utilisez les pages d'inventaire des performances pour afficher un résumé des informations de performances sur chacun des objets de stockage disponibles, tels que les clusters, les agrégats, les volumes, etc. Vous pouvez créer un lien vers les pages de détails de l'objet Performance pour afficher des informations détaillées sur un objet particulier.

Par défaut, les objets des pages d'affichage sont triés en fonction de la criticité des événements. Les objets avec des événements critiques sont répertoriés en premier, et les objets avec des événements d'avertissement sont répertoriés en second. Cela fournit une indication visuelle immédiate des problèmes qui doivent être résolus.

Vous pouvez exporter des données de ces pages vers des valeurs séparées par des virgules (`.csv`) fichier, fichier Microsoft Excel (`.xlsx`), ou (`.pdf`) document en utilisant le bouton **Rapports**, puis utilisez les données exportées pour créer des rapports. De plus, vous pouvez personnaliser la page, puis programmer la création et l'envoi régulier d'un rapport par courrier électronique à l'aide du bouton **Rapports programmés**.

Tous les champs de ces pages peuvent être utilisés dans des vues personnalisées et dans des rapports. Certains champs sont liés à des pages connexes permettant une vue plus détaillée.

Performances : vue Tous les clusters

La vue Performances : Tous les clusters affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque cluster surveillé par une instance de Unified Manager. Cette page vous permet de surveiller les performances de vos clusters et de résoudre les problèmes de performances et les événements de seuil.

Vous pouvez attribuer des stratégies de seuil de performance ou effacer des stratégies de seuil de n'importe

quel objet sur les pages d'inventaire d'objets à l'aide des boutons **Attribuer une stratégie de seuil de performance** et **Effacer la stratégie de seuil de performance**.

Voici quelques champs importants dans la vue Performances : Tous les clusters.

- Cluster FQDN : le nom de domaine complet (FQDN) du cluster.
- IOPS : les opérations d'entrée/sortie par seconde sur le cluster.
- MB/s : le débit sur le cluster, mesuré en Mio par seconde.
- Champs de capacité : Capacité libre et totale en Gio.
- Nom d'hôte ou adresse IP : le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du LIF de gestion de cluster.
- Version du système d'exploitation : la version du logiciel ONTAP installée sur le cluster.



Si différentes versions du logiciel ONTAP sont installées sur les nœuds du cluster, le numéro de version le plus bas est répertorié. Vous pouvez afficher la version ONTAP installée sur chaque nœud à partir de la vue Performances : tous les nœuds.

- Politique de seuil : la ou les politiques de seuil de performances définies par l'utilisateur qui sont actives sur cet objet de stockage. Vous pouvez positionner votre curseur sur les noms de stratégie contenant des points de suspension (...) pour afficher le nom complet de la stratégie ou la liste des noms de stratégie attribués. Les boutons Affecter la politique de seuil de performance et Effacer la politique de seuil de performance restent désactivés jusqu'à ce que vous sélectionniez un ou plusieurs objets en cliquant sur les cases à cocher situées à l'extrême gauche.

Performances : vue Tous les volumes

La vue Performances : Tous les volumes affiche un aperçu des événements de performances, des données de compteur et des informations de configuration pour chaque FlexVol volume et FlexGroup surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances de vos volumes et de résoudre les problèmes de performances et les événements de seuil.

Si vous souhaitez analyser la latence et le débit d'un objet spécifique, cliquez sur le bouton Plus d'options  puis **Analyser la charge de travail** et vous pouvez afficher les graphiques de performances et de capacité sur la page Analyse de la charge de travail. Vous pouvez afficher les détails sur System Manager, à condition que vous disposiez d'informations d'identification valides pour System Manager.



Pour les volumes de protection des données (DP), seules les valeurs de compteur pour le trafic généré par l'utilisateur sont affichées. Les volumes racine ne sont pas affichés sur cette page.

Voici quelques champs importants dans la vue Performances : Tous les volumes.

- Style : FlexVol ou FlexGroup.
- Latence : pour les volumes FlexVol , il s'agit du temps de réponse moyen du volume pour toutes les demandes d'E/S, exprimé en millisecondes par opération. Pour les volumes FlexGroup , il s'agit de la latence moyenne de tous les volumes constitutifs.
- IOPS/To : nombre d'opérations d'entrée/sortie traitées par seconde en fonction de l'espace total consommé par la charge de travail, en téraoctets. Ce compteur mesure les performances pouvant être fournies par une quantité donnée de capacité de stockage.
- IOPS : pour les volumes FlexVol , il s'agit du nombre d'opérations d'entrée/sortie par seconde pour le volume. Pour les volumes FlexGroup , il s'agit de la somme des IOPS pour tous les volumes constitutifs.

- Mo/s : pour les volumes FlexVol , il s'agit du débit sur le volume, mesuré en mégaoctets par seconde. Pour les volumes FlexGroup , il s'agit de la somme de Mo/s pour tous les volumes constitutifs.
- Champs de capacité : Capacité libre et totale en Gio.

Consultez les liens suivants pour plus d'informations :

- ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
- ["Suppression des politiques de seuil de performance des objets de stockage"](#)
- ["Types de charges de travail surveillées par Unified Manager"](#)
- ["Affichage des paramètres du groupe de politiques QoS appliqués à des volumes ou LUN spécifiques"](#)
- ["Comprendre les recommandations d'Unified Manager pour hiérarchiser les données vers le cloud"](#)
- ["Affichage des graphiques de performances pour comparer les volumes ou les LUN qui se trouvent dans le même groupe de stratégies QoS"](#)

Performances : vue Tous les agrégats

La vue Performances : tous les agrégats affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque agrégat surveillé par une instance de Unified Manager. Cette page vous permet de surveiller les performances de vos agrégats et de résoudre les problèmes de performances et les événements de seuil.

Voici quelques champs importants dans la vue Performances : Tous les agrégats.

- Type : Le type d'agrégat :
 - Disque dur
 - Hybride. Combine les disques durs et les SSD, mais le pool Flash n'a pas été activé.
 - Hybride (Flash Pool). Combine les disques durs et les SSD, et Flash Pool a été activé.
 - SSD
 - Disque SSD (FabricPool). Combine des SSD et un niveau cloud
 - Disque dur (FabricPool). Combine des disques durs et un niveau cloud
 - Disque VMD (SDS). Disques virtuels dans une machine virtuelle
 - Disque virtuel (FabricPool). Combine des disques virtuels et un niveau cloud
 - LUN (FlexArray)
- Rapport de données inactives : indique si la fonctionnalité de rapport de données inactives est activée ou désactivée sur cet agrégat. Lorsque cette option est activée, les volumes de cet agrégat affichent la quantité de données froides dans la vue Performances : Tous les volumes. La valeur de ce champ est « N/A » lorsque la version d' ONTAP ne prend pas en charge la création de rapports de données inactives.
- Politique de seuil : la ou les politiques de seuil de performances définies par l'utilisateur qui sont actives sur cet objet de stockage. Vous pouvez positionner votre curseur sur les noms de stratégie contenant des points de suspension (...) pour afficher le nom complet de la stratégie ou la liste des noms de stratégie attribués. Les boutons Affecter la politique de seuil de performance et Effacer la politique de seuil de performance restent désactivés jusqu'à ce que vous sélectionniez un ou plusieurs objets en cliquant sur les cases à cocher situées à l'extrême gauche. Consultez les liens suivants pour plus d'informations :
 - ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
 - ["Suppression des politiques de seuil de performance des objets de stockage"](#)

Performances : vue Tous les nœuds

La vue Performances : Tous les nœuds affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque nœud surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances de vos nœuds et de résoudre les problèmes de performances et les événements de seuil.



Flash Cache Reads renvoie le pourcentage d'opérations de lecture sur le nœud qui sont satisfaites par le cache, au lieu d'être renvoyées par le disque. Les données Flash Cache s'affichent uniquement pour les nœuds et uniquement lorsqu'un module Flash Cache est installé sur le nœud.

Dans le menu **Rapports**, l'option **Rapport d'inventaire matériel** est fournie lorsque Unified Manager et les clusters qu'il gère sont installés sur un site sans connectivité réseau externe. Ce bouton génère un fichier .csv contenant une liste complète des informations sur les clusters et les nœuds, telles que les numéros de modèle et de série du matériel, les types et nombres de disques, les licences installées, etc. Cette fonctionnalité de création de rapports est utile pour le renouvellement de contrat au sein de sites sécurisés qui ne sont pas connectés à la plateforme NetApp Active IQ. Vous pouvez attribuer des stratégies de seuil de performance ou effacer des stratégies de seuil de n'importe quel objet sur les pages d'inventaire d'objets à l'aide des boutons **Attribuer une stratégie de seuil de performance** et **Effacer la stratégie de seuil de performance**.

Consultez les liens suivants pour plus d'informations :

- ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
- ["Suppression des politiques de seuil de performance des objets de stockage"](#)
- ["Génération d'un rapport d'inventaire matériel pour le renouvellement du contrat"](#)

Performances : vue Toutes les machines virtuelles de stockage

La vue Performances : toutes les machines virtuelles de stockage affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque machine virtuelle de stockage (SVM) surveillée par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances de vos SVM et de résoudre les problèmes de performances et les événements de seuil. Le champ Latence de cette page indique le temps de réponse moyen pour toutes les demandes d'E/S, exprimé en millisecondes par opération.



Les SVM répertoriés sur cette page incluent uniquement les SVM de données et de cluster. Unified Manager n'utilise ni n'affiche les SVM d'administration ou de nœud.

Consultez les liens suivants pour plus d'informations :

- ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
- ["Suppression des politiques de seuil de performance des objets de stockage"](#)

Performances : vue de tous les LUN

La vue Performances : tous les LUN affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque LUN surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances de vos LUN et de résoudre les problèmes de performances et les événements de seuil.

Si vous souhaitez analyser la latence et le débit d'un objet spécifique, cliquez sur l'icône Plus , puis **Analyser la charge de travail** et vous pouvez afficher les graphiques de performances et de capacité sur la page

Analyse de la charge de travail.

Consultez les liens suivants pour plus d'informations :

- ["Surveillance des LUN dans une relation de groupe de cohérence"](#)
- ["Provisionnement des LUN"](#)
- ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
- ["Suppression des politiques de seuil de performance des objets de stockage"](#)
- ["Affichage des volumes ou des LUN qui se trouvent dans le même groupe de politiques QoS".](#)
- ["Affichage des paramètres du groupe de politiques QoS appliqués à des volumes ou LUN spécifiques"](#)
- ["Provisionnement des LUN à l'aide d'API"](#)

Performances : vue Tous les espaces de noms NVMe

La vue Performances : tous les espaces de noms NVMe affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque espace de noms NVMe surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances et la santé de vos espaces de noms, et de résoudre les problèmes et les événements de seuil.

Les informations suivantes, entre autres, sont rapportées : l'état actuel de l'espace de noms. * Hors ligne - L'accès en lecture ou en écriture à l'espace de noms n'est pas autorisé. * En ligne - L'accès en lecture et en écriture à l'espace de noms est autorisé. * NVFail - L'espace de noms a été automatiquement mis hors ligne en raison d'une défaillance de la NVRAM . * Erreur d'espace - L'espace de noms n'a plus d'espace.

Consultez les liens suivants pour plus d'informations :

- ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
- ["Suppression des politiques de seuil de performance des objets de stockage"](#)

Performances : vue Toutes les interfaces réseau

La vue Performances : toutes les interfaces réseau affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque interface réseau (LIF) surveillée par cette instance d'Unified Manager. Cette page vous permet de surveiller rapidement les performances de vos interfaces et de résoudre les problèmes de performances et les événements de seuil. Voici quelques champs importants dans la vue Performances : Toutes les interfaces réseau.

- IOPS : les opérations d'entrée/sortie par seconde. Les IOPS ne s'appliquent pas aux LIF NFS et CIFS et sont affichés comme N/A pour ces types.
- Latence : temps de réponse moyen pour toutes les requêtes d'E/S, exprimé en millisecondes par opération. La latence ne s'applique pas aux LIF NFS et CIFS et s'affiche comme N/A pour ces types.
- Emplacement d'origine : l'emplacement d'origine de l'interface, affiché sous la forme du nom du nœud et du nom du port, séparés par deux points (:). Si l'emplacement est affiché avec des points de suspension (...), vous pouvez positionner votre curseur sur le nom de l'emplacement pour afficher l'emplacement complet.
- Emplacement actuel : l'emplacement actuel de l'interface, affiché sous la forme du nom du nœud et du nom du port, séparés par deux points (:). Si l'emplacement est affiché avec des points de suspension (...), vous pouvez positionner votre curseur sur le nom de l'emplacement pour afficher l'emplacement complet.
- Rôle : Le rôle de l'interface : Données, Cluster, Gestion des nœuds ou Intercluster.



Les interfaces répertoriées sur cette page incluent les LIF de données, les LIF de cluster, les LIF de gestion de nœuds et les LIF interclusters. Unified Manager n'utilise ni n'affiche les LIF système.

Performances : vue Tous les ports

La vue Performances : Tous les ports affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque port surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances de vos ports et de résoudre les problèmes de performances et les événements de seuil. Pour un rôle de port, la fonction de port réseau est affichée, soit Données, soit Cluster. Les ports FCP ne peuvent pas avoir de rôle et le rôle est affiché comme N/A.



Les valeurs du compteur de performances sont affichées uniquement pour les ports physiques. Les valeurs de compteur ne sont pas affichées pour les VLAN ou les groupes d'interfaces.

Consultez les liens suivants pour plus d'informations :

- ["Attribution de politiques de seuil de performance aux objets de stockage"](#)
- ["Suppression des politiques de seuil de performance des objets de stockage"](#)

Performances : vue Groupes de politiques QoS

La vue Groupes de politiques QoS affiche les groupes de politiques QoS disponibles sur les clusters surveillés par Unified Manager. Cela inclut les politiques QoS traditionnelles, les politiques QoS adaptatives et les politiques QoS attribuées à l'aide des niveaux de service de performances.

Voici quelques champs importants dans la vue Performances : Groupes de stratégies QoS.

- **Groupe de politiques QoS** : le nom du groupe de politiques QoS. Pour les stratégies NetApp Service Level Manager (NSLM) 1.3 qui ont été importées dans Unified Manager 9.7 ou version ultérieure, le nom affiché ici inclut le nom SVM et d'autres informations qui ne figurent pas dans le nom lorsque le niveau de service de performances a été défini dans NSLM. Par exemple, le nom « NSLM_vs6_Performance_2_0 » signifie qu'il s'agit de la stratégie PSL « Performance » définie par le système NSLM créée sur SVM « vs6 » avec une latence attendue de « 2 ms/op ».
- **SVM** : la machine virtuelle de stockage (SVM) à laquelle appartient le groupe de politiques QoS. Vous pouvez cliquer sur le nom de la machine virtuelle de stockage pour accéder à la page de détails de cette machine virtuelle de stockage. Notez que ce champ est vide si la politique QoS a été créée sur la machine virtuelle de stockage d'administration, car ce type de machine virtuelle de stockage représente le cluster.
- **Débit minimal** : le débit minimal, en IOPS, que le groupe de politiques sera assuré de fournir. Pour les stratégies adaptatives, il s'agit du nombre minimum d'E/S par seconde attendu par To alloué au volume ou au LUN, en fonction de la taille allouée à l'objet de stockage.
- **Débit maximal** : débit, en IOPS et/ou Mo/s, que le groupe de politiques ne doit pas dépasser. Lorsque ce champ est vide, cela signifie que le maximum défini dans ONTAP est infini. Pour les stratégies adaptatives, il s'agit du nombre maximal (de pointe) d'E/S par seconde possible par To alloué au volume ou au LUN, en fonction de la taille allouée à l'objet de stockage ou de la taille utilisée de l'objet de stockage.
- **IOPS minimum absolu** : pour les stratégies adaptatives, il s'agit de la valeur IOPS minimum absolue utilisée comme remplacement lorsque les IOPS attendus sont inférieurs à cette valeur.
- **Taille du bloc** : la taille du bloc spécifiée pour la politique adaptative QoS.
- **Allocation minimale** : si « l'espace alloué » ou « l'espace utilisé » est utilisé pour déterminer le débit maximal (pic) IOPS.

- Latence attendue : la latence moyenne attendue pour les opérations d'entrée/sortie de stockage.
- Partagé : pour les stratégies QoS traditionnelles, indique si les valeurs de débit définies dans le groupe de stratégies sont partagées entre plusieurs objets.
- Objets associés : le nombre de charges de travail attribuées au groupe de politiques QoS. Vous pouvez cliquer sur le bouton développer (▼) à côté du nom du groupe de politiques QoS pour afficher plus de détails sur le groupe de politiques.
- Capacité allouée : la quantité d'espace actuellement utilisée par les objets du groupe de politiques QoS.
- Objets associés : le nombre de charges de travail attribuées au groupe de stratégies QoS, séparées en volumes et en LUN. Vous pouvez cliquer sur le numéro pour accéder à une page qui fournit plus de détails sur les volumes ou LUN sélectionnés.

Pour plus d'informations, consultez les rubriques sous "[Gestion des performances à l'aide des informations du groupe de stratégies QoS](#)".

Contenu de la page d'inventaire des performances de raffinement

Les pages d'inventaire des objets de performance contiennent des outils pour vous aider à affiner le contenu des données d'inventaire des objets, vous permettant de localiser des données spécifiques rapidement et facilement.

Les informations contenues dans les pages d'inventaire des objets de performance peuvent être volumineuses et s'étendre souvent sur plusieurs pages. Ce type de données complètes est excellent pour surveiller, suivre et améliorer les performances ; cependant, la localisation de données spécifiques nécessite des outils pour vous permettre de localiser rapidement les données que vous recherchez. Par conséquent, les pages d'inventaire des objets Performance contiennent des fonctionnalités de recherche, de tri et de filtrage. De plus, la recherche et le filtrage peuvent fonctionner ensemble pour affiner davantage vos résultats.

Rechercher sur les pages de performances de l'inventaire des objets

Vous pouvez rechercher des chaînes sur les pages de performances de l'inventaire des objets. Utilisez le champ **Rechercher** situé en haut à droite de la page pour localiser rapidement des données en fonction du nom de l'objet ou du nom de la politique. Cela vous permet de localiser rapidement des objets spécifiques et leurs données associées, ou de localiser rapidement des politiques et d'afficher les données d'objet de politique associées.

Étape

1. Effectuez l'une des options suivantes, en fonction de vos besoins de recherche :

Pour localiser ceci...	Tapez ceci...
Un objet spécifique	Saisissez le nom de l'objet dans le champ Rechercher et cliquez sur Rechercher . L'objet que vous avez recherché et ses données associées s'affichent.

Pour localiser ceci...	Tapez ceci...
Une politique de seuil de performance définie par l'utilisateur	Saisissez tout ou partie du nom de la politique dans le champ Rechercher , puis cliquez sur Rechercher . Les objets affectés à la politique que vous avez recherchée sont affichés.

Trier sur les pages Performances de l'inventaire des objets

Vous pouvez trier toutes les données des pages Performances de l'inventaire des objets par n'importe quelle colonne, par ordre croissant ou décroissant. Cela vous permet de localiser rapidement les données d'inventaire des objets, ce qui est utile lors de l'examen des performances ou du démarrage d'un processus de dépannage.

La colonne sélectionnée pour le tri est indiquée par un nom d'en-tête de colonne en surbrillance et une icône de flèche indiquant le sens de tri à droite du nom. Une flèche vers le haut indique l'ordre croissant ; une flèche vers le bas indique l'ordre décroissant. L'ordre de tri par défaut est par **Statut** (criticité de l'événement) par ordre décroissant, les événements de performances les plus critiques étant répertoriés en premier.

Étape

1. Vous pouvez cliquer sur le nom d'une colonne pour basculer l'ordre de tri de la colonne par ordre croissant ou décroissant.

Le contenu de la page Performances de l'inventaire des objets est trié par ordre croissant ou décroissant, en fonction de la colonne sélectionnée.

Filtrer les données dans les pages Performances de l'inventaire des objets

Vous pouvez filtrer les données dans les pages Performances de l'inventaire des objets pour localiser rapidement les données en fonction de critères spécifiques. Vous pouvez utiliser le filtrage pour affiner le contenu des pages Performances de l'inventaire des objets afin d'afficher uniquement les résultats que vous avez spécifiés. Cela fournit une méthode très efficace pour afficher uniquement les données de performances qui vous intéressent.

Vous pouvez utiliser le panneau Filtrage pour personnaliser la vue de la grille en fonction de vos préférences. Les options de filtre disponibles sont basées sur le type d'objet visualisé dans la grille. Si des filtres sont actuellement appliqués, le nombre de filtres appliqués s'affiche à droite du bouton Filtre.

Trois types de paramètres de filtre sont pris en charge.

Paramètre	Validation
Chaîne (texte)	Les opérateurs sont contient , commence par , se termine par et ne contient pas .
Nombre maximum	Les opérateurs sont supérieur à , inférieur à , dans le dernier et entre .

Paramètre	Validation
Enum (texte)	Les opérateurs sont is et is not .

Les champs Colonne, Opérateur et Valeur sont obligatoires pour chaque filtre ; les filtres disponibles reflètent les colonnes filtrables sur la page actuelle. Le nombre maximum de filtres que vous pouvez appliquer est de quatre. Les résultats filtrés sont basés sur des paramètres de filtre combinés. Les résultats filtrés s'appliquent à toutes les pages de votre recherche filtrée, pas seulement à la page actuellement affichée.

Vous pouvez ajouter des filtres à l'aide du panneau Filtrage.

1. En haut de la page, cliquez sur le bouton **Filtre**. Le panneau Filtrage s'affiche.
2. Cliquez sur la liste déroulante de gauche et sélectionnez un objet ; par exemple, *Cluster* ou un compteur de performances.
3. Cliquez sur la liste déroulante centrale et sélectionnez l'opérateur que vous souhaitez utiliser.
4. Dans la dernière liste, sélectionnez ou saisissez une valeur pour compléter le filtre pour cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Ajouter un filtre**. Un champ de filtre supplémentaire s'affiche. Complétez ce filtre en suivant le processus décrit dans les étapes précédentes. Notez qu'après avoir ajouté votre quatrième filtre, le bouton **+Ajouter un filtre** ne s'affiche plus.
6. Cliquez sur **Appliquer le filtre**. Les options de filtre sont appliquées à la grille et le nombre de filtres est affiché à droite du bouton Filtrer.
7. Utilisez le panneau Filtrage pour supprimer des filtres individuels en cliquant sur l'icône de la corbeille à droite du filtre à supprimer.
8. Pour supprimer tous les filtres, cliquez sur **Réinitialiser** en bas du panneau de filtrage.

Exemple de filtrage

L'illustration montre le panneau de filtrage avec trois filtres. Le bouton **+Ajouter un filtre** s'affiche lorsque vous avez moins que le maximum de quatre filtres.

The screenshot shows a filter panel with three active filters. Each filter consists of a column name, an operator, and a value. The first filter is 'MBps' with operator 'greater than' and value '5'. The second filter is 'Node' with operator 'name starts with' and value 'test'. The third filter is 'Type' with operator 'is' and value 'FCP Port'. To the right of each filter is a trash icon for removal. At the bottom left is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons.

Après avoir cliqué sur **Appliquer le filtre**, le panneau Filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Comprendre les recommandations d'Unified Manager pour hiérarchiser les données vers le cloud

La vue Performances : Tous les volumes affiche des informations relatives à la taille des

données utilisateur stockées sur le volume inactif (froid). Dans certains cas, Unified Manager identifie certains volumes qui bénéficieraient de la hiérarchisation des données inactives vers le niveau cloud (fournisseur de cloud ou StorageGRID) d'un agrégat compatible FabricPool.



FabricPool a été introduit dans ONTAP 9.2. Par conséquent, si vous utilisez une version du logiciel ONTAP antérieure à 9.2, la recommandation d'Unified Manager de hiérarchiser les données nécessite la mise à niveau de votre logiciel ONTAP. De plus, la **auto** La politique de hiérarchisation a été introduite dans ONTAP 9.4, et la **all** La politique de hiérarchisation a été introduite dans ONTAP 9.6. Par conséquent, si la recommandation consiste à utiliser la politique de hiérarchisation automatique, vous devez effectuer une mise à niveau vers ONTAP 9.4 ou une version supérieure.

Les trois champs suivants de la vue Performances : Tous les volumes fournissent des informations sur la possibilité d'améliorer l'utilisation du disque de votre système de stockage et d'économiser de l'espace sur le niveau de performances en déplaçant les données inactives vers le niveau cloud.

- **Politique de hiérarchisation**

La politique de hiérarchisation détermine si les données du volume restent sur le niveau de performance ou si certaines des données sont déplacées du niveau de performance vers le niveau cloud.

La valeur de ce champ indique la stratégie de hiérarchisation définie sur le volume, même si le volume ne réside pas actuellement sur un agrégat FabricPool. La politique de hiérarchisation prend effet uniquement lorsque le volume se trouve sur un agrégat FabricPool.

- **Données froides**

Les données froides affichent la taille des données utilisateur stockées sur le volume qui est inactif (froid).

Une valeur est affichée ici uniquement lors de l'utilisation du logiciel ONTAP 9.4 ou supérieur, car elle nécessite que l'agrégat sur lequel le volume est déployé possède le **inactive data reporting parameter** réglé sur **enabled**, et que le seuil minimum de jours de refroidissement a été atteint (pour les volumes qui utilisent le **snapshot-only** ou **auto** politique de hiérarchisation). Sinon, la valeur est répertoriée comme « N/A ».

- **Recommandation Cloud**

Une fois que suffisamment d'informations ont été capturées sur l'activité des données sur le volume, Unified Manager peut déterminer qu'aucune action n'est requise ou que vous pouvez économiser de l'espace sur le niveau de performance en hiérarchisant les données inactives vers le niveau cloud.



Le champ Données froides est mis à jour toutes les 15 minutes, mais le champ Recommandation Cloud est mis à jour tous les 7 jours lorsque l'analyse des données froides est effectuée sur le volume. Par conséquent, la quantité exacte de données froides peut différer selon les champs. Le champ Recommandation Cloud affiche la date à laquelle l'analyse a été exécutée.

Lorsque le rapport de données inactives est activé, le champ Données froides affiche la quantité exacte de données inactives. Sans la capacité de création de rapports sur les données inactives, Unified Manager utilise des statistiques de performances pour déterminer si les données sont inactives sur un volume. Dans ce cas, la quantité de données inactives n'est pas affichée dans le champ Données froides, mais elle s'affiche lorsque vous passez votre curseur sur le mot **Niveau** pour afficher la recommandation cloud.

Les recommandations cloud que vous verrez sont :

- **Apprentissage.** Les données collectées ne sont pas suffisantes pour formuler une recommandation.
- **Étage.** L'analyse a déterminé que le volume contient des données inactives (froides) et que vous devez configurer le volume pour déplacer ces données vers le niveau cloud. Dans certains cas, cela peut nécessiter que vous déplaciez d'abord le volume vers un agrégat compatible FabricPool. Dans d'autres cas où le volume est déjà sur un agrégat FabricPool, il vous suffit de modifier la politique de hiérarchisation.
- **Aucune action.** Soit le volume contient très peu de données inactives, soit le volume est déjà défini sur la stratégie de hiérarchisation « auto » sur un agrégat FabricPool, soit le volume est un volume de protection des données. Cette valeur s'affiche également lorsque le volume est hors ligne ou lorsqu'il est utilisé dans une configuration MetroCluster.

Pour déplacer un volume, ou pour modifier la stratégie de hiérarchisation des volumes ou les paramètres de rapport de données inactives agrégées, utilisez ONTAP System Manager, les commandes ONTAP CLI ou une combinaison de ces outils.

Si vous êtes connecté à Unified Manager avec le rôle d'administrateur d'application ou d'administrateur de stockage, le lien **Configurer le volume** est disponible dans la recommandation cloud lorsque vous passez votre curseur sur le mot **Niveau**. Cliquez sur ce bouton pour ouvrir la page Volumes dans le Gestionnaire système afin d'effectuer la modification recommandée.

Surveiller les performances à l'aide des pages de l'Explorateur de performances

Les pages de l'Explorateur de performances affichent des informations détaillées sur les performances de chaque objet d'un cluster. La page fournit une vue détaillée des performances de tous les objets du cluster, vous permettant de sélectionner et de comparer les données de performances d'objets spécifiques sur différentes périodes.

Vous pouvez également évaluer les performances globales de tous les objets et comparer les données de performances des objets dans un format côte à côte.

Comprendre l'objet racine

L'objet racine est la ligne de base par rapport à laquelle d'autres comparaisons d'objets sont effectuées. Cela vous permet d'afficher et de comparer les données d'autres objets à l'objet racine, fournissant une analyse des données de performances qui vous aide à dépanner et à améliorer les performances de l'objet.

Le nom de l'objet racine s'affiche en haut du volet de comparaison. Des objets supplémentaires s'affichent sous l'objet racine. Bien qu'il n'y ait aucune limite au nombre d'objets supplémentaires que vous pouvez ajouter au volet de comparaison, un seul objet racine est autorisé. Les données de l'objet racine s'affichent automatiquement dans les graphiques du volet Graphiques de compteur.

Vous ne pouvez pas modifier l'objet racine ; il est toujours défini sur la page d'objet que vous consultez. Par exemple, si vous ouvrez la page Volume Performance Explorer de Volume1, Volume1 est l'objet racine et ne peut pas être modifié. Si vous souhaitez comparer avec un autre objet racine, vous devez cliquer sur le lien d'un objet et ouvrir sa page de destination.



Les événements et les seuils sont affichés uniquement pour les objets racine.

Appliquer un filtrage pour réduire la liste des objets corrélés dans la grille

Le filtrage vous permet d'afficher un sous-ensemble d'objets plus petit et mieux défini dans la grille. Par exemple, si vous avez 25 volumes dans la grille, le filtrage vous permet d'afficher uniquement les volumes dont le débit est inférieur à 90 Mbit/s ou la latence supérieure à 1 ms/op.

Spécifier une plage de temps pour les objets corrélés

Le sélecteur de plage horaire sur la page Explorateur de performances vous permet de spécifier la plage horaire pour la comparaison des données d'objet. La spécification d'une plage horaire affine le contenu des pages de l'Explorateur de performances pour afficher uniquement les données d'objet dans la plage horaire que vous avez spécifiée.

L'affinement de la plage temporelle fournit une méthode efficace pour afficher uniquement les données de performances qui vous intéressent. Vous pouvez sélectionner une plage horaire prédéfinie ou spécifier une plage horaire personnalisée. La plage horaire par défaut correspond aux 72 heures précédentes.

Sélectionnez une plage horaire prédéfinie

La sélection d'une plage horaire prédéfinie est un moyen rapide et efficace de personnaliser et de concentrer la sortie des données lors de l'affichage des données de performances des objets de cluster. Lors de la sélection d'une plage horaire prédéfinie, des données allant jusqu'à 13 mois sont disponibles.

Étapes

1. En haut à droite de la page **Performance Explorer**, cliquez sur **Plage de temps**.
2. Sur le côté droit du panneau **Sélection de plage horaire**, sélectionnez une plage horaire prédéfinie.
3. Cliquez sur **Appliquer la plage**.

Spécifier une plage horaire personnalisée

La page Explorateur de performances vous permet de spécifier la plage de dates et d'heures pour vos données de performances. La spécification d'une plage horaire personnalisée offre une plus grande flexibilité que l'utilisation de plages horaires prédéfinies lors de l'affinage des données d'objets de cluster.

Vous pouvez sélectionner une plage horaire comprise entre une heure et 390 jours. 13 mois équivalent à 390 jours car chaque mois est compté comme 30 jours. La spécification d'une plage de dates et d'heures fournit plus de détails et vous permet de zoomer sur des événements de performance spécifiques ou sur une série d'événements. La spécification d'une plage horaire permet également de résoudre les problèmes de performances potentiels, car la spécification d'une plage de dates et d'heures affiche les données entourant l'événement de performances de manière plus détaillée. Utilisez le contrôle **Plage de temps** pour sélectionner des plages de dates et d'heures prédéfinies, ou spécifiez votre propre plage de dates et d'heures personnalisée allant jusqu'à 390 jours. Les boutons pour les plages de temps prédéfinies varient de la **Dernière heure** aux **13 derniers mois**.

La sélection de l'option **13 derniers mois** ou la spécification d'une plage de dates personnalisée supérieure à 30 jours affiche une boîte de dialogue vous avertissant que les données de performances affichées pour une période supérieure à 30 jours sont représentées sous forme de graphiques à l'aide de moyennes horaires et non d'un interrogation de données de 5 minutes. Par conséquent, une perte de granularité visuelle de la chronologie peut se produire. Si vous cliquez sur l'option **Ne plus afficher** dans la boîte de dialogue, le message n'apparaît pas lorsque vous sélectionnez l'option **13 derniers mois** ou spécifiez une plage de dates personnalisée supérieure à 30 jours. Les données récapitulatives s'appliquent également à une plage horaire plus petite, si la plage horaire comprend une heure/date située à plus de 30 jours d'aujourd'hui.

Lors de la sélection d'une plage horaire (personnalisée ou prédéfinie), les plages horaires de 30 jours ou moins sont basées sur des échantillons de données d'intervalle de 5 minutes. Les plages de temps supérieures à 30 jours sont basées sur des échantillons de données d'intervalle d'une heure.

1. Cliquez sur la liste déroulante **Plage de temps** et le panneau Plage de temps s'affiche.
2. Pour sélectionner une plage horaire prédéfinie, cliquez sur l'un des boutons **Dernier...** à droite du panneau **Plage horaire**. Lors de la sélection d'une plage horaire prédéfinie, des données allant jusqu'à 13 mois sont disponibles. Le bouton de plage horaire prédéfini que vous avez sélectionné est mis en surbrillance et les jours et heures correspondants s'affichent dans les calendriers et les sélecteurs d'heure.
3. Pour sélectionner une plage de dates personnalisée, cliquez sur la date de début dans le calendrier **De** sur la gauche. Cliquez sur < ou > pour naviguer vers l'avant ou vers l'arrière dans le calendrier. Pour spécifier la date de fin, cliquez sur une date dans le calendrier **À** sur la droite. Notez que la date de fin par défaut est aujourd'hui, sauf si vous spécifiez une date de fin différente. Le bouton **Plage personnalisée** à droite du panneau Plage de temps est mis en surbrillance, indiquant que vous avez sélectionné une plage de dates personnalisée.
4. Pour sélectionner une plage horaire personnalisée, cliquez sur le contrôle **Heure** sous le calendrier **De** et sélectionnez l'heure de début. Pour spécifier l'heure de fin, cliquez sur le contrôle **Heure** sous le calendrier **À** à droite et sélectionnez l'heure de fin. Le bouton **Plage personnalisée** à droite du panneau Plage horaire est mis en surbrillance, indiquant que vous avez sélectionné une plage horaire personnalisée.
5. En option, vous pouvez spécifier les heures de début et de fin lors de la sélection d'une plage de dates prédéfinie. Sélectionnez la plage de dates prédéfinie comme décrit précédemment, puis sélectionnez les heures de début et de fin comme décrit précédemment. Les dates sélectionnées sont mises en surbrillance dans les calendriers, vos heures de début et de fin spécifiées s'affichent dans les commandes **Heure** et le bouton **Plage personnalisée** est mis en surbrillance.
6. Après avoir sélectionné la plage de dates et d'heures, cliquez sur **Appliquer la plage**. Les statistiques de performance pour cette période s'affichent dans les graphiques et dans la chronologie des événements.

Définir la liste des objets corrélés pour la comparaison graphique

Vous pouvez définir une liste d'objets corrélés pour la comparaison des données et des performances dans le volet Graphique de compteur. Par exemple, si votre machine virtuelle de stockage (SVM) rencontre un problème de performances, vous pouvez comparer tous les volumes de la SVM pour identifier le volume susceptible d'être à l'origine du problème.

Vous pouvez ajouter n'importe quel objet de la grille d'objets corrélés aux volets Graphique de comparaison et de compteur. Cela vous permet de visualiser et de comparer les données de plusieurs objets et avec l'objet racine. Vous pouvez ajouter et supprimer des objets dans la grille d'objets corrélés ; toutefois, l'objet racine dans le volet Comparaison n'est pas amovible.



L'ajout de nombreux objets au volet de comparaison peut avoir un impact négatif sur les performances. Pour maintenir les performances, vous devez sélectionner un nombre limité de graphiques pour la comparaison des données.

Étapes

1. Dans la grille d'objets, recherchez l'objet que vous souhaitez ajouter et cliquez sur le bouton **Ajouter**.

Le bouton **Ajouter** devient gris et l'objet est ajouté à la liste des objets supplémentaires dans le volet Comparaison. Les données de l'objet sont ajoutées aux graphiques dans les volets Graphiques de compteur. La couleur de l'icône en forme d'œil de l'objet () correspond à la couleur de la ligne de tendance des données de l'objet dans les graphiques.

2. **Facultatif** : Masquer ou afficher les données des objets sélectionnés :

Pour faire cela...	Prenez cette mesure...
Masquer un objet sélectionné	Cliquez sur l'icône en forme d'œil de l'objet sélectionné () dans le volet de comparaison. Les données de l'objet sont masquées et l'icône en forme d'œil de cet objet devient grise.
Afficher un objet caché	Cliquez sur l'icône en forme d'œil gris de l'objet sélectionné dans le volet Comparaison. L'icône en forme d'œil revient à sa couleur d'origine et les données de l'objet sont réajoutées aux graphiques du volet Graphiques de compteur.

3. **Facultatif** : Supprimez les objets sélectionnés du volet **Comparaison** :

Pour faire cela...	Prenez cette mesure...
Supprimer un objet sélectionné	Passez la souris sur le nom de l'objet sélectionné dans le volet Comparaison pour afficher le bouton Supprimer l'objet (X), puis cliquez sur le bouton. L'objet est supprimé du volet de comparaison et ses données sont effacées des graphiques de compteurs.

Pour faire cela...	Prenez cette mesure...
Supprimer tous les objets sélectionnés	Cliquez sur le bouton Supprimer tous les objets (X) en haut du volet de comparaison. Tous les objets sélectionnés et leurs données sont supprimés, ne laissant que l'objet racine.

Comprendre les graphiques de compteurs

Les graphiques du volet Graphiques de compteur vous permettent d'afficher et de comparer les données de performances de l'objet racine et des objets que vous avez ajoutés à partir de la grille des objets corrélés. Cela peut vous aider à comprendre les tendances de performances et à isoler et résoudre les problèmes de performances.

Les graphiques de compteurs affichés par défaut sont les événements, la latence, les IOPS et les MBps. Les graphiques facultatifs que vous pouvez choisir d'afficher sont l'utilisation, la capacité de performance utilisée, les IOPS disponibles, les IOPS/To et le ratio d'échec de cache. De plus, vous pouvez choisir d'afficher les valeurs totales ou les valeurs de répartition pour les graphiques Latence, IOPS, Mbit/s et Capacité de performances utilisée.

L'Explorateur de performances affiche certains graphiques de compteurs par défaut, que l'objet de stockage les prenne tous en charge ou non. Lorsqu'un compteur n'est pas pris en charge, le graphique du compteur est vide et le message `Not applicable for <object>` est affiché.

Les graphiques affichent les tendances de performances pour l'objet racine et pour tous les objets que vous avez sélectionnés dans le volet Comparaison. Les données de chaque graphique sont organisées comme suit :

- **Axe X**

Affiche la période spécifiée. Si vous n'avez pas spécifié de plage horaire, la valeur par défaut est la période de 72 heures précédente.

- **Axe Y**

Affiche les unités de compteur propres à l'objet ou aux objets sélectionnés.

Les couleurs de la ligne de tendance correspondent à la couleur du nom de l'objet tel qu'il est affiché dans le volet de comparaison. Vous pouvez positionner votre curseur sur un point de n'importe quelle ligne de tendance pour afficher les détails du temps et de la valeur de ce point.

Si vous souhaitez étudier une période de temps spécifique dans un graphique, vous pouvez utiliser l'une des méthodes suivantes :

- Utilisez le bouton < pour développer le volet Graphiques de compteur afin qu'il couvre toute la largeur de la page.
- Utilisez le curseur (lorsqu'il se transforme en loupe) pour sélectionner une partie de la période dans le graphique afin de vous concentrer et d'agrandir cette zone. Vous pouvez cliquer sur Réinitialiser le zoom du graphique pour ramener le graphique à la période par défaut.
- Utilisez le bouton **Zoom View** pour afficher un grand graphique à compteur unique contenant des détails développés et des indicateurs de seuil.



Parfois, des écarts dans les lignes de tendance apparaissent. Les écarts signifient que Unified Manager n'a pas réussi à collecter les données de performances du système de stockage ou qu'Unified Manager était peut-être en panne.

Types de graphiques de compteurs de performances

Il existe des graphiques de performances standard qui affichent les valeurs de compteur pour l'objet de stockage sélectionné. Chacun des graphiques de compteurs de panne affiche les valeurs totales séparées en catégories de lecture, d'écriture et autres. De plus, certains graphiques de compteurs de pannes affichent des détails supplémentaires lorsque le graphique est affiché en vue Zoom.

Le tableau suivant présente les graphiques de compteurs de performances disponibles.

Cartes disponibles	Description du graphique
Événements	Affiche les événements critiques, d'erreur, d'avertissement et d'information en corrélation avec les graphiques statistiques de l'objet racine. Les événements de santé s'affichent en plus des événements de performance pour fournir une image complète des raisons pour lesquelles les performances peuvent être affectées.
Latence - Total	Nombre de millisecondes nécessaires pour répondre aux requêtes de l'application. Notez que les valeurs de latence moyennes sont pondérées en fonction des E/S.
Latence - Décomposition	Les mêmes informations sont affichées dans Latence totale, mais avec les données de performances séparées en lecture, écriture et autre latence. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, un LUN ou un espace de noms.
Latence - Composants du cluster	Les mêmes informations sont affichées dans Latence totale, mais avec les données de performances séparées en latence par composant de cluster. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un volume.
IOPS - Total	Nombre d'opérations d'entrée/sortie traitées par seconde. Lorsqu'il est affiché pour un nœud, la sélection de « Total » affiche les IOPS pour les données circulant via ce nœud qui peuvent résider sur le nœud local ou distant, et la sélection de « Total (local) » affiche les IOPS pour les données qui résident uniquement sur le nœud actuel.

Cartes disponibles	Description du graphique
IOPS - Répartition	Les mêmes informations sont affichées dans le total des IOPS, mais avec les données de performances séparées en lecture, écriture et autres IOPS. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, un LUN ou un espace de noms. Lorsqu'il est affiché dans la vue Zoom, le graphique des volumes affiche les valeurs de débit minimales et maximales de QoS, si elles sont configurées dans ONTAP. Lorsqu'il est affiché pour un nœud, la sélection de « Répartition » affiche la répartition des IOPS pour les données circulant via ce nœud qui peuvent résider sur le nœud local ou distant, et la sélection de « Répartition (local) » affiche la répartition des IOPS pour les données qui résident uniquement sur le nœud actuel.
IOPS - Protocoles	Les mêmes informations sont affichées dans le total des IOPS, mais les données de performances sont séparées en graphiques individuels pour le trafic des protocoles CIFS, NFS, FCP, NVMe et iSCSI. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM.
IOPS/To - Total	Nombre d'opérations d'entrée/sortie traitées par seconde en fonction de l'espace total consommé par la charge de travail, en téraoctets. Également appelé densité d'E/S, ce compteur mesure les performances pouvant être fournies par une quantité donnée de capacité de stockage. Lorsqu'il est affiché dans la vue Zoom, le graphique des volumes affiche les valeurs de débit de pointe et de qualité de service attendues, si elles sont configurées dans ONTAP. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un volume.
Mo/s - Total	Nombre de mégaoctets de données transférés vers et depuis l'objet par seconde.

Cartes disponibles	Description du graphique
MB/s - Décomposition	Les mêmes informations sont affichées dans le graphique Mo/s, mais avec les données de débit séparées en lectures de disque, lectures de cache Flash, écritures et autres. Lorsqu'il est affiché dans la vue Zoom, le graphique des volumes affiche les valeurs de débit maximal QoS, si elles sont configurées dans ONTAP. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, un LUN ou un espace de noms.  Les données Flash Cache s'affichent uniquement pour les nœuds et uniquement lorsqu'un module Flash Cache est installé sur le nœud.
Capacité de performance utilisée - Total	Pourcentage de capacité de performance consommée par le nœud ou l'agrégat.
Capacité de performance utilisée - Répartition	Capacité de performance Données utilisées séparées en protocoles utilisateur et processus d'arrière-plan du système. De plus, la quantité de capacité de performance libre est affichée.
IOPS disponibles - Total	Nombre d'opérations d'entrée/sortie par seconde actuellement disponibles (gratuites) sur cet objet. Ce nombre est le résultat de la soustraction des IOPS actuellement utilisées du nombre total d'IOPS que Unified Manager calcule que l'objet peut effectuer. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un nœud ou un agrégat.
Utilisation - Total	Pourcentage de ressources disponibles de l'objet en cours d'utilisation. L'utilisation indique l'utilisation des nœuds pour les nœuds, l'utilisation du disque pour les agrégats et l'utilisation de la bande passante pour les ports. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un nœud, un agrégat ou un port.
Taux d'échec du cache - Total	Pourcentage de demandes de lecture provenant d'applications clientes qui sont renvoyées depuis le disque au lieu d'être renvoyées depuis le cache. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un volume.

Sélectionnez les graphiques de performances à afficher

La liste déroulante Choisir les graphiques vous permet de sélectionner les types de graphiques de compteurs de performances à afficher dans le volet Graphiques de compteurs. Cela vous permet d'afficher des données et des compteurs spécifiques, en fonction de vos besoins en performances.

Étapes

1. Dans le volet **Graphiques de compteur**, cliquez sur la liste déroulante **Choisir des graphiques**.
2. Ajouter ou supprimer des graphiques :

À...	Fais ceci...
Ajouter ou supprimer des graphiques individuels	Cochez les cases à côté des graphiques que vous souhaitez afficher ou masquer
Ajouter tous les graphiques	Cliquez sur Sélectionner tout
Supprimer tous les graphiques	Cliquez sur Désélectionner tout

Vos sélections de graphiques sont affichées dans le volet Graphiques de compteur. Notez qu'à mesure que vous ajoutez des graphiques, les nouveaux graphiques sont insérés dans le volet Graphiques de compteur pour correspondre à l'ordre des graphiques répertoriés dans la liste déroulante Choisir les graphiques. La sélection de graphiques supplémentaires peut nécessiter un défilement supplémentaire.

Développer le volet Graphiques de compteur

Vous pouvez développer le volet Graphiques de compteur afin que les graphiques soient plus grands et plus lisibles.

Après avoir défini les objets de comparaison et la plage de temps des compteurs, vous pouvez afficher un volet Graphiques de compteurs plus grand. Vous utilisez le bouton < au milieu de la fenêtre Performance Explorer pour développer le volet.

Étape

1. Développez ou réduisez le volet **Graphiques de compteur**.

À...	Fais ceci...
Développez le volet Graphiques de compteur pour l'adapter à la largeur de la page	Cliquez sur le bouton <
Réduisez le volet des graphiques de compteurs à la moitié droite de la page	Cliquez sur le bouton >

Modifiez la focalisation des graphiques de compteur sur une période de temps plus courte

Vous pouvez utiliser votre souris pour réduire la plage de temps afin de vous concentrer sur une période de temps spécifique dans le volet Graphique du compteur ou dans la fenêtre Zoom des graphiques du compteur. Cela vous permet d'avoir une vue plus granulaire et microscopique de n'importe quelle partie de la chronologie des données de performance, des événements et des seuils.

Avant de commencer

Le curseur doit s'être transformé en loupe pour indiquer que cette fonctionnalité est active.



Lorsque vous utilisez cette fonctionnalité, qui modifie la chronologie pour afficher des valeurs correspondant à l'affichage plus granulaire, la plage de date et d'heure sur le sélecteur **Plage de temps** ne change pas par rapport aux valeurs d'origine du graphique.

Étapes

1. Pour zoomer sur une période de temps spécifique, cliquez à l'aide de la loupe et faites glisser la souris pour mettre en surbrillance la zone que vous souhaitez voir en détail.

Les valeurs du compteur pour la période que vous sélectionnez remplissent le graphique du compteur.

2. Pour revenir à la période de temps d'origine définie dans le sélecteur **Plage de temps**, cliquez sur le bouton **Réinitialiser le zoom du graphique**.

Le graphique du compteur s'affiche dans son état d'origine.

Afficher les détails de l'événement dans la chronologie des événements

Vous pouvez afficher tous les événements et leurs détails associés dans le volet Chronologie des événements de Performance Explorer. Il s'agit d'une méthode rapide et efficace permettant d'afficher tous les événements de santé et de performances qui se sont produits sur l'objet racine pendant une période spécifiée, ce qui peut être utile lors du dépannage des problèmes de performances.

Le volet Chronologie des événements affiche les événements critiques, d'erreur, d'avertissement et d'information qui se sont produits sur l'objet racine pendant la plage horaire sélectionnée. Chaque gravité d'événement a sa propre chronologie. Les événements uniques et multiples sont représentés par un point d'événement sur la chronologie. Vous pouvez positionner votre curseur sur un point d'événement pour voir les détails de l'événement. Pour augmenter la granularité visuelle de plusieurs événements, vous pouvez réduire la plage horaire. Cela répartit plusieurs événements en événements uniques, vous permettant de visualiser et d'étudier séparément chaque événement.

Chaque point d'événement de performance sur la chronologie des événements s'aligne verticalement avec un pic correspondant dans les lignes de tendance des graphiques de compteurs qui sont affichées sous la chronologie des événements. Cela fournit une corrélation visuelle directe entre les événements et les performances globales. Les événements de santé sont également affichés sur la chronologie, mais ces types d'événements ne correspondent pas nécessairement à un pic dans l'un des graphiques de performances.

Étapes

1. Dans le volet **Chronologie des événements**, placez le curseur sur un point d'événement sur une chronologie pour afficher un résumé de l'événement ou des événements à ce point d'événement.

Une boîte de dialogue contextuelle affiche des informations sur les types d'événements, la date et l'heure auxquelles les événements se sont produits, l'état et la durée de l'événement.

2. Afficher les détails complets de l'événement pour un ou plusieurs événements :

Pour faire cela...	Cliquez ici...
Afficher les détails d'un événement unique	Afficher les détails de l'événement dans la boîte de dialogue contextuelle.
Afficher les détails de plusieurs événements	Afficher les détails de l'événement dans la boîte de dialogue contextuelle.  Cliquer sur un seul événement dans la boîte de dialogue d'événements multiples affiche la page Détails de l'événement appropriée.

Graphiques de compteurs Vue zoom

Les graphiques de compteurs fournissent une vue zoom qui vous permet de zoomer sur les détails des performances sur la période spécifiée. Cela vous permet de voir les détails des performances et les événements avec une granularité beaucoup plus élevée, ce qui est bénéfique lors du dépannage des problèmes de performances.

Lorsqu'ils sont affichés en mode Zoom, certains graphiques de répartition fournissent des informations supplémentaires par rapport à celles qui s'affichent lorsque le graphique n'est pas en mode Zoom. Par exemple, les pages Zoom du graphique de répartition IOPS, IOPS/To et MBps affichent les valeurs de stratégie QoS pour les volumes et les LUN si elles ont été définies dans ONTAP.



Pour les stratégies de seuil de performances définies par le système, seules les stratégies « Ressources de nœud surutilisées » et « Limite de débit QoS dépassée » sont disponibles dans la liste **Stratégies**. Les autres politiques de seuil définies par le système ne sont pas disponibles pour le moment.

Afficher la vue Zoom des graphiques de compteur

La vue Zoom des graphiques de compteur fournit un niveau de détail plus fin pour le graphique de compteur sélectionné et sa chronologie associée. Cela agrandit les données du graphique du compteur, vous permettant d'avoir une vue plus précise des événements de performance et de leurs causes sous-jacentes.

Vous pouvez afficher la vue Zoom des graphiques de compteur pour n'importe quel graphique de compteur.

Étapes

1. Cliquez sur **Zoom View** pour ouvrir le graphique sélectionné dans une nouvelle fenêtre de navigateur.

2. Si vous visualisez un graphique de répartition, puis cliquez sur **Vue Zoom**, le graphique de répartition s'affiche en vue Zoom. Vous pouvez sélectionner **Total** en mode Zoom si vous souhaitez modifier l'option d'affichage.

Spécifiez la plage horaire dans la vue Zoom

Le contrôle **Plage de temps** dans la fenêtre Zoom des graphiques de compteur vous permet de spécifier une plage de dates et d'heures pour le graphique sélectionné. Cela vous permet de localiser rapidement des données spécifiques en fonction d'une plage horaire prédéfinie ou de votre propre plage horaire personnalisée.

Vous pouvez sélectionner une plage horaire comprise entre une heure et 390 jours. 13 mois équivalent à 390 jours car chaque mois est compté comme 30 jours. La spécification d'une plage de dates et d'heures fournit plus de détails et vous permet de zoomer sur des événements de performance spécifiques ou sur une série d'événements. La spécification d'une plage horaire permet également de résoudre les problèmes de performances potentiels, car la spécification d'une plage de dates et d'heures affiche les données entourant l'événement de performances de manière plus détaillée. Utilisez le contrôle **Plage de temps** pour sélectionner des plages de dates et d'heures prédéfinies, ou spécifiez votre propre plage de dates et d'heures personnalisée allant jusqu'à 390 jours. Les boutons pour les plages de temps prédéfinies varient de la **Dernière heure** aux **13 derniers mois**.

La sélection de l'option **13 derniers mois** ou la spécification d'une plage de dates personnalisée supérieure à 30 jours affiche une boîte de dialogue vous avertissant que les données de performances affichées pour une période supérieure à 30 jours sont représentées sous forme de graphiques à l'aide de moyennes horaires et non d'un interrogation de données de 5 minutes. Par conséquent, une perte de granularité visuelle de la chronologie peut se produire. Si vous cliquez sur l'option **Ne plus afficher** dans la boîte de dialogue, le message n'apparaît pas lorsque vous sélectionnez l'option **13 derniers mois** ou spécifiez une plage de dates personnalisée supérieure à 30 jours. Les données récapitulatives s'appliquent également à une plage horaire plus petite, si la plage horaire comprend une heure/date située à plus de 30 jours d'aujourd'hui.

Lors de la sélection d'une plage horaire (personnalisée ou prédéfinie), les plages horaires de 30 jours ou moins sont basées sur des échantillons de données d'intervalle de 5 minutes. Les plages de temps supérieures à 30 jours sont basées sur des échantillons de données d'intervalle d'une heure.

The screenshot shows a 'Plage de temps' (Time Range) dialog box. It features two calendar views for April 2015. The 'From' calendar has the 12th selected, and the 'To' calendar has the 15th selected. Below the calendars are time dropdowns set to 6:00 am. To the right is a list of predefined time ranges: Last Hour, Last 24 Hours, Last 72 Hours, Last 7 Days, Last 30 Days, Last 13 Months, and Custom Range. The 'Last 72 Hours' option is highlighted. At the bottom right are 'Cancel' and 'Apply Range' buttons.

1. Cliquez sur la liste déroulante **Plage de temps** et le panneau Plage de temps s'affiche.
2. Pour sélectionner une plage horaire prédéfinie, cliquez sur l'un des boutons **Dernier...** à droite du panneau **Plage horaire**. Lors de la sélection d'une plage horaire prédéfinie, des données allant jusqu'à 13 mois sont disponibles. Le bouton de plage horaire prédéfini que vous avez sélectionné est mis en surbrillance et les

jours et heures correspondants s'affichent dans les calendriers et les sélecteurs d'heure.

3. Pour sélectionner une plage de dates personnalisée, cliquez sur la date de début dans le calendrier **De** sur la gauche. Cliquez sur < ou > pour naviguer vers l'avant ou vers l'arrière dans le calendrier. Pour spécifier la date de fin, cliquez sur une date dans le calendrier **À** sur la droite. Notez que la date de fin par défaut est aujourd'hui, sauf si vous spécifiez une date de fin différente. Le bouton **Plage personnalisée** à droite du panneau Plage de temps est mis en surbrillance, indiquant que vous avez sélectionné une plage de dates personnalisée.
4. Pour sélectionner une plage horaire personnalisée, cliquez sur le contrôle **Heure** sous le calendrier **De** et sélectionnez l'heure de début. Pour spécifier l'heure de fin, cliquez sur le contrôle **Heure** sous le calendrier **À** à droite et sélectionnez l'heure de fin. Le bouton **Plage personnalisée** à droite du panneau Plage horaire est mis en surbrillance, indiquant que vous avez sélectionné une plage horaire personnalisée.
5. En option, vous pouvez spécifier les heures de début et de fin lors de la sélection d'une plage de dates prédéfinie. Sélectionnez la plage de dates prédéfinie comme décrit précédemment, puis sélectionnez les heures de début et de fin comme décrit précédemment. Les dates sélectionnées sont mises en surbrillance dans les calendriers, vos heures de début et de fin spécifiées s'affichent dans les commandes **Heure** et le bouton **Plage personnalisée** est mis en surbrillance.
6. Après avoir sélectionné la plage de dates et d'heures, cliquez sur **Appliquer la plage**. Les statistiques de performance pour cette période s'affichent dans les graphiques et dans la chronologie des événements.

Sélectionner les seuils de performance dans la vue Zoom des graphiques de compteurs

L'application de seuils dans la vue Zoom des graphiques de compteur fournit une vue détaillée des occurrences d'événements de seuil de performance. Cela vous permet d'appliquer ou de supprimer des seuils et d'afficher immédiatement les résultats, ce qui peut être utile pour décider si le dépannage doit être votre prochaine étape.

La sélection de seuils dans la vue Zoom des graphiques de compteur vous permet d'afficher des données précises sur les événements de seuil de performance. Vous pouvez appliquer n'importe quel seuil qui apparaît sous la zone **Politiques** de la vue Zoom des graphiques de compteur.

Une seule politique à la fois peut être appliquée à l'objet dans la vue Zoom des graphiques de compteur.

Étape

1. Sélectionnez ou désélectionnez le  qui est associé à une politique.

Le seuil sélectionné est appliqué à la vue Zoom des graphiques de compteur. Les seuils critiques sont affichés sous forme de ligne rouge ; les seuils d'avertissement sont affichés sous forme de ligne jaune.

Afficher la latence du volume par composant de cluster

Vous pouvez afficher des informations détaillées sur la latence d'un volume à l'aide de la page Explorateur de performances de volume. Le graphique du compteur Latence - Total affiche la latence totale sur le volume, et le graphique du compteur Latence - Répartition est utile pour déterminer l'impact de la latence de lecture et d'écriture sur le volume.

De plus, le graphique Latence - Composants du cluster affiche une comparaison détaillée de la latence de chaque composant du cluster pour aider à déterminer comment chaque composant contribue à la latence totale du volume. Les composants de cluster suivants sont affichés :

- Réseau

- Limite QoS maximale
- Limite QoS minimale
- Traitement du réseau
- Interconnexion de cluster
- Data Processing
- Opérations d'agrégats
- Activation du volume
- Ressources MetroCluster
- Latence du cloud
- Synchroniser SnapMirror

Étapes

1. Dans la page **Volume Performance Explorer** du volume sélectionné, dans le graphique de latence, sélectionnez **Cluster Components** dans le menu déroulant.

Le graphique Latence - Composants du cluster s'affiche.

2. Pour afficher une version plus grande du graphique, sélectionnez **Vue Zoom**.

Le tableau comparatif des composants du cluster est affiché. Vous pouvez restreindre la comparaison en désélectionnant ou en sélectionnant l'option  qui est associé à chaque composant du cluster.

3. Pour afficher les valeurs spécifiques, déplacez votre curseur dans la zone du graphique pour voir la fenêtre contextuelle.

Afficher le trafic IOPS SVM par protocole

Vous pouvez afficher des informations IOPS détaillées pour un SVM à l'aide de la page Explorateur Performances/SVM. Le graphique du compteur IOPS - Total affiche l'utilisation totale des IOPS sur le SVM, et le graphique du compteur IOPS - Breakdown est utile pour déterminer l'impact de la lecture, de l'écriture et d'autres IOPS sur le SVM.

De plus, le graphique IOPS - Protocoles affiche une comparaison détaillée du trafic IOPS pour chaque protocole utilisé sur le SVM. Les protocoles suivants sont disponibles :

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

Étapes

1. Dans la page **Performance/SVM Explorer** de votre SVM sélectionné, dans le graphique IOPS, sélectionnez **Protocoles** dans le menu déroulant.

Le graphique IOPS - Protocoles s'affiche.

2. Pour afficher une version plus grande du graphique, sélectionnez **Vue Zoom**.

Le tableau comparatif du protocole avancé IOPS est affiché. Vous pouvez restreindre la comparaison en désélectionnant ou en sélectionnant l'option  qui est associé à un protocole.

3. Pour afficher les valeurs spécifiques, déplacez votre curseur dans la zone de graphique de l'un ou l'autre graphique pour voir la fenêtre contextuelle.

Consultez les graphiques de volume et de latence LUN pour vérifier la garantie de performances

Vous pouvez afficher les volumes et les LUN auxquels vous avez souscrit dans le cadre du programme « Garantie de performances » pour vérifier que la latence n'a pas dépassé le niveau qui vous a été garanti.

La garantie de performance de latence est une valeur d'une milliseconde par opération qui ne doit pas être dépassée. Il est basé sur une moyenne horaire et non sur la période de collecte des performances par défaut de cinq minutes.

Étapes

1. Dans la vue **Performance : Tous les volumes** ou **Performance : Tous les LUN**, sélectionnez le volume ou le LUN qui vous intéresse.
2. Dans la page **Performance Explorer** pour le volume ou le LUN sélectionné, choisissez **Moyenne horaire** dans le sélecteur **Afficher les statistiques dans**.

La ligne horizontale dans le graphique de latence affichera une ligne plus lisse lorsque les collections de cinq minutes seront remplacées par la moyenne horaire.

3. Si vous avez d'autres volumes sur le même agrégat qui sont sous la garantie de performances, vous pouvez ajouter ces volumes pour afficher leur valeur de latence dans le même graphique.

Afficher les performances de tous les clusters SAN Array

Vous pouvez utiliser la vue Performances : Tous les clusters pour afficher l'état des performances de vos clusters Tous les clusters SAN Array.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez afficher des informations générales sur tous les clusters SAN Array dans la vue Performances : tous les clusters et des détails dans la page Explorateur de clusters/performances.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Assurez-vous que la colonne « Personnalité » est affichée dans la vue **Santé : Tous les clusters** ou ajoutez-la à l'aide du contrôle **Afficher/Masquer**.

Cette colonne affiche « Toutes les baies SAN » pour vos clusters Toutes les baies SAN.

3. Pour afficher des informations sur les performances de ces clusters, sélectionnez la vue **Performances : Tous les clusters**.

Affichez les informations de performances du cluster All SAN Array.

4. Pour afficher des informations détaillées sur les performances de ces clusters, cliquez sur le nom d'un cluster All SAN Array.
5. Cliquez sur l'onglet **Explorateur**.
6. Sur la page **Cluster / Performance Explorer**, sélectionnez **Nœuds sur ce cluster** dans le menu **Afficher et comparer**.

Vous pouvez comparer les statistiques de performances des deux nœuds de ce cluster pour vous assurer que la charge est presque identique sur les deux nœuds. S'il existe de grandes différences entre les deux nœuds, vous pouvez ajouter le deuxième nœud aux graphiques et comparer les valeurs sur une période plus longue pour identifier les éventuels problèmes de configuration.

Afficher les IOPS des nœuds en fonction des charges de travail qui résident uniquement sur le nœud local

Le graphique du compteur IOPS du nœud peut mettre en évidence les endroits où les opérations passent uniquement par le nœud local à l'aide d'un LIF réseau pour effectuer des opérations de lecture/écriture sur des volumes sur un nœud distant. Les graphiques IOPS - « Total (local) » et « Répartition (locale) » affichent les IOPS pour les données qui résident dans les volumes locaux uniquement sur le nœud actuel.

Les versions « locales » de ces graphiques de compteurs sont similaires aux graphiques de nœuds pour la capacité de performance et l'utilisation, car elles affichent également uniquement les statistiques des données résidant sur les volumes locaux.

En comparant les versions « locales » de ces graphiques de compteurs aux versions totales standard de ces graphiques de compteurs, vous pouvez voir s'il y a beaucoup de trafic circulant via le nœud local pour accéder aux volumes sur le nœud distant. Cette situation peut entraîner des problèmes de performances, éventuellement indiqués par une utilisation élevée sur le nœud, s'il y a trop d'opérations passant par le nœud local pour atteindre un volume sur un nœud distant. Dans ces cas, vous souhaitez peut-être déplacer un volume vers le nœud local ou créer un LIF sur le nœud distant où le trafic provenant des hôtes accédant à ce volume peut être connecté.

Étapes

1. Dans la page **Performance/Node Explorer** du nœud sélectionné, dans le graphique IOPS, sélectionnez **Total** dans le menu déroulant.

Le graphique IOPS - Total s'affiche.

2. Cliquez sur **Zoom View** pour afficher une version plus grande du graphique dans un nouvel onglet du navigateur.
3. De retour sur la page **Performance/Node Explorer**, dans le graphique IOPS, sélectionnez **Total (local)** dans le menu déroulant.

Le graphique IOPS - Total (local) s'affiche.

4. Cliquez sur **Zoom View** pour afficher une version plus grande du graphique dans un nouvel onglet du navigateur.
5. Visualisez les deux graphiques l'un à côté de l'autre et identifiez les zones où les valeurs IOPS semblent être très différentes.

6. Déplacez votre curseur sur ces zones pour comparer les IOPS locales et totales pour un moment précis.

Composants des pages de destination d'objets

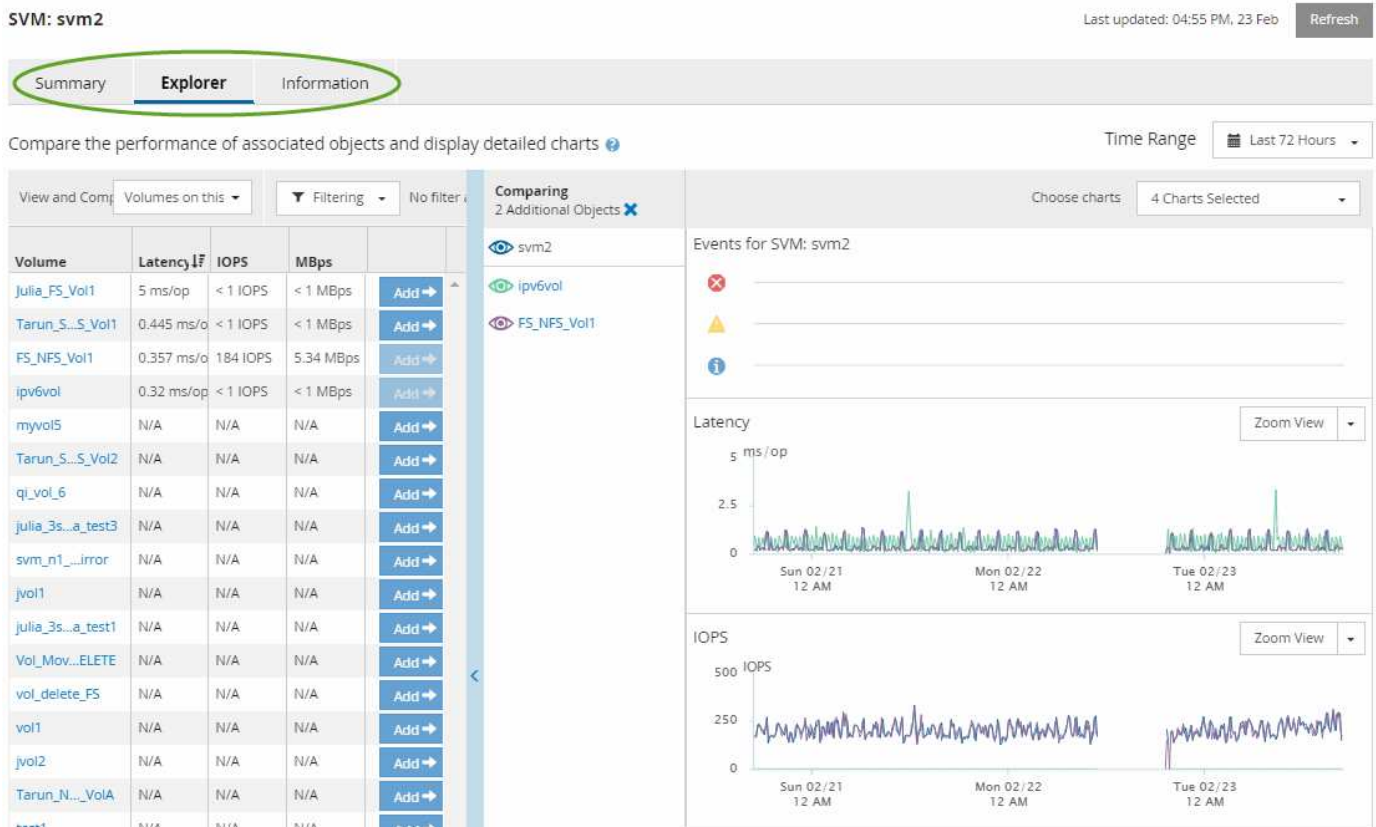
Les pages d'accueil des objets fournissent des détails sur tous les événements critiques, d'avertissement et d'information. Ils fournissent une vue détaillée des performances de tous les objets du cluster, vous permettant de sélectionner et de comparer des objets individuels sur différentes périodes.

Les pages d'accueil des objets vous permettent d'examiner les performances globales de tous les objets et de comparer les données de performances des objets dans un format côte à côte. Cela est utile lors de l'évaluation des performances et lors du dépannage des événements.



Les données affichées dans les panneaux récapitulatifs des compteurs et dans les graphiques des compteurs sont basées sur un intervalle d'échantillonnage de cinq minutes. Les données affichées dans la grille d'inventaire des objets sur le côté gauche de la page sont basées sur un intervalle d'échantillonnage d'une heure.

L'image suivante montre un exemple de page de destination d'objet affichant les informations de l'explorateur :



Selon l'objet de stockage visualisé, la page d'accueil de l'objet peut comporter les onglets suivants qui fournissent des données de performances sur l'objet :

- Résumé

Affiche trois ou quatre graphiques de compteurs contenant les événements et les performances par objet pour la période de 72 heures précédente, y compris une ligne de tendance qui montre les valeurs hautes et basses au cours de cette période.

- Explorateur

Affiche une grille d'objets de stockage liés à l'objet actuel, ce qui vous permet de comparer les valeurs de performances de l'objet actuel avec celles des objets associés. Cet onglet comprend jusqu'à onze graphiques de compteurs et un sélecteur de plage de temps, qui vous permettent d'effectuer diverses comparaisons.

- Information

Affiche les valeurs des attributs de configuration non liés aux performances concernant l'objet de stockage, notamment la version installée du logiciel ONTAP, le nom du partenaire HA et le nombre de ports et de LIF.

- Les meilleurs interprètes

Pour les clusters : affiche les objets de stockage qui ont les performances les plus élevées ou les performances les plus faibles, en fonction du compteur de performances que vous sélectionnez.

- Planification de basculement

Pour les nœuds : affiche l'estimation de l'impact sur les performances d'un nœud si le partenaire HA du nœud échoue.

- Détails

Pour les volumes : affiche des statistiques de performances détaillées pour toutes les activités et opérations d'E/S pour la charge de travail du volume sélectionné. Cet onglet est disponible pour les volumes FlexVol, les volumes FlexGroup et les constituants des FlexGroups.

Page de résumé

La page Résumé affiche des graphiques de compteurs contenant des détails sur les événements et les performances par objet pour la période de 72 heures précédente. Ces données ne sont pas actualisées automatiquement, mais sont à jour lors du dernier chargement de la page. Les graphiques de la page Résumé répondent à la question *Dois-je chercher plus loin ?*

Graphiques et statistiques de compteurs

Les graphiques récapitulatifs fournissent un aperçu rapide et de haut niveau pour la dernière période de 72 heures et vous aident à identifier les problèmes éventuels qui nécessitent une enquête plus approfondie.

Les statistiques du compteur de la page récapitulative sont affichées sous forme de graphiques.

Vous pouvez positionner votre curseur sur la ligne de tendance d'un graphique pour afficher les valeurs du compteur à un moment donné. Les graphiques récapitulatifs affichent également le nombre total d'événements critiques et d'avertissement actifs pour la période de 72 heures précédente pour les compteurs suivants :

- Latence

Temps de réponse moyen pour toutes les demandes d'E/S ; exprimé en millisecondes par opération.

Affiché pour tous les types d'objets.

- **IOPS**

Vitesse de fonctionnement moyenne ; exprimée en opérations d'entrée/sortie par seconde.

Affiché pour tous les types d'objets.

- **Mo/s**

Débit moyen ; exprimé en mégaoctets par seconde.

Affiché pour tous les types d'objets.

- **Capacité de performance utilisée**

Pourcentage de capacité de performance consommée par un nœud ou un agrégat.

Affiché uniquement pour les nœuds et les agrégats.

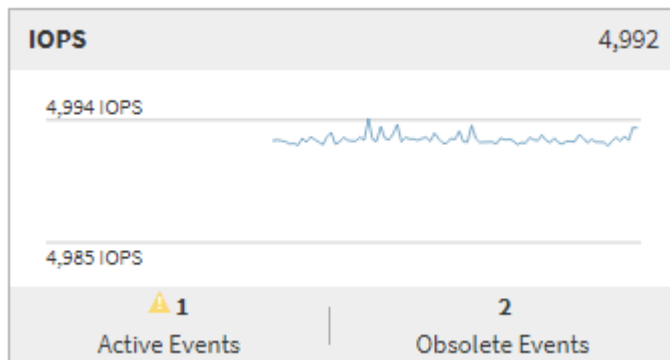
- **Utilisation**

Pourcentage d'utilisation de l'objet pour les nœuds et les agrégats, ou utilisation de la bande passante pour les ports.

Affiché uniquement pour les nœuds, les agrégats et les ports.

Positionner le curseur sur le nombre d'événements pour les événements actifs affiche le type et le nombre d'événements. Les événements critiques sont affichés en rouge (■), et les événements d'avertissement sont affichés en jaune (■).

Le nombre en haut à droite du graphique dans la barre grise est la valeur moyenne de la dernière période de 72 heures. Les chiffres affichés en bas et en haut du graphique de tendance sont les valeurs minimales et maximales pour la dernière période de 72 heures. La barre grise sous le graphique contient le nombre d'événements actifs (nouveaux et reconnus) et d'événements obsolètes de la dernière période de 72 heures.



- **Graphique du compteur de latence**

Le graphique du compteur de latence fournit un aperçu de haut niveau de la latence de l'objet pour la période de 72 heures précédente. La latence fait référence au temps de réponse moyen pour toutes les demandes d'E/S ; exprimé en millisecondes par opération, le temps de service, le temps d'attente ou les deux subis par un paquet de données ou un bloc dans le composant de stockage de cluster considéré.

Haut (valeur du compteur) : Le nombre dans l'en-tête affiche la moyenne de la période de 72 heures précédente.

Milieu (graphique des performances) : le nombre en bas du graphique affiche la latence la plus faible et le nombre en haut du graphique affiche la latence la plus élevée pour la période de 72 heures précédente. Placez votre curseur sur la ligne de tendance du graphique pour afficher la valeur de latence pour une durée spécifique.

En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page Inventaire des événements afin d'afficher les détails complets de l'événement.

- **Graphique du compteur IOPS**

Le graphique du compteur IOPS fournit un aperçu de haut niveau de l'état des IOPS de l'objet pour la période de 72 heures précédente. Les IOPS indiquent la vitesse du système de stockage en nombre d'opérations d'entrée/sortie par seconde.

Haut (valeur du compteur) : Le nombre dans l'en-tête affiche la moyenne de la période de 72 heures précédente.

Milieu (graphique de performances) : le nombre en bas du graphique affiche les IOPS les plus faibles et le nombre en haut du graphique affiche les IOPS les plus élevées pour la période de 72 heures précédente. Placez votre curseur sur la ligne de tendance du graphique pour afficher la valeur IOPS pour une période spécifique.

En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page Inventaire des événements afin d'afficher les détails complets de l'événement.

- **Graphique du compteur MB/s**

Le graphique du compteur MB/s affiche les performances MB/s de l'objet et indique la quantité de données transférées vers et depuis l'objet en mégaoctets par seconde. Le graphique du compteur MB/s fournit un aperçu de haut niveau de l'état de santé MB/s de l'objet pour la période de 72 heures précédente.

Haut (valeur du compteur) : Le nombre dans l'en-tête affiche le nombre moyen de Mo/s pour la période de 72 heures précédente.

Milieu (graphique de performances) : la valeur en bas du graphique affiche le nombre le plus bas de Mo/s, et la valeur en haut du graphique affiche le nombre le plus élevé de Mo/s pour la période de 72 heures précédente. Placez votre curseur sur la ligne de tendance du graphique pour afficher la valeur MB/s pour une période donnée.

En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page Inventaire des événements afin d'afficher les détails complets de l'événement.

- **Tableau des compteurs de capacité de performance utilisés**

Le graphique du compteur Capacité de performance utilisée affiche le pourcentage de capacité de performance consommée par l'objet.

Haut (valeur du compteur) : Le nombre dans l'en-tête affiche la capacité de performance moyenne utilisée pour la période de 72 heures précédente.

Milieu (graphique de performances) : la valeur en bas du graphique affiche le pourcentage de capacité de performances utilisée le plus bas, et la valeur en haut du graphique affiche le pourcentage de capacité

de performances utilisée le plus élevé pour la période de 72 heures précédente. Placez votre curseur sur la ligne de tendance du graphique pour afficher la valeur de capacité de performance utilisée pendant une période donnée.

En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page Inventaire des événements afin d'afficher les détails complets de l'événement.

• Tableau des compteurs d'utilisation

Le graphique du compteur d'utilisation affiche le pourcentage d'utilisation de l'objet. Le graphique du compteur d'utilisation fournit un aperçu de haut niveau du pourcentage d'utilisation de l'objet ou de la bande passante pour la période de 72 heures précédente.

Haut (valeur du compteur) : Le nombre dans l'en-tête affiche le pourcentage d'utilisation moyen pour la période de 72 heures précédente.

Milieu (graphique de performances) : la valeur en bas du graphique affiche le pourcentage d'utilisation le plus bas et la valeur en haut du graphique affiche le pourcentage d'utilisation le plus élevé pour la période de 72 heures précédente. Placez votre curseur sur la ligne de tendance du graphique pour afficher la valeur d'utilisation pour une période spécifique.

En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page Inventaire des événements afin d'afficher les détails complets de l'événement.

Événements

Le tableau de l'historique des événements, le cas échéant, répertorie les événements les plus récents survenus sur cet objet. Cliquer sur le nom de l'événement affiche les détails de l'événement sur la page Détails de l'événement.

Composants de la page Explorateur de performances

La page Explorateur de performances vous permet de comparer les performances d'objets similaires dans un cluster, par exemple, tous les volumes d'un cluster. Cela est utile lors du dépannage des événements de performances et du réglage précis des performances des objets. Vous pouvez également comparer des objets avec l'objet racine, qui constitue la base par rapport à laquelle d'autres comparaisons d'objets sont effectuées.

Vous pouvez cliquer sur le bouton **Passer à la vue Santé** pour afficher la page des détails de santé de cet objet. Dans certains cas, vous pouvez obtenir des informations importantes sur les paramètres de configuration de stockage de cet objet qui peuvent vous aider à résoudre un problème.

La page Explorateur de performances affiche une liste d'objets de cluster et leurs données de performances. Cette page affiche tous les objets de cluster du même type (par exemple, les volumes et leurs statistiques de performances spécifiques à l'objet) dans un format tabulaire. Cette vue fournit un aperçu efficace des performances des objets du cluster.



Si « N/A » apparaît dans une cellule du tableau, cela signifie qu'une valeur pour ce compteur n'est pas disponible car il n'y a aucune E/S sur cet objet à ce moment.

La page Explorateur de performances contient les composants suivants :

- **Plage horaire**

Vous permet de sélectionner une plage horaire pour les données de l'objet.

Vous pouvez choisir une plage prédéfinie ou spécifier votre propre plage horaire personnalisée.

- **Voir et comparer**

Vous permet de sélectionner le type d'objet corrélé à afficher dans la grille.

Les options disponibles dépendent du type d'objet racine et de ses données disponibles. Vous pouvez cliquer sur la liste déroulante Afficher et comparer pour sélectionner un type d'objet. Le type d'objet que vous sélectionnez s'affiche dans la liste.

- **Filtration**

Vous permet de réduire la quantité de données que vous recevez, en fonction de vos préférences.

Vous pouvez créer des filtres qui s'appliquent aux données de l'objet, par exemple, les IOPS supérieures à 4. Vous pouvez ajouter jusqu'à quatre filtres simultanés.

- **Comparaison**

Affiche une liste des objets que vous avez sélectionnés pour comparaison avec l'objet racine.

Les données des objets du volet Comparaison sont affichées dans les graphiques de compteurs.

- **Voir les statistiques dans**

Pour le volume et les LUN, vous permet de sélectionner si les statistiques sont affichées après chaque cycle de collecte (par défaut 5 minutes) ou si les statistiques sont affichées sous forme de moyenne horaire. Cette fonctionnalité vous permet d'afficher le graphique de latence à l'appui du programme « Garantie de performances » de NetApp .

- **Tableaux de compteurs**

Affiche les données graphiques pour chaque catégorie de performances d'objet.

En règle générale, seuls trois ou quatre graphiques sont affichés par défaut. Le composant Choisir des graphiques vous permet d'afficher des graphiques supplémentaires ou de masquer des graphiques spécifiques. Vous pouvez également choisir d'afficher ou de masquer la chronologie des événements.

- **Chronologie des événements**

Affiche les événements de performances et de santé se produisant sur la chronologie que vous avez sélectionnée dans le composant Plage de temps.

Gérer les performances à l'aide des informations du groupe de politiques QoS

Unified Manager vous permet d'afficher les groupes de politiques de qualité de service (QoS) disponibles sur tous les clusters que vous surveillez. Les politiques peuvent avoir

été définies à l'aide du logiciel ONTAP (System Manager ou ONTAP CLI) ou par les politiques de niveau de service de performance d'Unified Manager. Unified Manager affiche également les volumes et les LUN auxquels un groupe de politiques QoS est attribué.

Pour plus d'informations sur le réglage des paramètres QoS, consultez ["Aperçu de la gestion des performances"](#)

Comment la qualité de service du stockage peut contrôler le débit de la charge de travail

Vous pouvez créer un groupe de stratégies de qualité de service (QoS) pour contrôler la limite d'E/S par seconde (IOPS) ou de débit (Mo/s) pour les charges de travail qu'il contient. Si les charges de travail se trouvent dans un groupe de stratégies sans limite définie, tel que le groupe de stratégies par défaut, ou si la limite définie ne répond pas à vos besoins, vous pouvez augmenter la limite ou déplacer les charges de travail vers un groupe de stratégies nouveau ou existant qui a la limite souhaitée.

Les groupes de politiques QoS « traditionnels » peuvent être attribués à des charges de travail individuelles ; par exemple, un seul volume ou LUN. Dans ce cas, la charge de travail peut utiliser la limite de débit complète. Les groupes de politiques QoS peuvent également être attribués à plusieurs charges de travail ; dans ce cas, la limite de débit est « partagée » entre les charges de travail. Par exemple, une limite QoS de 9 000 IOPS attribuée à trois charges de travail empêcherait les IOPS combinées de dépasser 9 000 IOPS.

Les groupes de politiques QoS « adaptatifs » peuvent également être attribués à des charges de travail individuelles ou à plusieurs charges de travail. Cependant, même lorsqu'elle est affectée à plusieurs charges de travail, chaque charge de travail obtient la limite de débit complète au lieu de partager la valeur de débit avec d'autres charges de travail. De plus, les stratégies QoS adaptatives ajustent automatiquement le paramètre de débit en fonction de la taille du volume, par charge de travail, maintenant ainsi le rapport IOPS/téraoctets à mesure que la taille du volume change. Par exemple, si le pic est défini sur 5 000 IOPS/To dans une politique QoS adaptative, un volume de 10 To aura un débit maximal de 50 000 IOPS. Si le volume est redimensionné ultérieurement à 20 To, la QoS adaptative ajuste le maximum à 100 000 IOPS.

À partir d' ONTAP 9.5, vous pouvez inclure la taille du bloc lors de la définition d'une politique QoS adaptative. Cela convertit efficacement la politique d'un seuil IOPS/To à un seuil Mo/s pour les cas où les charges de travail utilisent des tailles de blocs très importantes et utilisent finalement un pourcentage important de débit.

Pour les stratégies QoS de groupe partagé, lorsque les IOPS ou les Mo/s de toutes les charges de travail d'un groupe de stratégies dépassent la limite définie, le groupe de stratégies limite les charges de travail pour restreindre leur activité, ce qui peut diminuer les performances de toutes les charges de travail du groupe de stratégies. Si un événement de performances dynamiques est généré par la limitation du groupe de stratégies, la description de l'événement affiche le nom du groupe de stratégies impliqué.

Dans la vue Performances : Tous les volumes, vous pouvez trier les volumes affectés par IOPS et Mo/s pour voir quelles charges de travail ont l'utilisation la plus élevée qui pourrait avoir contribué à l'événement. Dans la page Explorateur de performances/volumes, vous pouvez sélectionner d'autres volumes ou LUN sur le volume à comparer à l'utilisation du débit IOPS ou Mbit/s de la charge de travail affectée.

En attribuant les charges de travail qui utilisent de manière excessive les ressources du nœud à un paramètre de groupe de stratégies plus restrictif, le groupe de stratégies limite les charges de travail pour restreindre leur activité, ce qui peut réduire l'utilisation des ressources sur ce nœud. Cependant, si vous souhaitez que la charge de travail puisse utiliser davantage de ressources du nœud, vous pouvez augmenter la valeur du

groupe de stratégies.

Vous pouvez utiliser System Manager, les commandes ONTAP ou les niveaux de service de performances d'Unified Manager pour gérer les groupes de stratégies, y compris les tâches suivantes :

- Création d'un groupe de politiques
- Ajout ou suppression de charges de travail dans un groupe de stratégies
- Déplacer une charge de travail entre des groupes de stratégies
- Modification de la limite de débit d'un groupe de politiques
- Déplacer une charge de travail vers un autre agrégat et/ou nœud

Afficher tous les groupes de politiques QoS disponibles sur tous les clusters

Vous pouvez afficher une liste de tous les groupes de politiques QoS disponibles sur les clusters surveillés par Unified Manager. Cela inclut les politiques QoS traditionnelles, les politiques QoS adaptatives et les politiques QoS gérées par les politiques de niveau de service de performance Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Groupes de stratégies QoS**.

La vue Performances : Groupes de politiques QoS traditionnels s'affiche par défaut.

2. Affichez les paramètres de configuration détaillés pour chaque groupe de politiques QoS traditionnel disponible.
3. Cliquez sur le bouton Développer () à côté du nom du groupe de politiques QoS pour afficher plus de détails sur le groupe de politiques.
4. Dans le menu Affichage, sélectionnez l'une des options supplémentaires pour afficher tous les groupes de politiques QoS adaptatifs ou pour afficher tous les groupes de politiques QoS créés à l'aide des niveaux de service de performances Unified Manager.

Afficher les volumes ou les LUN qui se trouvent dans le même groupe de politiques QoS

Vous pouvez afficher une liste des volumes et des LUN qui ont été attribués au même groupe de politiques QoS.

Dans le cas de groupes de politiques QoS traditionnels qui sont « partagés » entre plusieurs volumes, cela peut être utile pour voir si certains volumes utilisent trop le débit défini pour le groupe de politiques. Cela peut également vous aider à décider si vous pouvez ajouter d'autres volumes au groupe de stratégies sans effet négatif sur les autres volumes.

Dans le cas des stratégies QoS adaptatives et des stratégies de niveaux de service de performances Unified Manager, il peut être utile d'afficher tous les volumes ou LUN qui utilisent un groupe de stratégies afin de voir quels objets seraient affectés si vous modifiiez les paramètres de configuration de la stratégie QoS.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Groupes de stratégies QoS**.

La vue Performances : Groupes de politiques QoS traditionnels s'affiche par défaut.

- Si vous êtes intéressé par le groupe politique traditionnel, restez sur cette page. Sinon, sélectionnez l'une des options d'affichage supplémentaires pour afficher tous les groupes de politiques QoS adaptatifs ou tous les groupes de politiques QoS créés par Unified Manager Performance Service Levels.
- Dans la politique QoS qui vous intéresse, cliquez sur le bouton Développer (▼) à côté du nom du groupe de politiques QoS pour afficher plus de détails.

Quality of Service - Performance / Adaptive QoS Policy Groups ?

Last updated: Jan 31, 2019, 1:56 PM

View Adaptive QoS Policy Groups Search Quality of Service

QoS Policy Group	Cluster	SVM	Min Through...	Max Through...	Absolute Min...	Block Size	Asso
▼ julia_vs2_cifs_Performance	opm-simplicity	julia_vs2_cifs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		1
▲ julia_vs1_nfs_Performance	opm-simplicity	julia_vs1_nfs	2048.0 IOPS/TB	4096.0 IOPS/TB	500IOPS		2
Details Allocated Capacity 0.99 TB 1.15 TB Associated Objects 2 Volumes 0 LUNs None Events None							
▼ julia_nfs_extreme_Extreme_Performance	ocum-mobility-01-02	julia_nfs_extreme	6144.0 IOPS/TB	12288.0 IOPS/TB	1000IOPS	any	1
▼ julia_extreme_jan16_aqos	ocum-mobility-01-02	julia_nfs_extreme	10000.0 IOPS/TB	12000.0 IOPS/TB	1000IOPS	any	1

- Cliquez sur le lien Volumes ou LUN pour afficher les objets utilisant cette stratégie QoS.

La page d'inventaire des performances pour les volumes ou les LUN s'affiche avec la liste triée des objets qui utilisent la stratégie QoS.

Afficher les paramètres du groupe de politiques QoS appliqués à des volumes ou des LUN spécifiques

Vous pouvez afficher les groupes de politiques QoS qui ont été appliqués à vos volumes et LUN, et vous pouvez accéder à la vue Groupes de politiques Performances/QoS pour afficher les paramètres de configuration détaillés de chaque politique QoS.

Les étapes permettant d'afficher la politique QoS appliquée à un volume sont présentées ci-dessous. Les étapes pour afficher ces informations pour un LUN sont similaires.

Étapes

- Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.

La vue Santé : tous les volumes s'affiche par défaut.

- Dans le menu Affichage, sélectionnez **Performances : volumes dans le groupe de stratégies QoS**.
- Localisez le volume que vous souhaitez examiner et faites défiler vers la droite jusqu'à ce que vous voyiez la colonne **Groupe de stratégies QoS**.
- Cliquez sur le nom du groupe de stratégies QoS.

La page Qualité de service correspondante s'affiche selon qu'il s'agit d'une politique QoS traditionnelle, d'une politique QoS adaptative ou d'une politique QoS créée à l'aide des niveaux de service de

performances Unified Manager.

5. Affichez les paramètres de configuration détaillés pour le groupe de politiques QoS.
6. Cliquez sur le bouton Développer () à côté du nom du groupe de politiques QoS pour afficher plus de détails sur le groupe de politiques.

Afficher les graphiques de performances pour comparer les volumes ou les LUN qui se trouvent dans le même groupe de stratégies QoS

Vous pouvez afficher les volumes et les LUN qui se trouvent dans les mêmes groupes de stratégies QoS, puis comparer les performances sur un seul graphique IOPS, Mo/s ou IOPS/To pour identifier les problèmes éventuels.

Les étapes permettant de comparer les performances des volumes dans le même groupe de politiques QoS sont présentées ci-dessous. Les étapes pour afficher ces informations pour un LUN sont similaires.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.

La vue Santé : tous les volumes s'affiche par défaut.

2. Dans le menu Affichage, sélectionnez **Performances : volumes dans le groupe de stratégies QoS**.
3. Cliquez sur le nom du volume que vous souhaitez examiner.

La page Explorateur de performances s'affiche pour le volume.

4. Dans le menu Afficher et comparer, sélectionnez **Volumes dans le même groupe de stratégies QoS**.

Les autres volumes qui partagent la même politique QoS sont répertoriés dans le tableau ci-dessous.

5. Cliquez sur le bouton **Ajouter** pour ajouter ces volumes aux graphiques afin de pouvoir comparer les IOPS, Mo/s, IOPS/To et d'autres compteurs de performances pour tous les volumes sélectionnés dans les graphiques.

Vous pouvez modifier la plage horaire pour afficher les performances sur différents intervalles de temps autres que la valeur par défaut de 72 heures.

Comment les différents types de politiques QoS sont affichés dans les graphiques de débit

Vous pouvez afficher les paramètres de stratégie de qualité de service (QoS) définis par ONTAP qui ont été appliqués à un volume ou à un LUN dans les graphiques Performance Explorer et Workload Analysis IOPS, IOPS/To et Mo/s. Les informations affichées dans les graphiques sont différentes selon le type de politique QoS appliquée à la charge de travail.

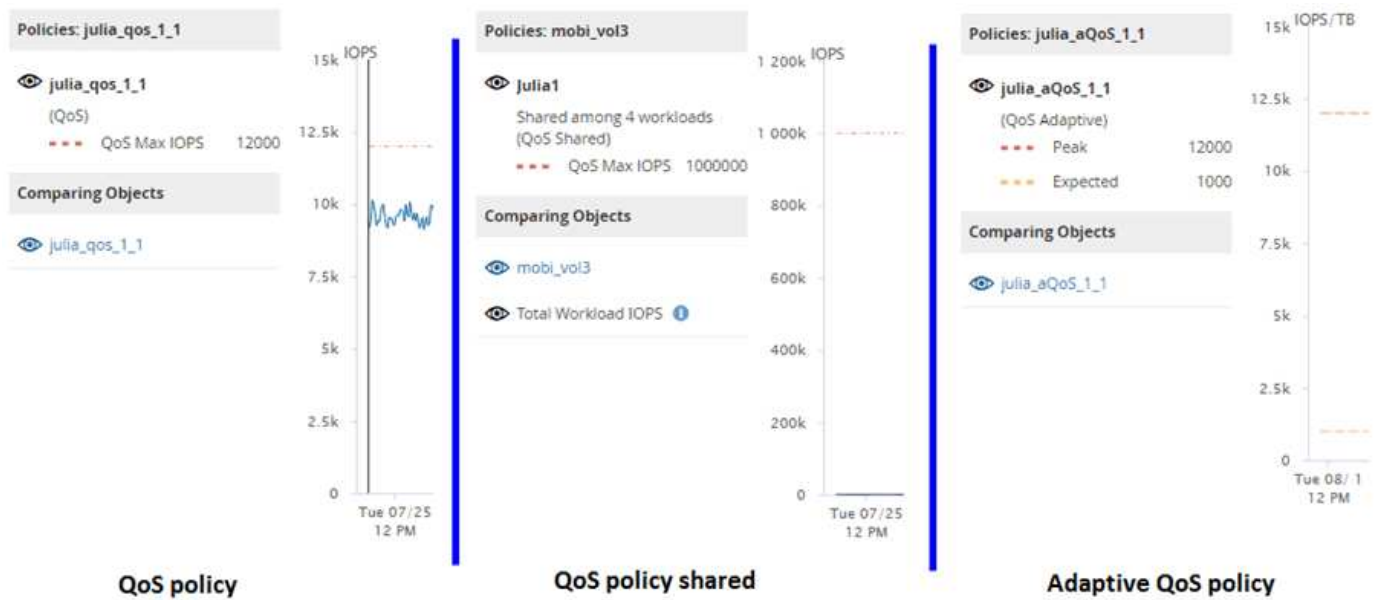
Un paramètre de débit maximal (ou « pic ») définit le débit maximal que la charge de travail peut consommer et limite ainsi l'impact sur les charges de travail concurrentes pour les ressources système. Un paramètre de débit minimum (ou « attendu ») définit le débit minimum qui doit être disponible pour la charge de travail afin qu'une charge de travail critique atteigne les objectifs de débit minimum, quelle que soit la demande des charges de travail concurrentes.

Les politiques QoS partagées et non partagées pour les IOPS et les Mo/s utilisent les termes « minimum » et « maximum » pour définir le plancher et le plafond. Les politiques QoS adaptatives pour IOPS/TB, qui ont été introduites dans ONTAP 9.3, utilisent les termes « attendu » et « pic » pour définir le plancher et le plafond.

Bien ONTAP vous permette de créer ces deux types de politiques QoS, selon la manière dont elles sont appliquées aux charges de travail, il existe trois manières d’afficher la politique QoS dans les graphiques de performances.

Type de politique	Fonctionnalité	Indicateur dans l'interface Unified Manager
Politique de QoS partagée attribuée à une seule charge de travail ou politique de QoS non partagée attribuée à une seule charge de travail ou à plusieurs charges de travail	Chaque charge de travail peut consommer le paramètre de débit spécifié	Affiche « (QoS) »
Politique partagée QoS attribuée à plusieurs charges de travail	Toutes les charges de travail partagent le paramètre de débit spécifié	Affiche « (QoS partagé) »
Politique de qualité de service adaptative attribuée à une ou plusieurs charges de travail	Chaque charge de travail peut consommer le paramètre de débit spécifié	Affiche « (QoS Adaptive) »

La figure suivante montre un exemple de la manière dont les trois options sont affichées dans les graphiques de compteurs.



Lorsqu’une politique QoS normale définie dans IOPS apparaît dans le graphique IOPS/TB pour une charge de travail, ONTAP convertit la valeur IOPS en valeur IOPS/TB et Unified Manager affiche cette politique dans le graphique IOPS/TB avec le texte « QoS, défini dans IOPS ».

Lorsqu’une stratégie QoS adaptative définie dans IOPS/TB apparaît dans le graphique IOPS pour une charge

de travail, ONTAP convertit la valeur IOPS/TB en valeur IOPS et Unified Manager affiche cette stratégie dans le graphique IOPS avec le texte « QoS adaptative - Utilisée, définie dans IOPS/TB » ou « QoS adaptative - Allouée, définie dans IOPS/TB » selon la configuration du paramètre d'allocation IOPS de pointe. Lorsque le paramètre d'allocation est défini sur « espace alloué », le pic d'IOPS est calculé en fonction de la taille du volume. Lorsque le paramètre d'allocation est défini sur « used-space », le pic d'IOPS est calculé en fonction de la quantité de données stockées dans le volume, en tenant compte de l'efficacité du stockage.



Le graphique IOPS/To affiche les données de performances uniquement lorsque la capacité logique utilisée par le volume est supérieure ou égale à 128 Go. Les écarts sont affichés dans le graphique lorsque la capacité utilisée tombe en dessous de 128 Go pendant la période sélectionnée.

Afficher les paramètres minimum et maximum de qualité de service de la charge de travail dans l’Explorateur de performances

Vous pouvez afficher les paramètres de stratégie de qualité de service (QoS) définis par ONTAP sur un volume ou un LUN dans les graphiques de l’Explorateur de performances. Un paramètre de débit maximal limite l’impact des charges de travail concurrentes sur les ressources système. Un paramètre de débit minimum garantit qu’une charge de travail critique répond aux objectifs de débit minimum, quelle que soit la demande des charges de travail concurrentes.

Les paramètres de débit QoS « minimum » et « maximum » IOPS et Mo/s ne s’affichent dans les graphiques de compteurs que s’ils ont été configurés dans ONTAP. Les paramètres de débit minimum sont disponibles uniquement sur les systèmes exécutant le logiciel ONTAP 9.2 ou une version ultérieure, uniquement sur les systèmes AFF , et ils ne peuvent être définis que pour les IOPS pour le moment.

Les politiques QoS adaptatives sont disponibles à partir d' ONTAP 9.3 et sont exprimées en IOPS/TB au lieu d'IOPS. Ces politiques ajustent automatiquement la valeur de la politique QoS en fonction de la taille du volume, par charge de travail, maintenant ainsi le rapport IOPS/téraoctets à mesure que la taille du volume change. Vous pouvez appliquer un groupe de politiques QoS adaptatif aux volumes uniquement. Les terminologies QoS « attendu » et « pic » sont utilisées pour les politiques QoS adaptatives au lieu de minimum et maximum.

Unified Manager génère des événements d’avertissement pour les violations de la politique QoS lorsque le débit de la charge de travail a dépassé le paramètre de politique QoS maximal défini au cours de chaque période de collecte des performances pour l’heure précédente. Le débit de la charge de travail peut dépasser le seuil QoS pendant une courte période uniquement au cours de chaque période de collecte, mais Unified Manager affiche le débit « moyen » pendant la période de collecte sur le graphique. Pour cette raison, vous pouvez voir des événements QoS alors que le débit d’une charge de travail n’a peut-être pas dépassé le seuil de stratégie indiqué dans le graphique.

Étapes

- 1. Dans la page **Performance Explorer** du volume ou du LUN sélectionné, effectuez les actions suivantes pour afficher les paramètres de plafond et de plancher QoS :

Si vous voulez...	Fais ceci...
Afficher le plafond IOPS (le QoS max)	Dans le graphique Total ou Répartition des IOPS, cliquez sur Zoom sur la vue .

Si vous voulez...	Fais ceci...
Afficher le plafond MB/s (le QoS max)	Dans le graphique Total ou Répartition MB/s, cliquez sur Zoom sur la vue .
Afficher le plancher IOPS (le QoS minimum)	Dans le graphique Total ou Répartition des IOPS, cliquez sur Zoom sur la vue .
Afficher le plafond IOPS/To (le pic de QoS)	Pour les volumes, dans le graphique IOPS/To, cliquez sur Zoom View .
Afficher le plancher IOPS/TB (la qualité de service attendue)	Pour les volumes, dans le graphique IOPS/To, cliquez sur Zoom View .

La ligne horizontale en pointillés indique la valeur de débit maximale ou minimale définie dans ONTAP. Vous pouvez également voir quand les modifications apportées aux valeurs QoS ont été mises en œuvre.

2. Pour afficher les valeurs IOPS et MB/s spécifiques par rapport au paramètre QoS, déplacez votre curseur dans la zone du graphique pour voir la fenêtre contextuelle.

Si vous remarquez que certains volumes ou LUN ont des IOPS ou des Mo/s très élevés et sollicitent les ressources système, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP pour ajuster les paramètres QoS afin que ces charges de travail n'affectent pas les performances des autres charges de travail.

Pour plus d'informations sur le réglage des paramètres QoS, consultez ["Aperçu de la gestion des performances"](#)

Gérer les performances à l'aide de la capacité de performance et des informations IOPS disponibles

La capacité de performance indique le débit que vous pouvez obtenir d'une ressource sans dépasser les performances utiles de cette ressource. Si l'on considère les compteurs de performances existants, la capacité de performance est le point auquel vous obtenez l'utilisation maximale d'un nœud ou d'un agrégat avant que la latence ne devienne un problème.

Unified Manager collecte des statistiques de capacité de performance à partir des nœuds et des agrégats de chaque cluster. *La capacité de performance utilisée* est le pourcentage de capacité de performance actuellement utilisée, et *la capacité de performance libre* est le pourcentage de capacité de performance encore disponible.

Alors que la capacité de performance libre fournit un pourcentage de la ressource qui est encore disponible, *available IOPS* vous indique le nombre d'IOPS qui peuvent être ajoutés à la ressource avant d'atteindre la capacité de performance maximale. En utilisant cette métrique, vous pouvez être sûr de pouvoir ajouter des charges de travail d'un nombre prédéterminé d'IOPS à une ressource.

Surveiller les informations sur la capacité de performance présente les avantages suivants :

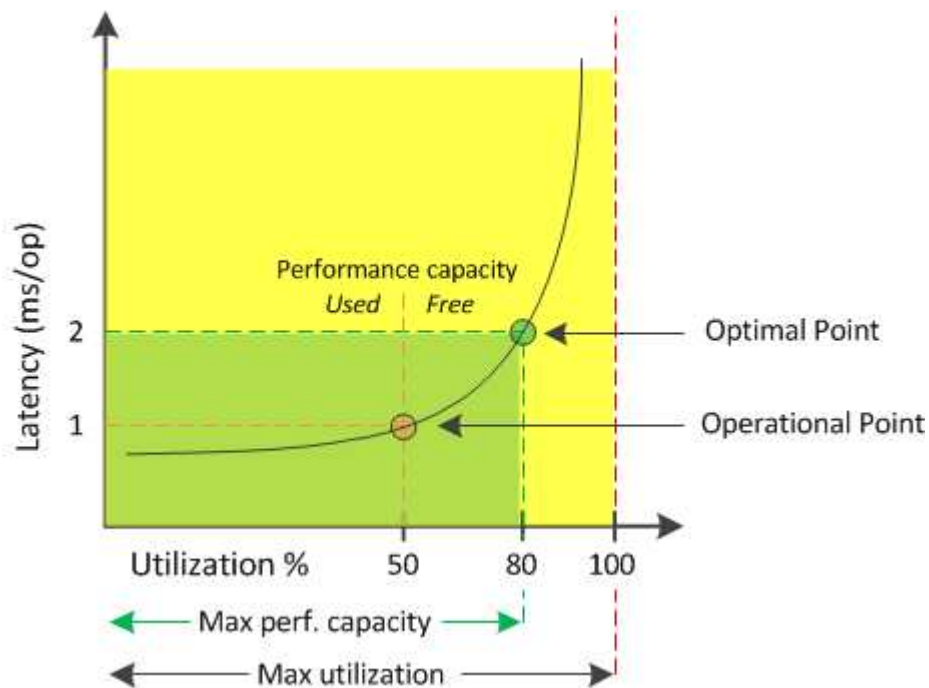
- Aide à l'approvisionnement et à l'équilibrage des flux de travail.

- Vous aide à éviter de surcharger un nœud ou de pousser ses ressources au-delà du point optimal, réduisant ainsi le besoin de dépannage.
- Vous aide à déterminer avec plus de précision où des équipements de stockage supplémentaires pourraient être nécessaires.

Quelle est la capacité de performance utilisée

Le compteur de capacité de performance utilisé vous aide à identifier si les performances d'un nœud ou d'un agrégat atteignent un point où les performances pourraient se dégrader si les charges de travail augmentent. Il peut également vous montrer si un nœud ou un agrégat est actuellement surutilisé pendant des périodes de temps spécifiques. La capacité de performance utilisée est similaire à l'utilisation, mais la première fournit plus d'informations sur les capacités de performance disponibles dans une ressource physique pour une charge de travail spécifique.

La capacité de performance optimale utilisée est le point auquel un nœud ou un agrégat a une utilisation et une latence optimales (temps de réponse) et est utilisé efficacement. Un exemple de courbe de latence par rapport à l'utilisation est présenté pour un agrégat dans la figure suivante.



Dans cet exemple, le *point opérationnel* identifie que l'agrégat fonctionne actuellement à 50 % d'utilisation avec une latence de 1,0 ms/op. Sur la base des statistiques capturées à partir de l'agrégat, Unified Manager détermine qu'une capacité de performance supplémentaire est disponible pour cet agrégat. Dans cet exemple, le *point optimal* est identifié comme le point où l'agrégat est à 80 % d'utilisation avec une latence de 2,0 ms/op. Par conséquent, vous pouvez ajouter davantage de volumes et de LUN à cet agrégat afin que vos systèmes soient utilisés plus efficacement.

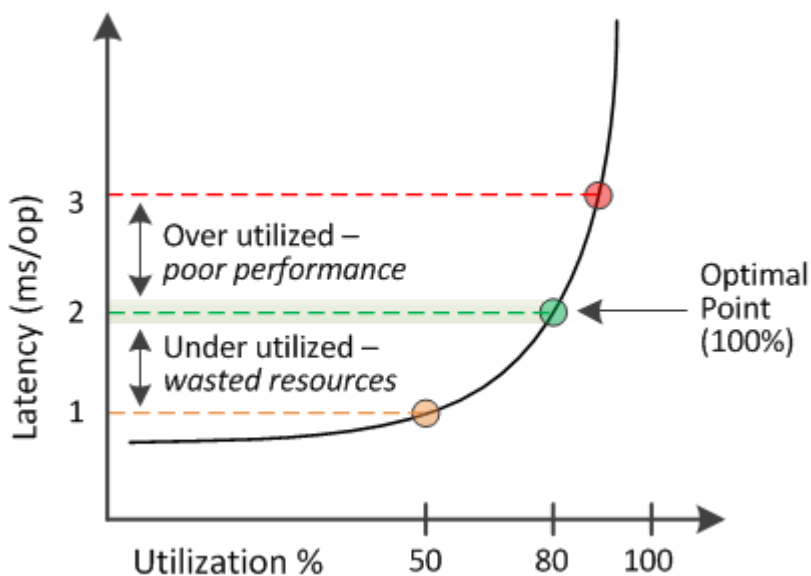
Le compteur de capacité de performance utilisé devrait être un nombre plus grand que le compteur « utilisation » car la capacité de performance ajoute un impact sur la latence. Par exemple, si un nœud ou un agrégat est utilisé à 70 %, la valeur de capacité de performance peut être comprise entre 80 % et 100 %, selon la valeur de latence.

Dans certains cas, cependant, le compteur d'utilisation peut être plus élevé sur la page Tableau de bord. Ceci est normal car le tableau de bord actualise les valeurs actuelles du compteur à chaque période de collecte ; il n'affiche pas les moyennes sur une période donnée comme les autres pages de l'interface utilisateur d'Unified Manager. Le compteur de capacité de performance utilisé est mieux utilisé comme indicateur de performance moyenne sur une période donnée, tandis que le compteur d'utilisation est mieux utilisé pour déterminer l'utilisation instantanée d'une ressource.

Que signifie la valeur de la capacité de performance utilisée

La valeur de capacité de performance utilisée vous aide à identifier les nœuds et les agrégats qui sont actuellement surutilisés ou sous-utilisés. Cela vous permet de redistribuer les charges de travail afin de rendre vos ressources de stockage plus efficaces.

La figure suivante montre la courbe de latence par rapport à l'utilisation d'une ressource et identifie, avec des points colorés, trois zones où le point opérationnel actuel pourrait être situé.



- Un pourcentage de capacité de performance utilisée égal à 100 est au point optimal.

Les ressources sont utilisées efficacement à ce stade.

- Un pourcentage de capacité de performance utilisée supérieur à 100 indique que le nœud ou l'agrégat est surutilisé et que les charges de travail reçoivent des performances sous-optimales.

Aucune nouvelle charge de travail ne doit être ajoutée à la ressource et les charges de travail existantes devront peut-être être redistribuées.

- Un pourcentage de capacité de performance utilisé inférieur à 100 indique que le nœud ou l'agrégat est sous-utilisé et que les ressources ne sont pas utilisées efficacement.

Des charges de travail supplémentaires peuvent être ajoutées à la ressource.



Contrairement à l'utilisation, le pourcentage de capacité de performance utilisé peut être supérieur à 100 %. Il n'y a pas de pourcentage maximum, mais les ressources se situent généralement entre 110 % et 140 % lorsqu'elles sont surutilisées. Des pourcentages plus élevés indiqueraient une ressource présentant de graves problèmes.

Quels sont les IOPS disponibles

Le compteur IOPS disponible identifie le nombre restant d'IOPS qui peuvent être ajoutés à un nœud ou à un agrégat avant que la ressource n'atteigne sa limite.

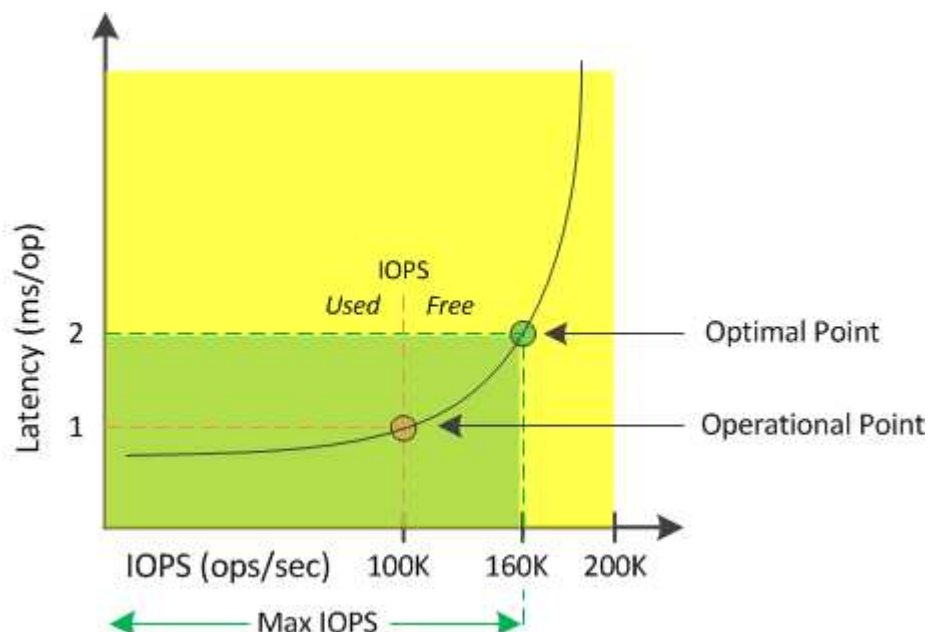
Le nombre total d'IOPS qu'un nœud peut fournir est basé sur les caractéristiques physiques du nœud, par exemple, le nombre de processeurs, la vitesse du processeur et la quantité de RAM. Le nombre total d'IOPS qu'un agrégat peut fournir est basé sur les propriétés physiques des disques, par exemple un disque SATA, SAS ou SSD.

Le nombre total d'IOPS de tous les volumes d'un agrégat peut ne pas correspondre au nombre total d'IOPS de l'agrégat. Ceci est abordé dans l'article suivant de la base de connaissances : [KB "Pourquoi la somme de tous les volumes IOP d'un agrégat ne correspond-elle pas aux volumes IOP agrégés ?"](#)

Alors que le compteur de capacité de performance disponible fournit le pourcentage d'une ressource qui est encore disponible, le compteur d'IOPS disponibles vous indique le nombre exact d'IOPS (charges de travail) qui peuvent être ajoutés à une ressource avant d'atteindre la capacité de performance maximale.

Par exemple, si vous utilisez une paire de systèmes de stockage FAS2520 et FAS8060, une valeur de capacité de performance libre de 30 % signifie que vous disposez d'une certaine capacité de performance libre. Cependant, cette valeur ne fournit pas de visibilité sur le nombre de charges de travail supplémentaires que vous pouvez déployer sur ces nœuds. Le compteur IOPS disponible peut indiquer que vous avez 500 IOPS disponibles sur le FAS8060, mais seulement 100 IOPS disponibles sur le FAS2520.

Un exemple de courbe de latence par rapport aux IOPS pour un nœud est présenté dans la figure suivante.



Le nombre maximal d'IOPS qu'une ressource peut fournir est le nombre d'IOPS lorsque le compteur de capacité de performance utilisée est à 100 % (le point optimal). Le point opérationnel identifie que le nœud fonctionne actuellement à 100 000 IOPS avec une latence de 1,0 ms/op. Sur la base des statistiques

capturées à partir du nœud, Unified Manager détermine que le nombre maximal d'IOPS pour le nœud est de 160 000, ce qui signifie qu'il y a 60 000 IOPS libres ou disponibles. Par conséquent, vous pouvez ajouter davantage de charges de travail à ce nœud afin que vos systèmes soient utilisés plus efficacement.



Lorsque l'activité utilisateur est minimale dans la ressource, la valeur IOPS disponible est calculée en supposant une charge de travail générique basée sur environ 4 500 IOPS par cœur de processeur. Cela est dû au fait qu'Unified Manager ne dispose pas des données nécessaires pour estimer avec précision les caractéristiques de la charge de travail traitée.

Afficher les valeurs utilisées de la capacité de performance des nœuds et des agrégats

Vous pouvez surveiller les valeurs de capacité de performances utilisées pour tous les nœuds ou pour tous les agrégats d'un cluster, ou vous pouvez afficher les détails d'un seul nœud ou agrégat.

Les valeurs de capacité de performance utilisées apparaissent dans le tableau de bord, les pages Inventaire des performances, la page Meilleurs interprètes, la page Créer une politique de seuil, les pages Explorateur de performances et dans les graphiques détaillés. Par exemple, la page Performances : tous les agrégats fournit une colonne Capacité de performance utilisée pour afficher la valeur de la capacité de performance utilisée pour tous les agrégats.

Aggregates ⓘ Last updated: 04:11 PM, 08 Feb Refresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Filtering ▾ No filter applied
Search Aggregates Data Search

▾ Assign Threshold Policy
Clear Threshold Policy

☐	Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
☐	✓	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
☐	✓	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
☐	✓	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
☐	✓	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
☐	✓	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
☐	✓	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
☐	✓	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
☐	✓	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
☐	⚠	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

Le compteur de capacité de performance utilisé vous permet d'identifier les éléments suivants :

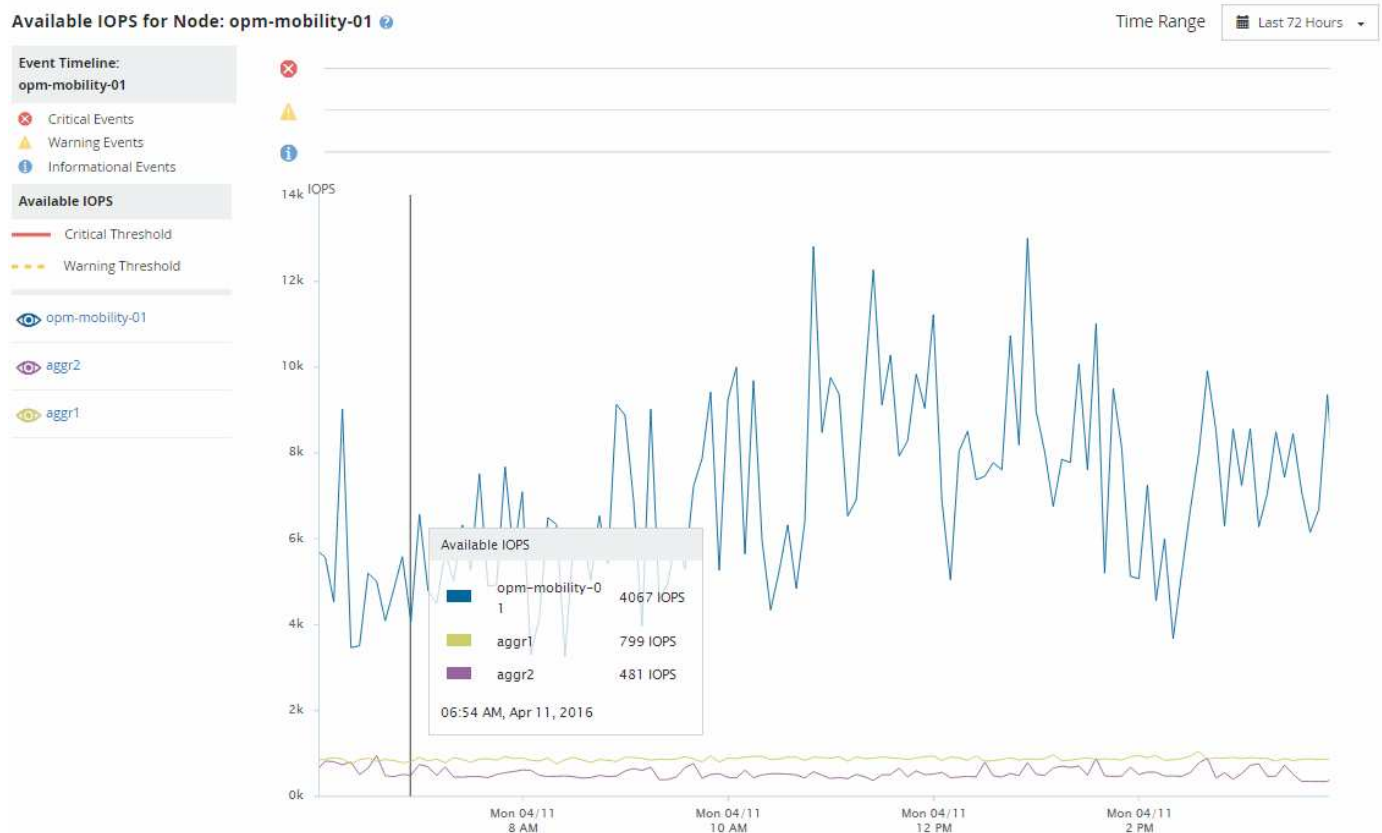
- Si des nœuds ou des agrégats sur des clusters ont une valeur de capacité de performance élevée utilisée
- Si des nœuds ou des agrégats sur des clusters ont des événements actifs de capacité de performance utilisée
- Les nœuds et les agrégats qui ont la valeur de capacité de performance utilisée la plus élevée et la plus basse dans un cluster
- Valeurs des compteurs de latence et d'utilisation en conjonction avec les nœuds ou les agrégats qui ont des valeurs de capacité de performance élevées utilisées
- Comment les valeurs de capacité de performance utilisées pour les nœuds d'une paire HA seront affectées si l'un des nœuds tombe en panne

- Les volumes et les LUN les plus utilisés sur un agrégat doté d'une capacité de performance élevée sont utilisés

Afficher les valeurs IOPS disponibles pour les nœuds et les agrégats

Vous pouvez surveiller les valeurs IOPS disponibles pour tous les nœuds ou pour tous les agrégats d'un cluster, ou vous pouvez afficher les détails d'un seul nœud ou agrégat.

Les valeurs IOPS disponibles apparaissent dans les pages Inventaire des performances et dans les graphiques de la page Explorateur des performances pour les nœuds et les agrégats. Par exemple, lorsque vous visualisez un nœud dans la page Explorateur de nœuds/performance, vous pouvez sélectionner le graphique de compteur « IOPS disponibles » dans la liste afin de pouvoir comparer les valeurs IOPS disponibles pour le nœud et plusieurs agrégats sur ce nœud.



Surveiller le compteur IOPS disponible vous permet d'identifier :

- Les nœuds ou agrégats qui ont les valeurs IOPS disponibles les plus élevées pour aider à déterminer où les futures charges de travail peuvent être déployées.
- Les nœuds ou agrégats qui ont les plus petites valeurs IOPS disponibles pour identifier les ressources que vous devez surveiller pour d'éventuels problèmes de performances futurs.
- Les volumes et LUN les plus occupés sur un agrégat qui a une petite valeur IOPS disponible.

Consultez les graphiques des compteurs de capacité de performance pour identifier les problèmes

Vous pouvez afficher les graphiques de capacité de performance utilisée pour les nœuds et les agrégats sur la page Explorateur de performances. Cela vous permet d'afficher des

données détaillées sur la capacité de performance des nœuds et des agrégats sélectionnés pour une période spécifique.

Le graphique de compteur standard affiche les valeurs de capacité de performance utilisées pour les nœuds ou agrégats sélectionnés. Le graphique du compteur de pannes affiche les valeurs de capacité de performance totales pour l'objet racine séparées en utilisation en fonction des protocoles utilisateur par rapport aux processus système en arrière-plan. De plus, la quantité de capacité de performance libre est également affichée.

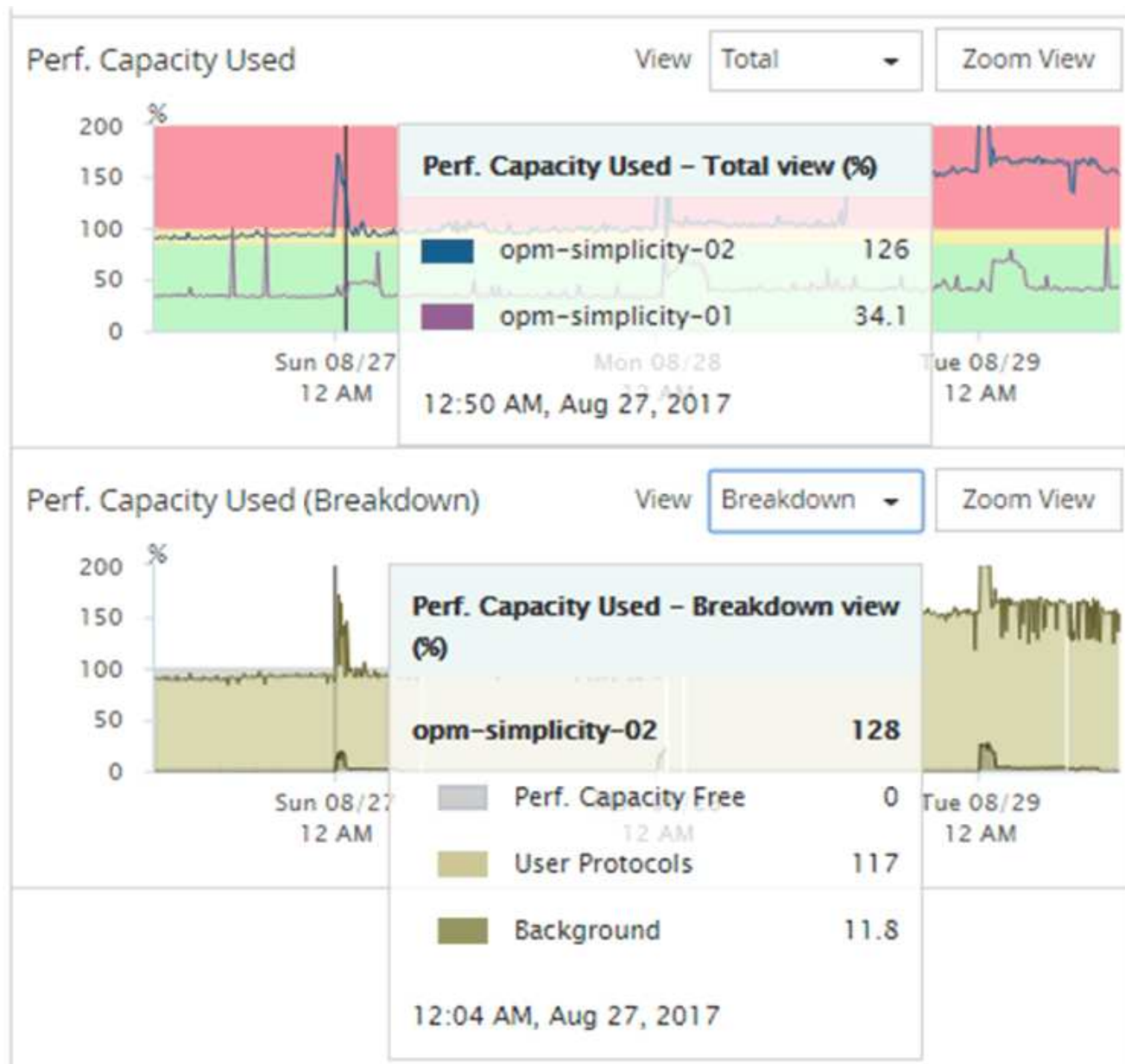


Étant donné que certaines activités d'arrière-plan associées à la gestion du système et des données sont identifiées comme des charges de travail utilisateur et classées comme protocoles utilisateur, le pourcentage de protocoles utilisateur peut sembler artificiellement élevé lorsque ces processus s'exécutent. Ces processus s'exécutent généralement vers minuit, lorsque l'utilisation du cluster est faible. Si vous constatez un pic d'activité du protocole utilisateur vers minuit, vérifiez si les tâches de sauvegarde de cluster ou d'autres activités en arrière-plan sont configurées pour s'exécuter à ce moment-là.

Étapes

1. Sélectionnez l'onglet **Explorer** à partir d'un nœud ou d'une page **Landing** agrégée.
2. Dans le volet **Graphiques de compteur**, cliquez sur **Choisir des graphiques**, puis sélectionnez **Perf. Tableau de capacité utilisée**.
3. Faites défiler vers le bas jusqu'à ce que vous puissiez voir le graphique.

Les couleurs du graphique standard indiquent quand l'objet est dans la plage optimale (jaune), quand l'objet est sous-utilisé (vert) et quand l'objet est surutilisé (rouge). Le graphique de répartition affiche les détails détaillés de la capacité de performance pour l'objet racine uniquement.



4. Si vous souhaitez afficher l'un ou l'autre des graphiques en taille réelle, cliquez sur **Zoom View**.

De cette manière, vous pouvez ouvrir plusieurs graphiques de compteurs dans des fenêtres séparées pour comparer les valeurs de capacité de performance utilisées avec les valeurs IOPS ou MBps sur la même période.

Capacité de performance utilisée, conditions de seuil de performance

Vous pouvez créer des stratégies de seuil de performances définies par l'utilisateur afin que les événements soient déclenchés lorsque la valeur de capacité de performances utilisée pour un nœud ou un agrégat dépasse le paramètre de seuil de capacité de performances utilisé défini.

De plus, les nœuds peuvent être configurés avec une politique de seuil de « reprise de la capacité de performance utilisée ». Cette politique de seuil totalise les statistiques de capacité de performance utilisées pour les deux nœuds d'une paire HA afin de déterminer si l'un des nœuds manquerait de capacité suffisante

en cas de défaillance de l'autre nœud. Étant donné que la charge de travail lors du basculement est la combinaison des charges de travail des deux nœuds partenaires, la même capacité de performance utilisée pour la stratégie de reprise peut être appliquée aux deux nœuds.



Cette équivalence de capacité de performance utilisée est généralement vraie entre les nœuds. Toutefois, s'il existe un trafic inter-nœuds significativement plus important destiné à l'un des nœuds via son partenaire de basculement, la capacité de performance totale utilisée lors de l'exécution de toutes les charges de travail sur un nœud partenaire par rapport à l'autre nœud partenaire peut être légèrement différente selon le nœud défaillant.

Les conditions de capacité de performances utilisées peuvent également être utilisées comme paramètres de seuil de performances secondaires pour créer une stratégie de seuil combinée lors de la définition de seuils pour les LUN et les volumes. La condition de capacité de performance utilisée est appliquée à l'agrégat ou au nœud sur lequel réside le volume ou le LUN. Par exemple, vous pouvez créer une politique de seuil de combinaison en utilisant les critères suivants :

Objet de stockage	Compteur de performance	Seuil d'alerte	Seuil critique	Durée
Volume	Latence	15 ms/op	25 ms/op	20 minutes
Agrégat	Capacité de performance utilisée	80%	95%	

Les stratégies de seuil de combinaison entraînent la génération d'un événement uniquement lorsque les deux conditions sont violées pendant toute la durée.

Utilisez le compteur de capacité de performance utilisée pour gérer les performances

En règle générale, les organisations souhaitent fonctionner avec un pourcentage de capacité de performance utilisée inférieur à 100 afin que les ressources soient utilisées efficacement tout en réservant une capacité de performance supplémentaire pour répondre aux demandes des périodes de pointe. Vous pouvez utiliser des stratégies de seuil pour personnaliser le moment où les alertes sont envoyées pour les valeurs de capacité utilisée à hautes performances.

Vous pouvez établir des objectifs spécifiques en fonction de vos exigences de performance. Par exemple, les sociétés de services financiers pourraient réserver davantage de capacité de performance pour garantir l'exécution rapide des transactions. Ces entreprises pourraient vouloir fixer des seuils de capacité de performance utilisés dans la fourchette de 70 à 80 %. Les entreprises de fabrication ayant des marges plus faibles pourraient choisir de réserver moins de capacité de performance si elles sont prêtes à risquer leurs performances pour mieux gérer les coûts informatiques. Ces entreprises pourraient fixer des seuils de capacité de performance utilisés dans la fourchette de 85 à 95 pour cent.

Lorsque la valeur de capacité de performance utilisée dépasse le pourcentage défini dans une stratégie de seuil définie par l'utilisateur, Unified Manager envoie un e-mail d'alerte et ajoute l'événement à la page Inventaire des événements. Cela vous permet de gérer les problèmes potentiels avant qu'ils n'affectent les performances. Ces événements peuvent également être utilisés comme indicateurs indiquant que vous devez effectuer des déplacements et des modifications de charge de travail au sein de vos nœuds et agrégats.

Comprendre et utiliser la page Planification du basculement de nœud

La page Planification du basculement des performances/nœuds estime l'impact sur les performances d'un nœud si le nœud partenaire haute disponibilité (HA) du nœud échoue. Unified Manager base les estimations sur les performances historiques des nœuds de la paire HA.

L'estimation de l'impact sur les performances d'un basculement vous aide à planifier les scénarios suivants :

- Si un basculement dégrade systématiquement les performances estimées du nœud de reprise à un niveau inacceptable, vous pouvez envisager de prendre des mesures correctives pour réduire l'impact sur les performances dû à un basculement.
- Avant de lancer un basculement manuel pour effectuer des tâches de maintenance matérielle, vous pouvez estimer comment le basculement affecte les performances du nœud de reprise afin de déterminer le meilleur moment pour effectuer la tâche.

Utilisez la page Planification du basculement des nœuds pour déterminer les actions correctives

En fonction des informations affichées dans la page Planification du basculement des performances/nœuds, vous pouvez prendre des mesures pour garantir qu'un basculement n'entraîne pas une chute des performances d'une paire HA en dessous d'un niveau acceptable.

Par exemple, pour réduire l'impact estimé sur les performances d'un basculement, vous pouvez déplacer certains volumes ou LUN d'un nœud de la paire HA vers d'autres nœuds du cluster. Cela garantit que le nœud principal peut continuer à fournir des performances acceptables après un basculement.

Composants de la page de planification du basculement de nœud

Les composants de la page Planification du basculement des performances/nœuds sont affichés dans une grille et dans le volet Comparaison. Ces sections vous permettent d'évaluer l'impact d'un basculement de nœud sur les performances du nœud de reprise.

Grille de statistiques de performance

La page Planification du basculement des performances/nœuds affiche une grille contenant des statistiques sur la latence, les IOPS, l'utilisation et la capacité de performances utilisée.



Les valeurs de latence et d'IOPS affichées sur cette page et dans la page Explorateur de performances/nœuds peuvent ne pas correspondre, car différents compteurs de performances sont utilisés pour calculer les valeurs permettant de prédire le basculement du nœud.

Dans la grille, chaque nœud se voit attribuer l'un des rôles suivants :

- Primaire

Le nœud qui prend le relais du partenaire HA lorsque ce dernier échoue. L'objet racine est toujours le nœud principal.

- Partenaire

Le nœud qui échoue dans le scénario de basculement.

- Prise de contrôle estimée

Identique au nœud principal. Les statistiques de performances affichées pour ce nœud montrent les performances du nœud de reprise après avoir pris le contrôle du partenaire défaillant.



Bien que la charge de travail du nœud de reprise soit équivalente aux charges de travail combinées des deux nœuds après un basculement, les statistiques du nœud de reprise estimé ne sont pas la somme des statistiques du nœud principal et du nœud partenaire. Par exemple, si la latence du nœud principal est de 2 ms/op et la latence du nœud partenaire est de 3 ms/op, le nœud de reprise estimé peut avoir une latence de 4 ms/op. Cette valeur est un calcul effectué par Unified Manager.

Vous pouvez cliquer sur le nom du nœud Partenaire si vous souhaitez qu'il devienne l'objet racine. Une fois la page Explorateur de performances/performances de nœud affichée, vous pouvez cliquer sur l'onglet **Planification du basculement** pour voir comment les performances évoluent dans ce scénario de défaillance de nœud. Par exemple, si Node1 est le nœud principal et Node2 est le nœud partenaire, vous pouvez cliquer sur Node2 pour en faire le nœud principal. De cette façon, vous pouvez voir comment les performances estimées changent en fonction du nœud défaillant.

Comparaison du volet

La liste suivante décrit les composants affichés par défaut dans le volet de comparaison :

- **Tableaux des événements**

Ils sont affichés dans le même format que ceux de la page Performances/Explorateur de performances des nœuds. Ils concernent uniquement le nœud principal.

- **Contre-graphiques**

Ils affichent des statistiques historiques pour le compteur de performances affiché dans la grille. Dans chaque graphique, le graphique du nœud de basculement estimé affiche les performances estimées si un basculement s'est produit à un moment donné.

Par exemple, supposons que le graphique d'utilisation affiche 73 % pour le nœud de prise de contrôle estimée à 11 h le 8 février. Si un basculement avait eu lieu à ce moment-là, l'utilisation du nœud de reprise aurait été de 73 %.

Les statistiques historiques vous aident à trouver le moment optimal pour lancer un basculement, minimisant ainsi la possibilité de surcharge du nœud de reprise. Vous pouvez planifier un basculement uniquement aux moments où les performances prévues du nœud de reprise sont acceptables.

Par défaut, les statistiques de l'objet racine et du nœud partenaire sont affichées dans le volet Comparaison. Contrairement à la page Explorateur de performances/performances des nœuds, cette page n'affiche pas le bouton **Ajouter** pour vous permettre d'ajouter des objets à des fins de comparaison de statistiques.

Vous pouvez personnaliser le volet Comparaison de la même manière que dans la page Performances/Explorateur de performances des nœuds. La liste suivante montre des exemples de personnalisation des graphiques :

- Cliquez sur le nom d'un nœud pour afficher ou masquer les statistiques du nœud dans les graphiques de compteur.
- Cliquez sur **Zoom View** pour afficher un graphique détaillé d'un compteur particulier dans une nouvelle fenêtre.

Utiliser une politique de seuil avec la page Planification du basculement de nœud

Vous pouvez créer une stratégie de seuil de nœud afin d'être averti dans la page Planification du basculement des performances/nœuds lorsqu'un basculement potentiel dégraderait les performances du nœud de reprise à un niveau inacceptable.

La politique de seuil de performances définie par le système nommée « Paire de nœuds HA surutilisée » génère un événement d'avertissement si le seuil est dépassé pendant six périodes de collecte consécutives (30 minutes). Le seuil est considéré comme dépassé si la capacité de performance combinée utilisée des nœuds d'une paire HA dépasse 200 %.

L'événement de la stratégie de seuil définie par le système vous avertit du fait qu'un basculement entraînera une augmentation de la latence du nœud de reprise à un niveau inacceptable. Lorsque vous voyez un événement généré par cette stratégie pour un nœud particulier, vous pouvez accéder à la page Planification du basculement des performances/nœuds pour ce nœud afin d'afficher la valeur de latence prévue en raison d'un basculement.

Outre l'utilisation de cette stratégie de seuil définie par le système, vous pouvez créer des stratégies de seuil à l'aide du compteur « Capacité de performance utilisée - Reprise », puis appliquer la stratégie aux nœuds sélectionnés. La spécification d'un seuil inférieur à 200 % vous permet de recevoir un événement avant que le seuil de la politique définie par le système ne soit dépassé. Vous pouvez également spécifier la période minimale pendant laquelle le seuil est dépassé à moins de 30 minutes si vous souhaitez être averti avant que l'événement de stratégie défini par le système ne soit généré.

Par exemple, vous pouvez définir une stratégie de seuil pour générer un événement d'avertissement si la capacité de performance combinée utilisée des nœuds d'une paire HA dépasse 175 % pendant plus de 10 minutes. Vous pouvez appliquer cette politique à Node1 et Node2, qui forment une paire HA. Après avoir reçu une notification d'événement d'avertissement pour Node1 ou Node2, vous pouvez afficher la page Planification du basculement des performances/nœuds pour ce nœud afin d'évaluer l'impact estimé sur les performances du nœud de reprise. Vous pouvez prendre des mesures correctives pour éviter de surcharger le nœud de reprise si un basculement se produit. Si vous agissez lorsque la capacité de performance combinée utilisée des nœuds est inférieure à 200 %, la latence du nœud de reprise n'atteint pas un niveau inacceptable même si un basculement se produit pendant cette période.

Utilisez le tableau de répartition de la capacité de performance utilisée pour la planification du basculement

Le graphique détaillé de la capacité de performance utilisée - Répartition montre la capacité de performance utilisée pour le nœud principal et le nœud partenaire. Il indique également la quantité de capacité de performance libre sur le nœud de reprise estimé. Ces informations vous aident à déterminer si vous pourriez avoir un problème de performances en cas de défaillance du nœud partenaire.

En plus d'afficher la capacité de performance totale utilisée pour les nœuds, le graphique de répartition divise les valeurs de chaque nœud en protocoles utilisateur et processus d'arrière-plan.

- Les protocoles utilisateur sont les opérations d'E/S des applications utilisateur vers et depuis le cluster.

- Les processus d'arrière-plan sont les processus système internes impliqués dans l'efficacité du stockage, la réplication des données et la santé du système.

Ce niveau de détail supplémentaire vous permet de déterminer si un problème de performances est causé par l'activité de l'application utilisateur ou par des processus système en arrière-plan, tels que la déduplication, la reconstruction RAID, le nettoyage du disque et les copies SnapMirror .

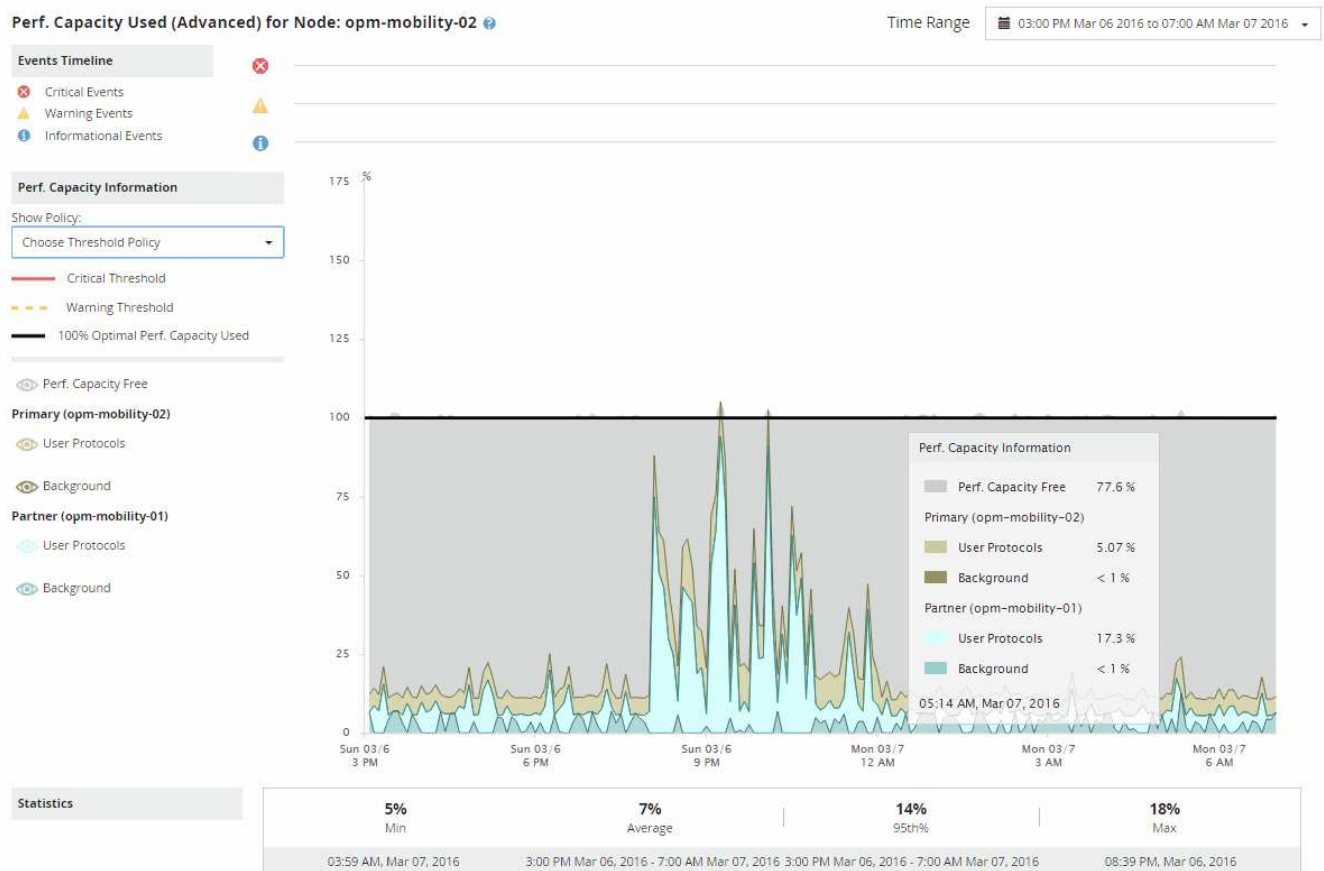
Étapes

1. Accédez à la page **Planification du basculement des performances/nœuds** pour le nœud qui servira de nœud de reprise estimé.
2. À partir du sélecteur **Plage de temps**, choisissez la période pendant laquelle les statistiques historiques sont affichées dans la grille du compteur et les graphiques du compteur.

Les graphiques de compteurs avec les statistiques du nœud principal, du nœud partenaire et du nœud de prise de contrôle estimée sont affichés.

3. Dans la liste **Choisir des graphiques**, sélectionnez **Perf. Capacité utilisée**.
4. Dans le **Perf. Tableau de capacité utilisée**, sélectionnez **Ventilation** et cliquez sur **Zoom**.

Le graphique détaillé pour Perf. La capacité utilisée est affichée.



5. Déplacez le curseur sur le graphique détaillé pour afficher les informations sur la capacité de performance utilisée dans la fenêtre contextuelle.

La Perf. Le pourcentage de capacité libre correspond à la capacité de performance disponible sur le nœud de reprise estimé. Il indique la capacité de performance restante sur le nœud de reprise après un basculement. Si la valeur est de 0 %, un basculement entraînera une augmentation de la latence à un

niveau inacceptable sur le nœud de reprise.

6. Envisagez de prendre des mesures correctives pour éviter un faible pourcentage de capacité de performance libre.

Si vous prévoyez de lancer un basculement pour la maintenance du nœud, choisissez un moment pour faire échouer le nœud partenaire lorsque le pourcentage de capacité de performance libre n'est pas à 0.

Collecter des données et surveiller les performances de la charge de travail

Unified Manager collecte et analyse l'activité de la charge de travail toutes les 5 minutes pour identifier les événements de performances et détecte les modifications de configuration toutes les 15 minutes. Il conserve un maximum de 30 jours de données historiques de performances et d'événements de 5 minutes, et il utilise ces données pour prévoir la plage de latence attendue pour toutes les charges de travail surveillées.

Unified Manager doit collecter au moins 3 jours d'activité de charge de travail avant de pouvoir commencer son analyse et avant que la prévision de latence pour le temps de réponse d'E/S puisse être affichée sur la page Analyse de la charge de travail et sur la page Détails de l'événement. Pendant que cette activité est collectée, la prévision de latence n'affiche pas tous les changements survenant à partir de l'activité de charge de travail. Après avoir collecté 3 jours d'activité, Unified Manager ajuste les prévisions de latence toutes les 24 heures à 00h00, pour refléter les changements d'activité de charge de travail et établir un seuil de performance dynamique plus précis.

Au cours des 4 premiers jours pendant lesquels Unified Manager surveille une charge de travail, si plus de 24 heures se sont écoulées depuis la dernière collecte de données, les graphiques de latence n'afficheront pas la prévision de latence pour cette charge de travail. Les événements détectés avant la dernière collecte sont toujours disponibles.



L'heure d'été (DST) modifie l'heure système, ce qui modifie les prévisions de latence des statistiques de performances pour les charges de travail surveillées. Unified Manager commence immédiatement à corriger les prévisions de latence, ce qui prend environ 15 jours. Pendant ce temps, vous pouvez continuer à utiliser Unified Manager, mais, étant donné qu'Unified Manager utilise la prévision de latence pour détecter les événements dynamiques, certains événements peuvent ne pas être précis. Les événements détectés avant le changement d'heure ne sont pas affectés.

Types de charges de travail surveillées par Unified Manager

Vous pouvez utiliser Unified Manager pour surveiller les performances de deux types de charges de travail : définies par l'utilisateur et définies par le système.

- **Charges de travail définies par l'utilisateur**

Le débit d'E/S des applications vers le cluster. Il s'agit de processus impliqués dans les demandes de lecture et d'écriture. Un volume, un LUN, un partage NFS, un partage SMB/CIFS et une charge de travail sont des charges de travail définies par l'utilisateur.



Unified Manager surveille uniquement l'activité de charge de travail sur le cluster. Il ne surveille pas les applications, les clients ou les chemins entre les applications et le cluster.

Si une ou plusieurs des conditions suivantes sont remplies pour une charge de travail, celle-ci ne peut pas être surveillée par Unified Manager :

- Il s'agit d'une copie de protection des données (DP) en mode lecture seule. (Les volumes DP sont surveillés pour le trafic généré par l'utilisateur.)
- Il s'agit d'un clone de données hors ligne.
- Il s'agit d'un volume en miroir dans une configuration MetroCluster .

• **Charges de travail définies par le système**

Les processus internes impliqués dans l'efficacité du stockage, la réplication des données et la santé du système, notamment :

- Efficacité du stockage, comme la déduplication
- Santé du disque, qui comprend la reconstruction RAID, le nettoyage du disque, etc.
- Réplication de données, telles que les copies SnapMirror
- Activités de gestion
- Santé du système de fichiers, qui comprend diverses activités WAFL
- Scanners de systèmes de fichiers, tels que WAFL Scan
- Copier le déchargement, comme les opérations d'efficacité du stockage déchargées à partir des hôtes VMware
- Santé du système, comme les déplacements de volumes, la compression des données, etc.
- Volumes non surveillés

Les données de performances des charges de travail définies par le système s'affichent dans l'interface graphique utilisateur uniquement lorsque le composant de cluster utilisé par ces charges de travail est en conflit. Par exemple, vous ne pouvez pas rechercher le nom d'une charge de travail définie par le système pour afficher ses données de performances dans l'interface graphique.

Valeurs de mesure des performances de la charge de travail

Unified Manager mesure les performances des charges de travail sur un cluster en fonction des valeurs statistiques historiques et attendues, qui constituent la prévision de latence des valeurs des charges de travail. Il compare les valeurs statistiques réelles de la charge de travail aux prévisions de latence pour déterminer quand les performances de la charge de travail sont trop élevées ou trop faibles. Une charge de travail qui ne fonctionne pas comme prévu déclenche un événement de performance dynamique pour vous en informer.

Dans l'illustration suivante, la valeur réelle, en rouge, représente les statistiques de performances réelles dans la période. La valeur réelle a dépassé le seuil de performance, qui correspond aux limites supérieures de la prévision de latence. Le pic est la valeur réelle la plus élevée dans la période. L'écart mesure le changement entre les valeurs attendues (la prévision) et les valeurs réelles, tandis que l'écart maximal indique le plus grand changement entre les valeurs attendues et les valeurs réelles.



Le tableau suivant répertorie les valeurs de mesure des performances de la charge de travail.

Mesures	Description
Activité	Pourcentage de la limite QoS utilisée par les charges de travail du groupe de politiques. <i>i</i> Si Unified Manager détecte une modification dans un groupe de stratégies, comme l'ajout ou la suppression d'un volume ou la modification de la limite QoS, les valeurs réelles et attendues peuvent dépasser 100 % de la limite définie. Si une valeur dépasse 100 % de la limite définie, elle est affichée comme > 100 %. Si une valeur est inférieure à 1 % de la limite définie, elle est affichée comme < 1 %.
Réel	La valeur de performance mesurée à un moment précis pour une charge de travail donnée.
Déviaton	L'écart entre les valeurs attendues et les valeurs réelles. Il s'agit du rapport entre la valeur réelle moins la valeur attendue et la valeur supérieure de la plage attendue moins la valeur attendue. <i>i</i> Une valeur d'écart négative indique que les performances de la charge de travail sont inférieures aux attentes, tandis qu'une valeur d'écart positive indique que les performances de la charge de travail sont supérieures aux attentes.

Mesures	Description
Attendu	Les valeurs attendues sont basées sur l'analyse des données de performances historiques pour une charge de travail donnée. Unified Manager analyse ces valeurs statistiques pour déterminer la plage attendue (prévision de latence) des valeurs.
Prévision de latence (plage attendue)	La prévision de latence est une prédiction des valeurs de performances supérieures et inférieures attendues à un moment précis. Pour la latence de la charge de travail, les valeurs supérieures constituent le seuil de performance. Lorsque la valeur réelle dépasse le seuil de performance, Unified Manager déclenche un événement de performance dynamique.
Culminer	La valeur maximale mesurée sur une période donnée.
Écart de pointe	La valeur d'écart maximale mesurée sur une période donnée.
Profondeur de la file d'attente	Le nombre de demandes d'E/S en attente au niveau du composant d'interconnexion.
Utilisation	Pour les composants de traitement du réseau, de traitement des données et d'agrégation, le pourcentage de temps d'occupation nécessaire pour terminer les opérations de charge de travail sur une période donnée. Par exemple, le pourcentage de temps nécessaire aux composants de traitement du réseau ou de traitement des données pour traiter une demande d'E/S ou pour qu'un agrégat réponde à une demande de lecture ou d'écriture.
Débit d'écriture	Quantité de débit d'écriture, en mégaoctets par seconde (Mo/s), des charges de travail d'un cluster local vers le cluster partenaire dans une configuration MetroCluster .

Quelle est la plage de performances attendue

La prévision de latence est une prédiction des valeurs de performances supérieures et inférieures attendues à un moment précis. Pour la latence de la charge de travail, les valeurs supérieures constituent le seuil de performance. Lorsque la valeur réelle dépasse le seuil de performance, Unified Manager déclenche un événement de performance dynamique.

Par exemple, pendant les heures ouvrables normales entre 9h00 et 17h00, la plupart des employés peuvent consulter leur courrier électronique entre 9h00 et 10h30. La demande accrue sur les serveurs de messagerie signifie une augmentation de l'activité de charge de travail sur le stockage back-end pendant cette période.

Les employés peuvent remarquer un temps de réponse lent de leurs clients de messagerie.

Pendant l'heure du déjeuner, entre 12h00 et 13h00, et à la fin de la journée de travail après 17h00, la plupart des employés sont probablement loin de leur ordinateur. La demande sur les serveurs de messagerie diminue généralement, ce qui diminue également la demande sur le stockage back-end. Alternativement, il pourrait y avoir des opérations de charge de travail planifiées, telles que des sauvegardes de stockage ou des analyses antivirus, qui démarrent après 17h00 et augmentent l'activité sur le stockage back-end.

Sur plusieurs jours, l'augmentation et la diminution de l'activité de la charge de travail déterminent la plage attendue (prévision de latence) de l'activité, avec des limites supérieures et inférieures pour une charge de travail. Lorsque l'activité de charge de travail réelle d'un objet se situe en dehors des limites supérieures ou inférieures et reste en dehors des limites pendant un certain temps, cela peut indiquer que l'objet est surutilisé ou sous-utilisé.

Comment la prévision de latence est formée

Unified Manager doit collecter au moins 3 jours d'activité de charge de travail avant de pouvoir commencer son analyse et avant que la prévision de latence pour le temps de réponse d'E/S puisse être affichée dans l'interface graphique. La collecte de données minimale requise ne tient pas compte de tous les changements survenant en raison de l'activité de charge de travail. Après avoir collecté les 3 premiers jours d'activité, Unified Manager ajuste les prévisions de latence toutes les 24 heures à minuit pour refléter les changements d'activité de charge de travail et établir un seuil de performance dynamique plus précis.



L'heure d'été (DST) modifie l'heure système, ce qui modifie les prévisions de latence des statistiques de performances pour les charges de travail surveillées. Unified Manager commence immédiatement à corriger les prévisions de latence, ce qui prend environ 15 jours. Pendant ce temps, vous pouvez continuer à utiliser Unified Manager, mais, étant donné qu'Unified Manager utilise la prévision de latence pour détecter les événements dynamiques, certains événements peuvent ne pas être précis. Les événements détectés avant le changement d'heure ne sont pas affectés.

Comment la prévision de latence est utilisée dans l'analyse des performances

Unified Manager utilise la prévision de latence pour représenter l'activité de latence d'E/S (temps de réponse) typique pour vos charges de travail surveillées. Il vous avertit lorsque la latence réelle d'une charge de travail dépasse les limites supérieures de la prévision de latence, ce qui déclenche un événement de performances dynamique, afin que vous puissiez analyser le problème de performances et prendre des mesures correctives pour le résoudre.

La prévision de latence définit la base de référence des performances pour la charge de travail. Au fil du temps, Unified Manager apprend des mesures de performances passées pour prévoir les niveaux de performances et d'activité attendus pour la charge de travail. La limite supérieure de la plage attendue établit le seuil de performance dynamique. Unified Manager utilise la ligne de base pour déterminer quand la latence réelle est supérieure ou inférieure à un seuil, ou en dehors des limites de la plage attendue. La comparaison entre les valeurs réelles et les valeurs attendues crée un profil de performance pour la charge de travail.

Lorsque la latence réelle d'une charge de travail dépasse le seuil de performances dynamiques, en raison d'une contention sur un composant du cluster, la latence est élevée et la charge de travail s'exécute plus lentement que prévu. Les performances des autres charges de travail qui partagent les mêmes composants de cluster peuvent également être plus lentes que prévu.

Unified Manager analyse l'événement de franchissement de seuil et détermine si l'activité est un événement

de performance. Si l'activité de charge de travail élevée reste constante pendant une longue période, par exemple plusieurs heures, Unified Manager considère l'activité comme normale et ajuste dynamiquement la prévision de latence pour former le nouveau seuil de performances dynamique.

Certaines charges de travail peuvent avoir une activité constamment faible, où la prévision de latence pour la latence ne présente pas un taux de changement élevé au fil du temps. Pour minimiser le nombre d'événements lors de l'analyse des événements de performances, Unified Manager déclenche un événement uniquement pour les volumes à faible activité dont les opérations et les latences sont beaucoup plus élevées que prévu.



Dans cet exemple, la latence d'un volume a une prévision de latence, en gris, de 3,5 millisecondes par opération (ms/op) à son niveau le plus bas et de 5,5 ms/op à son niveau le plus élevé. Si la latence réelle, en bleu, augmente soudainement à 10 ms/op, en raison d'un pic intermittent de trafic réseau ou d'une contention sur un composant du cluster, elle est alors supérieure à la prévision de latence et a dépassé le seuil de performance dynamique.

Lorsque le trafic réseau a diminué ou que le composant du cluster n'est plus en conflit, la latence revient dans les prévisions de latence. Si la latence reste égale ou supérieure à 10 ms/op pendant une longue période, vous devrez peut-être prendre des mesures correctives pour résoudre l'événement.

Comment Unified Manager utilise la latence de la charge de travail pour identifier les problèmes de performances

La latence de la charge de travail (temps de réponse) est le temps nécessaire à un volume d'un cluster pour répondre aux demandes d'E/S des applications clientes. Unified Manager utilise la latence pour détecter et vous alerter des événements de performances.

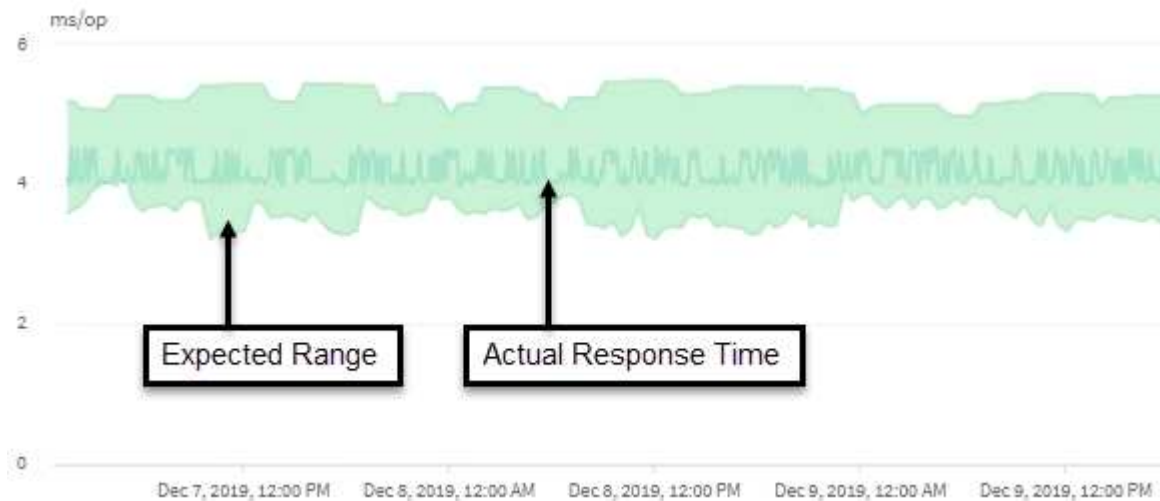
Une latence élevée signifie que les requêtes des applications vers un volume d'un cluster prennent plus de temps que d'habitude. La cause de la latence élevée pourrait provenir du cluster lui-même, en raison d'une contention sur un ou plusieurs composants du cluster. Une latence élevée peut également être causée par des problèmes extérieurs au cluster, tels que des goulots d'étranglement du réseau, des problèmes avec le client hébergeant les applications ou des problèmes avec les applications elles-mêmes.



Unified Manager surveille uniquement l'activité de charge de travail sur le cluster. Il ne surveille pas les applications, les clients ou les chemins entre les applications et le cluster.

Les opérations sur le cluster, telles que la réalisation de sauvegardes ou l'exécution de déduplication, qui augmentent leur demande de composants de cluster partagés par d'autres charges de travail peuvent également contribuer à une latence élevée. Si la latence réelle dépasse le seuil de performances dynamiques de la plage attendue (prévision de latence), Unified Manager analyse l'événement pour déterminer s'il s'agit d'un événement de performances que vous devrez peut-être résoudre. La latence est mesurée en millisecondes par opération (ms/op).

Sur le graphique Total de latence de la page Analyse de la charge de travail, vous pouvez afficher une analyse des statistiques de latence pour voir comment l'activité des processus individuels, tels que les demandes de lecture et d'écriture, se compare aux statistiques de latence globales. La comparaison vous aide à déterminer quelles opérations ont l'activité la plus élevée ou si des opérations spécifiques ont une activité anormale qui a un impact sur la latence d'un volume. Lors de l'analyse des événements de performances, vous pouvez utiliser les statistiques de latence pour déterminer si un événement a été causé par un problème sur le cluster. Vous pouvez également identifier les activités de charge de travail spécifiques ou les composants de cluster impliqués dans l'événement.



Cet exemple montre le graphique de latence. Le temps de réponse réel (latence) est une ligne bleue et la prévision de latence (plage attendue) est verte.

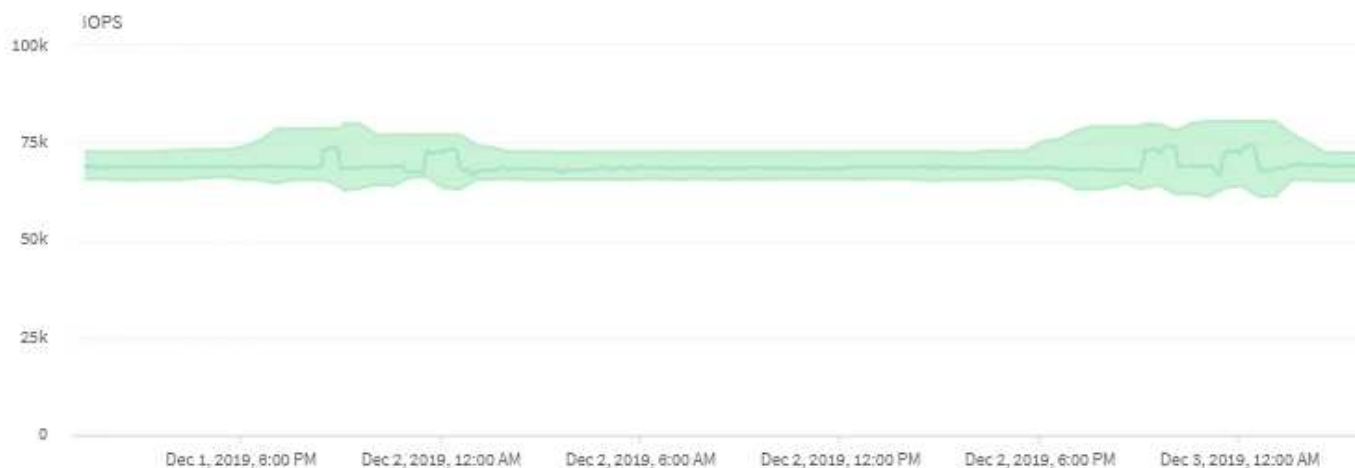


Il peut y avoir des lacunes dans la ligne bleue si Unified Manager n'a pas pu collecter de données. Cela peut se produire parce que le cluster ou le volume était inaccessible, qu'Unified Manager a été désactivé pendant cette période ou que la collecte prenait plus de 5 minutes.

Comment les opérations de cluster peuvent affecter la latence de la charge de travail

Les opérations (IOPS) représentent l'activité de toutes les charges de travail définies par l'utilisateur et par le système sur un cluster. Les statistiques IOPS vous aident à déterminer si les processus de cluster, tels que la réalisation de sauvegardes ou l'exécution de la déduplication, ont un impact sur la latence de la charge de travail (temps de réponse) ou peuvent avoir provoqué ou contribué à un événement de performances.

Lors de l'analyse des événements de performances, vous pouvez utiliser les statistiques IOPS pour déterminer si un événement de performances a été causé par un problème sur le cluster. Vous pouvez identifier les activités de charge de travail spécifiques qui pourraient avoir été les principaux contributeurs à l'événement de performance. Les IOPS sont mesurés en opérations par seconde (ops/sec).



Cet exemple montre le graphique IOPS. Les statistiques d'opérations réelles sont une ligne bleue et les prévisions IOPS des statistiques d'opérations sont vertes.



Dans certains cas où un cluster est surchargé, Unified Manager peut afficher le message `Data collection is taking too long on Cluster cluster_name`. Cela signifie que suffisamment de statistiques ont été collectées pour qu'Unified Manager puisse les analyser. Vous devez réduire les ressources utilisées par le cluster afin que les statistiques puissent être collectées.

Surveillance des performances des configurations MetroCluster

Unified Manager vous permet de surveiller le débit d'écriture entre les clusters dans une configuration MetroCluster pour identifier les charges de travail avec un débit d'écriture élevé.

Si ces charges de travail hautes performances entraînent des temps de réponse d'E/S élevés sur d'autres volumes du cluster local, Unified Manager déclenche des événements de performances pour vous en informer.



Unified Manager traite les clusters d'une configuration MetroCluster comme des clusters individuels. Il ne fait pas de distinction entre les clusters partenaires ni ne corrèle le débit d'écriture de chaque cluster.

Lorsqu'un cluster local dans une configuration MetroCluster reflète ses données sur son cluster partenaire, les données sont écrites dans la NVRAM puis transférées via les liaisons inter-commutateurs (ISL) vers les agrégats distants. Unified Manager analyse la NVRAM pour identifier les charges de travail dont le débit d'écriture élevé surutilise la NVRAM, plaçant la NVRAM en conflit.

Les charges de travail dont l'écart dans le temps de réponse a dépassé le seuil de performance sont appelées *victimes* et les charges de travail dont l'écart dans le débit d'écriture vers la NVRAM est plus élevé que d'habitude, provoquant la contention, sont appelées *intimidateurs*. Étant donné que seules les demandes d'écriture sont mises en miroir sur le cluster partenaire, Unified Manager n'analyse pas le débit de lecture.

Vous pouvez afficher le débit de n'importe lequel des clusters d'une configuration MetroCluster en analysant les charges de travail des LUN et des volumes correspondants à partir des écrans suivants. Vous pouvez filtrer les résultats par cluster. Depuis le volet de navigation de gauche :

- **Stockage > Clusters > Performances : vue Tous les clusters.** Voir

- **Stockage > Volumes > Performances : vue Tous les volumes.**
- **Stockage > LUN > Performances : vue Tous les LUN.**
- **Analyse de la charge de travail > Toutes les charges de travail**

Informations connexes

["Analyse et notification des événements de performance"](#)

["Analyse des événements de performance pour une configuration MetroCluster"](#)

["Rôles des charges de travail impliquées dans un événement de performance"](#)

["Identifier les charges de travail des victimes impliquées dans un événement de performance"](#)

["Identifier les charges de travail des intimidateurs impliqués dans un événement de performance"](#)

["Identifier les charges de travail des requins impliquées dans un événement de performance"](#)

Comprendre les événements et les alertes de performance

Les événements de performances sont des incidents liés aux performances de la charge de travail sur un cluster. Ils vous aident à identifier les charges de travail avec des temps de réponse lents. En plus des événements de santé survenus au même moment, vous pouvez déterminer les problèmes qui pourraient avoir causé ou contribué aux délais de réponse lents.

Lorsque Unified Manager détecte plusieurs occurrences de la même condition d'événement pour le même composant de cluster, il traite toutes les occurrences comme un événement unique et non comme des événements distincts.

Vous pouvez configurer des alertes pour envoyer automatiquement une notification par e-mail lorsque des événements de performances de certains types de gravité se produisent.

Sources d'événements de performance

Les événements de performances sont des problèmes liés aux performances de la charge de travail sur un cluster. Ils vous aident à identifier les objets de stockage avec des temps de réponse lents, également appelés latence élevée. En plus d'autres événements de santé survenus au même moment, vous pouvez déterminer les problèmes qui pourraient avoir causé ou contribué aux délais de réponse lents.

Unified Manager reçoit les événements de performance des sources suivantes :

- **Événements de politique de seuil de performance définis par l'utilisateur**

Problèmes de performances basés sur les valeurs de seuil personnalisées que vous avez définies. Vous configurez des stratégies de seuil de performances pour les objets de stockage (par exemple, les agrégats et les volumes), afin que des événements soient générés lorsqu'une valeur de seuil pour un compteur de performances a été dépassée.

Vous devez définir une politique de seuil de performances et l'attribuer à un objet de stockage pour

recevoir ces événements.

- **Événements de politique de seuil de performance définis par le système**

Problèmes de performances basés sur des valeurs de seuil définies par le système. Ces politiques de seuil sont incluses avec l'installation d'Unified Manager pour couvrir les problèmes de performances courants.

Ces stratégies de seuil sont activées par défaut et vous pouvez voir des événements peu de temps après l'ajout d'un cluster.

- **Événements de seuil de performance dynamique**

Problèmes de performances résultant de pannes ou d'erreurs dans une infrastructure informatique, ou de charges de travail surutilisant les ressources du cluster. La cause de ces événements peut être un problème simple qui se corrige de lui-même au fil du temps ou qui peut être résolu par une réparation ou un changement de configuration. Un événement de seuil dynamique indique que les charges de travail sur un système ONTAP sont lentes en raison d'autres charges de travail avec une utilisation élevée de composants de cluster partagés.

Ces seuils sont activés par défaut et vous pouvez voir des événements après trois jours de collecte de données à partir d'un nouveau cluster.

Types de gravité des événements de performance

Chaque événement de performance est associé à un type de gravité pour vous aider à hiérarchiser les événements qui nécessitent une action corrective immédiate.

- **Critique**

Un événement de performance s'est produit qui pourrait entraîner une interruption de service si des mesures correctives ne sont pas prises immédiatement.

Les événements critiques sont envoyés uniquement à partir de seuils définis par l'utilisateur.

- **Avertissement**

Un compteur de performances pour un objet de cluster est hors de portée normale et doit être surveillé pour s'assurer qu'il n'atteint pas la gravité critique. Les événements de cette gravité n'entraînent pas d'interruption de service et aucune mesure corrective immédiate n'est nécessaire.

Les événements d'avertissement sont envoyés à partir de seuils définis par l'utilisateur, définis par le système ou dynamiques.

- **Information**

L'événement se produit lorsqu'un nouvel objet est découvert ou lorsqu'une action utilisateur est effectuée. Par exemple, lorsqu'un objet de stockage est supprimé ou lorsqu'il y a des modifications de configuration, l'événement avec le type de gravité Information est généré.

Les événements d'information sont envoyés directement depuis ONTAP lorsqu'il détecte un changement de configuration.

Pour plus d'informations, consultez les liens suivants :

- "Que se passe-t-il lorsqu'un événement est reçu"
- "Quelles informations sont contenues dans un e-mail d'alerte"
- "Ajout d'alertes"
- "Ajout d'alertes pour les événements de performance"

Modifications de configuration détectées par Unified Manager

Unified Manager surveille vos clusters pour détecter les modifications de configuration afin de vous aider à déterminer si une modification a pu provoquer ou contribuer à un événement de performances. Les pages de l'Explorateur de performances affichent une icône d'événement de modification (●) pour indiquer la date et l'heure à laquelle le changement a été détecté.

Vous pouvez consulter les graphiques de performances dans les pages de l'Explorateur de performances et dans la page Analyse de la charge de travail pour voir si l'événement de modification a eu un impact sur les performances de l'objet de cluster sélectionné. Si le changement a été détecté au même moment ou à peu près au même moment qu'un événement de performance, le changement a peut-être contribué au problème, ce qui a provoqué le déclenchement de l'alerte d'événement.

Unified Manager peut détecter les événements de changement suivants, classés comme événements informatifs :

- Un volume se déplace entre les agrégats.

Unified Manager peut détecter quand le déplacement est en cours, terminé ou échoué. Si Unified Manager est en panne pendant un déplacement de volume, lorsqu'il est de nouveau opérationnel, il détecte le déplacement de volume et affiche un événement de modification pour celui-ci.

- La limite de débit (Mo/s ou IOPS) d'un groupe de politiques QoS contenant une ou plusieurs charges de travail surveillées change.

La modification d'une limite de groupe de stratégies peut provoquer des pics intermittents de latence (temps de réponse), ce qui peut également déclencher des événements pour le groupe de stratégies. La latence revient progressivement à la normale et tous les événements provoqués par les pics deviennent obsolètes.

- Un nœud d'une paire HA prend en charge ou restitue le stockage de son nœud partenaire.

Unified Manager peut détecter quand l'opération de prise de contrôle, de prise de contrôle partielle ou de restitution a été terminée. Si la prise de contrôle est provoquée par un nœud paniqué, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de restauration ONTAP s'est terminée avec succès.

La version précédente et la nouvelle version sont affichées.

Types de politiques de seuil de performance définies par le système

Unified Manager fournit certaines stratégies de seuil standard qui surveillent les performances du cluster et génèrent automatiquement des événements. Ces stratégies sont activées par défaut et génèrent des événements d'avertissement ou d'information

lorsque les seuils de performances surveillés sont dépassés.



Les stratégies de seuil de performances définies par le système ne sont pas activées sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select .

Si vous recevez des événements inutiles provenant de stratégies de seuil de performances définies par le système, vous pouvez désactiver les événements pour des stratégies individuelles à partir de la page Configuration des événements.

Politiques de seuil de cluster

Les stratégies de seuil de performances de cluster définies par le système sont attribuées, par défaut, à chaque cluster surveillé par Unified Manager :

- **Déséquilibre de charge du cluster**

Identifie les situations dans lesquelles un nœud fonctionne à une charge beaucoup plus élevée que les autres nœuds du cluster, ce qui affecte potentiellement les latences de charge de travail.

Pour ce faire, il compare la valeur de capacité de performance utilisée pour tous les nœuds d'un cluster afin de déterminer si un nœud a dépassé la valeur seuil de 30 % pendant plus de 24 heures. Il s'agit d'un événement d'avertissement.

- **Déséquilibre des capacités du cluster**

Identifie les situations dans lesquelles un agrégat a une capacité utilisée beaucoup plus élevée que les autres agrégats du cluster, affectant ainsi potentiellement l'espace requis pour les opérations.

Cela se fait en comparant la valeur de capacité utilisée pour tous les agrégats du cluster pour voir s'il existe une différence de 70 % entre les agrégats. Il s'agit d'un événement d'avertissement.

Politiques de seuil de nœud

Les stratégies de seuil de performances des nœuds définies par le système sont attribuées, par défaut, à chaque nœud des clusters surveillés par Unified Manager :

- **Seuil de capacité de performance utilisé dépassé**

Identifie les situations dans lesquelles un seul nœud fonctionne au-dessus des limites de son efficacité opérationnelle et affecte donc potentiellement les latences de charge de travail.

Il le fait en recherchant les nœuds qui utilisent plus de 100 % de leur capacité de performance pendant plus de 12 heures. Il s'agit d'un événement d'avertissement.

- **Paire de nœuds HA surutilisée**

Identifie les situations dans lesquelles les nœuds d'une paire HA fonctionnent au-dessus des limites de l'efficacité opérationnelle de la paire HA.

Pour ce faire, il examine la valeur de la capacité de performance utilisée pour les deux nœuds de la paire HA. Si la capacité de performance combinée utilisée par les deux nœuds dépasse 200 % pendant plus de 12 heures, un basculement du contrôleur aura un impact sur les latences de la charge de travail. Il s'agit d'un événement informatif.

• Fragmentation du disque du nœud

Identifie les situations dans lesquelles un ou plusieurs disques d'un agrégat sont fragmentés, ce qui ralentit les services système clés et affecte potentiellement les latences de charge de travail sur un nœud.

Il le fait en examinant certains ratios d'opérations de lecture et d'écriture sur tous les agrégats d'un nœud. Cette politique peut également être déclenchée lors de la resynchronisation de SyncMirror ou lorsque des erreurs sont détectées lors des opérations de nettoyage du disque. Il s'agit d'un événement d'avertissement.



La stratégie « Fragmentation du disque de nœud » analyse les agrégats HDD uniquement ; les agrégats Flash Pool, SSD et FabricPool ne sont pas analysés.

Politiques de seuil global

La stratégie de seuil de performance agrégée définie par le système est attribuée par défaut à chaque agrégat des clusters surveillés par Unified Manager :

• Disques agrégés surutilisés

Identifie les situations dans lesquelles un agrégat fonctionne au-dessus des limites de son efficacité opérationnelle, affectant ainsi potentiellement les latences de charge de travail. Il identifie ces situations en recherchant des agrégats où les disques de l'agrégat sont utilisés à plus de 95 % pendant plus de 30 minutes. Cette politique multicondition effectue ensuite l'analyse suivante pour aider à déterminer la cause du problème :

- Un disque de l'agrégat subit-il actuellement une activité de maintenance en arrière-plan ?

Certaines des activités de maintenance en arrière-plan qu'un disque peut subir sont la reconstruction du disque, le nettoyage du disque, la resynchronisation SyncMirror et la réparation.

- Existe-t-il un goulot d'étranglement des communications dans l'interconnexion Fibre Channel de l'étagère de disques ?
- Y a-t-il trop peu d'espace libre dans l'ensemble ? Un événement d'avertissement est émis pour cette politique uniquement si une (ou plusieurs) des trois politiques subordonnées sont également considérées comme violées. Un événement de performance n'est pas déclenché si seuls les disques de l'ensemble sont utilisés à plus de 95 %.



La stratégie « Disques agrégés surutilisés » analyse les agrégats HDD uniquement et les agrégats Flash Pool (hybrides) ; les agrégats SSD et FabricPool ne sont pas analysés.

Politiques de seuil de latence de la charge de travail

Les stratégies de seuil de latence de charge de travail définies par le système sont attribuées à toute charge de travail disposant d'une stratégie de niveau de service de performances configurée avec une valeur de « latence attendue » définie :

• Seuil de latence du volume de charge de travail/LUN dépassé tel que défini par le niveau de service de performance

Identifie les volumes (partages de fichiers) et les LUN qui ont dépassé leur limite de « latence attendue » et qui affectent les performances de la charge de travail. Il s'agit d'un événement d'avertissement.

Pour ce faire, il recherche les charges de travail qui ont dépassé la valeur de latence attendue pendant 30 % du temps au cours de l'heure précédente.

Politiques de seuil de qualité de service

Les stratégies de seuil de performances QoS définies par le système sont attribuées à toute charge de travail disposant d'une stratégie de débit maximal QoS ONTAP configurée (IOPS, IOPS/To ou Mo/s). Unified Manager déclenche un événement lorsque la valeur de débit de la charge de travail est inférieure de 15 % à la valeur QoS configurée :

- **Seuil QoS Max IOPS ou MB/s**

Identifie les volumes et les LUN qui ont dépassé leur limite maximale d'IOPS ou de débit en Mo/s de QoS et qui affectent la latence de la charge de travail. Il s'agit d'un événement d'avertissement.

Lorsqu'une charge de travail unique est attribuée à un groupe de politiques, elle le fait en recherchant les charges de travail qui ont dépassé le seuil de débit maximal défini dans le groupe de politiques QoS attribué au cours de chaque période de collecte de l'heure précédente.

Lorsque plusieurs charges de travail partagent une même politique QoS, le système le fait en ajoutant les IOPS ou les Mo/s de toutes les charges de travail de la politique et en vérifiant ce total par rapport au seuil.

- **QoS Peak IOPS/To ou IOPS/To avec seuil de taille de bloc**

Identifie les volumes qui ont dépassé leur limite de débit IOPS/To de pointe QoS adaptative (ou IOPS/To avec limite de taille de bloc) et qui affectent la latence de la charge de travail. Il s'agit d'un événement d'avertissement.

Pour ce faire, il convertit le seuil IOPS/To de pointe défini dans la politique QoS adaptative en une valeur IOPS maximale QoS basée sur la taille de chaque volume, puis il recherche les volumes qui ont dépassé le seuil IOPS maximal QoS pendant chaque période de collecte des performances pour l'heure précédente.



Cette politique s'applique aux volumes uniquement lorsque le cluster est installé avec le logiciel ONTAP 9.3 et versions ultérieures.

Lorsque l'élément « taille de bloc » a été défini dans la politique QoS adaptative, le seuil est converti en une valeur maximale QoS en Mo/s en fonction de la taille de chaque volume. Il recherche ensuite les volumes qui ont dépassé le débit maximal QoS en Mo/s au cours de chaque période de collecte des performances de l'heure précédente.



Cette politique s'applique aux volumes uniquement lorsque le cluster est installé avec le logiciel ONTAP 9.5 et versions ultérieures.

Analyse et notification des événements de performance

Les événements de performances vous informent des problèmes de performances d'E/S sur une charge de travail causés par une contention sur un composant de cluster. Unified Manager analyse l'événement pour identifier toutes les charges de travail impliquées, le composant en conflit et si l'événement constitue toujours un problème que vous devrez peut-être résoudre.

Unified Manager surveille la latence d'E/S (temps de réponse) et les IOPS (opérations) des volumes d'un cluster. Lorsque d'autres charges de travail utilisent de manière excessive un composant de cluster, par exemple, le composant est en conflit et ne peut pas fonctionner à un niveau optimal pour répondre aux demandes de charge de travail. Les performances d'autres charges de travail qui utilisent le même composant peuvent être affectées, ce qui entraîne une augmentation de leurs latences. Si la latence dépasse le seuil de performances dynamiques, Unified Manager déclenche un événement de performances pour vous en informer.

Analyse des événements

Unified Manager effectue les analyses suivantes, en utilisant les statistiques de performance des 15 jours précédents, pour identifier les charges de travail des victimes, les charges de travail des intimidateurs et le composant de cluster impliqué dans un événement :

- Identifie les charges de travail victimes dont la latence a dépassé le seuil de performance dynamique, qui est la limite supérieure de la prévision de latence :
 - Pour les volumes sur les agrégats hybrides HDD ou Flash Pool (niveau local), les événements sont déclenchés uniquement lorsque la latence est supérieure à 5 millisecondes (ms) et que les IOPS sont supérieures à 10 opérations par seconde (ops/sec).
 - Pour les volumes sur des agrégats entièrement SSD ou des agrégats FabricPool (niveau cloud), les événements sont déclenchés uniquement lorsque la latence est supérieure à 1 ms et que les IOPS sont supérieures à 100 opérations/s.
- Identifie le composant du cluster en conflit.



Si la latence des charges de travail des victimes au niveau de l'interconnexion du cluster est supérieure à 1 ms, Unified Manager considère cela comme significatif et déclenche un événement pour l'interconnexion du cluster.

- Identifie les charges de travail abusives qui utilisent de manière excessive le composant du cluster et le mettent en conflit.
- Il classe les charges de travail impliquées, en fonction de leur écart dans l'utilisation ou l'activité d'un composant du cluster, pour déterminer quels intimidateurs ont le plus grand changement dans l'utilisation du composant du cluster et quelles victimes sont les plus touchées.

Un événement peut se produire pendant un bref instant, puis se corriger une fois que le composant qu'il utilise n'est plus en conflit. Un événement continu est un événement qui se reproduit pour le même composant du cluster dans un intervalle de cinq minutes et reste dans l'état actif. Pour les événements continus, Unified Manager déclenche une alerte après avoir détecté le même événement pendant deux intervalles d'analyse consécutifs.

Lorsqu'un événement est résolu, il reste disponible dans Unified Manager dans le cadre de l'enregistrement des problèmes de performances passés pour un volume. Chaque événement possède un ID unique qui identifie le type d'événement ainsi que les volumes, le cluster et les composants du cluster impliqués.



Un seul volume peut être impliqué dans plusieurs événements à la fois.

État de l'événement

Les événements peuvent être dans l'un des états suivants :

- **Actif**

Indique que l'événement de performance est actuellement actif (nouveau ou reconnu). Le problème à l'origine de l'événement ne s'est pas corrigé ou n'a pas été résolu. Le compteur de performances de l'objet de stockage reste au-dessus du seuil de performances.

- **Obsolète**

Indique que l'événement n'est plus actif. Le problème à l'origine de l'événement s'est corrigé ou a été résolu. Le compteur de performances de l'objet de stockage n'est plus au-dessus du seuil de performances.

Notification d'événement

Les événements sont affichés sur la page Tableau de bord et sur de nombreuses autres pages de l'interface utilisateur, et les alertes pour ces événements sont envoyées aux adresses e-mail spécifiées. Vous pouvez afficher des informations d'analyse détaillées sur un événement et obtenir des suggestions pour le résoudre sur la page Détails de l'événement et sur la page Analyse de la charge de travail.

Interaction événementielle

Sur la page Détails de l'événement et sur la page Analyse de la charge de travail, vous pouvez interagir avec les événements des manières suivantes :

- En déplaçant la souris sur un événement, un message s'affiche indiquant la date et l'heure à laquelle l'événement a été détecté.

S'il y a plusieurs événements pour la même période, le message indique le nombre d'événements.

- Cliquer sur un seul événement affiche une boîte de dialogue qui présente des informations plus détaillées sur l'événement, y compris les composants du cluster impliqués.

Le composant en litige est entouré et surligné en rouge. Vous pouvez cliquer sur **Afficher l'analyse complète** pour afficher l'analyse complète sur la page Détails de l'événement. S'il existe plusieurs événements pour la même période, la boîte de dialogue affiche les détails sur les trois événements les plus récents. Vous pouvez cliquer sur un événement pour afficher l'analyse de l'événement sur la page Détails de l'événement.

Comment Unified Manager détermine l'impact sur les performances d'un événement

Unified Manager utilise l'écart d'activité, d'utilisation, de débit d'écriture, d'utilisation des composants du cluster ou de latence d'E/S (temps de réponse) pour une charge de travail afin de déterminer le niveau d'impact sur les performances de la charge de travail. Ces informations déterminent le rôle de chaque charge de travail dans l'événement et la manière dont elles sont classées sur la page Détails de l'événement.

Unified Manager compare les dernières valeurs analysées pour une charge de travail à la plage de valeurs attendue (prévision de latence). La différence entre les dernières valeurs analysées et la plage de valeurs attendue identifie les charges de travail dont les performances ont été les plus impactées par l'événement.

Par exemple, supposons qu'un cluster contienne deux charges de travail : la charge de travail A et la charge de travail B. La latence prévue pour la charge de travail A est de 5 à 10 millisecondes par opération (ms/op) et sa latence réelle est généralement d'environ 7 ms/op. La prévision de latence pour la charge de travail B est de 10 à 20 ms/op et sa latence réelle est généralement d'environ 15 ms/op. Les deux charges de travail sont

bien dans les limites de leurs prévisions de latence. En raison d'une contention sur le cluster, la latence des deux charges de travail augmente à 40 ms/op, dépassant le seuil de performances dynamiques, qui correspond aux limites supérieures de la prévision de latence, et déclenchant des événements. L'écart de latence, entre les valeurs attendues et les valeurs supérieures au seuil de performance, pour la charge de travail A est d'environ 33 ms/op, et l'écart pour la charge de travail B est d'environ 25 ms/op. La latence des deux charges de travail atteint 40 ms/op, mais la charge de travail A a eu le plus grand impact sur les performances car elle présentait un écart de latence plus élevé à 33 ms/op.

Sur la page Détails de l'événement, dans la section Diagnostic système, vous pouvez trier les charges de travail en fonction de leur écart d'activité, d'utilisation ou de débit pour un composant de cluster. Vous pouvez également trier les charges de travail par latence. Lorsque vous sélectionnez une option de tri, Unified Manager analyse l'écart d'activité, d'utilisation, de débit ou de latence depuis que l'événement a été détecté par rapport aux valeurs attendues pour déterminer l'ordre de tri de la charge de travail. Pour la latence, les points rouges (●) indiquent un franchissement de seuil de performance par une charge de travail victime, et l'impact ultérieur sur la latence. Chaque point rouge indique un niveau d'écart plus élevé en termes de latence, ce qui vous aide à identifier les charges de travail victimes dont la latence a été la plus impactée par un événement.

Composants de cluster et pourquoi ils peuvent être en conflit

Vous pouvez identifier les problèmes de performances du cluster lorsqu'un composant du cluster entre en conflit. Les performances des charges de travail qui utilisent le composant ralentissent et leur temps de réponse (latence) aux demandes des clients augmente, ce qui déclenche un événement dans Unified Manager.

Un composant en conflit ne peut pas fonctionner à un niveau optimal. Ses performances ont diminué et les performances des autres composants et charges de travail du cluster, appelés *victimes*, pourraient avoir une latence accrue. Pour sortir un composant de la compétition, vous devez réduire sa charge de travail ou augmenter sa capacité à gérer davantage de travail, afin que les performances puissent revenir à des niveaux normaux. Étant donné qu'Unified Manager collecte et analyse les performances de la charge de travail à des intervalles de cinq minutes, il détecte uniquement lorsqu'un composant de cluster est systématiquement surutilisé. Les pics transitoires de surconsommation qui ne durent que peu de temps dans l'intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être en conflit car une ou plusieurs charges de travail sur celui-ci sont en concurrence pour que leurs demandes d'E/S soient satisfaites. D'autres charges de travail sur l'agrégat peuvent être affectées, ce qui entraîne une diminution de leurs performances. Pour réduire la quantité d'activité sur l'agrégat, vous pouvez prendre différentes mesures, telles que déplacer une ou plusieurs charges de travail vers un agrégat ou un nœud moins occupé, afin de réduire la demande de charge de travail globale sur l'agrégat actuel. Pour un groupe de politiques QoS, vous pouvez ajuster la limite de débit ou déplacer les charges de travail vers un autre groupe de politiques, afin que les charges de travail ne soient plus limitées.

Unified Manager surveille les composants de cluster suivants pour vous alerter lorsqu'ils sont en conflit :

- **Réseau**

Représente le temps d'attente des demandes d'E/S par les protocoles réseau externes sur le cluster. Le temps d'attente est le temps passé à attendre que les transactions « transfert prêt » se terminent avant que le cluster puisse répondre à une demande d'E/S. Si le composant réseau est en conflit, cela signifie qu'un temps d'attente élevé au niveau de la couche de protocole a un impact sur la latence d'une ou plusieurs charges de travail.

- **Traitement réseau**

Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre la couche de protocole et le cluster. Le traitement du réseau de gestion des nœuds a peut-être changé depuis la détection de l'événement. Si le composant de traitement réseau est en conflit, cela signifie qu'une utilisation élevée au niveau du nœud de traitement réseau a un impact sur la latence d'une ou plusieurs charges de travail.

Lorsque vous utilisez un cluster All SAN Array dans une configuration active-active, la valeur de latence de traitement réseau s'affiche pour les deux nœuds afin que vous puissiez vérifier que les nœuds partagent la charge de manière égale.

- **Limite QoS Max**

Représente le paramètre de débit maximal (pic) du groupe de politiques de qualité de service (QoS) de stockage attribué à la charge de travail. Si le composant du groupe de stratégies est en conflit, cela signifie que toutes les charges de travail du groupe de stratégies sont limitées par la limite de débit définie, ce qui a un impact sur la latence d'une ou plusieurs de ces charges de travail.

- **Limite QoS minimale**

Représente la latence d'une charge de travail provoquée par le paramètre de débit QoS minimum (attendu) attribué à d'autres charges de travail. Si le minimum de QoS défini sur certaines charges de travail utilise la majorité de la bande passante pour garantir le débit promis, d'autres charges de travail seront limitées et verront plus de latence.

- **Interconnexion de cluster**

Représente les câbles et les adaptateurs avec lesquels les nœuds en cluster sont physiquement connectés. Si le composant d'interconnexion du cluster est en conflit, cela signifie que le temps d'attente élevé pour les demandes d'E/S au niveau de l'interconnexion du cluster a un impact sur la latence d'une ou plusieurs charges de travail.

- *** Data Processing***

Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient la charge de travail. Le nœud gérant le traitement des données peut avoir changé depuis la détection de l'événement. Si le composant de traitement des données est en conflit, cela signifie qu'une utilisation élevée au niveau du nœud de traitement des données a un impact sur la latence d'une ou plusieurs charges de travail.

- **Activation du volume**

Représente le processus qui suit l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1 000 volumes sont actifs, ce processus suit le nombre de volumes critiques qui doivent accéder aux ressources via le nœud en même temps. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques subiront une latence comme indiqué ici.

- *** Ressources MetroCluster ***

Représente les ressources MetroCluster, y compris la NVRAM et les liaisons inter-commutateurs (ISL), utilisées pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster est en conflit, cela signifie que le débit d'écriture est élevé à partir des charges de travail sur le cluster local ou qu'un problème d'intégrité de la liaison affecte la latence d'une ou plusieurs charges de travail sur le cluster local. Si le cluster n'est pas dans une configuration MetroCluster, cette icône ne s'affiche pas.

- **Opérations d'agrégation ou d'agrégation SSD**

Représente l'agrégat de stockage sur lequel les charges de travail s'exécutent. Si le composant agrégé est en conflit, cela signifie qu'une utilisation élevée de l'agrégat a un impact sur la latence d'une ou plusieurs charges de travail. Un agrégat se compose de tous les disques durs, ou d'un mélange de disques durs et de SSD (un agrégat Flash Pool), ou d'un mélange de disques durs et d'un niveau cloud (un agrégat FabricPool). Un « agrégat SSD » se compose de tous les SSD (un agrégat entièrement flash) ou d'un mélange de SSD et d'un niveau cloud (un agrégat FabricPool).

- **Latence du cloud**

Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et le niveau cloud sur lequel les données utilisateur sont stockées. Si le composant de latence du cloud est en conflit, cela signifie qu'une grande quantité de lectures provenant de volumes hébergés sur le niveau cloud a un impact sur la latence d'une ou plusieurs charges de travail.

- **Synchroniser SnapMirror**

Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur du volume principal vers le volume secondaire dans une relation synchrone SnapMirror . Si le composant de synchronisation SnapMirror est en conflit, cela signifie que l'activité des opérations synchrones SnapMirror a un impact sur la latence d'une ou plusieurs charges de travail.

Rôles des charges de travail impliquées dans un événement de performance

Unified Manager utilise des rôles pour identifier l'implication d'une charge de travail dans un événement de performance. Les rôles incluent les victimes, les tyrans et les requins. Une charge de travail définie par l'utilisateur peut être à la fois une victime, un tyran et un requin.

Rôle	Description
Victime	Une charge de travail définie par l'utilisateur dont les performances ont diminué en raison d'autres charges de travail, appelées intimidateurs, qui utilisent de manière excessive un composant de cluster. Seules les charges de travail définies par l'utilisateur sont identifiées comme victimes. Unified Manager identifie les charges de travail des victimes en fonction de leur écart de latence, lorsque la latence réelle, lors d'un événement, a considérablement augmenté par rapport à sa prévision de latence (plage attendue).
Intimidateur	Une charge de travail définie par l'utilisateur ou par le système dont la surutilisation d'un composant de cluster a entraîné une diminution des performances d'autres charges de travail, appelées victimes. Unified Manager identifie les charges de travail malveillantes en fonction de leur écart dans l'utilisation d'un composant de cluster, lorsque l'utilisation réelle, lors d'un événement, a considérablement augmenté par rapport à sa plage d'utilisation prévue.

Rôle	Description
Requin	Une charge de travail définie par l'utilisateur avec l'utilisation la plus élevée d'un composant de cluster par rapport à toutes les charges de travail impliquées dans un événement. Unified Manager identifie les charges de travail des requins en fonction de leur utilisation d'un composant de cluster lors d'un événement.

Les charges de travail sur un cluster peuvent partager de nombreux composants du cluster, tels que les agrégats et le processeur pour le traitement du réseau et des données. Lorsqu'une charge de travail, telle qu'un volume, augmente son utilisation d'un composant de cluster au point que le composant ne peut plus répondre efficacement aux demandes de charge de travail, le composant est en conflit. La charge de travail qui utilise de manière excessive un composant de cluster est un obstacle. Les autres charges de travail qui partagent ces composants et dont les performances sont affectées par l'intimidateur sont les victimes. L'activité des charges de travail définies par le système, telles que la déduplication ou les copies instantanées, peut également dégénérer en « harcèlement ».

Lorsqu'Unified Manager détecte un événement, il identifie toutes les charges de travail et tous les composants de cluster impliqués, y compris les charges de travail malveillantes qui ont provoqué l'événement, le composant de cluster en conflit et les charges de travail victimes dont les performances ont diminué en raison de l'activité accrue des charges de travail malveillantes.



Si Unified Manager ne peut pas identifier les charges de travail malveillantes, il alerte uniquement sur les charges de travail victimes et le composant de cluster impliqué.

Unified Manager peut identifier les charges de travail victimes de charges de travail abusives et également identifier quand ces mêmes charges de travail deviennent des charges de travail abusives. Une charge de travail peut être un obstacle pour elle-même. Par exemple, une charge de travail très performante qui est limitée par une limite de groupe de stratégies entraîne la limitation de toutes les charges de travail du groupe de stratégies, y compris elle-même. Une charge de travail qui est un tyran ou une victime dans un événement de performance en cours peut changer de rôle ou ne plus participer à l'événement.

Gérer les seuils de performance

Les stratégies de seuil de performances vous permettent de déterminer le point auquel Unified Manager génère un événement pour informer les administrateurs système des problèmes susceptibles d'avoir un impact sur les performances de la charge de travail. Ces politiques de seuil sont appelées seuils de performance définis par l'utilisateur.

Cette version prend en charge les seuils de performances définis par l'utilisateur, définis par le système et dynamiques. Grâce à des seuils de performances dynamiques et définis par le système, Unified Manager analyse l'activité de la charge de travail pour déterminer la valeur de seuil appropriée. Avec des seuils définis par l'utilisateur, vous pouvez définir les limites de performances supérieures pour de nombreux compteurs de performances et pour de nombreux objets de stockage.



Les seuils de performances définis par le système et les seuils de performances dynamiques sont définis par Unified Manager et ne sont pas configurables. Si vous recevez des événements inutiles provenant de stratégies de seuil de performances définies par le système, vous pouvez désactiver des stratégies individuelles à partir de la page Configuration des événements.

Comment fonctionnent les politiques de seuil de performance définies par l'utilisateur

Vous définissez des stratégies de seuil de performances sur les objets de stockage (par exemple, sur les agrégats et les volumes) afin qu'un événement puisse être envoyé à l'administrateur de stockage pour informer l'administrateur que le cluster rencontre un problème de performances.

Vous créez une politique de seuil de performances pour un objet de stockage en :

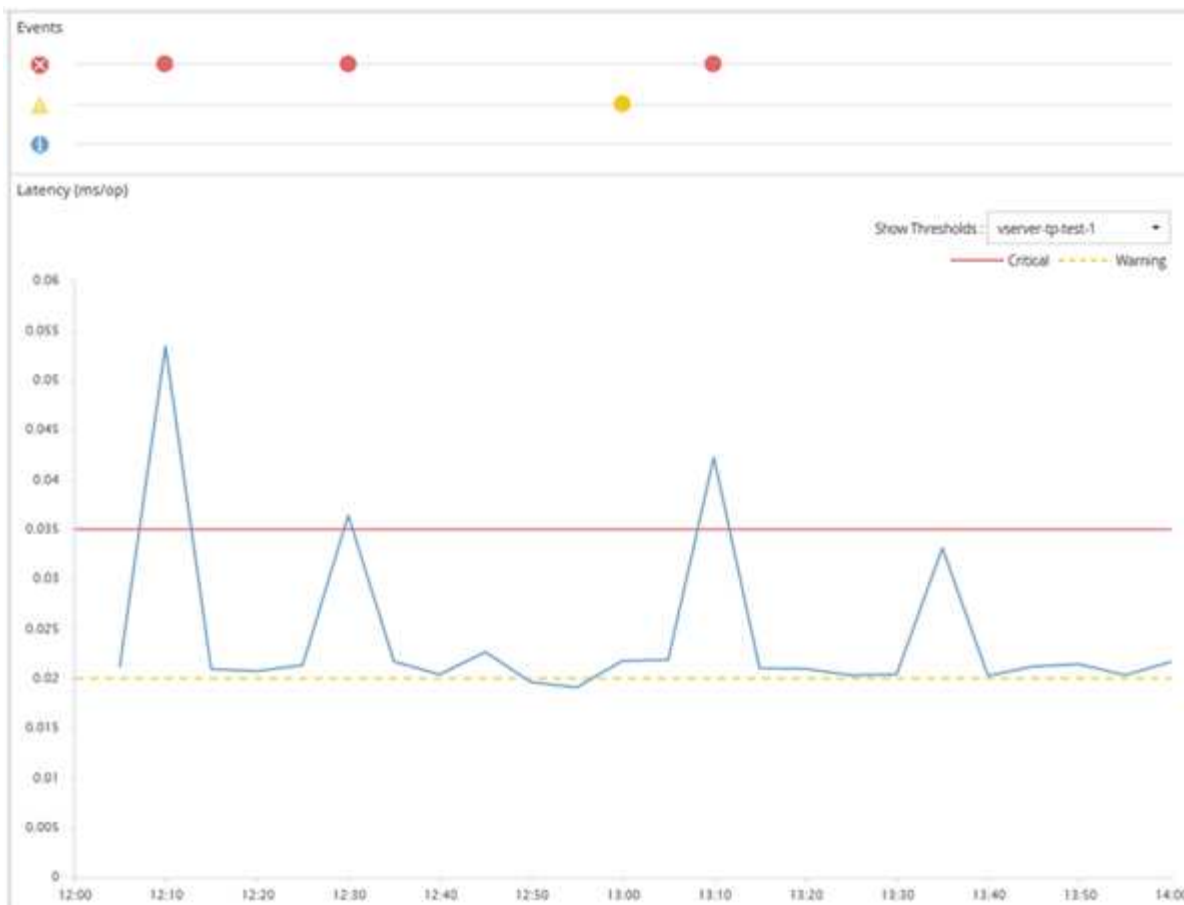
- Sélection d'un objet de stockage
- Sélection d'un compteur de performance associé à cet objet
- Spécification des valeurs qui définissent les limites supérieures du compteur de performances considérées comme des situations d'avertissement et critiques
- Spécifier une période de temps qui définit la durée pendant laquelle le compteur doit dépasser la limite supérieure

Par exemple, vous pouvez définir une stratégie de seuil de performances sur un volume afin de recevoir une notification d'événement critique chaque fois que les IOPS de ce volume dépassent 750 opérations par seconde pendant 10 minutes consécutives. Cette même politique de seuil peut également spécifier qu'un événement d'avertissement doit être envoyé lorsque les IOPS dépassent 500 opérations par seconde pendant 10 minutes.



La version actuelle fournit des seuils qui envoient des événements lorsqu'une valeur de compteur dépasse le paramètre de seuil. Vous ne pouvez pas définir de seuils qui envoient des événements lorsqu'une valeur de compteur tombe en dessous d'un paramètre de seuil.

Un exemple de graphique de compteur est présenté ici, indiquant qu'un seuil d'avertissement (icône jaune) a été franchi à 1h00 et qu'un seuil critique (icône rouge) a été franchi à 12h10, 12h30 et 1h10 :



Un dépassement de seuil doit se produire en continu pendant la durée spécifiée. Si le seuil descend en dessous des valeurs limites pour une raison quelconque, une violation ultérieure est considérée comme le début d'une nouvelle durée.

Certains objets de cluster et compteurs de performances vous permettent de créer une stratégie de seuil combinée qui nécessite que deux compteurs de performances dépassent leurs limites maximales avant qu'un événement ne soit généré. Par exemple, vous pouvez créer une politique de seuil en utilisant les critères suivants :

Objet de cluster	Compteur de performance	Seuil d'alerte	Seuil critique	Durée
Volume	Latence	10 millisecondes	20 millisecondes	15 minutes
Agrégat	Utilisation	65%	85%	

Les stratégies de seuil qui utilisent deux objets de cluster provoquent la génération d'un événement uniquement lorsque les deux conditions sont violées. Par exemple, en utilisant la politique de seuil définie dans le tableau :

Si la latence du volume est moyenne...	Et l'utilisation globale du disque est...	Alors...
15 millisecondes	50%	Aucun événement n'est signalé.

Si la latence du volume est moyenne...	Et l'utilisation globale du disque est...	Alors...
15 millisecondes	75%	Un événement d'avertissement est signalé.
25 millisecondes	75%	Un événement d'avertissement est signalé.
25 millisecondes	90%	Un événement critique est signalé.

Que se passe-t-il lorsqu'une politique de seuil de performance est violée ?

Lorsqu'une valeur de compteur dépasse sa valeur de seuil de performance définie pendant la durée spécifiée dans la durée, le seuil est dépassé et un événement est signalé.

L'événement provoque le lancement des actions suivantes :

- L'événement s'affiche dans le tableau de bord, la page Résumé du cluster de performances, la page Événements et la page Inventaire des performances spécifique à l'objet.
- (facultatif) Une alerte par courrier électronique concernant l'événement peut être envoyée à un ou plusieurs destinataires de courrier électronique, et une interruption SNMP peut être envoyée à un récepteur d'interruption.
- (facultatif) Un script peut être exécuté pour modifier ou mettre à jour automatiquement les objets de stockage.

La première action est toujours exécutée. Vous configurez si les actions facultatives sont exécutées dans la page Configuration des alertes. Vous pouvez définir des actions uniques selon qu'une politique de seuil d'avertissement ou de seuil critique est violée.

Après une violation de la politique de seuil de performances sur un objet de stockage, aucun autre événement n'est généré pour cette politique jusqu'à ce que la valeur du compteur passe en dessous de la valeur de seuil, auquel cas la durée est réinitialisée pour cette limite. Tant que le seuil continue d'être dépassé, l'heure de fin de l'événement est continuellement mise à jour pour refléter le fait que cet événement est en cours.

Un événement de seuil capture ou gèle les informations liées à la gravité et à la définition de la politique afin que des informations de seuil uniques s'affichent avec l'événement, même si la politique de seuil est modifiée à l'avenir.

Quels compteurs de performance peuvent être suivis à l'aide de seuils

Certains compteurs de performances courants, tels que les IOPS et les Mo/s, peuvent avoir des seuils définis pour tous les objets de stockage. Il existe d'autres compteurs qui peuvent avoir des seuils définis uniquement pour certains objets de stockage.

Compteurs de performances disponibles

Objet de stockage	Compteur de performance	Description
Cluster	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le cluster par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis ce cluster par seconde.	Nœud
Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le nœud par seconde.	Mo/s
Nombre moyen de mégaoctets de données transférés vers et depuis ce nœud par seconde.	Latence	Nombre moyen de millisecondes nécessaires au nœud pour répondre aux demandes d'application.
Utilisation	Pourcentage moyen du processeur et de la RAM du nœud qui sont utilisés.	Capacité de performance utilisée
Pourcentage moyen de la capacité de performance consommée par le nœud.	Capacité de performance utilisée - Reprise	Pourcentage moyen de la capacité de performance consommée par le nœud, plus la capacité de performance de son nœud partenaire.
Agrégat	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par l'agrégat par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis cet agrégat par seconde.	Latence
Nombre moyen de millisecondes nécessaires à l'agrégat pour répondre aux demandes d'application.	Utilisation	Pourcentage moyen des disques de l'agrégat qui sont utilisés.
Capacité de performance utilisée	Pourcentage moyen de la capacité de performance consommée par l'agrégat.	Machine virtuelle de stockage
Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le SVM par seconde.	Mo/s

Objet de stockage	Compteur de performance	Description
Nombre moyen de mégaoctets de données transférés vers et depuis ce SVM par seconde.	Latence	Nombre moyen de millisecondes nécessaires au SVM pour répondre aux demandes d'application.
Volume	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le volume par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis ce volume par seconde.	Latence
Nombre moyen de millisecondes nécessaires au volume pour répondre aux demandes d'application.	Taux d'échec de cache	Pourcentage moyen de demandes de lecture provenant d'applications clientes renvoyées depuis le volume au lieu d'être renvoyées depuis le cache.
LUN	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le LUN par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis ce LUN par seconde.	Latence
Nombre moyen de millisecondes nécessaires au LUN pour répondre aux demandes d'application.	Espace de noms	Op E/S par sec
Nombre moyen d'opérations d'entrée/sortie traitées par l'espace de noms par seconde.	Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis cet espace de noms par seconde.
Latence	Nombre moyen de millisecondes nécessaires à l'espace de noms pour répondre aux demandes d'application.	Port
Utilisation de la bande passante	Pourcentage moyen de la bande passante disponible du port qui est utilisée.	Mo/s
Nombre moyen de mégaoctets de données transférés vers et depuis ce port par seconde.	Interface réseau (LIF)	Mo/s

Quels objets et compteurs peuvent être utilisés dans les politiques de seuil combinées

Seuls certains compteurs de performances peuvent être utilisés ensemble dans les stratégies combinées. Lorsque des compteurs de performances primaires et secondaires sont spécifiés, les deux compteurs de performances doivent dépasser leurs limites maximales avant qu'un événement ne soit généré.

Objet de stockage principal et compteur	Objet de stockage secondaire et compteur
Latence du volume	IOPS du volume
Volume Mo/s	Utilisation globale
Capacité de performance globale utilisée	Utilisation des nœuds
Capacité de performance du nœud utilisée	Capacité de performance du nœud utilisée - Prise de contrôle
Latence LUN	IOPS LUN
Mo/s de LUN	Utilisation globale
Capacité de performance globale utilisée	Utilisation des nœuds
Capacité de performance du nœud utilisée	Capacité de performance du nœud utilisée - Prise de contrôle



Lorsqu'une stratégie de combinaison de volumes est appliquée à un volume FlexGroup, au lieu d'un FlexVol volume, seuls les attributs « Volume IOPS » et « Volume MB/s » peuvent être sélectionnés comme compteur secondaire. Si la politique de seuil contient l'un des attributs de nœud ou d'agrégat, la politique ne sera pas appliquée au volume FlexGroup et vous recevrez un message d'erreur décrivant ce cas. Cela est dû au fait que les volumes FlexGroup peuvent exister sur plusieurs nœuds ou agrégats.

Créer des politiques de seuil de performance définies par l'utilisateur

Vous créez des stratégies de seuil de performances pour les objets de stockage afin que des notifications soient envoyées lorsqu'un compteur de performances dépasse une valeur spécifique. La notification d'événement identifie que le cluster rencontre un problème de performances.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Vous créez des stratégies de seuil de performances en saisissant les valeurs de seuil sur la page Créer une stratégie de seuil de performances. Vous pouvez créer de nouvelles politiques en définissant toutes les valeurs de politique dans cette page, ou vous pouvez faire une copie d'une politique existante et modifier les valeurs

dans la copie (appelé *clonage*).

Les valeurs de seuil valides sont comprises entre 0,001 et 10 000 000 pour les nombres, entre 0,001 et 100 pour les pourcentages et entre 0,001 et 200 pour les pourcentages de capacité de performance utilisée.



La version actuelle fournit des seuils qui envoient des événements lorsqu'une valeur de compteur dépasse le paramètre de seuil. Vous ne pouvez pas définir de seuils qui envoient des événements lorsqu'une valeur de compteur tombe en dessous d'un paramètre de seuil.

Étapes

- 1. Dans le volet de navigation de gauche, sélectionnez **Seuils d'événement > Performances**.

La page Seuils de performance s'affiche.

- 2. Cliquez sur le bouton approprié selon que vous souhaitez créer une nouvelle politique ou cloner une politique similaire et modifier la version clonée.

À...	Cliquez...
Créer une nouvelle politique	Créer
Cloner une politique existante	Sélectionnez une politique existante et cliquez sur Cloner

La page Créer une politique de seuil de performances ou Cloner une politique de seuil de performances s'affiche.

- 3. Définissez la politique de seuil en spécifiant les valeurs de seuil du compteur de performances que vous souhaitez définir pour des objets de stockage spécifiques :
 - a. Sélectionnez le type d'objet de stockage et spécifiez un nom et une description pour la politique.
 - b. Sélectionnez le compteur de performances à suivre et spécifiez les valeurs limites qui définissent les événements d'avertissement et critiques.

Vous devez définir au moins un avertissement ou une limite critique. Vous n'avez pas besoin de définir les deux types de limites.

- c. Sélectionnez un compteur de performances secondaire, si nécessaire, et spécifiez les valeurs limites pour les événements d'avertissement et critiques.

L'inclusion d'un compteur secondaire nécessite que les deux compteurs dépassent les valeurs limites avant que le seuil ne soit dépassé et qu'un événement ne soit signalé. Seuls certains objets et compteurs peuvent être configurés à l'aide d'une politique de combinaison.

- d. Sélectionnez la durée pendant laquelle les valeurs limites doivent être dépassées pour qu'un événement soit envoyé.

Lors du clonage d'une politique existante, vous devez saisir un nouveau nom pour la politique.

- 4. Cliquez sur **Enregistrer** pour enregistrer la politique.

Vous êtes renvoyé à la page Seuils de performance. Un message de réussite en haut de la page confirme que la stratégie de seuil a été créée et fournit un lien vers la page Inventaire pour ce type d'objet afin que

vous puissiez appliquer immédiatement la nouvelle stratégie aux objets de stockage.

Si vous souhaitez appliquer la nouvelle politique de seuil aux objets de stockage à ce stade, vous pouvez cliquer sur le lien **Accéder au type d'objet maintenant** pour accéder à la page Inventaire.

Attribuer des politiques de seuil de performance aux objets de stockage

Vous attribuez une stratégie de seuil de performances définie par l'utilisateur à un objet de stockage afin qu'Unified Manager signale un événement si la valeur du compteur de performances dépasse le paramètre de stratégie.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

La ou les politiques de seuil de performances que vous souhaitez appliquer à l'objet doivent exister.

Vous ne pouvez appliquer qu'une seule politique de performances à la fois à un objet ou à un groupe d'objets.

Vous pouvez attribuer un maximum de trois stratégies de seuil à chaque objet de stockage. Lors de l'attribution de politiques à plusieurs objets, si l'un des objets dispose déjà du nombre maximal de politiques attribuées, Unified Manager exécute les actions suivantes :

- Applique la politique à tous les objets sélectionnés qui n'ont pas atteint leur maximum
- Ignore les objets qui ont atteint le nombre maximal de politiques
- Affiche un message indiquant que la politique n'a pas été attribuée à tous les objets

Étapes

1. À partir de la page d'inventaire des performances de n'importe quel objet de stockage, sélectionnez l'objet ou les objets auxquels vous souhaitez attribuer une politique de seuil :

Pour attribuer des seuils à...	Cliquez...
Un seul objet	La case à cocher à gauche de cet objet.
Plusieurs objets	La case à cocher à gauche de chaque objet.
Tous les objets sur la page	Le ☐ liste déroulante et choisissez Sélectionner tous les objets sur cette page.
Tous les objets du même type	Le ☐ liste déroulante et choisissez Sélectionner tous les objets.

Vous pouvez utiliser la fonctionnalité de tri et de filtrage pour affiner la liste des objets sur la page d'inventaire afin de faciliter l'application de politiques de seuil à de nombreux objets.

2. Faites votre sélection, puis cliquez sur **Attribuer une stratégie de seuil de performance.**

La page Attribuer une stratégie de seuil de performances s'affiche, affichant une liste des stratégies de seuil qui existent pour ce type spécifique d'objet de stockage.

3. Cliquez sur chaque politique pour afficher les détails des paramètres de seuil de performances afin de vérifier que vous avez sélectionné la politique de seuil correcte.
4. Après avoir sélectionné la politique de seuil appropriée, cliquez sur **Attribuer une politique**.

Un message de réussite en haut de la page confirme que la stratégie de seuil a été attribuée à l'objet ou aux objets et fournit un lien vers la page Alerte afin que vous puissiez configurer les paramètres d'alerte pour cet objet et cette stratégie.

Si vous souhaitez que des alertes soient envoyées par courrier électronique ou sous forme d'interruption SNMP pour vous avertir qu'un événement de performance particulier a été généré, vous devez configurer les paramètres d'alerte dans la page Configuration des alertes.

Afficher les politiques de seuil de performance

Vous pouvez afficher toutes les stratégies de seuil de performances actuellement définies à partir de la page Seuils de performances.

La liste des stratégies de seuil est triée par ordre alphabétique par nom de stratégie et inclut des stratégies pour tous les types d'objets de stockage. Vous pouvez cliquer sur un en-tête de colonne pour trier les politiques par cette colonne. Si vous recherchez une politique spécifique, utilisez les mécanismes de filtrage et de recherche pour affiner la liste des politiques de seuil qui apparaissent dans la liste d'inventaire.

Vous pouvez passer votre curseur sur le nom de la politique et le nom de la condition pour voir les détails de configuration de la politique. De plus, vous pouvez utiliser les boutons fournis pour créer, cloner, modifier et supprimer des stratégies de seuil définies par l'utilisateur.

Étape

1. Dans le volet de navigation de gauche, sélectionnez **Seuils d'événement > Performances**.

La page Seuils de performance s'affiche.

Modifier les politiques de seuil de performance définies par l'utilisateur

Vous pouvez modifier les paramètres de seuil pour les stratégies de seuil de performances existantes. Cela peut être utile si vous constatez que vous recevez trop ou trop peu d'alertes pour certaines conditions de seuil.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Vous ne pouvez pas modifier le nom de la politique ni le type d'objet de stockage surveillé pour les politiques de seuil existantes.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Seuils d'événement > Performances**.

La page Seuils de performance s'affiche.

2. Sélectionnez la politique de seuil que vous souhaitez modifier et cliquez sur **Modifier**.

La page Modifier la politique de seuil de performance s'affiche.

3. Apportez vos modifications à la politique de seuil et cliquez sur **Enregistrer**.

Vous êtes renvoyé à la page Seuils de performance.

Une fois enregistrées, les modifications sont immédiatement mises à jour sur tous les objets de stockage qui utilisent la politique.

Selon le type de modifications que vous avez apportées à la stratégie, vous souhaitez peut-être vérifier les paramètres d'alerte configurés pour les objets qui utilisent la stratégie dans la page Configuration des alertes.

Supprimer les politiques de seuil de performance des objets de stockage

Vous pouvez supprimer une stratégie de seuil de performances définie par l'utilisateur d'un objet de stockage lorsque vous ne souhaitez plus qu'Unified Manager surveille la valeur du compteur de performances.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Vous ne pouvez supprimer qu'une seule politique à la fois d'un objet sélectionné.

Vous pouvez supprimer une politique de seuil de plusieurs objets de stockage en sélectionnant plusieurs objets dans la liste.

Étapes

1. À partir de la page **inventaire** de n'importe quel objet de stockage, sélectionnez un ou plusieurs objets auxquels au moins une stratégie de seuil de performances est appliquée.

Pour effacer les seuils de...	Fais ceci...
Un seul objet	Cochez la case à gauche de cet objet.
Plusieurs objets	Cochez la case à gauche de chaque objet.
Tous les objets sur la page	Cliquez  dans l'en-tête de la colonne.

2. Cliquez sur **Effacer la politique de seuil de performance**.

La page Effacer la politique de seuil s'affiche, présentant une liste des politiques de seuil actuellement attribuées aux objets de stockage.

3. Sélectionnez la politique de seuil que vous souhaitez supprimer des objets et cliquez sur **Effacer la politique**.

Lorsque vous sélectionnez une politique de seuil, les détails de la politique s'affichent afin que vous puissiez confirmer que vous avez sélectionné la politique appropriée.

Que se passe-t-il lorsqu'une politique de seuil de performance est modifiée

Si vous ajustez la valeur du compteur ou la durée d'une stratégie de seuil de

performances existante, la modification de stratégie est appliquée à tous les objets de stockage qui utilisent la stratégie. Le nouveau paramètre s'applique immédiatement et Unified Manager commence à comparer les valeurs des compteurs de performances aux nouveaux paramètres de seuil pour toutes les données de performances nouvellement collectées.

Si des événements actifs existent pour les objets qui utilisent la stratégie de seuil modifiée, les événements sont marqués comme obsolètes et la stratégie de seuil commence à surveiller le compteur en tant que stratégie de seuil nouvellement définie.

Lors de la visualisation du compteur sur lequel le seuil a été appliqué dans la vue détaillée des graphiques de compteur, les lignes de seuil critique et d'avertissement reflètent les paramètres de seuil actuels. Les paramètres de seuil d'origine n'apparaissent pas sur cette page, même si vous consultez les données historiques lorsque l'ancien paramètre de seuil était en vigueur.



Étant donné que les anciens paramètres de seuil n'apparaissent pas dans la vue détaillée des graphiques de compteur, vous pouvez voir des événements historiques qui apparaissent sous les lignes de seuil actuelles.

Qu'advient-il des politiques de seuil de performance lorsqu'un objet est déplacé ?

Étant donné que les stratégies de seuil de performances sont attribuées aux objets de stockage, si vous déplacez un objet, toutes les stratégies de seuil attribuées restent attachées à l'objet une fois le déplacement terminé. Par exemple, si vous déplacez un volume ou un LUN vers un autre agrégat, les stratégies de seuil restent actives pour le volume ou le LUN sur le nouvel agrégat.

Si une condition de compteur secondaire existe pour la stratégie de seuil (une stratégie de combinaison) (par exemple, si une condition supplémentaire est attribuée à un agrégat ou à un nœud), la condition de compteur secondaire est appliquée au nouvel agrégat ou nœud vers lequel le volume ou le LUN a été déplacé.

Si de nouveaux événements actifs existent pour les objets qui utilisent la stratégie de seuil modifiée, les événements sont marqués comme obsolètes et la stratégie de seuil commence à surveiller le compteur en tant que stratégie de seuil nouvellement définie.

Une opération de déplacement de volume amène ONTAP à envoyer un événement de modification d'information. Une icône d'événement de modification apparaît dans la chronologie des événements sur la page Explorateur de performances et la page Analyse de la charge de travail pour indiquer l'heure à laquelle l'opération de déplacement a été terminée.



Si vous déplacez un objet vers un autre cluster, la stratégie de seuil définie par l'utilisateur est supprimée de l'objet. Si nécessaire, vous devez attribuer une politique de seuil à l'objet une fois l'opération de déplacement terminée. Cependant, les politiques de seuil dynamiques et définies par le système sont appliquées automatiquement à un objet après son déplacement vers un nouveau cluster.

Fonctionnalité de la politique de seuil lors de la prise de contrôle et de la restitution de HA

Lorsqu'une opération de prise de contrôle ou de restitution se produit dans une configuration à haute disponibilité (HA), les objets déplacés d'un nœud à l'autre conservent leurs politiques de seuil de la même manière que dans les opérations de déplacement manuel. Étant donné qu'Unified Manager vérifie les

modifications de configuration du cluster toutes les 15 minutes, l'impact du basculement vers le nouveau nœud n'est pas identifié avant la prochaine interrogation de la configuration du cluster.



Si une opération de prise de contrôle et de restitution se produit au cours de la période de collecte des modifications de configuration de 15 minutes, il est possible que vous ne voyiez pas les statistiques de performances passer d'un nœud à l'autre.

Fonctionnalité de la politique de seuil lors de la relocalisation globale

Si vous déplacez un agrégat d'un nœud à un autre à l'aide de la `aggregate relocation start` commande, les politiques de seuil simples et combinées sont conservées sur tous les objets et la partie nœud de la politique de seuil est appliquée au nouveau nœud.

Fonctionnalité de la politique de seuil lors du basculement de MetroCluster

Les objets qui se déplacent d'un cluster à un autre dans une configuration MetroCluster ne conservent pas leurs paramètres de stratégie de seuil définis par l'utilisateur. Si nécessaire, vous pouvez appliquer des stratégies de seuil sur les volumes et les LUN qui ont été déplacés vers le cluster partenaire. Une fois qu'un objet est revenu à son cluster d'origine, la politique de seuil définie par l'utilisateur est réappliquée automatiquement.

Pour plus d'informations, voir ["Comportement du volume lors du basculement et du retour en arrière"](#).

Analyser les événements de performance

Vous pouvez analyser les événements de performances pour identifier quand ils ont été détectés, s'ils sont actifs (nouveaux ou reconnus) ou obsolètes, les charges de travail et les composants de cluster impliqués, ainsi que les options permettant de résoudre les événements par vous-même.

Afficher des informations sur les événements de performance

Vous pouvez utiliser la page d'inventaire Gestion des événements pour afficher une liste de tous les événements de performances sur les clusters surveillés par Unified Manager. En consultant ces informations, vous pouvez déterminer les événements les plus critiques, puis accéder aux informations détaillées pour déterminer la cause de l'événement.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

La liste des événements est triée par heure détectée, les événements les plus récents étant répertoriés en premier. Vous pouvez cliquer sur un en-tête de colonne pour trier les événements en fonction de cette colonne. Par exemple, vous pouvez trier par colonne Statut pour afficher les événements par gravité. Si vous recherchez un événement spécifique, ou un type d'événement spécifique, vous pouvez utiliser les mécanismes de filtrage et de recherche pour affiner la liste des événements qui apparaissent dans la liste.

Les événements de toutes les sources sont affichés sur cette page :

- Politique de seuil de performance définie par l'utilisateur

- Politique de seuil de performance définie par le système
- Seuil de performance dynamique

La colonne Type d'événement répertorie la source de l'événement. Vous pouvez sélectionner un événement pour afficher les détails de l'événement dans la page Détails de l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans le menu Affichage, sélectionnez **Événements de performance actifs**.

La page affiche tous les événements de performance nouveaux et reconnus qui ont été générés au cours des 7 derniers jours.

3. Localisez un événement que vous souhaitez analyser et cliquez sur le nom de l'événement.

La page des détails de l'événement s'affiche.



Vous pouvez également afficher la page de détails d'un événement en cliquant sur le lien du nom de l'événement à partir de la page Performance Explorer et d'un e-mail d'alerte.

Analyser les événements à partir de seuils de performance définis par l'utilisateur

Les événements générés à partir de seuils définis par l'utilisateur indiquent qu'un compteur de performances pour un certain objet de stockage, par exemple un agrégat ou un volume, a dépassé le seuil que vous avez défini dans la stratégie. Cela indique que l'objet du cluster rencontre un problème de performances.

Vous utilisez la page Détails de l'événement pour analyser l'événement de performance et prendre des mesures correctives, si nécessaire, pour ramener les performances à la normale.

Répondre aux événements de seuil de performance définis par l'utilisateur

Vous pouvez utiliser Unified Manager pour examiner les événements de performances causés par un compteur de performances dépassant un seuil d'avertissement ou critique défini par l'utilisateur. Vous pouvez également utiliser Unified Manager pour vérifier l'intégrité du composant du cluster afin de voir si les événements d'intégrité récents détectés sur le composant ont contribué à l'événement de performance.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux ou obsolètes.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Consultez la **Description**, qui décrit la violation de seuil qui a provoqué l'événement.

Par exemple, le message « Une valeur de latence de 456 ms/op a déclenché un événement d'AVERTISSEMENT basé sur un paramètre de seuil de 400 ms/op » indique qu'un événement d'avertissement de latence s'est produit pour l'objet.

3. Passez votre curseur sur le nom de la politique pour afficher les détails sur la politique de seuil qui a déclenché l'événement.

Cela inclut le nom de la politique, le compteur de performances évalué, la valeur du compteur qui doit être dépassée pour être considérée comme un événement critique ou d'avertissement et la durée pendant laquelle le compteur doit dépasser la valeur.

4. Notez l'**heure de déclenchement de l'événement** afin de pouvoir déterminer si d'autres événements auraient pu se produire au même moment et auraient pu contribuer à cet événement.
5. Suivez l'une des options ci-dessous pour enquêter davantage sur l'événement, afin de déterminer si vous devez effectuer des actions pour résoudre le problème de performances :

Option	Mesures d'enquête possibles
Cliquez sur le nom de l'objet source pour afficher la page de l'Explorateur pour cet objet.	Cette page vous permet d'afficher les détails de l'objet et de comparer cet objet avec d'autres objets de stockage similaires pour voir si d'autres objets de stockage présentent un problème de performances à peu près au même moment. Par exemple, pour voir si d'autres volumes du même agrégat rencontrent également un problème de performances.
Cliquez sur le nom du cluster pour afficher la page Résumé du cluster.	Cette page vous permet d'afficher les détails du cluster sur lequel réside cet objet pour voir si d'autres problèmes de performances se sont produits à peu près au même moment.

Analyser les événements à partir des seuils de performance définis par le système

Les événements générés à partir de seuils de performances définis par le système indiquent qu'un compteur de performances, ou un ensemble de compteurs de performances, pour un certain objet de stockage a franchi le seuil d'une politique définie par le système. Cela indique que l'objet de stockage, par exemple un agrégat ou un nœud, rencontre un problème de performances.

Vous utilisez la page Détails de l'événement pour analyser l'événement de performance et prendre des mesures correctives, si nécessaire, pour ramener les performances à la normale.



Les stratégies de seuil définies par le système ne sont pas activées sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select .

Répondre aux événements de seuil de performance définis par le système

Vous pouvez utiliser Unified Manager pour enquêter sur les événements de performances provoqués par un compteur de performances dépassant un seuil d'avertissement défini par le système. Vous pouvez également utiliser Unified Manager pour vérifier l'intégrité du composant du cluster afin de voir si les événements récents détectés sur le composant ont contribué à l'événement de performance.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux ou obsolètes.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Consultez la **Description**, qui décrit la violation de seuil qui a provoqué l'événement.

Par exemple, le message « La valeur d'utilisation du nœud de 90 % a déclenché un événement d'AVERTISSEMENT basé sur un paramètre de seuil de 85 % » indique qu'un événement d'avertissement d'utilisation du nœud s'est produit pour l'objet de cluster.

3. Notez l'**heure de déclenchement de l'événement** afin de pouvoir déterminer si d'autres événements auraient pu se produire au même moment et auraient pu contribuer à cet événement.
4. Sous **Diagnostic système**, examinez la brève description du type d'analyse que la stratégie définie par le système exécute sur l'objet de cluster.

Pour certains événements, une icône verte ou rouge s'affiche à côté du diagnostic pour indiquer si un problème a été détecté dans ce diagnostic particulier. Pour les autres types d'événements définis par le système, les graphiques de compteurs affichent les performances de l'objet.

5. Sous **Actions suggérées**, cliquez sur le lien **Aidez-moi à faire ceci** pour afficher les actions suggérées que vous pouvez effectuer pour essayer de résoudre l'événement de performance par vous-même.

Répondre aux événements de performance du groupe de politiques QoS

Unified Manager génère des événements d'avertissement de politique QoS lorsque le débit de la charge de travail (IOPS, IOPS/To ou MBps) a dépassé le paramètre de politique QoS ONTAP défini et que la latence de la charge de travail est affectée. Ces événements définis par le système offrent la possibilité de corriger les problèmes de performances potentiels avant que de nombreuses charges de travail ne soient affectées par la latence.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Unified Manager génère des événements d'avertissement pour les violations de la politique QoS lorsque le débit de la charge de travail a dépassé le paramètre de politique QoS défini au cours de chaque période de collecte des performances de l'heure précédente. Le débit de la charge de travail peut dépasser le seuil QoS pendant une courte période uniquement au cours de chaque période de collecte, mais Unified Manager affiche uniquement le débit « moyen » pendant la période de collecte sur le graphique. Pour cette raison, vous pouvez recevoir des événements QoS alors que le débit d'une charge de travail n'a peut-être pas dépassé le seuil de stratégie indiqué dans le graphique.

Vous pouvez utiliser le Gestionnaire système ou les commandes ONTAP pour gérer les groupes de stratégies, y compris les tâches suivantes :

- Création d'un nouveau groupe de politiques pour la charge de travail
- Ajout ou suppression de charges de travail dans un groupe de stratégies

- Déplacer une charge de travail entre des groupes de stratégies
- Modification de la limite de débit d'un groupe de politiques
- Déplacer une charge de travail vers un autre agrégat ou nœud

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Consultez la **Description**, qui décrit la violation de seuil qui a provoqué l'événement.

Par exemple, le message « Une valeur IOPS de 1 352 IOPS sur vol1_NFS1 a déclenché un événement d'AVERTISSEMENT pour identifier des problèmes de performances potentiels pour la charge de travail » indique qu'un événement QoS Max IOPS s'est produit sur le volume vol1_NFS1.

3. Consultez la section **Informations sur l'événement** pour voir plus de détails sur le moment où l'événement s'est produit et sur la durée pendant laquelle il a été actif.

De plus, pour les volumes ou les LUN qui partagent le débit d'une stratégie QoS, vous pouvez voir les noms des trois principales charges de travail qui consomment le plus d'IOPS ou de MBps.

4. Dans la section **Diagnostic du système**, examinez les deux graphiques : un pour le nombre total moyen d'IOPS ou de MBps (selon l'événement) et un pour la latence. En les organisant de cette manière, vous pouvez voir quels composants du cluster affectent le plus la latence lorsque la charge de travail approche la limite maximale de QoS.

Pour un événement de politique QoS partagé, les trois principales charges de travail sont affichées dans le graphique de débit. Si plus de trois charges de travail partagent la politique QoS, les charges de travail supplémentaires sont ajoutées ensemble dans une catégorie « Autres charges de travail ». De plus, le graphique de latence indique la latence moyenne sur toutes les charges de travail qui font partie de la politique QoS.

Notez que pour les événements de politique QoS adaptative, les graphiques IOPS et MBps affichent les valeurs IOPS ou MBps ONTAP converties à partir de la politique de seuil IOPS/To attribuée en fonction de la taille du volume.

5. Dans la section **Actions suggérées**, examinez les suggestions et déterminez les actions à effectuer pour éviter une augmentation de la latence de la charge de travail.

Si nécessaire, cliquez sur le bouton **Aide** pour afficher plus de détails sur les actions suggérées que vous pouvez effectuer pour essayer de résoudre l'événement de performance.

Comprendre les événements à partir de politiques QoS adaptatives qui ont une taille de bloc définie

Les groupes de politiques QoS adaptatifs adaptent automatiquement un plafond ou un plancher de débit en fonction de la taille du volume, en maintenant le rapport entre les IOPS et les To lorsque la taille du volume change. À partir d'ONTAP 9.5, vous pouvez spécifier la taille du bloc dans la politique QoS pour appliquer efficacement un seuil Mo/s en même temps.

L'attribution d'un seuil IOPS dans une politique QoS adaptative limite uniquement le nombre d'opérations qui se produisent dans chaque charge de travail. En fonction de la taille de bloc définie sur le client qui génère les charges de travail, certaines IOPS incluent beaucoup plus de données et placent donc une charge beaucoup plus importante sur les nœuds qui traitent les opérations.

La valeur Mo/s pour une charge de travail est générée à l'aide de la formule suivante :

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

Si une charge de travail atteint en moyenne 3 000 IOPS et que la taille de bloc sur le client est définie sur 32 Ko, le débit en Mo/s effectif pour cette charge de travail est de 96. Si cette même charge de travail a une moyenne de 3 000 IOPS et que la taille du bloc sur le client est définie sur 48 Ko, le débit en Mo/s effectif pour cette charge de travail est de 144. Vous pouvez voir que le nœud traite 50 % de données en plus lorsque la taille du bloc est plus grande.

Examinons la politique QoS adaptative suivante qui a une taille de bloc définie et comment les événements sont déclenchés en fonction de la taille de bloc définie sur le client.

Créez une politique et définissez le débit maximal sur 2 500 IOPS/To avec une taille de bloc de 32 Ko. Cela définit effectivement le seuil Mo/s à 80 Mo/s $((2500 \text{ IOPS} * 32 \text{ Ko}) / 1000)$ pour un volume avec une capacité utilisée de 1 To. Notez que Unified Manager génère un événement d'avertissement lorsque la valeur de débit est inférieure de 10 % au seuil défini. Les événements sont générés dans les situations suivantes :

Capacité utilisée	L'événement est généré lorsque le débit dépasse ce nombre de ...	
	Op E/S par sec	Mo/s
1 To	2 250 IOPS	72 Mo/s
2 To	4 500 IOPS	144 Mo/s
5 To	11 250 IOPS	360 Mo/s

Si le volume utilise 2 To d'espace disponible, que les IOPS sont de 4 000 et que la taille du bloc QoS est définie sur 32 Ko sur le client, le débit Mo/s est de 128 Mo/s $((4\,000 \text{ IOPS} * 32 \text{ Ko}) / 1\,000)$. Aucun événement n'est généré dans ce scénario car 4 000 IOPS et 128 Mo/s sont inférieurs au seuil pour un volume qui utilise 2 To d'espace.

Si le volume utilise 2 To d'espace disponible, que les IOPS sont de 4 000 et que la taille du bloc QoS est définie sur 64 Ko sur le client, le débit en Mo/s est de 256 Mo/s $((4\,000 \text{ IOPS} * 64 \text{ Ko}) / 1\,000)$. Dans ce cas, les 4 000 IOPS ne génèrent pas d'événement, mais la valeur Mo/s de 256 Mo/s est supérieure au seuil de 144 Mo/s et un événement est généré.

Pour cette raison, lorsqu'un événement est déclenché en fonction d'une violation de Mo/s pour une politique de QoS adaptative qui inclut la taille du bloc, un graphique Mo/s s'affiche dans la section Diagnostic système de la page Détails de l'événement. Si l'événement est déclenché en raison d'une violation d'IOPS pour la politique QoS adaptative, un graphique IOPS s'affiche dans la section Diagnostic système. Si une violation se produit à la fois pour les IOPS et les MB/s, vous recevrez deux événements.

Pour plus d'informations sur le réglage des paramètres QoS, consultez ["Aperçu de la gestion des performances"](#) .

Répondre aux événements de performances surutilisés des ressources des nœuds

Unified Manager génère des événements d'avertissement de surutilisation des ressources de nœud lorsqu'un seul nœud fonctionne au-dessus des limites de son

efficacité opérationnelle, ce qui affecte potentiellement les latences de charge de travail. Ces événements définis par le système offrent la possibilité de corriger les problèmes de performances potentiels avant que de nombreuses charges de travail ne soient affectées par la latence.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux ou obsolètes.

Unified Manager génère des événements d'avertissement pour les violations de politique de surutilisation des ressources de nœud en recherchant les nœuds qui utilisent plus de 100 % de leur capacité de performance pendant plus de 30 minutes.

Vous pouvez utiliser le Gestionnaire système ou les commandes ONTAP pour corriger ce type de problème de performances, notamment les tâches suivantes :

- Création et application d'une politique QoS à tous les volumes ou LUN qui utilisent trop les ressources système
- Réduire la limite de débit maximale QoS d'un groupe de politiques auquel des charges de travail ont été appliquées
- Déplacer une charge de travail vers un autre agrégat ou nœud
- Augmenter la capacité en ajoutant des disques au nœud ou en effectuant une mise à niveau vers un nœud doté d'un processeur plus rapide et de plus de RAM

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Consultez la **Description**, qui décrit la violation de seuil qui a provoqué l'événement.

Par exemple, le message « Perf. La valeur de capacité utilisée de 139 % sur simplicity-02 a déclenché un événement d'AVERTISSEMENT pour identifier des problèmes de performances potentiels dans l'unité de traitement de données. « » indique que la capacité de performance sur le nœud simplicity-02 est surutilisée et affecte les performances du nœud.

3. Dans la section **Diagnostic du système**, examinez les trois graphiques : un pour la capacité de performance utilisée sur le nœud, un pour les IOPS de stockage moyennes utilisées par les charges de travail les plus importantes et un pour la latence sur les charges de travail les plus importantes. En les organisant de cette manière, vous pouvez voir quelles charges de travail sont à l'origine de la latence sur le nœud.

Vous pouvez afficher les charges de travail auxquelles des stratégies QoS sont appliquées et celles qui ne le sont pas en déplaçant votre curseur sur le graphique IOPS.

4. Dans la section **Actions suggérées**, examinez les suggestions et déterminez les actions à effectuer pour éviter une augmentation de la latence de la charge de travail.

Si nécessaire, cliquez sur le bouton **Aide** pour afficher plus de détails sur les actions suggérées que vous pouvez effectuer pour essayer de résoudre l'événement de performance.

Répondre aux événements de déséquilibre des performances des clusters

Unified Manager génère des événements d'avertissement de déséquilibre de cluster

lorsqu'un nœud d'un cluster fonctionne à une charge beaucoup plus élevée que les autres nœuds, ce qui affecte potentiellement les latences de charge de travail. Ces événements définis par le système offrent la possibilité de corriger les problèmes de performances potentiels avant que de nombreuses charges de travail ne soient affectées par la latence.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Unified Manager génère des événements d'avertissement pour les violations de la politique de seuil de déséquilibre du cluster en comparant la valeur de capacité de performance utilisée pour tous les nœuds du cluster pour voir s'il existe une différence de charge de 30 % entre les nœuds.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les charges de travail les plus performantes vers un nœud moins utilisé :

- Les nœuds du même cluster qui sont moins utilisés
- Les agrégats sur le nouveau nœud qui sont les moins utilisés
- Les volumes les plus performants sur le nœud actuel

Étapes

1. Affichez la page des détails de l'événement pour afficher des informations sur l'événement.
2. Consultez la **Description**, qui décrit la violation de seuil qui a provoqué l'événement.

Par exemple, le message « Le compteur de capacité de performance utilisée indique une différence de charge de 62 % entre les nœuds du cluster Dallas-1-8 et a déclenché un événement d'AVERTISSEMENT basé sur le seuil système de 30 % » indique que la capacité de performance sur l'un des nœuds est surutilisée et affecte les performances du nœud.

3. Consultez le texte dans les **Actions suggérées** pour déplacer un volume hautes performances du nœud avec la valeur de capacité de performances utilisée la plus élevée vers un nœud avec la valeur de capacité de performances utilisée la plus faible.
4. Identifiez les nœuds avec la valeur de capacité de performance utilisée la plus élevée et la plus faible :
 - a. Dans la section **Informations sur l'événement**, cliquez sur le nom du cluster source.
 - b. Dans la page **Résumé des clusters/performances**, cliquez sur **Nœuds** dans la zone **Objets gérés**.
 - c. Dans la page d'inventaire **Nœuds**, triez les nœuds par la colonne **Capacité de performance utilisée**.
 - d. Identifiez les nœuds avec la valeur de capacité de performance utilisée la plus élevée et la plus faible et notez ces noms.
5. Identifiez le volume utilisant le plus d'IOPS sur le nœud qui a la valeur de capacité de performance utilisée la plus élevée :
 - a. Cliquez sur le nœud avec la valeur de capacité de performance utilisée la plus élevée.
 - b. Dans la page **Nœud / Explorateur de performances**, sélectionnez **Agrégats sur ce nœud** dans le menu **Afficher et comparer**.
 - c. Cliquez sur l'agrégat avec la valeur de capacité de performance utilisée la plus élevée.
 - d. Dans la page **Explorateur d'agrégats/performances**, sélectionnez **Volumes sur cet agrégat** dans le menu **Afficher et comparer**.
 - e. Triez les volumes par la colonne **IOPS** et notez le nom du volume utilisant le plus d'IOPS et le nom de

l'agrégat où réside le volume.

6. Identifiez l'agrégat avec l'utilisation la plus faible sur le nœud qui a la valeur de capacité de performance utilisée la plus faible :
 - a. Cliquez sur **Stockage > Agrégats** pour afficher la page d'inventaire **Agrégats**.
 - b. Sélectionnez la vue **Performance : tous les agrégats**.
 - c. Cliquez sur le bouton **Filtre** et ajoutez un filtre où « Nœud » correspond au nom du nœud avec la valeur de capacité de performance utilisée la plus faible que vous avez notée à l'étape 4.
 - d. Notez le nom de l'agrégat qui a la valeur de capacité de performance utilisée la plus faible.
7. Déplacez le volume du nœud surchargé vers l'agrégat que vous avez identifié comme ayant une faible utilisation sur le nouveau nœud.

Vous pouvez effectuer l'opération de déplacement à l'aide d' ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même événement de déséquilibre de cluster à partir de ce cluster.

Analyser les événements à partir de seuils de performance dynamiques

Les événements générés à partir de seuils dynamiques indiquent que le temps de réponse réel (latence) d'une charge de travail est trop élevé ou trop faible par rapport à la plage de temps de réponse attendue. Vous utilisez la page Détails de l'événement pour analyser l'événement de performance et prendre des mesures correctives, si nécessaire, pour ramener les performances à la normale.



Les seuils de performances dynamiques ne sont pas activés sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select .

Identifier les charges de travail des victimes impliquées dans un événement de performance dynamique

Dans Unified Manager, vous pouvez identifier les charges de travail de volume qui présentent l'écart le plus élevé en termes de temps de réponse (latence) causé par un composant de stockage en conflit. L'identification de ces charges de travail vous aide à comprendre pourquoi les applications clientes qui y accèdent fonctionnent plus lentement que d'habitude.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance dynamiques nouveaux, reconnus ou obsolètes.

La page Détails de l'événement affiche une liste des charges de travail définies par l'utilisateur et par le système, classées en fonction de l'écart le plus élevé en termes d'activité ou d'utilisation sur le composant ou les plus impactées par l'événement. Les valeurs sont basées sur les pics identifiés par Unified Manager lors de la détection et de la dernière analyse de l'événement.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Dans les graphiques Latence de la charge de travail et Activité de la charge de travail, sélectionnez **Charges de travail des victimes**.
3. Passez votre curseur sur les graphiques pour afficher les principales charges de travail définies par l'utilisateur qui affectent le composant et le nom de la charge de travail victime.

Identifier les charges de travail des intimidateurs impliquées dans un événement de performance dynamique

Dans Unified Manager, vous pouvez identifier les charges de travail présentant l'écart d'utilisation le plus élevé pour un composant de cluster en conflit. L'identification de ces charges de travail vous aide à comprendre pourquoi certains volumes du cluster ont des temps de réponse lents (latence).

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance dynamiques nouveaux, reconnus ou obsolètes.

La page Détails de l'événement affiche une liste des charges de travail définies par l'utilisateur et par le système, classées en fonction de l'utilisation la plus élevée du composant ou les plus impactées par l'événement. Les valeurs sont basées sur les pics identifiés par Unified Manager lors de la détection et de la dernière analyse de l'événement.

Étapes

1. Affichez la page Détails de l'événement pour afficher des informations sur l'événement.
2. Dans les graphiques Latence de la charge de travail et Activité de la charge de travail, sélectionnez **Charges de travail d'intimidation**.
3. Passez votre curseur sur les graphiques pour afficher les principales charges de travail définies par l'utilisateur qui affectent le composant.

Identifier les charges de travail des requins impliquées dans un événement de performance dynamique

Dans Unified Manager, vous pouvez identifier les charges de travail présentant l'écart d'utilisation le plus élevé pour un composant de stockage en conflit. L'identification de ces charges de travail vous aide à déterminer si ces charges de travail doivent être déplacées vers un cluster moins utilisé.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il existe des événements dynamiques de performance nouveaux, reconnus ou obsolètes.

La page Détails de l'événement affiche une liste des charges de travail définies par l'utilisateur et par le système, classées en fonction de l'utilisation la plus élevée du composant ou les plus impactées par l'événement. Les valeurs sont basées sur les pics identifiés par Unified Manager lors de la détection et de la dernière analyse de l'événement.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.

2. Dans les graphiques Latence de la charge de travail et Activité de la charge de travail, sélectionnez **Charges de travail Shark**.
3. Passez votre curseur sur les graphiques pour afficher les principales charges de travail définies par l'utilisateur qui affectent le composant et le nom de la charge de travail du requin.

Analyse des événements de performance pour une configuration MetroCluster

Vous pouvez utiliser Unified Manager pour analyser un événement de performances pour une configuration MetroCluster . Vous pouvez identifier les charges de travail impliquées dans l'événement et examiner les actions suggérées pour le résoudre.

Les événements de performances de MetroCluster peuvent être dus à des charges de travail *bully* qui utilisent de manière excessive les liaisons inter-commutateurs (ISL) entre les clusters, ou à des problèmes d'intégrité des liaisons. Unified Manager surveille chaque cluster dans une configuration MetroCluster indépendamment, sans tenir compte des événements de performances sur un cluster partenaire.

Les événements de performances des deux clusters dans la configuration MetroCluster sont également affichés sur la page Tableau de bord d'Unified Manager. Vous pouvez également consulter les pages Santé d'Unified Manager pour vérifier l'état de chaque cluster et afficher leur relation.

Analyser un événement de performance dynamique sur un cluster dans une configuration MetroCluster

Vous pouvez utiliser Unified Manager pour analyser le cluster dans une configuration MetroCluster sur lequel un événement de performances a été détecté. Vous pouvez identifier le nom du cluster, l'heure de détection de l'événement et les charges de travail *bully* et *victim* impliquées.

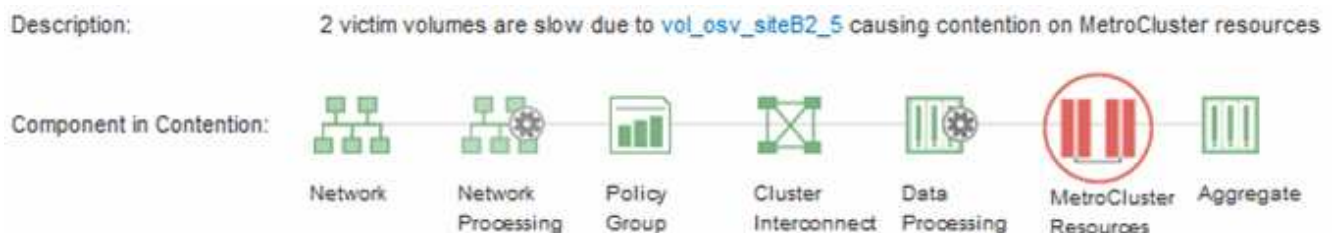
Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performances nouveaux, reconnus ou obsolètes pour une configuration MetroCluster .
- Les deux clusters de la configuration MetroCluster doivent être surveillés par la même instance de Unified Manager.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Consultez la description de l'événement pour voir les noms des charges de travail impliquées et le nombre de charges de travail impliquées.

Dans cet exemple, l'icône Ressources MetroCluster est rouge, indiquant que les ressources MetroCluster sont en conflit. Vous positionnez votre curseur sur l'icône pour afficher une description de l'icône.

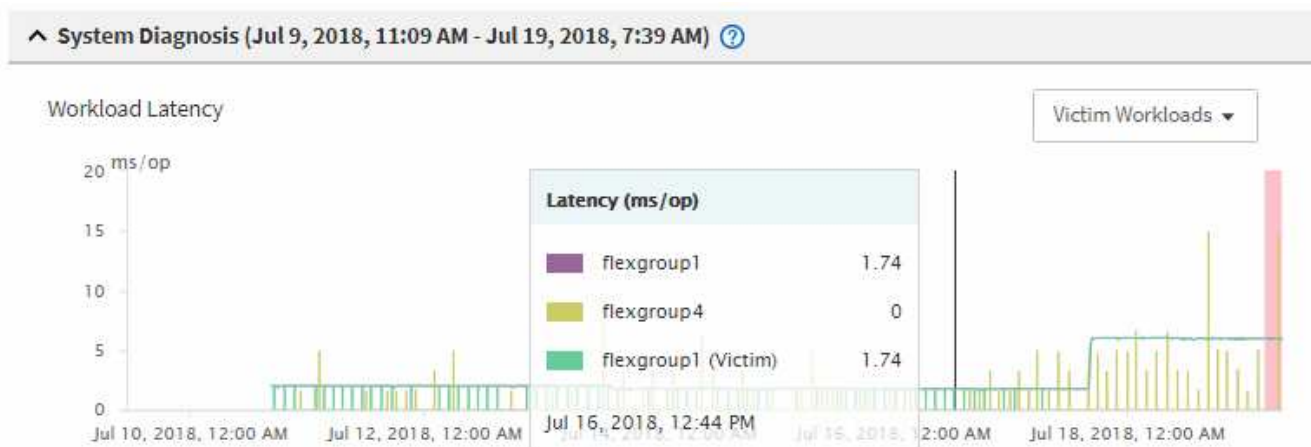


3. Notez le nom du cluster et l'heure de détection des événements, que vous pouvez utiliser pour analyser

les événements de performances sur le cluster partenaire.

4. Dans les graphiques, examinez les charges de travail *victim*es pour confirmer que leurs temps de réponse sont supérieurs au seuil de performances.

Dans cet exemple, la charge de travail de la victime est affichée dans le texte de survol. Les graphiques de latence affichent, à un niveau élevé, un modèle de latence cohérent pour les charges de travail des victimes impliquées. Même si la latence anormale des charges de travail de la victime a déclenché l'événement, un modèle de latence cohérent peut indiquer que les charges de travail fonctionnent dans la plage prévue, mais qu'un pic d'E/S a augmenté la latence et déclenché l'événement.



Si vous avez récemment installé une application sur un client qui accède à ces charges de travail de volume et que cette application leur envoie une grande quantité d'E/S, vous pouvez vous attendre à une augmentation de leurs latences. Si la latence des charges de travail revient dans la plage attendue, que l'état de l'événement devient obsolète et reste dans cet état pendant plus de 30 minutes, vous pouvez probablement ignorer l'événement. Si l'événement est en cours et reste dans le nouvel état, vous pouvez l'examiner plus en détail pour déterminer si d'autres problèmes ont provoqué l'événement.

5. Dans le graphique Débit de charge de travail, sélectionnez **Charges de travail d'intimidation** pour afficher les charges de travail d'intimidation.

La présence de charges de travail malveillantes indique que l'événement a pu être provoqué par une ou plusieurs charges de travail sur le cluster local surutilisant les ressources MetroCluster. Les charges de travail des intimidateurs présentent un écart élevé dans le débit d'écriture (Mo/s).

Ce graphique affiche, à un niveau élevé, le modèle de débit d'écriture (Mo/s) pour les charges de travail. Vous pouvez examiner le modèle d'écriture en Mo/s pour identifier un débit anormal, ce qui peut indiquer qu'une charge de travail utilise de manière excessive les ressources MetroCluster.

Si aucune charge de travail d'intimidation n'est impliquée dans l'événement, l'événement peut avoir été causé par un problème de santé avec le lien entre les clusters ou un problème de performances sur le cluster partenaire. Vous pouvez utiliser Unified Manager pour vérifier l'état des deux clusters dans une configuration MetroCluster. Vous pouvez également utiliser Unified Manager pour vérifier et analyser les événements de performances sur le cluster partenaire.

Analyser un événement de performance dynamique pour un cluster distant sur une configuration MetroCluster

Vous pouvez utiliser Unified Manager pour analyser les événements de performances dynamiques sur un cluster distant dans une configuration MetroCluster. L'analyse vous aide à déterminer si un événement sur le cluster distant a provoqué un événement sur

son cluster partenaire.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir analysé un événement de performance sur un cluster local dans une configuration MetroCluster et obtenu l'heure de détection de l'événement.
- Vous devez avoir vérifié l'état du cluster local et de son cluster partenaire impliqué dans l'événement de performance et obtenu le nom du cluster partenaire.

Étapes

1. Connectez-vous à l'instance Unified Manager qui surveille le cluster partenaire.
2. Dans le volet de navigation de gauche, cliquez sur **Événements** pour afficher la liste des événements.
3. Dans le sélecteur **Plage de temps**, sélectionnez **Dernière heure**, puis cliquez sur **Appliquer la plage**.
4. Dans le sélecteur **Filtrage**, sélectionnez **Cluster** dans le menu déroulant de gauche, saisissez le nom du cluster partenaire dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

S'il n'y a aucun événement pour le cluster sélectionné au cours de la dernière heure, cela indique que le cluster n'a rencontré aucun problème de performances pendant la période où l'événement a été détecté sur son partenaire.

5. Si le cluster sélectionné comporte des événements détectés au cours de la dernière heure, comparez l'heure de détection de l'événement à l'heure de détection de l'événement sur le cluster local.

Si ces événements impliquent des charges de travail d'intimidation provoquant une contention sur le composant de traitement des données, un ou plusieurs de ces intimidateurs peuvent avoir provoqué l'événement sur le cluster local. Vous pouvez cliquer sur l'événement pour l'analyser et consulter les actions suggérées pour le résoudre sur la page Détails de l'événement.

Si ces événements n'impliquent pas de charges de travail d'intimidation, ils n'ont pas provoqué l'événement de performance sur le cluster local.

Répondre à un événement de performance dynamique causé par la limitation du groupe de politiques QoS

Vous pouvez utiliser Unified Manager pour enquêter sur un événement de performances provoqué par un groupe de politiques de qualité de service (QoS) limitant le débit de la charge de travail (Mo/s). La limitation a augmenté les temps de réponse (latence) des charges de travail de volume dans le groupe de politiques. Vous pouvez utiliser les informations sur l'événement pour déterminer si de nouvelles limites sur les groupes de stratégies sont nécessaires pour arrêter la limitation.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Lisez la **Description**, qui affiche le nom des charges de travail impactées par la limitation.



La description peut afficher la même charge de travail pour la victime et l'intimidateur, car la limitation fait de la charge de travail une victime d'elle-même.

3. Enregistrez le nom du volume à l'aide d'une application telle qu'un éditeur de texte.

Vous pouvez effectuer une recherche sur le nom du volume pour le localiser ultérieurement.

4. Dans les graphiques Latence de la charge de travail et Utilisation de la charge de travail, sélectionnez **Charges de travail Bully**.
5. Passez votre curseur sur les graphiques pour afficher les principales charges de travail définies par l'utilisateur qui affectent le groupe de stratégies.

La charge de travail en haut de la liste présente l'écart le plus élevé et a provoqué la limitation. L'activité correspond au pourcentage de la limite du groupe de stratégies utilisé par chaque charge de travail.

6. Dans la zone **Actions suggérées**, cliquez sur le bouton **Analyser la charge de travail** pour la charge de travail la plus élevée.
7. Dans la page Analyse de la charge de travail, définissez le graphique Latence pour afficher tous les composants du cluster et le graphique Débit pour afficher la répartition.

Les graphiques de répartition sont affichés sous le graphique de latence et le graphique IOPS.

8. Comparez les limites QoS dans le graphique **Latence** pour voir quelle quantité de limitation a eu un impact sur la latence au moment de l'événement.

Le groupe de politiques QoS a un débit maximal de 1 000 opérations par seconde (op/sec), que les charges de travail qu'il contient ne peuvent pas dépasser collectivement. Au moment de l'événement, les charges de travail du groupe de politiques avaient un débit combiné de plus de 1 200 opérations/s, ce qui a obligé le groupe de politiques à réduire son activité à 1 000 opérations/s.

9. Comparez les valeurs de **latence de lecture/écriture** aux valeurs de **lectures/écritures/autres**.

Les deux graphiques montrent un nombre élevé de demandes de lecture avec une latence élevée, mais le nombre de demandes et la quantité de latence pour les demandes d'écriture sont faibles. Ces valeurs vous aident à déterminer s'il existe un débit élevé ou un nombre élevé d'opérations qui ont augmenté la latence. Vous pouvez utiliser ces valeurs lorsque vous décidez d'imposer une limite de groupe de politiques au débit ou aux opérations.

10. Utilisez ONTAP System Manager pour augmenter la limite actuelle du groupe de stratégies à 1 300 opérations/s.
11. Après une journée, revenez à Unified Manager et saisissez la charge de travail que vous avez enregistrée à l'étape 3 dans la page **Analyse de la charge de travail**.
12. Sélectionnez le graphique de répartition du débit.

Le graphique Lectures/écritures/autres s'affiche.

13. En haut de la page, pointez votre curseur sur l'icône de changement d'événement () pour le changement de limite du groupe de politiques.
14. Comparez le graphique **Lectures/écritures/autres** au graphique **Latence**.

Les demandes de lecture et d'écriture sont les mêmes, mais la limitation a été arrêtée et la latence a diminué.

Répondre à un événement de performance dynamique causé par une panne de disque

Vous pouvez utiliser Unified Manager pour enquêter sur un événement de performances causé par des charges de travail surutilisant un agrégat. Vous pouvez également utiliser Unified Manager pour vérifier l'intégrité de l'agrégat afin de voir si les événements d'intégrité récents détectés sur l'agrégat ont contribué à l'événement de performance.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Lisez la **Description**, qui décrit les charges de travail impliquées dans l'événement et le composant de cluster en conflit.

Il existe plusieurs volumes victimes dont la latence a été affectée par le composant de cluster en conflit. L'agrégat, qui se trouve au milieu d'une reconstruction RAID pour remplacer le disque défaillant par un disque de rechange, est le composant du cluster en conflit. Sous Composant en conflit, l'icône Agrégation est surlignée en rouge et le nom de l'agrégat est affiché entre parenthèses.

3. Dans le graphique d'utilisation de la charge de travail, sélectionnez **Charges de travail d'intimidation**.
4. Passez votre curseur sur le graphique pour afficher les principales charges de travail qui affectent le composant.

Les charges de travail principales avec l'utilisation maximale la plus élevée depuis la détection de l'événement sont affichées en haut du graphique. L'une des charges de travail les plus importantes est la charge de travail définie par le système Disk Health, qui indique une reconstruction RAID. Une reconstruction est le processus interne impliqué dans la reconstruction de l'agrégat avec le disque de rechange. La charge de travail Disk Health, ainsi que d'autres charges de travail sur l'agrégat, ont probablement provoqué la contention sur l'agrégat et l'événement associé.

5. Après avoir confirmé que l'activité de la charge de travail Disk Health a provoqué l'événement, attendez environ 30 minutes que la reconstruction se termine et qu'Unified Manager analyse l'événement et détecte si l'agrégat est toujours en conflit.
6. Actualisez les **Détails de l'événement**.

Une fois la reconstruction RAID terminée, vérifiez que l'état est obsolète, indiquant que l'événement est résolu.

7. Dans le graphique d'utilisation de la charge de travail, sélectionnez **Charges de travail d'intimidation** pour afficher les charges de travail globales par utilisation maximale.
8. Dans la zone **Actions suggérées**, cliquez sur le bouton **Analyser la charge de travail** pour la charge de travail la plus élevée.
9. Dans la page **Analyse de la charge de travail**, définissez la plage de temps pour afficher les dernières 24 heures (1 jour) de données pour le volume sélectionné.

Dans la chronologie des événements, un point rouge (●) indique quand l'événement de défaillance du disque s'est produit.

10. Dans le graphique Utilisation des nœuds et des agrégats, masquez la ligne des statistiques des nœuds

afin que seule la ligne d'agrégats reste.

11. Comparez les données de ce graphique aux données au moment de l'événement dans le graphique **Latence**.

Au moment de l'événement, l'utilisation globale affiche une quantité élevée d'activité de lecture et d'écriture, causée par les processus de reconstruction RAID, ce qui a augmenté la latence du volume sélectionné. Quelques heures après l'événement, les lectures et les écritures ainsi que la latence ont diminué, confirmant que l'agrégat n'est plus en conflit.

Répondre à un événement de performance dynamique causé par une prise de contrôle HA

Vous pouvez utiliser Unified Manager pour examiner un événement de performances causé par un traitement de données élevé sur un nœud de cluster qui se trouve dans une paire haute disponibilité (HA). Vous pouvez également utiliser Unified Manager pour vérifier l'état des nœuds afin de voir si des événements d'état récents détectés sur les nœuds ont contribué à l'événement de performance.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Lisez la **Description**, qui décrit les charges de travail impliquées dans l'événement et le composant de cluster en conflit.

Il existe un volume victime dont la latence a été impactée par le composant de cluster en conflit. Le nœud de traitement des données, qui a repris toutes les charges de travail de son nœud partenaire, est le composant du cluster en conflit. Sous Composant en conflit, l'icône Data Processing est surlignée en rouge et le nom du nœud qui gère le traitement des données au moment de l'événement est affiché entre parenthèses.

3. Dans la **Description**, cliquez sur le nom du volume.

La page Volume Performance Explorer s'affiche. En haut de la page, dans la chronologie des événements, une icône d'événement de changement () indique l'heure à laquelle Unified Manager a détecté le début de la prise de contrôle HA.

4. Pointez votre curseur sur l'icône d'événement de modification pour la prise de contrôle HA et les détails sur la prise de contrôle HA s'affichent dans le texte de survol.

Dans le graphique de latence, un événement indique que le volume sélectionné a franchi le seuil de performances en raison d'une latence élevée à peu près au même moment que la prise de contrôle HA.

5. Cliquez sur **Zoom View** pour afficher le graphique de latence sur une nouvelle page.
6. Dans le menu Affichage, sélectionnez **Composants du cluster** pour afficher la latence totale par composant du cluster.
7. Pointez le curseur de votre souris sur l'icône de changement d'événement pour le début de la prise de contrôle HA et comparez la latence du traitement des données à la latence totale.

Au moment de la prise de contrôle de HA, il y a eu un pic dans le traitement des données en raison de la

demande accrue de charge de travail sur le nœud de traitement des données. L'utilisation accrue du processeur a augmenté la latence et a déclenché l'événement.

8. Après avoir réparé le nœud défaillant, utilisez ONTAP System Manager pour effectuer un retour HA, qui déplace les charges de travail du nœud partenaire vers le nœud corrigé.
9. Une fois la restitution HA terminée, après la découverte de configuration suivante dans Unified Manager (environ 15 minutes), recherchez l'événement et la charge de travail déclenchés par la prise de contrôle HA dans la page d'inventaire **Gestion des événements**.

L'événement déclenché par la prise de contrôle HA a désormais un état obsolète, ce qui indique que l'événement est résolu. La latence au niveau du composant de traitement des données a diminué, ce qui a diminué la latence totale. Le nœud que le volume sélectionné utilise désormais pour le traitement des données a résolu l'événement.

Résoudre les événements de performance

Vous pouvez utiliser les actions suggérées pour essayer de résoudre vous-même les événements de performances. Les trois premières suggestions sont toujours affichées et les actions sous la quatrième suggestion sont spécifiques au type d'événement affiché.

Les liens **Aidez-moi à faire ceci** fournissent des informations supplémentaires pour chaque action suggérée, y compris des instructions pour effectuer une action spécifique. Certaines actions peuvent impliquer l'utilisation d'Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP CLI ou d'une combinaison de ces outils.

Confirmez que la latence est dans la plage attendue

Lorsqu'un composant de cluster est en conflit, les charges de travail de volume qui l'utilisent peuvent avoir un temps de réponse (latence) réduit. Vous pouvez examiner la latence de chaque charge de travail victime sur le composant en conflit pour confirmer que sa latence réelle se situe dans la plage attendue. Vous pouvez également cliquer sur le nom d'un volume pour afficher les données historiques du volume.

Si l'événement de performance est dans un état obsolète, la latence de chaque victime impliquée dans l'événement peut être revenue dans sa plage attendue.

Examiner l'impact des modifications de configuration sur les performances de la charge de travail

Les modifications de configuration sur le cluster, telles qu'un disque défaillant, un basculement HA ou un volume déplacé, peuvent avoir un impact négatif sur les performances du volume et entraîner une augmentation de la latence.

Dans Unified Manager, vous pouvez consulter la page Analyse de la charge de travail pour voir quand une modification de configuration récente s'est produite et la comparer aux opérations et à la latence (temps de réponse) pour voir s'il y a eu un changement d'activité pour la charge de travail du volume sélectionné.

Les pages de performances d'Unified Manager ne peuvent détecter qu'un nombre limité d'événements de modification. Les pages de santé fournissent des alertes pour d'autres événements causés par des modifications de configuration. Vous pouvez rechercher le volume dans Unified Manager pour voir l'historique

des événements.

Options permettant d'améliorer les performances de la charge de travail côté client

Vous pouvez vérifier vos charges de travail client, telles que les applications ou les bases de données, qui envoient des E/S aux volumes impliqués dans un événement de performances pour déterminer si une modification côté client peut corriger l'événement.

Lorsque les clients connectés aux volumes d'un cluster augmentent leurs demandes d'E/S, le cluster doit travailler davantage pour répondre à la demande. Si vous savez quels clients ont un nombre élevé de demandes d'E/S sur un volume particulier du cluster, vous pouvez améliorer les performances du cluster en ajustant le nombre de clients accédant au volume ou en diminuant la quantité d'E/S sur le volume. Vous pouvez également appliquer ou augmenter une limite sur le groupe de politiques QoS dont le volume est membre.

Vous pouvez examiner les clients et leurs applications pour déterminer si les clients envoient plus d'E/S que d'habitude, ce qui peut provoquer une contention sur un composant de cluster. Sur la page Détails de l'événement, la section Diagnostic système affiche les charges de travail de volume les plus importantes utilisant le composant en conflit. Si vous savez quel client accède à un volume particulier, vous pouvez accéder au client pour déterminer si le matériel client ou une application ne fonctionne pas comme prévu ou effectue plus de travail que d'habitude.

Dans une configuration MetroCluster, les demandes d'écriture sur un volume d'un cluster local sont mises en miroir sur un volume du cluster distant. Le maintien de la synchronisation du volume source sur le cluster local avec le volume de destination sur le cluster distant peut également augmenter la demande des deux clusters dans la configuration MetroCluster. En réduisant les demandes d'écriture sur ces volumes en miroir, les clusters peuvent effectuer moins d'opérations de synchronisation, ce qui réduit l'impact sur les performances des autres charges de travail.

Vérifiez les problèmes de client ou de réseau

Lorsque les clients connectés aux volumes d'un cluster augmentent leurs demandes d'E/S, le cluster doit travailler davantage pour répondre à la demande. La demande accrue sur le cluster peut mettre un composant en conflit, augmenter la latence des charges de travail qui l'utilisent et déclencher un événement dans Unified Manager.

Sur la page Détails de l'événement, la section Diagnostic système affiche les charges de travail de volume les plus importantes utilisant le composant en conflit. Si vous savez quel client accède à un volume particulier, vous pouvez accéder au client pour déterminer si le matériel client ou une application ne fonctionne pas comme prévu ou effectue plus de travail que d'habitude. Vous devrez peut-être contacter votre administrateur client ou votre fournisseur d'applications pour obtenir de l'aide.

Vous pouvez vérifier votre infrastructure réseau pour déterminer s'il existe des problèmes matériels, des goulots d'étranglement ou des charges de travail concurrentes qui pourraient avoir entraîné des demandes d'E/S entre le cluster et les clients connectés plus lentes que prévu. Vous devrez peut-être contacter votre administrateur réseau pour obtenir de l'aide.

Vérifiez si d'autres volumes du groupe de politiques QoS présentent une activité inhabituellement élevée

Vous pouvez examiner les charges de travail dans le groupe de stratégies de qualité de service (QoS) avec le changement d'activité le plus élevé pour déterminer si plusieurs

charges de travail ont provoqué l'événement. Vous pouvez également voir si d'autres charges de travail dépassent toujours la limite de débit définie ou si elles sont de retour dans leur plage d'activité prévue.

Sur la page Détails de l'événement, dans la section Diagnostic système, vous pouvez trier les charges de travail par écart de pointe d'activité pour afficher les charges de travail avec le changement d'activité le plus élevé en haut du tableau. Ces charges de travail pourraient être celles des « intimidateurs » dont l'activité a dépassé la limite fixée et pourrait avoir provoqué l'événement.

Vous pouvez accéder à la page Analyse de la charge de travail pour chaque charge de travail de volume afin d'examiner son activité IOPS. Si la charge de travail comporte des périodes d'activité opérationnelle très élevée, elle peut avoir contribué à l'événement. Vous pouvez modifier les paramètres du groupe de stratégies pour la charge de travail ou déplacer la charge de travail vers un autre groupe de stratégies.

Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP CLI pour gérer les groupes de stratégies, comme suit :

- Créer un groupe de politiques.
- Ajoutez ou supprimez des charges de travail dans un groupe de stratégies.
- Déplacer une charge de travail entre des groupes de stratégies.
- Modifier la limite de débit d'un groupe de politiques.

Déplacer les interfaces logiques (LIF)

Le déplacement des interfaces logiques (LIF) vers un port moins fréquenté peut aider à améliorer l'équilibrage de la charge, à faciliter les opérations de maintenance et le réglage des performances, et à réduire l'accès indirect.

L'accès indirect peut réduire l'efficacité du système. Cela se produit lorsqu'une charge de travail de volume utilise différents nœuds pour le traitement du réseau et le traitement des données. Pour réduire l'accès indirect, vous pouvez réorganiser les LIF, ce qui implique de déplacer les LIF pour utiliser le même nœud pour le traitement du réseau et le traitement des données. Vous pouvez configurer l'équilibrage de charge pour ONTAP déplace automatiquement les LIF occupés vers un autre port ou vous pouvez déplacer un LIF manuellement.

Avantages	Considérations	
• Améliorer l'équilibrage de la charge. • Réduire l'accès indirect.		Lors du déplacement d'un LIF connecté à des partages CIFS, les clients accédant aux partages CIFS sont déconnectés. Toutes les demandes de lecture ou d'écriture sur les partages CIFS sont interrompues.

Vous utilisez les commandes ONTAP pour configurer l'équilibrage de charge. Pour plus d'informations, consultez la documentation réseau ONTAP .

Vous utilisez ONTAP System Manager et les commandes ONTAP CLI pour déplacer les LIF manuellement.

Exécutez les opérations d'efficacité du stockage à des heures moins chargées

Vous pouvez modifier la politique ou la planification qui gère les opérations d'efficacité du stockage pour qu'elles s'exécutent lorsque les charges de travail du volume impacté sont moins occupées.

Les opérations d'efficacité du stockage peuvent utiliser une grande quantité de ressources CPU du cluster et devenir un obstacle pour les volumes sur lesquels les opérations sont exécutées. Si les volumes victimes présentent une activité élevée au moment même où les opérations d'efficacité du stockage sont exécutées, leur latence peut augmenter et déclencher un événement.

Sur la page Détails de l'événement, la section Diagnostic système affiche les charges de travail dans le groupe de stratégies QoS par écart de pointe d'activité pour identifier les charges de travail les plus importantes. Si vous voyez « efficacité de stockage » affiché en haut du tableau, ces opérations intimident les charges de travail des victimes. En modifiant la politique ou la planification d'efficacité pour qu'elle s'exécute lorsque ces charges de travail sont moins occupées, vous pouvez empêcher les opérations d'efficacité du stockage de provoquer des conflits sur un cluster.

Vous pouvez utiliser ONTAP System Manager pour gérer les politiques d'efficacité. Vous pouvez utiliser les commandes ONTAP pour gérer les politiques et les planifications d'efficacité.

Qu'est-ce que l'efficacité de stockage

L'efficacité du stockage vous permet de stocker la quantité maximale de données au moindre coût et s'adapte à la croissance rapide des données tout en consommant moins d'espace. La stratégie de NetApp en matière d'efficacité du stockage repose sur la base intégrée de la virtualisation du stockage et du stockage unifié fournie par son système d'exploitation principal ONTAP et son système de fichiers Write Anywhere File Layout (WAFL).

L'efficacité du stockage inclut l'utilisation de technologies telles que le provisionnement léger, la copie Snapshot, la déduplication, la compression de données, FlexClone, la réplication légère avec SnapVault et le volume SnapMirror, RAID-DP, Flash Cache, l'agrégation Flash Pool et les agrégats compatibles FabricPool qui contribuent à augmenter l'utilisation du stockage et à réduire les coûts de stockage.

L'architecture de stockage unifiée vous permet de consolider efficacement un réseau de stockage (SAN), un stockage en réseau (NAS) et un stockage secondaire sur une seule plate-forme.

Les lecteurs de disque haute densité, tels que les lecteurs SATA (Serial Advanced Technology Attachment) configurés dans un agrégat Flash Pool ou avec la technologie Flash Cache et RAID-DP, augmentent l'efficacité sans affecter les performances et la résilience.

Un agrégat compatible FabricPool inclut un agrégat entièrement SSD ou un agrégat HDD (à partir de ONTAP 9.8) comme niveau de performances local et un magasin d'objets que vous spécifiez comme niveau cloud. La configuration de FabricPool vous aide à gérer le niveau de stockage (le niveau local ou le niveau cloud) dans lequel les données doivent être stockées en fonction de la fréquence d'accès aux données.

Des technologies telles que le provisionnement léger, la copie Snapshot, la déduplication, la compression des données, la réplication légère avec SnapVault et le volume SnapMirror et FlexClone offrent de meilleures économies. Vous pouvez utiliser ces technologies individuellement ou ensemble pour obtenir une efficacité de stockage maximale.

Ajouter des disques et réaffecter des données

Vous pouvez ajouter des disques à un agrégat pour augmenter la capacité de stockage et les performances de cet agrégat. Après avoir ajouté les disques, vous constaterez une amélioration des performances de lecture uniquement après avoir réaffecté les données sur les disques que vous avez ajoutés.

Vous pouvez utiliser ces instructions lorsque Unified Manager a reçu des événements agrégés déclenchés par des seuils dynamiques ou par des seuils de performances définis par le système :

- Lorsque vous avez reçu un événement de seuil dynamique, sur la page Détails de l'événement, l'icône du composant de cluster qui représente l'agrégat en conflit est surlignée en rouge.

Sous l'icône, entre parenthèses, se trouve le nom de l'agrégat, qui identifie l'agrégat auquel vous pouvez ajouter des disques.

- Lorsque vous avez reçu un événement de seuil défini par le système, sur la page Détails de l'événement, le texte de description de l'événement répertorie le nom de l'agrégat qui rencontre le problème.

Vous pouvez ajouter des disques et réaffecter des données sur cet agrégat.

Les disques que vous ajoutez à l'agrégat doivent déjà exister dans le cluster. Si le cluster ne dispose pas de disques supplémentaires disponibles, vous devrez peut-être contacter votre administrateur ou acheter des disques supplémentaires. Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour ajouter des disques à un agrégat.



Vous devez réaffecter les données lorsque vous utilisez uniquement des agrégats HDD et Flash Pool. Ne réallocation pas les données sur les agrégats SSD ou FabricPool .

Comment l'activation du cache Flash sur un nœud peut améliorer les performances de la charge de travail

Vous pouvez améliorer les performances de la charge de travail en activant la mise en cache intelligente des données Flash Cache™ sur chaque nœud du cluster.

Un module Flash Cache, ou module de mémoire basé sur PCIe, optimise les performances des charges de travail à lecture intensive aléatoire en fonctionnant comme un cache de lecture externe intelligent. Ce matériel fonctionne en tandem avec le composant logiciel WAFL External Cache d' ONTAP.

Dans Unified Manager, sur la page Détails de l'événement, l'icône du composant de cluster qui représente l'agrégat en conflit est surlignée en rouge. Sous l'icône, entre parenthèses, se trouve le nom de l'agrégat, qui identifie l'agrégat. Vous pouvez activer Flash Cache sur le nœud sur lequel réside l'agrégat.

Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour voir si Flash Cache est installé ou activé, et pour l'activer s'il n'est pas déjà activé. La commande suivante indique si Flash Cache est activé sur un nœud spécifique : **cluster::> run local options flexscale.enable**

Pour plus d'informations sur Flash Cache et les exigences d'utilisation, consultez le rapport technique suivant :

["Rapport technique 3832 : Guide des meilleures pratiques pour le cache Flash"](#)

Comment l'activation de Flash Pool sur un agrégat de stockage peut améliorer les performances de la charge de travail

Vous pouvez améliorer les performances de la charge de travail en activant la fonctionnalité Flash Pool sur un agrégat. Un Flash Pool est un agrégat qui intègre à la fois des disques durs et des SSD. Les disques durs sont utilisés pour le stockage principal et les SSD fournissent un cache de lecture et d'écriture haute performance pour améliorer les performances globales.

Dans Unified Manager, la page Détails de l'événement affiche le nom de l'agrégat en conflit. Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour voir si Flash Pool est activé pour un agrégat. Si vous avez installé des SSD, vous pouvez utiliser l'interface de ligne de commande pour l'activer. Si vous avez installé des SSD, vous pouvez exécuter la commande suivante sur l'agrégat pour voir si Flash Pool est activé : `cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`

Dans cette commande, *aggr_name* est le nom de l'agrégat, tel que l'agrégat en litige.

Pour plus d'informations sur Flash Pool et les exigences d'utilisation, consultez le [_Guide de gestion du stockage physique Clustered Data ONTAP](#) .

Vérification de l'état de la configuration de MetroCluster

Vous pouvez utiliser Unified Manager pour vérifier l'état des clusters dans une configuration MetroCluster sur IP ou FC. L'état de santé et les événements vous aident à déterminer s'il existe des problèmes matériels ou logiciels susceptibles d'avoir un impact sur les performances de vos charges de travail.

Si vous configurez Unified Manager pour envoyer des alertes par e-mail, vous pouvez vérifier votre e-mail pour détecter tout problème de santé sur le cluster local ou distant qui pourrait avoir contribué à un événement de performances. Dans l'interface graphique d'Unified Manager, vous pouvez sélectionner **Gestion des événements** pour afficher une liste des événements actuels, puis utiliser les filtres pour afficher uniquement les événements de configuration MetroCluster .

Pour plus d'informations, voir "[Vérification de l'état des clusters dans une configuration MetroCluster](#)"

Vérification de la configuration de MetroCluster

Vous pouvez éviter les problèmes de performances pour les charges de travail en miroir dans un MetroCluster sur des configurations FC et IP en vous assurant que la configuration MetroCluster est correctement configurée. Vous pouvez également améliorer les performances de la charge de travail en modifiant la configuration ou en mettant à niveau les composants logiciels ou matériels.

Se référer à "[Documentation de MetroCluster](#)" pour les instructions de configuration des clusters dans la configuration MetroCluster , y compris les commutateurs Fibre Channel (FC), les câbles et les liaisons inter-commutateurs (ISL). Il vous aide également à configurer le logiciel MetroCluster afin que les clusters locaux et distants puissent communiquer avec les données du volume miroir. Pour obtenir des informations spécifiques à votre configuration MetroCluster sur IP, consultez "[Installer une configuration IP MetroCluster](#)" .

Vous pouvez comparer votre configuration MetroCluster aux exigences de "[Documentation de MetroCluster](#)" pour déterminer si la modification ou la mise à niveau des composants de votre configuration MetroCluster

peut améliorer les performances de la charge de travail. Cette comparaison peut vous aider à répondre aux questions suivantes :

- Les contrôleurs sont-ils adaptés à vos charges de travail ?
- Avez-vous besoin de mettre à niveau vos offres ISL vers une bande passante plus large pour gérer davantage de débit ?
- Pouvez-vous ajuster les crédits tampon à tampon (BBC) sur vos commutateurs pour augmenter la bande passante ?
- Si vos charges de travail ont un débit d'écriture élevé sur le stockage SSD (Solid State Drive), devez-vous mettre à niveau vos ponts FC vers SAS pour prendre en charge le débit ?

Informations connexes

- Pour plus d'informations sur le remplacement ou la mise à niveau des composants MetroCluster , consultez le ["Documentation de MetroCluster"](#) .
- Pour plus d'informations sur la mise à niveau des contrôleurs, voir ["Mise à niveau des contrôleurs dans une configuration MetroCluster FC à l'aide de la commutation et du retour arrière"](#) et ["Mise à niveau des contrôleurs dans une configuration IP MetroCluster à l'aide de la commutation et du retour arrière"](#)

Déplacer les charges de travail vers un autre agrégat

Vous pouvez utiliser Unified Manager pour vous aider à identifier un agrégat moins occupé que l'agrégat dans lequel résident actuellement vos charges de travail, puis vous pouvez déplacer les volumes ou les LUN sélectionnés vers cet agrégat. Le déplacement des charges de travail hautement performantes vers un agrégat moins chargé, ou vers un agrégat avec stockage flash activé, permet à la charge de travail de fonctionner plus efficacement.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir enregistré le nom de l'agrégat qui rencontre actuellement un problème de performances.
- Vous devez avoir enregistré la date et l'heure à laquelle l'agrégat a reçu l'événement.
- Unified Manager doit avoir collecté et analysé un mois ou plus de données de performance.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les charges de travail très performantes vers un agrégat moins utilisé :

- Les agrégats du même cluster qui sont moins utilisés
- Les volumes les plus performants de l'agrégat actuel

Étapes

1. Identifiez l'agrégat du cluster qui est le moins utilisé :

a. Depuis la page des détails de l'**Événement**, cliquez sur le nom du cluster sur lequel réside l'agrégat.

Les détails du cluster sont affichés sur la page d'accueil Performances/Cluster.

b. Sur la page **Résumé**, cliquez sur **Agrégats** dans le volet **Objets gérés**.

La liste des agrégats de ce cluster est affichée.

c. Cliquez sur la colonne **Utilisation** pour trier les agrégats par ordre d'utilisation.

Vous pouvez également identifier les agrégats qui ont la plus grande **capacité libre**. Cela fournit une liste d'agrégats potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les charges de travail.

2. Identifiez les volumes les plus performants de l'agrégat qui ont reçu l'événement :

a. Cliquez sur l'agrégat qui présente le problème de performances.

Les détails agrégés sont affichés dans la page Explorateur de performances/agrégats.

b. Dans le sélecteur **Plage de temps**, sélectionnez **30 derniers jours**, puis cliquez sur **Appliquer la plage**.

Cela vous permet d'afficher une période d'historique des performances plus longue que la période par défaut de 72 heures. Vous souhaitez déplacer un volume qui utilise beaucoup de ressources de manière constante, et pas seulement au cours des 72 dernières heures.

c. À partir du contrôle **Afficher et comparer**, sélectionnez **Volumes sur cet agrégat**.

Une liste des volumes FlexVol et des volumes constitutifs FlexGroup sur cet agrégat est affichée.

d. Triez les volumes par Mo/s le plus élevé, puis par IOPS le plus élevé, pour voir les volumes les plus performants.

e. Notez les noms des volumes que vous souhaitez déplacer vers un autre agrégat.

3. Déplacez les volumes les plus performants vers l'agrégat que vous avez identifié comme ayant une faible utilisation.

Vous pouvez effectuer l'opération de déplacement à l'aide d' ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacer les charges de travail vers un autre nœud

Vous pouvez utiliser Unified Manager pour vous aider à identifier un agrégat sur un nœud différent qui est moins occupé que le nœud sur lequel vos charges de travail s'exécutent actuellement, puis vous pouvez déplacer les volumes sélectionnés vers cet agrégat. Le déplacement des charges de travail hautement performantes vers un agrégat sur un nœud moins occupé permet aux charges de travail sur les deux nœuds de fonctionner plus efficacement.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir enregistré le nom du nœud qui rencontre actuellement un problème de performances.
- Vous devez avoir enregistré la date et l'heure à laquelle le nœud a reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé les données de performance pendant un mois ou plus.

Cette procédure vous aide à identifier les ressources suivantes afin de pouvoir déplacer les charges de travail les plus performantes vers un nœud moins utilisé :

- Les nœuds du même cluster qui ont la plus grande capacité de performance libre
- Les agrégats sur le nouveau nœud qui ont la plus grande capacité de performance libre
- Les volumes les plus performants sur le nœud actuel

Étapes

1. Identifiez un nœud dans le cluster qui a la plus grande capacité de performance libre :

a. Sur la page **Détails de l'événement**, cliquez sur le nom du cluster sur lequel réside le nœud.

Les détails du cluster sont affichés sur la page d'accueil Performances/Cluster.

b. Dans l'onglet **Résumé**, cliquez sur **Nœuds** dans le volet **Objets gérés**.

La liste des nœuds de ce cluster est affichée.

c. Cliquez sur la colonne **Capacité de performance utilisée** pour trier les nœuds par pourcentage le plus faible utilisé.

Cela fournit une liste de nœuds potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

d. Notez le nom du nœud vers lequel vous souhaitez déplacer les charges de travail.

2. Identifiez un agrégat sur le nouveau nœud qui est le moins utilisé :

a. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats** et sélectionnez **Performances > Tous les agrégats** dans le menu Affichage.

La vue Performances : tous les agrégats s'affiche.

b. Cliquez sur **Filtrage**, sélectionnez **Nœud** dans le menu déroulant de gauche, saisissez le nom du nœud dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

La vue Performances : Tous les agrégats s'affiche à nouveau avec la liste des agrégats disponibles sur ce nœud.

c. Cliquez sur la colonne **Capacité de performance utilisée** pour trier les agrégats par ordre de moindre utilisation.

Cela fournit une liste d'agrégats potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les charges de travail.

3. Identifiez les charges de travail les plus performantes du nœud qui a reçu l'événement :

a. Retournez à la page **Détails de l'événement** pour l'événement.

b. Dans le champ **Volumes concernés**, cliquez sur le lien correspondant au nombre de volumes.

La vue Performances : Tous les volumes s'affiche avec une liste filtrée des volumes sur ce nœud.

c. Cliquez sur la colonne **Capacité totale** pour trier les volumes en fonction du plus grand espace alloué.

Cela fournit une liste de volumes potentiels que vous souhaitez peut-être déplacer.

d. Notez les noms des volumes que vous souhaitez déplacer et les noms des agrégats actuels sur lesquels ils résident.

4. Déplacez les volumes vers les agrégats que vous avez identifiés comme ayant la plus grande capacité de performance libre sur le nouveau nœud.

Vous pouvez effectuer l'opération de déplacement à l'aide d' ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vous pouvez vérifier si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacer les charges de travail vers un agrégat sur un nœud différent

Vous pouvez utiliser Unified Manager pour vous aider à identifier un agrégat sur un nœud différent qui est moins occupé que le nœud sur lequel vos charges de travail s'exécutent actuellement, puis vous pouvez déplacer les volumes sélectionnés vers cet agrégat. Le déplacement de charges de travail hautement performantes vers un agrégat sur un nœud moins occupé permet aux charges de travail sur les deux nœuds de fonctionner plus efficacement.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir enregistré le nom du nœud qui rencontre actuellement un problème de performances.
- Vous devez avoir enregistré la date et l'heure à laquelle le nœud a reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé un mois ou plus de données de performance.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les charges de travail les plus performantes vers un nœud moins utilisé :

- Les nœuds du même cluster qui sont moins utilisés
- Les agrégats sur le nouveau nœud qui sont les moins utilisés
- Les volumes les plus performants sur le nœud actuel

Étapes

1. Identifiez un nœud du cluster qui est le moins utilisé :
 - a. Depuis la page des détails de l'**Événement**, cliquez sur le nom du cluster sur lequel réside le nœud.

Les détails du cluster sont affichés sur la page d'accueil Performances/Cluster.
 - b. Sur la page **Résumé**, cliquez sur **Nœuds** dans le volet **Objets gérés**.

La liste des nœuds de ce cluster est affichée.
 - c. Cliquez sur la colonne **Utilisation** pour trier les nœuds par ordre d'utilisation.

Vous pouvez également identifier les nœuds qui ont la plus grande **capacité libre**. Cela fournit une liste de nœuds potentiels vers lesquels vous souhaiterez peut-être déplacer des charges de travail.
 - d. Notez le nom du nœud vers lequel vous souhaitez déplacer les charges de travail.
2. Identifiez un agrégat sur le nouveau nœud qui est le moins utilisé :
 - a. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats** et sélectionnez

Performances > Tous les agrégats dans le menu Affichage.

La vue Performances : tous les agrégats s'affiche.

- b. Cliquez sur **Filtrage**, sélectionnez **Nœud** dans le menu déroulant de gauche, saisissez le nom du nœud dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

La vue Performances : Tous les agrégats s'affiche à nouveau avec la liste des agrégats disponibles sur ce nœud.

- c. Cliquez sur la colonne **Utilisation** pour trier les agrégats par ordre d'utilisation.

Vous pouvez également identifier les agrégats qui ont la plus grande **capacité libre**. Cela fournit une liste d'agrégats potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

- d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les charges de travail.

3. Identifiez les charges de travail les plus performantes du nœud qui a reçu l'événement :

- a. Retournez à la page de détails de l'événement.
- b. Dans le champ **Volumes concernés**, cliquez sur le lien correspondant au nombre de volumes.

La vue Performances : Tous les volumes s'affiche avec une liste filtrée des volumes sur ce nœud.

- c. Cliquez sur la colonne **Capacité totale** pour trier les volumes en fonction du plus grand espace alloué.

Cela fournit une liste de volumes potentiels que vous souhaitez peut-être déplacer.

- d. Notez les noms des volumes que vous souhaitez déplacer et les noms des agrégats actuels sur lesquels ils résident.

4. Déplacez les volumes vers les agrégats que vous avez identifiés comme ayant une faible utilisation sur le nouveau nœud.

Vous pouvez effectuer l'opération de déplacement à l'aide d' ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacer les charges de travail vers un nœud dans une autre paire HA

Vous pouvez utiliser Unified Manager pour vous aider à identifier un agrégat sur un nœud dans une paire haute disponibilité (HA) différente qui dispose d'une capacité de performance libre supérieure à la paire HA sur laquelle vos charges de travail s'exécutent actuellement. Vous pouvez ensuite déplacer les volumes sélectionnés vers des agrégats sur la nouvelle paire HA.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Votre cluster doit être composé d'au moins deux paires HA

Vous ne pouvez pas utiliser ce processus de correction si vous n'avez qu'une seule paire HA dans votre cluster.

- Vous devez avoir enregistré les noms des deux nœuds de la paire HA qui rencontrent actuellement un problème de performances.
- Vous devez avoir enregistré la date et l'heure à laquelle les nœuds ont reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé les données de performance pendant un mois ou plus.

Le déplacement de charges de travail hautement performantes vers un agrégat sur un nœud avec plus de capacité de performance libre permet aux charges de travail sur les deux nœuds de fonctionner plus efficacement. Cette procédure vous aide à identifier les ressources suivantes afin de pouvoir déplacer des charges de travail très performantes vers un nœud disposant de plus de capacité de performance libre sur une autre paire HA :

- Les nœuds d'une paire HA différente sur le même cluster qui ont la plus grande capacité de performance libre
- Les agrégats sur les nouveaux nœuds qui ont la plus grande capacité de performance libre
- Les volumes les plus performants sur les nœuds actuels

Étapes

1. Identifiez les nœuds qui font partie d'une paire HA différente sur le même cluster :

- a. Sur la page **Détails de l'événement**, cliquez sur le nom du cluster sur lequel résident les nœuds.

Les détails du cluster sont affichés sur la page d'accueil Performances/Cluster.

- b. Sur la page **Résumé**, cliquez sur **Nœuds** dans le volet **Objets gérés**.

La liste des nœuds de ce cluster s'affiche dans la vue Performances : Tous les nœuds.

- c. Notez les noms des nœuds qui se trouvent dans des paires HA différentes de la paire HA qui rencontre actuellement un problème de performances.

2. Identifiez un nœud dans la nouvelle paire HA qui a la plus grande capacité de performance libre :

- a. Dans la vue **Performance : Tous les nœuds**, cliquez sur la colonne **Capacité de performance utilisée** pour trier les nœuds par pourcentage le plus faible utilisé.

Cela fournit une liste de nœuds potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

- b. Notez le nom du nœud sur une autre paire HA vers laquelle vous souhaitez déplacer les charges de travail.

3. Identifiez un agrégat sur le nouveau nœud qui a la plus grande capacité de performance libre :

- a. Dans la vue **Performance : tous les nœuds**, cliquez sur le nœud.

Les détails du nœud sont affichés dans la page Performances/Explorateur de nœuds.

- b. Dans le menu **Afficher et comparer**, sélectionnez **Agrégats sur ce nœud**.

Les agrégats de ce nœud sont affichés dans la grille.

- c. Cliquez sur la colonne **Capacité de performance utilisée** pour trier les agrégats par ordre de moindre utilisation.

Cela fournit une liste d'agrégats potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

- d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les charges de travail.
4. Identifiez les charges de travail les plus performantes des nœuds qui ont reçu l'événement :
 - a. Retournez à la page de détails de l'événement.
 - b. Dans le champ **Volumes affectés**, cliquez sur le lien correspondant au nombre de volumes pour le premier nœud.

La vue Performances : Tous les volumes s'affiche avec une liste filtrée des volumes sur ce nœud.
 - c. Cliquez sur la colonne **Capacité totale** pour trier les volumes en fonction du plus grand espace alloué.

Cela fournit une liste de volumes potentiels que vous souhaitez peut-être déplacer.
 - d. Notez les noms des volumes que vous souhaitez déplacer et les noms des agrégats actuels sur lesquels ils résident.
 - e. Exécutez les étapes 4c et 4d pour le deuxième nœud qui faisait partie de cet événement afin d'identifier les volumes possibles que vous souhaitez également déplacer à partir de ce nœud.
5. Déplacez les volumes vers les agrégats que vous avez identifiés comme ayant la plus grande capacité de performance libre sur le nouveau nœud.

Vous pouvez effectuer l'opération de déplacement à l'aide d' ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vous pouvez vérifier si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacer les charges de travail vers un autre nœud dans une autre paire HA

Vous pouvez utiliser Unified Manager pour vous aider à identifier un agrégat sur un nœud dans une paire HA différente qui est moins occupée que la paire HA sur laquelle vos charges de travail s'exécutent actuellement. Vous pouvez ensuite déplacer les volumes sélectionnés vers des agrégats sur la nouvelle paire HA. Le déplacement de charges de travail hautement performantes vers un agrégat sur un nœud moins occupé permet aux charges de travail sur les deux nœuds de fonctionner plus efficacement.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Votre cluster doit être composé d'au moins deux paires HA ; vous ne pouvez pas utiliser ce processus de correction si vous n'avez qu'une seule paire HA dans votre cluster.
- Vous devez avoir enregistré les noms des deux nœuds de la paire HA qui rencontrent actuellement le problème de performances.
- Vous devez avoir enregistré la date et l'heure à laquelle les nœuds ont reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé un mois ou plus de données de performance.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les charges de travail les plus performantes vers un nœud moins utilisé sur une autre paire HA :

- Les nœuds d'une paire HA différente sur le même cluster qui sont moins utilisés
- Les agrégats sur les nouveaux nœuds qui sont les moins utilisés

- Les volumes les plus performants sur les nœuds actuels

Étapes

1. Identifiez les nœuds qui font partie d'une paire HA différente sur le même cluster :

- Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters** et sélectionnez **Performances > Tous les clusters** dans le menu Affichage.

La vue Performances : tous les clusters s'affiche.

- Cliquez sur le numéro dans le champ **Nombre de nœuds** pour le cluster actuel.

La vue Performances : tous les nœuds s'affiche.

- Notez les noms des nœuds qui se trouvent dans des paires HA différentes de la paire HA qui rencontre actuellement le problème de performances.

2. Identifiez un nœud dans la nouvelle paire HA qui est le moins utilisé :

- Cliquez sur la colonne **Utilisation** pour trier les nœuds par ordre d'utilisation.

Vous pouvez également identifier les nœuds qui ont la plus grande **capacité libre**. Cela fournit une liste de nœuds potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

- Notez le nom du nœud vers lequel vous souhaitez déplacer les charges de travail.

3. Identifiez un agrégat sur le nouveau nœud qui est le moins utilisé :

- Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats** et sélectionnez **Performances > Tous les agrégats** dans le menu Affichage.

La vue Performances : tous les agrégats s'affiche.

- Cliquez sur **Filtrage**, sélectionnez **Nœud** dans le menu déroulant de gauche, saisissez le nom du nœud dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

La vue Performances : Tous les agrégats s'affiche à nouveau avec la liste des agrégats disponibles sur ce nœud.

- Cliquez sur la colonne **Utilisation** pour trier les agrégats par ordre d'utilisation.

Vous pouvez également identifier les agrégats qui ont la plus grande **capacité libre**. Cela fournit une liste d'agrégats potentiels vers lesquels vous souhaitez peut-être déplacer des charges de travail.

- Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les charges de travail.

4. Identifiez les charges de travail les plus performantes des nœuds qui ont reçu l'événement :

- Retournez à la page de détails de l'événement.

- Dans le champ **Volumes affectés**, cliquez sur le lien correspondant au nombre de volumes pour le premier nœud.

La vue Performances : Tous les volumes s'affiche avec une liste filtrée des volumes sur ce nœud.

- Cliquez sur la colonne **Capacité totale** pour trier les volumes en fonction du plus grand espace alloué.

Cela fournit une liste de volumes potentiels que vous souhaitez peut-être déplacer.

- d. Notez les noms des volumes que vous souhaitez déplacer et les noms des agrégats actuels sur lesquels ils résident.
 - e. Exécutez les étapes 4c et 4d pour le deuxième nœud qui faisait partie de cet événement afin d'identifier les volumes possibles que vous souhaitez également déplacer à partir de ce nœud.
5. Déplacez les volumes vers les agrégats que vous avez identifiés comme ayant une faible utilisation sur le nouveau nœud.

Vous pouvez effectuer l'opération de déplacement à l'aide d' ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Utilisez les paramètres de stratégie QoS pour prioriser le travail sur ce nœud

Vous pouvez définir une limite sur un groupe de stratégies QoS pour contrôler la limite de débit d'E/S par seconde (IOPS) ou Mbit/s pour les charges de travail qu'il contient. Si les charges de travail se trouvent dans un groupe de stratégies sans limite définie, tel que le groupe de stratégies par défaut, ou si la limite définie ne répond pas à vos besoins, vous pouvez augmenter la limite définie ou déplacer les charges de travail vers un groupe de stratégies nouveau ou existant qui a la limite souhaitée.

Si un événement de performances sur un nœud est provoqué par des charges de travail surutilisant les ressources du nœud, la description de l'événement sur la page Détails de l'événement affiche un lien vers la liste des volumes impliqués. Dans la page Performances/Volumes, vous pouvez trier les volumes affectés par IOPS et Mbit/s pour voir quelles charges de travail ont l'utilisation la plus élevée qui pourrait avoir contribué à l'événement.

En attribuant les volumes qui utilisent de manière excessive les ressources du nœud à un paramètre de groupe de stratégies plus restrictif, le groupe de stratégies limite les charges de travail pour restreindre leur activité, ce qui peut réduire l'utilisation des ressources sur ce nœud.

Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour gérer les groupes de stratégies, y compris les tâches suivantes :

- Création d'un groupe de politiques
- Ajout ou suppression de charges de travail dans un groupe de stratégies
- Déplacer une charge de travail entre des groupes de stratégies
- Modification de la limite de débit d'un groupe de politiques

Supprimer les volumes et les LUN inactifs

Lorsque l'espace libre agrégé a été identifié comme un problème, vous pouvez rechercher les volumes et les LUN inutilisés et les supprimer de l'agrégat. Cela peut aider à résoudre le problème de manque d'espace disque.

Si un événement de performance sur un agrégat est causé par un espace disque insuffisant, il existe plusieurs manières de déterminer quels volumes et LUN ne sont plus utilisés.

Pour identifier les volumes inutilisés :

- Sur la page Détails de l'événement, le champ **Nombre d'objets affectés** fournit un lien qui affiche la liste des volumes affectés.

Cliquez sur le lien pour afficher les volumes dans la vue Performances : Tous les volumes. À partir de là, vous pouvez trier les volumes affectés par **IOPS** pour voir quels volumes n'ont pas été actifs.

Pour identifier les LUN inutilisés :

1. À partir de la page Détails de l'événement, notez le nom de l'agrégat sur lequel l'événement s'est produit.
2. Dans le volet de navigation de gauche, cliquez sur **Stockage > LUN** et sélectionnez **Performances > Tous les LUN** dans le menu Affichage.
3. Cliquez sur **Filtrage**, sélectionnez **Agrégat** dans le menu déroulant de gauche, saisissez le nom de l'agrégat dans le champ de texte, puis cliquez sur **Appliquer le filtre**.
4. Triez la liste résultante des LUN affectés par **IOPS** pour afficher les LUN qui ne sont pas actifs.

Une fois que vous avez identifié les volumes et les LUN inutilisés, vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour supprimer ces objets.

Ajouter des disques et effectuer une reconstruction de la disposition globale

Vous pouvez ajouter des disques à un agrégat pour augmenter la capacité de stockage et les performances de cet agrégat. Après avoir ajouté les disques, vous ne constatez une amélioration des performances qu'après la reconstruction de l'agrégat.

Lorsque vous recevez un événement de seuil défini par le système sur la page Détails de l'événement, le texte de description de l'événement répertorie le nom de l'agrégat qui rencontre le problème. Vous pouvez ajouter des disques et reconstruire des données sur cet agrégat.

Les disques que vous ajoutez à l'agrégat doivent déjà exister dans le cluster. Si le cluster ne dispose pas de disques supplémentaires disponibles, vous devrez peut-être contacter votre administrateur ou acheter des disques supplémentaires. Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour ajouter des disques à un agrégat.

["Rapport technique 3838 : Guide de configuration du sous-système de stockage"](#)

Configurer une connexion entre un serveur Unified Manager et un fournisseur de données externe

Une connexion entre un serveur Unified Manager et un fournisseur de données externe vous permet d'envoyer des données de performances de cluster à un serveur externe afin que les gestionnaires de stockage puissent tracer les mesures de performances à l'aide d'un logiciel tiers.

Une connexion entre un serveur Unified Manager et un fournisseur de données externe est établie via l'option de menu intitulée « Fournisseur de données externe » dans la console de maintenance.

Données de performance pouvant être envoyées à un serveur externe

Unified Manager collecte une variété de données de performances à partir de tous les

clusters qu'il surveille. Vous pouvez envoyer des groupes spécifiques de données à un serveur externe.

En fonction des données de performance que vous souhaitez représenter graphiquement, vous pouvez choisir d'envoyer l'un des groupes de statistiques suivants :

Groupe de statistiques	Données incluses	Détails
Moniteur de performances	Statistiques de performances de haut niveau pour les objets suivants : • LUN • Volumes	Ce groupe fournit le nombre total d'IOPS ou de latences pour tous les LUN et volumes de tous les clusters surveillés. Ce groupe fournit le plus petit nombre de statistiques.
Utilisation des ressources	Statistiques d'utilisation des ressources pour les objets suivants : • Nœuds • Agrégats	Ce groupe fournit des statistiques d'utilisation pour le nœud et les ressources physiques agrégées dans tous les clusters surveillés. Il fournit également les statistiques collectées dans le groupe Moniteur de performances.
Zoom avant	Statistiques de lecture/écriture de bas niveau et par protocole pour tous les objets suivis : • Nœuds • Agrégats • LUN • Volumes • Disques • Les LIF • Ports/cartes réseau	Ce groupe fournit des répartitions en lecture/écriture et par protocole pour les sept types d'objets suivis dans tous les clusters surveillés. Il fournit également les statistiques collectées dans le groupe Moniteur de performances et dans le groupe Utilisation des ressources. Ce groupe fournit le plus grand nombre de statistiques.



Si le nom d'un cluster ou d'un objet de cluster est modifié sur le système de stockage, l'ancien et le nouveau objet contiendront des données de performances sur le serveur externe (appelé « metric_path »). Les deux objets ne sont pas corrélés comme le même objet. Par exemple, si vous modifiez le nom d'un volume de « volume1_acct » à « acct_vol1 », vous verrez les anciennes données de performances pour l'ancien volume et les nouvelles données de performances pour le nouveau volume.

Consultez l'article 30096 de la base de connaissances pour obtenir la liste de tous les compteurs de performances qui peuvent être envoyés à un fournisseur de données externe.

["Compteurs de performances Unified Manager pouvant être exportés vers un fournisseur de données externe"](#)

Configurer Graphite pour recevoir les données de performance d'Unified Manager

Graphite est un outil logiciel ouvert permettant de collecter et de représenter graphiquement les données de performances des systèmes informatiques. Votre serveur et votre logiciel Graphite doivent être configurés correctement pour recevoir des données statistiques d'Unified Manager.

NetApp ne teste ni ne vérifie les versions spécifiques de Graphite ou d'autres outils tiers.



Le serveur Graphite ne reçoit pas de données de performances pour les volumes d'Unified Manager.

Après avoir installé Graphite conformément aux instructions d'installation, vous devez apporter les modifications suivantes pour prendre en charge le transfert de données statistiques depuis Unified Manager :

- Dans le `/opt/graphite/conf/carbon.conf` fichier, le nombre maximum de fichiers pouvant être créés sur le serveur Graphite par minute doit être défini sur 200(**MAX_CREATES_PER_MINUTE = 200**).

Selon le nombre de clusters dans votre configuration et les objets statistiques que vous avez sélectionnés pour l'envoi, il peut y avoir des milliers de nouveaux fichiers qui doivent être créés initialement. À 200 fichiers par minute, il faudra peut-être 15 minutes ou plus avant que tous les fichiers métriques soient initialement créés. Une fois tous les fichiers métriques uniques créés, ce paramètre n'est plus pertinent.

- Si vous exécutez Graphite sur un serveur déployé à l'aide d'une adresse IPv6, la valeur de `LINE_RECEIVER_INTERFACE` dans le `/opt/graphite/conf/carbon.conf` le fichier doit être modifié de « 0.0.0.0 » à « :: »(**LINE_RECEIVER_INTERFACE = ::**)
- Dans le `/opt/graphite/conf/storage-schemas.conf` fichier, le `retentions` le paramètre doit être utilisé pour définir la fréquence sur 5 minutes et la période de conservation sur le nombre de jours pertinent pour votre environnement.

La période de conservation peut être aussi longue que votre environnement le permet, mais la valeur de fréquence doit être définie sur 5 minutes pour au moins un paramètre de conservation. Dans l'exemple suivant, une section est définie pour Unified Manager à l'aide de `pattern` paramètre et les valeurs définissent la fréquence initiale à 5 minutes et la période de conservation à 100 jours : **[OPM]**

```
pattern = ^netapp-performance\..
```

```
retentions = 5m:100d
```



Si la balise du fournisseur par défaut est modifiée de « netapp-performance » à quelque chose de différent, cette modification doit être reflétée dans le `pattern` paramètre également.



Si le serveur Graphite n'est pas disponible lorsque le serveur Unified Manager tente d'envoyer des données de performances, les données ne sont pas envoyées et il y aura un écart dans les données collectées.

Configurer une connexion d'un serveur Unified Manager à un fournisseur de données externe

Unified Manager peut envoyer des données de performances du cluster à un serveur externe. Vous pouvez spécifier le type de données statistiques envoyées et l'intervalle auquel les données sont envoyées.

Avant de commencer

- Vous devez disposer d'un identifiant utilisateur autorisé à vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez disposer des informations suivantes sur le fournisseur de données externe :
 - Nom du serveur ou adresse IP (IPv4 ou IPv6)
 - Port par défaut du serveur (si vous n'utilisez pas le port par défaut 2003)
- Vous devez avoir configuré le serveur distant et le logiciel tiers afin qu'il puisse recevoir des données statistiques du serveur Unified Manager.
- Vous devez savoir quel groupe de statistiques vous souhaitez envoyer :
 - PERFORMANCE_INDICATOR : Statistiques du moniteur de performances
 - RESOURCE_UTILIZATION : Statistiques d'utilisation des ressources et de surveillance des performances
 - DRILL_DOWN : Toutes les statistiques
- Vous devez connaître l'intervalle de temps auquel vous souhaitez transmettre les statistiques : 5, 10 ou 15 minutes

Par défaut, Unified Manager collecte des statistiques à des intervalles de 5 minutes. Si vous définissez l'intervalle de transmission sur 10 (ou 15) minutes, la quantité de données envoyées lors de chaque transmission est deux (ou trois) fois plus importante que lorsque vous utilisez l'intervalle par défaut de 5 minutes.



Si vous modifiez l'intervalle de collecte des performances d'Unified Manager à 10 ou 15 minutes, vous devez modifier l'intervalle de transmission afin qu'il soit égal ou supérieur à l'intervalle de collecte d'Unified Manager.

Vous pouvez configurer une connexion entre un serveur Unified Manager et un serveur de fournisseur de données externe.

Étapes

1. Connectez-vous en tant qu'utilisateur de maintenance à la console de maintenance du serveur Unified Manager.

Les invites de la console de maintenance d'Unified Manager s'affichent.

2. Dans la console de maintenance, saisissez le numéro de l'option de menu **Fournisseur de données externes**.

Le menu Connexion au serveur externe s'affiche.

3. Tapez le numéro de l'option de menu **Ajouter/Modifier la connexion au serveur**.

Les informations de connexion actuelles au serveur sont affichées.

4. Lorsque vous y êtes invité, saisissez **y** pour continuer.
5. Lorsque vous y êtes invité, entrez l'adresse IP ou le nom du serveur de destination et les informations sur le port du serveur (si différent du port par défaut 2003).
6. Lorsque vous y êtes invité, saisissez **y** pour vérifier que les informations que vous avez saisies sont correctes.
7. Appuyez sur n'importe quelle touche pour revenir au menu Connexion au serveur externe.
8. Tapez le numéro de l'option de menu **Modifier la configuration du serveur**.

Les informations de configuration actuelles du serveur sont affichées.

9. Lorsque vous y êtes invité, saisissez **y** pour continuer.
10. Lorsque vous y êtes invité, saisissez le type de statistiques à envoyer, l'intervalle de temps auquel les statistiques sont envoyées et si vous souhaitez activer la transmission des statistiques maintenant :

Pour..	Entrer...
ID du groupe de statistiques	0 - PERFORMANCE_INDICATOR (par défaut) 1 - UTILISATION DES RESSOURCES 2 - DRILL_DOWN
Étiquette du fournisseur	Un nom descriptif pour le dossier dans lequel les statistiques seront stockées sur le serveur externe. "netapp-performance" est le nom par défaut, mais vous pouvez saisir une autre valeur. En utilisant la notation pointée, vous pouvez définir une structure de dossiers hiérarchique. Par exemple, en entrant stats.performance.netapp les statistiques seront situées dans stats > performance > netapp.
Intervalle de transmission	5 (défaut), 10 , ou 15 minutes
Activer/désactiver	0 - Désactiver 1 - Activer (par défaut)

11. Lorsque vous y êtes invité, saisissez **y** pour vérifier que les informations que vous avez saisies sont correctes.
12. Appuyez sur n'importe quelle touche pour revenir au menu Connexion au serveur externe.
13. Taper **x** pour quitter la console de maintenance.

Une fois la connexion configurée, les données de performances sélectionnées sont envoyées au serveur de destination à l'intervalle de temps que vous avez spécifié. Il faut quelques minutes avant que les métriques commencent à apparaître dans l'outil externe. Vous devrez peut-être actualiser votre navigateur pour voir les

nouvelles mesures dans la hiérarchie des mesures.

Surveiller et gérer la santé du cluster

Introduction à la surveillance de l'état de santé Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous aide à surveiller un grand nombre de systèmes exécutant le logiciel ONTAP via une interface utilisateur centralisée. L'infrastructure du serveur Unified Manager offre une évolutivité, une capacité de support et des capacités de surveillance et de notification améliorées.

Les principales fonctionnalités d'Unified Manager incluent la surveillance, l'alerte, la gestion de la disponibilité et de la capacité des clusters, la gestion des capacités de protection et le regroupement des données de diagnostic et leur envoi au support technique.

Vous pouvez utiliser Unified Manager pour surveiller vos clusters. Lorsque des problèmes surviennent dans le cluster, Unified Manager vous informe des détails de ces problèmes via des événements. Certains événements vous proposent également une mesure corrective que vous pouvez prendre pour corriger les problèmes. Vous pouvez configurer des alertes pour les événements afin que lorsque des problèmes surviennent, vous soyez averti par e-mail et par des interruptions SNMP.

Vous pouvez utiliser Unified Manager pour gérer les objets de stockage dans votre environnement en les associant à des annotations. Vous pouvez créer des annotations personnalisées et associer dynamiquement des clusters, des machines virtuelles de stockage (SVM) et des volumes aux annotations via des règles.

Vous pouvez également planifier les besoins de stockage de vos objets de cluster à l'aide des informations fournies dans les graphiques de capacité et d'état, pour l'objet de cluster concerné.

Capacité physique et logique

Unified Manager utilise les concepts d'espace physique et logique utilisés pour les objets de stockage ONTAP.

- **Capacité physique** : l'espace physique fait référence aux blocs physiques de stockage utilisés dans le volume. La « capacité physique utilisée » est généralement inférieure à la capacité logique utilisée en raison de la réduction des données résultant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- **Capacité logique** : L'espace logique fait référence à l'espace utilisable (les blocs logiques) dans un volume. L'espace logique fait référence à la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats de la déduplication ou de la compression. « L'espace logique utilisé » correspond à l'espace physique utilisé, plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure apparaît souvent plus grande que la capacité physique utilisée car elle ne reflète pas la compression des données et les autres réductions de l'espace physique. Ainsi, la capacité logique totale pourrait être supérieure à l'espace provisionné.

Unités de mesure de capacité

Unified Manager calcule la capacité de stockage en fonction d'unités binaires de 1024 (2^{10}) octets. Dans ONTAP 9.10.0 et les versions antérieures, ces unités étaient affichées sous la forme Ko, Mo, Go, To et Po. À partir d'ONTAP 9.10.1, ils sont affichés dans Unified Manager sous la forme Kio, Mio, Gio, Tio et Pio.



Les unités utilisées pour le débit continuent d'être les kilooctets par seconde (Kbps), les mégaoctets par seconde (Mbps), les gigaoctets par seconde (Gbps) ou les téraoctets par seconde (Tbps), etc., pour toutes les versions d' ONTAP.

Unité de capacité affichée dans Unified Manager pour ONTAP 9.10.0 et versions antérieures	Unité de capacité affichée dans Unified Manager pour ONTAP 9.10.1	Calcul	Valeur en octets
Ko	KiB	1024	1024 octets
MB	Mio	1024 * 1024	1 048 576 octets
GB	Gio	1024 * 1024 * 1024	1 073 741 824 octets
To	Tio	1024 * 1024 * 1024 * 1024	1 099 511 627 776 octets

Fonctionnalités de surveillance de l'état de santé d'Unified Manager

Unified Manager repose sur une infrastructure de serveur qui offre évolutivité, prise en charge et capacités de surveillance et de notification améliorées. Unified Manager prend en charge la surveillance des systèmes exécutant le logiciel ONTAP .

Unified Manager comprend les fonctionnalités suivantes :

- Découverte, surveillance et notifications pour les systèmes installés avec le logiciel ONTAP :
 - Objets physiques : nœuds, disques, étagères de disques, paires SFO, ports et cache Flash
 - Objets logiques : clusters, machines virtuelles de stockage (SVM), agrégats, volumes, LUN, espaces de noms, qtrees, LIF, copies Snapshot, chemins de jonction, partages NFS, partages SMB, quotas d'utilisateurs et de groupes, groupes de politiques QoS et groupes d'initiateurs
 - Protocoles : CIFS, NFS, FC, iSCSI, NVMe et FCoE
 - Efficacité du stockage : agrégats SSD, agrégats Flash Pool, agrégats FabricPool , déduplication et compression
 - Protection : relations SnapMirror (synchrone et asynchrone) et relations SnapVault
- Affichage de l'état de découverte et de surveillance du cluster
- Configurations MetroCluster sur FC et IP : affichage et surveillance de la configuration, des problèmes et de l'état de connectivité des composants du cluster. Commutateurs et ponts MetroCluster pour les configurations MetroCluster sur FC
- Alertes, événements et infrastructure de seuil améliorés
- Authentification LDAP, LDAPS, SAML et prise en charge des utilisateurs locaux
- RBAC (pour un ensemble prédéfini de rôles)
- AutoSupport et pack d'assistance
- Tableau de bord amélioré pour afficher la capacité, la disponibilité, la protection et les performances de

l'environnement

- Interopérabilité des déplacements de volumes, historique des déplacements de volumes et historique des modifications des chemins de jonction
- Zone d'impact qui affiche graphiquement les ressources impactées par des événements tels que Certains disques défaillants, La mise en miroir agrégée MetroCluster dégradée et Les disques de rechange MetroCluster laissés pour compte
- Zone d'effet possible qui affiche l'effet des événements MetroCluster
- Zone d'actions correctives suggérées qui affiche les actions qui peuvent être effectuées pour résoudre des événements tels que Certains disques défectueux, La mise en miroir agrégée MetroCluster dégradée et Les disques de rechange MetroCluster laissés pour compte
- Zone Ressources susceptibles d'être impactées qui affiche les ressources susceptibles d'être impactées par des événements tels que l'événement Volume hors ligne, l'événement Volume restreint et l'événement Espace de volume à provisionnement léger à risque
- Prise en charge des SVM avec volumes FlexVol ou FlexGroup
- Prise en charge de la surveillance des volumes racine des nœuds
- Surveillance améliorée des copies d'instantanés, y compris le calcul de l'espace récupérable et la suppression des copies d'instantanés
- Annotations pour les objets de stockage
- Création et gestion de rapports sur les informations des objets de stockage, telles que la capacité physique et logique, l'utilisation, les économies d'espace, les performances et les événements associés
- Intégration avec OnCommand Workflow Automation pour exécuter des workflows

Storage Automation Store contient des packs de flux de travail de stockage automatisés certifiés NetApp développés pour être utilisés avec OnCommand Workflow Automation (WFA). Vous pouvez télécharger les packs, puis les importer dans WFA pour les exécuter. Les flux de travail automatisés sont disponibles ici :

["Magasin d'automatisation du stockage"](#)

Interfaces Unified Manager utilisées pour gérer l'état du système de stockage

Ces sections contiennent des informations sur les deux interfaces utilisateur fournies par Active IQ Unified Manager pour résoudre les problèmes de capacité de stockage, de disponibilité et de protection des données. Les deux interfaces utilisateur sont l'interface Web Unified Manager et la console de maintenance.

Si vous souhaitez utiliser les fonctionnalités de protection dans Unified Manager, vous devez également installer et configurer OnCommand Workflow Automation (WFA).

Interface utilisateur Web d'Unified Manager

L'interface utilisateur Web d'Unified Manager permet à un administrateur de surveiller et de résoudre les problèmes de cluster liés à la capacité de stockage, à la disponibilité et à la protection des données.

Ces sections décrivent certains flux de travail courants qu'un administrateur peut suivre pour résoudre les problèmes de capacité de stockage, de disponibilité des données ou de protection affichés dans l'interface utilisateur Web d'Unified Manager.

Console de maintenance

La console de maintenance Unified Manager permet à un administrateur de surveiller, de diagnostiquer et de résoudre les problèmes de système d'exploitation, les problèmes de mise à niveau de version, les problèmes d'accès utilisateur et les problèmes de réseau liés au serveur Unified Manager lui-même. Si l'interface Web d'Unified Manager n'est pas disponible, la console de maintenance est la seule forme d'accès à Unified Manager.

Vous pouvez utiliser ces informations pour accéder à la console de maintenance et l'utiliser pour résoudre les problèmes liés au fonctionnement du serveur Unified Manager.

Gestion et surveillance des clusters et de la santé des objets du cluster

Unified Manager utilise des requêtes API périodiques et un moteur de collecte de données pour collecter les données des clusters. En ajoutant des clusters à la base de données Unified Manager, vous pouvez surveiller et gérer ces clusters pour détecter tout risque de disponibilité et de capacité.

Comprendre la surveillance des clusters

Vous pouvez ajouter des clusters à la base de données Unified Manager pour surveiller la disponibilité, la capacité et d'autres détails des clusters, tels que l'utilisation du processeur, les statistiques d'interface, l'espace disque libre, l'utilisation de qtree et l'environnement du châssis.

Des événements sont générés si l'état est anormal ou lorsqu'un seuil prédéfini est dépassé. Si configuré pour le faire, Unified Manager envoie une notification à un destinataire spécifié lorsqu'un événement déclenche une alerte.

Comprendre les volumes racine des nœuds

Vous pouvez surveiller le volume racine du nœud à l'aide d'Unified Manager. La meilleure pratique est que le volume racine du nœud ait une capacité suffisante pour empêcher le nœud de tomber en panne.

Lorsque la capacité utilisée du volume racine du nœud dépasse 80 % de la capacité totale du volume racine du nœud, l'événement Espace du volume racine du nœud presque plein est généré. Vous pouvez configurer une alerte pour l'événement pour recevoir une notification. Vous pouvez prendre les mesures appropriées pour empêcher la panne du nœud en utilisant ONTAP System Manager ou l'interface de ligne de commande ONTAP .



La fonctionnalité de surveillance des volumes racine des nœuds n'est pas disponible si les clusters exécutent la version ONTAP 9.14.1 ou ultérieure.

Comprendre les événements et les seuils pour les agrégats de racines de nœuds

Vous pouvez surveiller l'agrégat racine du nœud à l'aide d'Unified Manager. La meilleure pratique consiste à provisionner de manière épaisse le volume racine dans l'agrégat racine pour empêcher l'arrêt du nœud.

Par défaut, les événements de capacité et de performances ne sont pas générés pour les agrégats racine. De plus, les valeurs de seuil utilisées par Unified Manager ne s'appliquent pas aux agrégats racines des nœuds. Seul un représentant du support technique peut modifier les paramètres pour que ces événements soient générés. Lorsque les paramètres sont modifiés par le représentant du support technique, les valeurs de seuil de capacité sont appliquées à l'agrégat racine du nœud.

Vous pouvez prendre les mesures appropriées pour empêcher l'arrêt du nœud en utilisant ONTAP System Manager ou l'interface de ligne de commande ONTAP .



La fonctionnalité de surveillance des agrégats racines de nœuds n'est pas disponible si les clusters exécutent la version ONTAP 9.14.1 ou ultérieure.

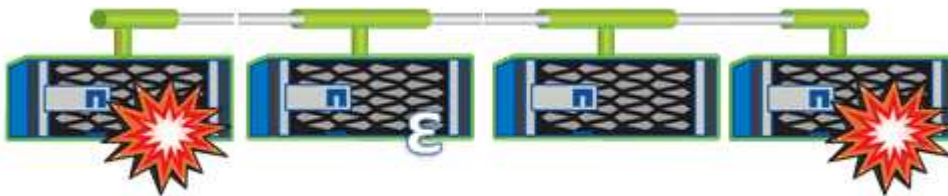
Comprendre le quorum et l'épsilon

Le quorum et l'épsilon sont des mesures importantes de la santé et du fonctionnement des clusters qui, ensemble, indiquent comment les clusters relèvent les défis potentiels en matière de communication et de connectivité.

Quorum est une condition préalable pour un cluster pleinement fonctionnel. Lorsqu'un cluster est en quorum, une simple majorité de nœuds sont sains et peuvent communiquer entre eux. Lorsque le quorum est perdu, le cluster perd la capacité d'accomplir les opérations normales du cluster. Un seul ensemble de nœuds peut avoir le quorum à un moment donné, car tous les nœuds partagent collectivement une vue unique des données. Par conséquent, si deux nœuds non communicants sont autorisés à modifier les données de manière divergente, il n'est plus possible de rapprocher les données dans une vue de données unique.

Chaque nœud du cluster participe à un protocole de vote qui élit un nœud maître ; chaque nœud restant est un nœud secondaire. Le nœud maître est responsable de la synchronisation des informations sur l'ensemble du cluster. Lorsque le quorum est atteint, il est maintenu par un vote continu. Si le nœud maître est hors ligne et que le cluster est toujours en quorum, un nouveau maître est élu par les nœuds qui restent en ligne.

Étant donné qu'il existe un risque d'égalité dans un cluster comportant un nombre pair de nœuds, un nœud possède un poids de vote fractionnaire supplémentaire appelé epsilon. Si la connectivité entre deux parties égales d'un grand cluster échoue, le groupe de nœuds contenant epsilon maintient le quorum, en supposant que tous les nœuds sont sains. Par exemple, l'illustration suivante montre un cluster à quatre nœuds dans lequel deux des nœuds sont tombés en panne. Cependant, comme l'un des nœuds survivants détient epsilon, le cluster reste en quorum même s'il n'y a pas une majorité simple de nœuds sains.



Epsilon est automatiquement attribué au premier nœud lors de la création du cluster. Si le nœud qui contient epsilon devient défectueux, prend le contrôle de son partenaire de haute disponibilité ou est repris par son partenaire de haute disponibilité, alors epsilon est automatiquement réaffecté à un nœud sain dans une autre paire HA.

La mise hors ligne d'un nœud peut affecter la capacité du cluster à rester en quorum. Par conséquent, ONTAP émet un message d'avertissement si vous tentez une opération qui va soit sortir le cluster du quorum, soit le placer à une panne d'une perte de quorum. Vous pouvez désactiver les messages d'avertissement de quorum en utilisant la commande `cluster quorum-service options modify` au niveau de privilège avancé.

En général, en supposant une connectivité fiable entre les nœuds du cluster, un cluster plus grand est plus stable qu'un cluster plus petit. L'exigence de quorum d'une majorité simple de la moitié des nœuds plus epsilon est plus facile à maintenir dans un cluster de 24 nœuds que dans un cluster de deux nœuds.

Un cluster à deux nœuds présente des défis uniques pour maintenir le quorum. Les clusters à deux nœuds utilisent le cluster HA, dans lequel aucun nœud ne détient d'epsilon ; au lieu de cela, les deux nœuds sont interrogés en permanence pour garantir que si l'un des nœuds tombe en panne, l'autre dispose d'un accès complet en lecture-écriture aux données, ainsi que d'un accès aux interfaces logiques et aux fonctions de gestion.

Afficher la liste et les détails des clusters

Vous pouvez utiliser la vue Santé : Tous les clusters pour afficher votre inventaire de clusters. La vue Capacité : Tous les clusters vous permet d'afficher des informations résumées sur la capacité de stockage et l'utilisation dans tous les clusters.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez également afficher les détails des clusters individuels tels que l'état de santé, la capacité, la configuration, les LIF, les nœuds et les disques de ce cluster à l'aide de la page Détails du cluster/de l'état de santé.

Les détails de la vue Santé : Tous les clusters, de la vue Capacité : Tous les clusters et de la page Détails du cluster/Santé vous aident à planifier votre stockage. Par exemple, avant de provisionner un nouvel agrégat, vous pouvez sélectionner un cluster spécifique dans la vue Santé : tous les clusters et obtenir des détails sur la capacité pour déterminer si le cluster dispose de l'espace requis.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Dans le menu Affichage, sélectionnez la vue **Santé : Tous les clusters** pour afficher les informations d'intégrité ou la vue **Capacité : Tous les clusters** pour afficher les détails sur la capacité de stockage et l'utilisation dans tous les clusters.
3. Cliquez sur le nom d'un cluster pour afficher les détails complets du cluster dans la page de détails **Cluster / Santé**.

Informations connexes

- ["Page de détails sur les clusters/la santé"](#)
- ["Performances : vue Tous les clusters"](#)
- ["Surveillance des configurations MetroCluster"](#)
- ["Affichage de l'état de sécurité des clusters et des machines virtuelles de stockage"](#)
- ["Quels critères de sécurité sont évalués"](#)

Vérifier la santé des clusters dans une configuration MetroCluster

Vous pouvez utiliser Active IQ Unified Manager (Unified Manager) pour vérifier l'intégrité opérationnelle des clusters et de leurs composants dans les configurations MetroCluster over FC et MetroCluster over IP. Si les clusters ont été impliqués dans un événement de

performances détecté par Unified Manager, l'état d'intégrité peut vous aider à déterminer si un problème matériel ou logiciel a contribué à l'événement.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir analysé un événement de performance pour une configuration MetroCluster et obtenu le nom du cluster impliqué.
- Les deux clusters de la configuration MetroCluster sur FC et IP doivent être surveillés par la même instance de Unified Manager.

Déterminer l'état du cluster dans MetroCluster via la configuration FC

Suivez ces étapes pour déterminer l'état du cluster dans une configuration MetroCluster sur FC.

Étapes

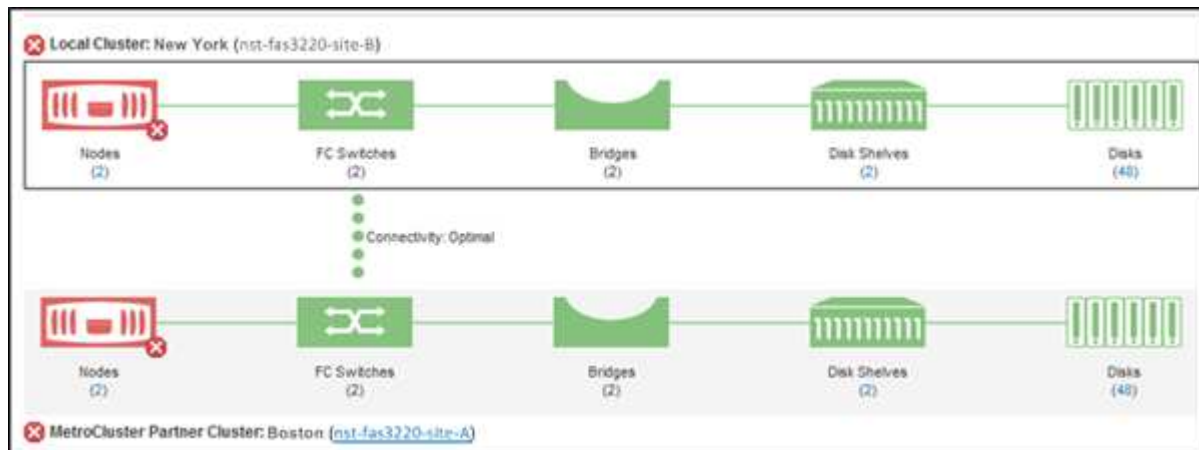
1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements** pour afficher la liste des événements.
2. Dans le panneau de filtre, sélectionnez tous les filtres MetroCluster sous la catégorie **Type de source**. Vous voyez tous les événements déclenchés dans votre environnement pour toutes les configurations MetroCluster .
3. À côté d'un événement MetroCluster , cliquez sur le nom du cluster.



Si aucun événement MetroCluster n'est affiché, vous pouvez utiliser la barre de recherche pour rechercher le nom du cluster impliqué dans l'événement lié à votre configuration MetroCluster sur FC.

La vue Santé : tous les clusters s'affiche avec des informations détaillées sur l'événement.

4. Sélectionnez l'onglet * MetroCluster Connectivity* pour afficher l'état de la connexion entre le cluster sélectionné et son cluster partenaire.

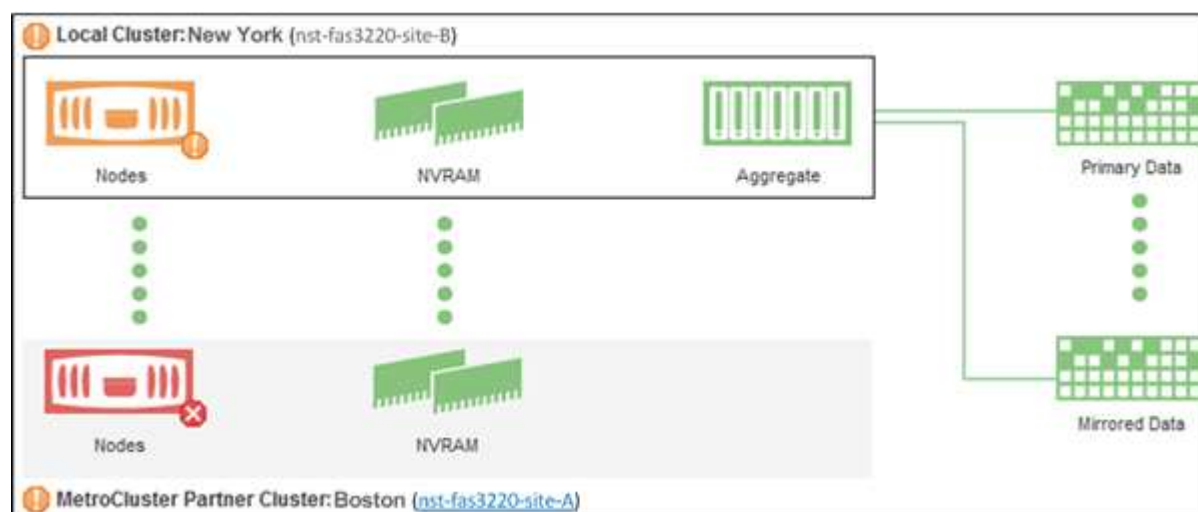


Dans cet exemple, les noms et les composants du cluster local et de son cluster partenaire sont affichés. Une icône jaune ou rouge indique un événement de santé pour le composant en surbrillance. L'icône Connectivité représente le lien entre les clusters. Vous pouvez pointer le curseur de votre souris sur une icône pour afficher les informations sur l'événement ou cliquer sur l'icône pour afficher les événements. Un problème de santé sur l'un ou l'autre cluster pourrait avoir contribué à l'événement de performance.

Unified Manager surveille le composant NVRAM du lien entre les clusters. Si l'icône des commutateurs FC

sur le cluster local ou partenaire ou l'icône de connectivité est rouge, un problème d'intégrité de la liaison peut avoir provoqué l'événement de performances.

5. Sélectionnez l'onglet * Réplication MetroCluster *.



Dans cet exemple, si l'icône NVRAM sur le cluster local ou partenaire est jaune ou rouge, un problème d'intégrité avec la NVRAM peut avoir provoqué l'événement de performance. S'il n'y a pas d'icônes rouges ou jaunes sur la page, un problème de performances sur le cluster partenaire peut avoir provoqué l'événement de performances.

Déterminer l'état du cluster dans la configuration MetroCluster sur IP

Suivez ces étapes pour déterminer l'état du cluster dans une configuration MetroCluster sur IP.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements** pour afficher la liste des événements.
2. Dans le panneau de filtre, sous la catégorie **Type de source**, sélectionnez le MetroCluster Relationship filtre. Vous voyez tous les événements déclenchés dans votre environnement pour toutes les configurations MetroCluster .



Si vous ne pouvez pas voir les événements MetroCluster signalés, vous pouvez utiliser la barre de recherche pour rechercher par nom du cluster impliqué dans l'événement lié à votre configuration MetroCluster sur IP.

3. À côté de l'événement MetroCluster concerné, cliquez sur le nom du cluster. La page Clusters s'affiche avec les détails de ce cluster. Pour plus d'informations sur la détermination des problèmes de santé, consultez ["Surveiller les problèmes de connectivité dans la configuration MetroCluster sur IP"](#) .

Afficher l'état de santé et de capacité de tous les clusters SAN Array

Vous pouvez utiliser les pages d'inventaire du cluster pour afficher l'état d'intégrité et de capacité de tous vos clusters SAN Array.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez afficher des informations générales sur tous les clusters SAN Array dans la vue Santé : Tous les clusters et la vue Capacité : Tous les clusters. De plus, vous pouvez afficher les détails dans la page Détails du cluster / Santé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Assurez-vous que la colonne « Personnalité » est affichée dans la vue **Santé : Tous les clusters** ou ajoutez-la à l'aide du contrôle **Afficher/Masquer**.

Cette colonne affiche « Toutes les baies SAN » pour vos clusters Toutes les baies SAN.
3. Vérifiez les informations.
4. Pour afficher des informations sur la capacité de stockage dans ces clusters, sélectionnez la vue Capacité : Tous les clusters.
5. Pour afficher des informations détaillées sur l'état et la capacité de stockage de ces clusters, cliquez sur le nom d'un cluster All SAN Array.

Afficher les détails dans les onglets Santé, Capacité et Nœuds dans la page Détails du cluster/Santé

Afficher la liste et les détails des nœuds

Vous pouvez utiliser la vue Santé : tous les nœuds pour afficher la liste des nœuds de vos clusters. Vous pouvez utiliser la page Détails du cluster/de l'état de santé pour afficher des informations détaillées sur les nœuds qui font partie du cluster surveillé.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez afficher des détails tels que l'état du nœud, le cluster qui contient le nœud, les détails de la capacité globale (utilisée et totale) et les détails de la capacité brute (utilisable, de réserve et totale). Vous pouvez également obtenir des informations sur les paires HA, les étagères de disques et les ports.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Nœuds**.
2. Dans la vue **Santé : Tous les nœuds**, cliquez sur le nœud dont vous souhaitez afficher les détails.

Les informations détaillées du nœud sélectionné sont affichées dans la page Détails du cluster / Santé. Le volet de gauche affiche la liste des paires HA. Par défaut, les détails HA sont ouverts, ce qui affiche les détails de l'état HA et les événements liés à la paire HA sélectionnée.

3. Pour afficher d'autres détails sur le nœud, effectuez l'action appropriée :

Pour voir...	Cliquez...
Détails sur les étagères de disques	Étagères à disques.
Informations relatives au port	Ports.

Pour plus d'informations, voir :

- "Performances : vue Tous les nœuds"
- "Affichage des valeurs IOPS disponibles pour les nœuds et les agrégats"
- "Affichage des valeurs utilisées de la capacité de performance des nœuds et des agrégats"

Générer un rapport d'inventaire matériel pour le renouvellement du contrat

Vous pouvez générer un rapport contenant une liste complète des informations sur les clusters et les nœuds, telles que les numéros de modèle et de série du matériel, les types et le nombre de disques, les licences installées, etc. Ce rapport est utile pour le renouvellement de contrat au sein de sites sécurisés (sites « dark ») qui ne sont pas connectés à la plateforme NetAppActive IQ.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Nœuds**.
2. Accédez à la vue **Santé : Tous les nœuds** ou à la vue **Performances : Tous les nœuds**.
3. Sélectionnez **Rapports > * > Rapport d'inventaire du matériel***.

Le rapport d'inventaire du matériel est téléchargé sous forme de fichier .csv avec des informations complètes à la date du jour.

4. Fournissez ces informations à votre contact de support NetApp pour le renouvellement du contrat.

Afficher la liste et les détails des machines virtuelles de stockage

À partir de la vue Santé : toutes les machines virtuelles de stockage, vous pouvez surveiller votre inventaire de machines virtuelles de stockage (SVM). Vous pouvez utiliser la page Détails de la machine virtuelle de stockage / Santé pour afficher des informations détaillées sur les SVM surveillées.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez afficher les détails du SVM, tels que la capacité, l'efficacité et la configuration d'un SVM. Vous pouvez également afficher des informations sur les périphériques associés et les alertes associées à ce SVM.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.
2. Choisissez l'une des méthodes suivantes pour afficher les détails du SVM :
 - Pour afficher des informations sur l'état de santé de toutes les machines virtuelles de stockage dans tous les clusters, dans le menu Affichage, sélectionnez Santé : vue Toutes les machines virtuelles de stockage.
 - Pour afficher les détails complets, cliquez sur le nom de la machine virtuelle de stockage.

Vous pouvez également afficher les détails complets en cliquant sur **Afficher les détails** dans la boîte de dialogue des détails minimaux.

3. Affichez les objets liés au SVM en cliquant sur **Afficher les éléments associés** dans la boîte de dialogue des détails minimaux.

Informations connexes

- ["Machine virtuelle de stockage : page des détails de santé"](#)
- ["Performances : vue Toutes les machines virtuelles de stockage"](#)
- ["Sécurité : Vue anti-ransomware"](#)
- ["Affichage de l'état de sécurité des clusters et des machines virtuelles de stockage"](#)
- ["Relation : vue Toutes les relations"](#)

Voir la liste globale et les détails

À partir de la vue Santé : Tous les agrégats, vous pouvez surveiller votre inventaire d'agrégats. La vue Capacité : Tous les agrégats vous permet d'afficher des informations sur la capacité et l'utilisation des agrégats dans tous les clusters.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez afficher des détails tels que la capacité et la configuration globales, ainsi que les informations sur le disque à partir de la page Détails agrégés/santé. Vous pouvez utiliser ces détails avant de configurer les paramètres de seuil si nécessaire.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Choisissez l'une des méthodes suivantes pour afficher les détails agrégés :
 - Pour afficher des informations sur l'état de santé de tous les agrégats dans tous les clusters, dans le menu Affichage, sélectionnez État de santé : vue Tous les agrégats.
 - Pour afficher des informations sur la capacité et l'utilisation de tous les agrégats dans tous les clusters, dans le menu Affichage, sélectionnez Capacité : vue Tous les agrégats.
 - Pour afficher les détails complets, cliquez sur le nom de l'agrégat.

Vous pouvez également afficher les détails complets en cliquant sur **Afficher les détails** dans la boîte de dialogue des détails minimaux.

3. Affichez les objets liés à l'agrégat en cliquant sur **Afficher les éléments associés** dans la boîte de dialogue des détails minimaux.

Informations connexes

- ["Page de détails sur l'agrégat / la santé"](#)
- ["Performances : vue Tous les agrégats"](#)
- ["Personnalisation des rapports de capacité globale"](#)

Afficher les informations sur la capacité de FabricPool

Vous pouvez afficher les informations de capacité de FabricPool pour les clusters, les

agrégats et les volumes sur les pages d’inventaire et de détails de capacité et de performances pour ces objets. Ces pages affichent également les informations de miroir FabricPool lorsqu’un niveau de miroir a été configuré.

Ces pages affichent des informations telles que la capacité disponible sur le niveau de performances local et sur le niveau cloud, la quantité de capacité utilisée dans les deux niveaux, les agrégats attachés à un niveau cloud et les volumes qui implémentent les fonctionnalités FabricPool en déplaçant certaines informations vers le niveau cloud.

Lorsqu’un niveau de cloud est mis en miroir sur un autre fournisseur de cloud (le « niveau miroir »), les deux niveaux de cloud sont affichés dans la page Détails d’agrégation/de santé.

Étapes

1. Effectuez l’une des opérations suivantes :

Pour afficher les informations de capacité pour...	Fais ceci...
Groupes	a. Dans la vue Capacité : Tous les clusters, cliquez sur un cluster. b. Sur la page Détails du cluster/santé, cliquez sur l’onglet Configuration. L’écran affiche les noms de tous les niveaux de cloud auxquels ce cluster est connecté.
Agrégats	a. Dans la vue Capacité : Tous les agrégats, cliquez sur un agrégat où le champ Type indique « SSD (FabricPool) » ou « HDD (FabricPool) ». b. Sur la page Détails de l’agrégat / de la santé, cliquez sur l’onglet Capacité. L’écran affiche la capacité totale utilisée dans le niveau cloud. c. Cliquez sur l’onglet Informations sur le disque. L’écran affiche le nom du niveau de cloud et la capacité utilisée. d. Cliquez sur l’onglet Configuration. L’écran affiche le nom du niveau de cloud et d’autres informations détaillées sur le niveau de cloud.

Pour afficher les informations de capacité pour...	Fais ceci...
Volumes	a. Dans la vue Capacité : Tous les volumes, cliquez sur un volume où un nom de stratégie apparaît dans le champ « Stratégie de hiérarchisation ». b. Sur la page Détails Volume / Santé, cliquez sur l'onglet Configuration. L'écran affiche le nom de la stratégie de hiérarchisation FabricPool attribuée au volume.

- Dans la page **Analyse de la charge de travail**, vous pouvez sélectionner « Vue du niveau Cloud » dans la zone **Tendance de capacité** pour voir la capacité utilisée dans le niveau de performance local et dans le niveau Cloud au cours du mois précédent.

Pour plus d'informations sur les agrégats FabricPool, voir "[Présentation des disques et des agrégats](#)".

Afficher les détails du pool de stockage

Vous pouvez afficher les détails du pool de stockage pour surveiller l'état du pool de stockage, le cache total et disponible, ainsi que les allocations utilisées et disponibles.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

- Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
- Cliquez sur un nom d'agrégat.

Les détails de l'agrégat sélectionné sont affichés.

- Cliquez sur l'onglet **Informations sur le disque**.

Les informations détaillées sur le disque sont affichées.



La table Cache s'affiche uniquement lorsque l'agrégat sélectionné utilise un pool de stockage.

- Dans la table Cache, déplacez le pointeur sur le nom du pool de stockage requis.

Les détails du pool de stockage sont affichés.

Afficher la liste des volumes et les détails

À partir de la vue Santé : Tous les volumes, vous pouvez surveiller votre inventaire de volumes. La vue Capacité : Tous les volumes vous permet d'afficher des informations sur la capacité et l'utilisation des volumes d'un cluster.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez également utiliser la page Détails Volume/Santé pour afficher des informations détaillées sur les volumes surveillés, notamment la capacité, l'efficacité, la configuration et la protection des volumes. Vous pouvez également afficher des informations sur les périphériques associés et les alertes associées pour un volume spécifique.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Choisissez l'une des méthodes suivantes pour afficher les détails du volume :
 - Pour afficher des informations détaillées sur l'état de santé des volumes d'un cluster, dans le menu Affichage, sélectionnez Santé : vue Tous les volumes.
 - Pour afficher des informations détaillées sur la capacité et l'utilisation des volumes d'un cluster, dans le menu Affichage, sélectionnez Capacité : vue Tous les volumes.
 - Pour afficher les détails complets, cliquez sur le nom du volume.

Vous pouvez également afficher les détails complets en cliquant sur **Afficher les détails** dans la boîte de dialogue des détails minimaux.

3. **Facultatif** : affichez les objets associés au volume en cliquant sur **Afficher les éléments associés** dans la boîte de dialogue des détails minimaux.

Informations connexes

- ["Volume : Page de détails sur la santé"](#)
- ["Performances : vue Tous les volumes"](#)
- ["Sécurité : Vue anti-ransomware"](#)
- ["Affichage des relations de protection des volumes"](#)
- ["Création d'un rapport pour afficher les graphiques de capacité de volume disponibles"](#)

Afficher les détails sur les actions NFS

Vous pouvez afficher les détails de tous les partages NFS, tels que leur état, le chemin associé au volume (volumes FlexGroup ou volumes FlexVol), les niveaux d'accès des clients aux partages NFS et la politique d'exportation définie pour les volumes exportés. Utilisez la vue Santé : tous les partages NFS pour voir tous les partages NFS sur tous les clusters surveillés et utilisez la page Détails de la machine virtuelle de stockage / Santé pour afficher tous les partages NFS sur une machine virtuelle de stockage (SVM) spécifique.

Avant de commencer

- La licence NFS doit être activée sur le cluster.
- Les interfaces réseau servant les partages NFS doivent être configurées.
- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, suivez les étapes ci-dessous selon que vous souhaitez afficher tous les partages NFS ou uniquement les partages NFS d'un SVM particulier.

À...	Suivez ces étapes...
Afficher tous les partages NFS	Cliquez sur Stockage > Partages NFS
Afficher les partages NFS pour un seul SVM	a. Cliquez sur Stockage > VM de stockage b. Cliquez sur le SVM pour lequel vous souhaitez afficher les détails des partages NFS. c. Dans la page Détails de la machine virtuelle de stockage / Santé, cliquez sur l'onglet Partages NFS.

Pour plus d'informations, voir "[Provisionnement des volumes de partage de fichiers](#)" et "[Provisionnement des partages de fichiers CIFS et NFS à l'aide d'API](#)".

Afficher les détails des actions SMB/CIFS

Vous pouvez afficher les détails de tous les partages SMB/CIFS, tels que le nom du partage, le chemin de jonction, les objets contenus, les paramètres de sécurité et les stratégies d'exportation définies pour le partage. Utilisez la vue Santé : tous les partages SMB pour voir tous les partages SMB sur tous les clusters surveillés et utilisez la page Détails de la machine virtuelle de stockage / Santé pour afficher tous les partages SMB sur une machine virtuelle de stockage (SVM) spécifique.

Avant de commencer

- La licence CIFS doit être activée sur le cluster.
- Les interfaces réseau desservant les partages SMB/CIFS doivent être configurées.
- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.



Les partages dans les dossiers ne sont pas affichés.

Étape

1. Dans le volet de navigation de gauche, suivez les étapes ci-dessous selon que vous souhaitez afficher tous les partages SMB/CIFS ou uniquement les partages d'un SVM particulier.

À...	Suivez ces étapes...
Afficher toutes les actions SMB/CIFS	Cliquez sur Stockage > Partages SMB

À...	Suivez ces étapes...
Afficher les parts SMB/CIFS pour un seul SVM	a. Cliquez sur Stockage > VM de stockage b. Cliquez sur le SVM pour lequel vous souhaitez afficher les détails du partage SMB/CIFS. c. Dans la page Détails de la machine virtuelle de stockage / Santé, cliquez sur l'onglet Partages SMB .

Pour plus d'informations, voir ["Provisionnement des partages de fichiers CIFS et NFS à l'aide d'API"](#).

Afficher la liste des copies Snapshot

Vous pouvez afficher la liste des copies instantanées pour un volume sélectionné. Vous pouvez utiliser la liste des copies Snapshot pour calculer la quantité d'espace disque qui peut être récupérée si une ou plusieurs copies Snapshot sont supprimées, et vous pouvez supprimer les copies Snapshot si nécessaire.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Le volume contenant les copies Snapshot doit être en ligne.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans la vue **Santé : tous les volumes**, sélectionnez le volume qui contient les copies instantanées que vous souhaitez afficher.
3. Dans la page de détails **Volume / Santé**, cliquez sur l'onglet **Capacité**.
4. Dans le volet **Détails** de l'onglet **Capacité**, dans la section Autres détails, cliquez sur le lien à côté de **Copies instantanées**.

Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

Informations connexes

["Page Santé/Volumes"](#)

Supprimer les copies instantanées

Vous pouvez supprimer une copie Snapshot pour économiser de l'espace ou libérer de l'espace disque, ou vous pouvez supprimer la copie Snapshot si elle n'est plus nécessaire.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Le volume doit être en ligne.

Pour supprimer une copie Snapshot occupée ou verrouillée, vous devez avoir libéré la copie Snapshot de l'application qui l'utilisait.

- Vous ne pouvez pas supprimer la copie Snapshot de base dans un volume parent si un volume FlexClone utilise cette copie Snapshot.

La copie Snapshot de base est la copie Snapshot utilisée pour créer le volume FlexClone et affiche l'état *Busy* et la dépendance des applications comme *Busy*, *Vclone* dans le volume parent.

- Vous ne pouvez pas supprimer une copie Snapshot verrouillée utilisée dans une relation SnapMirror .

La copie instantanée est verrouillée et est requise pour la prochaine mise à jour.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans la vue **Santé : tous les volumes**, sélectionnez le volume qui contient les copies instantanées que vous souhaitez afficher.

La liste des copies Snapshot s'affiche.

3. Dans la page de détails **Volume / Santé**, cliquez sur l'onglet **Capacité**.
4. Dans le volet **Détails** de l'onglet **Capacité**, dans la section Autres détails, cliquez sur le lien à côté de **Copies instantanées**.

Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

5. Dans la vue **Copies d'instantanés**, sélectionnez les copies d'instantanés que vous souhaitez supprimer, puis cliquez sur **Supprimer la sélection**.

Calculer l'espace récupérable pour les copies Snapshot

Vous pouvez calculer la quantité d'espace disque qui peut être récupérée si une ou plusieurs copies Snapshot sont supprimées.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Le volume doit être en ligne.
- Le volume doit être un FlexVol volume; cette capacité n'est pas prise en charge avec les volumes FlexGroup .

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans la vue **Santé : tous les volumes**, sélectionnez le volume qui contient les copies instantanées que vous souhaitez afficher.

La liste des copies Snapshot s'affiche.

3. Dans la page de détails **Volume / Santé**, cliquez sur l'onglet **Capacité**.
4. Dans le volet **Détails** de l'onglet **Capacité**, dans la section Autres détails, cliquez sur le lien à côté de **Copies instantanées**.

Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

5. Dans la vue **Copies instantanées**, sélectionnez les copies instantanées pour lesquelles vous souhaitez calculer l'espace récupérable.
6. Cliquez sur **Calculer**.

L'espace récupérable (en pourcentage, en Ko, Mo, Go, etc.) sur le volume est affiché.

7. Pour recalculer l'espace récupérable, sélectionnez les copies Snapshot requises et cliquez sur **Recalculer**.

Description des fenêtres et des boîtes de dialogue des objets de cluster

Vous pouvez afficher tous vos clusters et objets de cluster à partir de la page d'objet de stockage correspondante. Vous pouvez également afficher les détails à partir de la page de détails de l'objet de stockage correspondant. Vous pouvez désormais lancer l'interface utilisateur du Gestionnaire de système à partir des sections STOCKAGE et PROTECTION suivantes de l'INVENTAIRE.

- Pages Inventaire du cluster, Santé du cluster et Performances du cluster
- Pages Inventaire global, Santé globale et Performances globales
- Pages Inventaire des volumes, Santé des volumes et Performances des volumes
- Pages Inventaire des nœuds et Performances des nœuds
- Pages Inventaire StorageVM, Santé StorageVM et Performances StorageVM
- Pages de relation de protection

Flux de travail et tâches de santé communs d'Unified Manager

Certains flux de travail et tâches administratifs courants associés à Unified Manager incluent la sélection des clusters de stockage à surveiller ; le diagnostic des conditions qui affectent négativement la disponibilité, la capacité et la protection des données ; la restauration des données perdues ; la configuration et la gestion des volumes ; et le regroupement et l'envoi des données de diagnostic au support technique (si nécessaire).

Unified Manager permet aux administrateurs de stockage d'afficher un tableau de bord, d'évaluer la capacité globale, la disponibilité et l'état de protection des clusters de stockage gérés, puis d'identifier, de localiser, de diagnostiquer et d'attribuer rapidement la résolution de tout problème spécifique pouvant survenir.

Les problèmes les plus importants liés à un cluster, une machine virtuelle de stockage (SVM), un volume ou un volume FlexGroup qui affectent la capacité de stockage ou la disponibilité des données de vos objets de stockage gérés sont affichés dans les graphiques et événements d'intégrité du système sur la page Tableau de bord. Lorsque des problèmes critiques sont identifiés, cette page fournit des liens pour prendre en charge les flux de travail de dépannage appropriés.

Unified Manager peut également être inclus dans des flux de travail qui incluent des outils de gestion associés, tels que OnCommand Workflow Automation (WFA), pour prendre en charge la configuration directe des ressources de stockage.

Les flux de travail courants liés aux tâches administratives suivantes sont décrits dans ce document :

- Diagnostiquer et gérer les problèmes de disponibilité

Si une panne matérielle ou des problèmes de configuration des ressources de stockage entraînent l'affichage d'événements de disponibilité des données sur la page Tableau de bord, les administrateurs de stockage peuvent suivre les liens intégrés pour afficher les informations de connectivité sur la ressource de stockage affectée, afficher des conseils de dépannage et attribuer la résolution des problèmes à d'autres administrateurs.

- Configuration et surveillance des incidents de performance

L'administrateur peut surveiller et gérer les performances des ressources du système de stockage surveillées. Voir le "[Introduction à la surveillance des performances Active IQ Unified Manager](#)" pour plus d'informations.

- Diagnostic et gestion des problèmes de capacité de volume

Si des problèmes de capacité de stockage de volume s'affichent sur la page Tableau de bord, les administrateurs de stockage peuvent suivre les liens intégrés pour afficher les tendances actuelles et historiques liées à la capacité de stockage du volume affecté, afficher des conseils de dépannage et attribuer la résolution des problèmes à d'autres administrateurs.

- Configuration, surveillance et diagnostic des problèmes de relation de protection

Après avoir créé et configuré des relations de protection, les administrateurs de stockage peuvent afficher les problèmes potentiels liés aux relations de protection, l'état actuel des relations de protection, les informations de réussite des tâches de protection actuelles et historiques sur les relations affectées et des conseils de dépannage. Voir le "[Création, surveillance et dépannage des relations de protection](#)" pour plus d'informations.

- Création de fichiers de sauvegarde et restauration de données à partir de fichiers de sauvegarde.
- Association d'objets de stockage à des annotations

En associant des objets de stockage à des annotations, les administrateurs de stockage peuvent filtrer et afficher les événements liés aux objets de stockage, ce qui permet aux administrateurs de stockage de hiérarchiser et de résoudre les problèmes associés aux événements.

- Utilisation des API REST pour vous aider à gérer vos clusters en affichant les informations d'intégrité, de capacité et de performances capturées par Unified Manager. Voir "[Prise en main des API REST Active IQ Unified Manager](#)" pour plus d'informations.
- Envoi d'un dossier de support au support technique

Les administrateurs de stockage peuvent récupérer et envoyer un ensemble de support au support technique à l'aide de la console de maintenance. Les dossiers d'assistance doivent être envoyés au support technique lorsque le problème nécessite un diagnostic et un dépannage plus détaillés que ceux fournis par un message AutoSupport .

Surveiller et résoudre les problèmes de disponibilité des données

Unified Manager surveille la fiabilité avec laquelle les utilisateurs autorisés peuvent accéder à vos données stockées, vous avertit des conditions qui bloquent ou entravent cet accès et vous permet de diagnostiquer ces conditions et d'attribuer et de suivre leur

résolution.

Les rubriques relatives au flux de travail de disponibilité de cette section décrivent des exemples de la manière dont un administrateur de stockage peut utiliser l'interface utilisateur Web d'Unified Manager pour découvrir, diagnostiquer et attribuer des résolutions aux conditions matérielles et logicielles qui affectent négativement la disponibilité des données.

Rechercher et résoudre les problèmes de liaison d'interconnexion de basculement de stockage

Ce flux de travail fournit un exemple de la manière dont vous pouvez rechercher, évaluer et résoudre les conditions de liaison d'interconnexion de basculement de stockage en panne. Dans ce scénario, vous êtes un administrateur utilisant Unified Manager pour analyser les risques de basculement de stockage avant de démarrer une mise à niveau de la version ONTAP sur vos nœuds.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Si les interconnexions de basculement de stockage entre les nœuds de paires HA échouent lors d'une tentative de mise à niveau sans interruption, la mise à niveau échoue. Par conséquent, la pratique courante consiste pour l'administrateur à surveiller et à confirmer la fiabilité du basculement de stockage sur les nœuds de cluster ciblés pour la mise à niveau avant le début d'une mise à niveau.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans la page d'inventaire **Gestion des événements**, sélectionnez **Événements de disponibilité active**.
3. En haut de la colonne **Nom** de la page d'inventaire **Gestion des événements**, cliquez sur  et entrez `*failover` dans la zone de texte pour limiter l'événement à afficher aux événements liés au basculement de stockage.

Tous les événements passés liés aux conditions de basculement du stockage sont affichés.

Dans ce scénario, Unified Manager affiche l'événement « Interconnexion de basculement de stockage : une ou plusieurs liaisons sont hors service » dans sa section Incidents de disponibilité.

4. Si un ou plusieurs événements liés au basculement du stockage s'affichent sur la page d'inventaire **Gestion des événements**, procédez comme suit :

- a. Cliquez sur le lien du titre de l'événement pour afficher les détails de cet événement.

Dans cet exemple, vous cliquez sur le titre de l'événement « Interconnexion de basculement de stockage avec une ou plusieurs liaisons désactivées ».

La page Détails de l'événement pour cet événement s'affiche.

- a. Sur la page Détails de l'événement, vous pouvez effectuer une ou plusieurs des tâches suivantes :
 - Consultez le message d'erreur dans le champ Cause et évaluez le problème.
 - Affecter l'événement à un administrateur.
 - Reconnaître l'événement.

Informations connexes

"Page de détails de l'événement"

"Rôles et capacités des utilisateurs d'Unified Manager"

Exécuter une action corrective pour les liaisons d'interconnexion de basculement de stockage en panne

Lorsque vous affichez la page Détails de l'événement d'un événement lié au basculement de stockage, vous pouvez consulter les informations récapitulatives de la page pour déterminer l'urgence de l'événement, la cause possible du problème et la résolution possible du problème.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Dans cet exemple de scénario, le résumé de l'événement fourni sur la page Détails de l'événement contient les informations suivantes sur la condition de défaillance de la liaison d'interconnexion de basculement de stockage :

```
Event: Storage Failover Interconnect One or More Links Down
```

```
Summary
```

```
Severity: Warning
```

```
State: New
```

```
Impact Level: Risk
```

```
Impact Area: Availability
```

```
Source: aardvark
```

```
Source Type: Node
```

```
Acknowledged By:
```

```
Resolved By:
```

```
Assigned To:
```

```
Cause: At least one storage failover interconnected link  
       between the nodes aardvark and bonobo is down.  
       RDMA interconnect is up (Link0 up, Link1 down)
```

Les informations d'exemple d'événement indiquent qu'un lien d'interconnexion de basculement de stockage, Link1, entre les nœuds de paire HA aardvark et bonobo est en panne, mais que Link0 entre Apple et Boy est actif. Étant donné qu'un lien est actif, l'accès à la mémoire dynamique à distance (RDMA) fonctionne toujours et une tâche de basculement de stockage peut toujours réussir.

Cependant, pour éviter toute défaillance des liens et toute désactivation totale de la protection de basculement du stockage, vous décidez de diagnostiquer plus en détail la raison de la panne de Link1.

Étapes

1. À partir de la page Détails de l'événement, vous pouvez cliquer sur le lien vers l'événement spécifié dans le champ Source pour obtenir plus de détails sur d'autres événements pouvant être liés à la condition de liaison d'interconnexion de basculement de stockage interrompue.

Dans cet exemple, la source de l'événement est le nœud nommé aardvark. Cliquer sur ce nom de nœud

affiche les détails HA pour la paire HA affectée, aardvark et bonobo, dans l'onglet Nœuds de la page Détails du cluster/santé, et affiche d'autres événements qui se sont récemment produits sur la paire HA affectée.

2. Consultez les **Détails HA** pour plus d'informations concernant l'événement.

Dans cet exemple, les informations pertinentes se trouvent dans la table Événements. Le tableau affiche l'événement « Connexion de basculement de stockage : une ou plusieurs liaisons interrompues », l'heure à laquelle l'événement a été généré et, encore une fois, le nœud à partir duquel cet événement est originaire.

À l'aide des informations d'emplacement du nœud dans les détails HA, demandez ou effectuez personnellement une inspection physique et une réparation du problème de basculement de stockage sur les nœuds de paire HA affectés.

Informations connexes

["Page de détails de l'événement"](#)

["Rôles et capacités des utilisateurs d'Unified Manager"](#)

Résoudre les problèmes de volume hors ligne

Ce flux de travail fournit un exemple de la manière dont vous pouvez évaluer et résoudre un événement hors ligne de volume qu'Unified Manager peut afficher dans la page d'inventaire de gestion des événements. Dans ce scénario, vous êtes un administrateur utilisant Unified Manager pour résoudre un ou plusieurs événements de volume hors ligne.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Les volumes peuvent être signalés hors ligne pour plusieurs raisons :

- L'administrateur SVM a délibérément mis le volume hors ligne.
- Le nœud du cluster d'hébergement du volume est en panne et le basculement du stockage vers son partenaire de paire HA a également échoué.
- La machine virtuelle de stockage (SVM) hébergeant le volume est arrêtée car le nœud hébergeant le volume racine de cette SVM est en panne.
- L'agrégat d'hébergement du volume est en panne en raison d'une défaillance simultanée de deux disques RAID.

Vous pouvez utiliser la page d'inventaire Gestion des événements et les pages de détails Cluster/Santé, VM de stockage/Santé et Volume/Santé pour confirmer ou éliminer une ou plusieurs de ces possibilités.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans la page d'inventaire **Gestion des événements**, sélectionnez **Événements de disponibilité active**.
3. Cliquez sur le lien hypertexte affiché pour l'événement Volume hors ligne.

La page Détails de l'événement pour l'incident de disponibilité s'affiche.

4. Sur cette page, vérifiez les notes pour toute indication que l'administrateur SVM a mis le volume en question hors ligne.
5. Sur la page de détails de l'**Événement**, vous pouvez consulter les informations pour une ou plusieurs des tâches suivantes :

- Consultez les informations affichées dans le champ Cause pour obtenir des conseils de diagnostic possibles.

Dans cet exemple, les informations du champ Cause vous informent uniquement que le volume est hors ligne.

- Consultez la zone Notes et mises à jour pour toute indication indiquant que l'administrateur SVM a délibérément mis le volume en question hors ligne.
- Cliquez sur la source de l'événement, dans ce cas le volume signalé hors ligne, pour obtenir plus d'informations sur ce volume.
- Affecter l'événement à un administrateur.
- Reconnaissez l'événement ou, le cas échéant, marquez-le comme résolu.

Exécuter des actions de diagnostic pour les conditions de volume hors ligne

Après avoir accédé à la page des détails Volume/Santé d'un volume signalé comme étant hors ligne, vous pouvez rechercher des informations supplémentaires utiles pour diagnostiquer l'état hors ligne du volume.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Si le volume signalé comme hors ligne n'a pas été mis hors ligne délibérément, ce volume peut être hors ligne pour plusieurs raisons.

À partir de la page de détails Volume/Santé du volume hors ligne, vous pouvez accéder à d'autres pages et volets pour confirmer ou éliminer les causes possibles :

- Cliquez sur les liens de la page de détails **Volume / Santé** pour déterminer si le volume est hors ligne parce que son nœud hôte est en panne et que le basculement de stockage vers son partenaire de paire HA a également échoué.

Voir "[Déterminer si une condition de volume hors ligne est causée par un nœud en panne](#)".

- Cliquez sur les liens de la page de détails **Volume / Santé** pour déterminer si le volume est hors ligne et si sa machine virtuelle de stockage hôte (SVM) est arrêtée car le nœud hébergeant le volume racine de cette SVM est en panne.

Voir "[Déterminer si un volume est hors ligne et si SVM est arrêté parce qu'un nœud est en panne](#)".

- Cliquez sur les liens de la page de détails **Volume / Santé** pour déterminer si le volume est hors ligne en raison de disques défectueux dans son agrégat d'hôtes.

Voir "[Déterminer si un volume est hors ligne en raison de disques défectueux dans un ensemble](#)".

Informations connexes

"[Rôles et capacités des utilisateurs d'Unified Manager](#)"

Déterminer si un volume est hors ligne parce que son nœud hôte est en panne

Vous pouvez utiliser l'interface utilisateur Web Unified Manager pour confirmer ou éliminer la possibilité qu'un volume soit hors ligne parce que son nœud hôte est en panne et que le basculement de stockage vers son partenaire de paire HA échoue.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Pour déterminer si la condition de volume hors ligne est causée par une défaillance du nœud d'hébergement et un basculement de stockage infructueux ultérieur, effectuez les actions suivantes :

Étapes

1. Recherchez et cliquez sur le lien hypertexte affiché sous SVM dans le volet **Périphériques associés** de la page de détails **Volume / Santé** du volume hors ligne.

La page Détails de la machine virtuelle de stockage / Santé affiche des informations sur la machine virtuelle de stockage d'hébergement (SVM) du volume hors ligne.

2. Dans le volet **Périphériques associés** de la page de détails **VM de stockage / Santé**, recherchez et cliquez sur le lien hypertexte affiché sous Volumes.

La vue Santé : Tous les volumes affiche un tableau d'informations sur tous les volumes hébergés par le SVM.

3. Dans l'en-tête de la colonne État de la vue **Santé : Tous les volumes**, cliquez sur le symbole de filtre  , puis sélectionnez l'option **Hors ligne**.

Seuls les volumes SVM qui sont hors ligne sont répertoriés.

4. Dans la vue Santé : Tous les volumes, cliquez sur le symbole de la grille  , puis sélectionnez l'option **Nœuds de cluster**.

Vous devrez peut-être faire défiler la zone de sélection de la grille pour localiser l'option **Nœuds de cluster**.

La colonne Nœuds de cluster est ajoutée à l'inventaire des volumes et affiche le nom du nœud qui héberge chaque volume hors ligne.

5. Dans la vue **Santé : tous les volumes**, recherchez la liste du volume hors ligne et, dans sa colonne Nœud de cluster, cliquez sur le nom de son nœud d'hébergement.

L'onglet Nœuds de la page Détails du cluster/santé affiche l'état de la paire de nœuds HA à laquelle appartient le nœud d'hébergement. L'état du nœud d'hébergement et la réussite de toute opération de basculement de cluster sont indiqués sur l'écran.

Après avoir confirmé que la condition de volume hors ligne existe parce que son nœud hôte est en panne et que le basculement de stockage vers le partenaire de paire HA a échoué, contactez l'administrateur ou l'opérateur approprié pour redémarrer manuellement le nœud en panne et résoudre le problème de basculement de stockage.

Déterminer si un volume est hors ligne et si son SVM est arrêté parce qu'un nœud est en panne

Vous pouvez utiliser l'interface utilisateur Web d'Unified Manager pour confirmer ou éliminer la possibilité qu'un volume soit hors ligne car sa machine virtuelle de stockage hôte (SVM) est arrêtée en raison de l'arrêt du nœud hébergeant le volume racine de cette SVM.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Pour déterminer si la condition de volume hors ligne est due à l'arrêt de son SVM hôte parce que le nœud hébergeant le volume racine de ce SVM est en panne, effectuez les actions suivantes :

Étapes

1. Recherchez et cliquez sur le lien hypertexte affiché sous le SVM dans le volet **Périphériques associés** de la page de détails **Volume / Santé** du volume hors ligne.

La page Détails de la machine virtuelle de stockage / Santé affiche l'état « en cours d'exécution » ou « arrêté » de la SVM d'hébergement. Si l'état du SVM est en cours d'exécution, la condition de volume hors ligne n'est pas causée par le fait que le nœud hébergeant le volume racine de ce SVM est en panne.

2. Si l'état du SVM est arrêté, cliquez sur **Afficher les SVM** pour identifier plus précisément la cause de l'arrêt du SVM d'hébergement.
3. Dans l'en-tête de la colonne SVM de la vue **Santé : toutes les machines virtuelles de stockage**, cliquez sur le symbole de filtre  puis tapez le nom du SVM arrêté.

Les informations relatives à ce SVM sont affichées dans un tableau.

4. Dans la vue **Santé : toutes les machines virtuelles de stockage**, cliquez sur  puis sélectionnez l'option **Volume racine**.

La colonne Volume racine est ajoutée à l'inventaire SVM et affiche le nom du volume racine du SVM arrêté.

5. Dans la colonne Volume racine, cliquez sur le nom du volume racine pour afficher la page de détails **Storage VM / Health** pour ce volume.

Si l'état du volume racine SVM est (En ligne), la condition hors ligne du volume d'origine n'est pas due au fait que le nœud hébergeant le volume racine de ce SVM est en panne.

6. Si l'état du volume racine SVM est (Hors ligne), recherchez et cliquez sur le lien hypertexte affiché sous Agrégation dans le volet Périphériques associés de la page Détails du volume/de l'état du volume racine SVM.
7. Recherchez et cliquez sur le lien hypertexte affiché sous Nœud dans le volet **Périphériques associés** de la page de détails **Agrégat/Santé** de l'agrégat.

L'onglet Nœuds de la page Détails du cluster/de l'état affiche l'état de la paire de nœuds HA à laquelle appartient le nœud d'hébergement du volume racine SVM. L'état du nœud est indiqué sur l'écran.

Après avoir confirmé que l'état hors ligne du volume est dû à l'état hors ligne de la SVM hôte de ce volume, qui est elle-même due au fait que le nœud qui héberge le volume racine de cette SVM est en panne, contactez l'administrateur ou l'opérateur approprié pour redémarrer manuellement le nœud en panne.

Déterminer si un volume est hors ligne en raison de disques défectueux dans un ensemble

Vous pouvez utiliser l'interface utilisateur Web d'Unified Manager pour confirmer ou éliminer la possibilité qu'un volume soit hors ligne car des problèmes de disque RAID ont mis son agrégat hôte hors ligne.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Pour déterminer si l'état du volume hors ligne est dû à des problèmes de disque RAID qui mettent l'agrégat d'hébergement hors ligne, effectuez les actions suivantes :

Étapes

1. Recherchez et cliquez sur le lien hypertexte affiché sous Agrégation dans le volet **Périphériques associés** de la page de détails **Volume / Santé**.

La page Détails de l'agrégat / Santé affiche l'état en ligne ou hors ligne de l'agrégat d'hébergement. Si l'état global est en ligne, les problèmes de disque RAID ne sont pas la cause de la mise hors ligne du volume.

2. Si l'état global est hors ligne, cliquez sur **Informations sur le disque** et recherchez les événements de disque cassé dans la liste **Événements** de l'onglet **Informations sur le disque**.
3. Pour identifier plus précisément les disques défectueux, cliquez sur le lien hypertexte affiché sous Nœud dans le volet **Périphériques associés**.

La page Détails du cluster / Santé s'affiche.

4. Cliquez sur **Disques**, puis sélectionnez **Cassé** dans le volet **Filtres** pour répertorier tous les disques dans un état cassé.

Si les disques en état cassé ont provoqué l'état hors ligne de l'agrégat hôte, le nom de l'agrégat s'affiche dans la colonne Agrégation impactée.

Après avoir confirmé que l'état hors ligne du volume est causé par des disques RAID cassés et l'agrégat d'hôtes hors ligne qui en résulte, contactez l'administrateur ou l'opérateur approprié pour remplacer manuellement les disques cassés et remettre l'agrégat en ligne.

Résoudre les problèmes de capacité

Ce flux de travail fournit un exemple de la manière dont vous pouvez résoudre un problème de capacité. Dans ce scénario, vous êtes administrateur ou opérateur et vous accédez à la page Tableau de bord d'Unified Manager pour voir si l'un des objets de stockage surveillés présente des problèmes de capacité. Vous souhaitez déterminer la cause possible et la résolution du problème.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Sur la page Tableau de bord, recherchez un événement d'erreur « Espace volume plein » dans le panneau Capacité sous la liste déroulante des événements.

Étapes

1. Dans le panneau **Capacité** de la page **Tableau de bord**, cliquez sur le nom de l'événement d'erreur d'espace de volume plein.

La page Détails de l'événement pour l'erreur s'affiche.

2. À partir de la page de détails de l'**Événement**, vous pouvez effectuer une ou plusieurs des tâches suivantes :
 - Consultez le message d'erreur dans le champ Cause et cliquez sur les suggestions sous Actions correctives suggérées pour consulter les descriptions des corrections possibles.
 - Cliquez sur le nom de l'objet, dans ce cas un volume, dans le champ Source pour obtenir des détails sur l'objet.
 - Recherchez des notes qui pourraient avoir été ajoutées à propos de cet événement.
 - Ajoutez une note à l'événement.
 - Affecter l'événement à un autre utilisateur.
 - Reconnaître l'événement.
 - Marquer l'événement comme résolu.

Informations connexes

["Page de détails de l'événement"](#)

Exécuter les actions correctives suggérées pour un volume complet

Après avoir reçu un événement d'erreur « Espace volume plein », vous examinez les actions correctives suggérées sur la page Détails de l'événement et décidez d'effectuer l'une des actions suggérées.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Un utilisateur avec n'importe quel rôle peut effectuer toutes les tâches de ce workflow qui utilisent Unified Manager.

Dans cet exemple, vous avez vu un événement d'erreur d'espace de volume plein sur la page d'inventaire de gestion des événements d'Unified Manager et avez cliqué sur le nom de l'événement.

Les actions correctives possibles que vous pourriez effectuer pour un volume complet incluent les suivantes :

- Activation de la croissance automatique, de la déduplication ou de la compression sur le volume
- Redimensionner ou déplacer le volume
- Suppression ou déplacement de données du volume

Bien que toutes ces actions doivent être effectuées à partir d' ONTAP System Manager ou de l'interface de ligne de commande ONTAP , vous pouvez utiliser Unified Manager pour rechercher les informations dont vous pourriez avoir besoin pour déterminer les actions à entreprendre.

Étapes

1. À partir de la page des détails de l'**Événement**, cliquez sur le nom du volume dans le champ Source pour afficher les détails sur le volume affecté.

2. Sur la page de détails **Volume / Santé**, cliquez sur **Configuration** et constatez que la déduplication et la compression sont déjà activées sur le volume.

Vous décidez de redimensionner le volume.

3. Dans le volet **Périphériques associés**, cliquez sur le nom de l'agrégat d'hébergement pour voir si l'agrégat peut prendre en charge un volume plus important.
4. Sur la page de détails **Agrégat / Santé**, vous voyez que l'agrégat hébergeant le volume complet dispose de suffisamment de capacité non engagée. Vous utilisez donc ONTAP System Manager pour redimensionner le volume, lui donnant ainsi plus de capacité.

Informations connexes

["Page de détails de l'événement"](#)

Gérer les seuils de santé

Vous pouvez configurer des valeurs de seuil de santé globales pour tous les agrégats, volumes et qtrees afin de suivre toute violation de seuil de santé.

Quels sont les seuils de santé de la capacité de stockage

Un seuil de santé de capacité de stockage est le point auquel le serveur Unified Manager génère des événements pour signaler tout problème de capacité avec les objets de stockage. Vous pouvez configurer des alertes pour envoyer une notification chaque fois que de tels événements se produisent.

Les seuils de santé de la capacité de stockage pour tous les agrégats, volumes et qtrees sont définis sur des valeurs par défaut. Vous pouvez modifier les paramètres selon vos besoins pour un objet ou un groupe d'objets.

Configurer les paramètres de seuil de santé globaux

Vous pouvez configurer des conditions de seuil de santé globales pour la capacité, la croissance, la réserve de snapshots, les quotas et les inodes pour surveiller efficacement la taille de votre agrégat, de votre volume et de votre qtree. Vous pouvez également modifier les paramètres de génération d'événements en cas de dépassement des seuils de décalage.

Les paramètres de seuil de santé global s'appliquent à tous les objets auxquels ils sont associés, tels que les agrégats, les volumes, etc. Lorsque les seuils sont franchis, un événement est généré et, si des alertes sont configurées, une notification d'alerte est envoyée. Les seuils par défaut sont définis sur les valeurs recommandées, mais vous pouvez les modifier pour générer des événements à des intervalles adaptés à vos besoins spécifiques. Lorsque les seuils sont modifiés, des événements sont générés ou rendus obsolètes lors du cycle de surveillance suivant.

Les paramètres de seuil de santé global sont accessibles à partir de la section Seuils d'événement du menu de navigation de gauche. Vous pouvez également modifier les paramètres de seuil pour des objets individuels, à partir de la page d'inventaire ou de la page de détails de cet objet.

- Pour plus d'informations, voir ["Configuration des valeurs de seuil de santé globales globales"](#) .

Vous pouvez configurer les paramètres de seuil de santé pour la capacité, la croissance et les copies instantanées pour tous les agrégats afin de suivre toute violation de seuil.

- Pour plus d'informations, voir ["Configuration des valeurs de seuil de santé du volume global"](#) .

Vous pouvez modifier les paramètres de seuil de santé pour la capacité, les copies instantanées, les quotas qtree, la croissance du volume, l'espace de réserve d'écrasement et les inodes pour tous les volumes afin de suivre toute violation de seuil.

- Pour plus d'informations, voir ["Configuration des valeurs de seuil de santé globales de Qtree"](#) .

Vous pouvez modifier les paramètres de seuil de santé pour la capacité de tous les qtrees afin de suivre toute violation de seuil.

- Pour plus d'informations, voir ["Modification des paramètres de seuil de santé de décalage pour les relations de protection non gérées"](#) .

Vous pouvez augmenter ou diminuer le pourcentage de délai d'avertissement ou d'erreur afin que les événements soient générés à des intervalles plus adaptés à vos besoins.

Configurer les valeurs de seuil de santé globales globales

Vous pouvez configurer des valeurs de seuil de santé globales pour tous les agrégats afin de suivre toute violation de seuil. Des événements appropriés sont générés pour les dépassements de seuil et vous pouvez prendre des mesures préventives en fonction de ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de meilleures pratiques pour les seuils qui s'appliquent à tous les agrégats surveillés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous configurez les options globalement, les valeurs par défaut des objets sont modifiées. Cependant, si les valeurs par défaut ont été modifiées au niveau de l'objet, les valeurs globales ne sont pas modifiées.

Les options de seuil ont des valeurs par défaut pour une meilleure surveillance. Cependant, vous pouvez modifier les valeurs en fonction des exigences de votre environnement.

Lorsque la croissance automatique est activée sur les volumes qui résident sur l'agrégat, les seuils de capacité agrégée sont considérés comme dépassés en fonction de la taille de volume maximale définie par la croissance automatique, et non en fonction de la taille de volume d'origine.



Les valeurs de seuil de santé ne s'appliquent pas à l'agrégat racine du nœud.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Seuils d'événement > Agrégation**.
2. Configurez les valeurs de seuil appropriées pour la capacité, la croissance et les copies instantanées.
3. Cliquez sur **Enregistrer**.

Informations connexes

["Ajout d'utilisateurs"](#)

Configurer les valeurs de seuil de santé du volume global

Vous pouvez configurer les valeurs de seuil de santé globales pour tous les volumes afin de suivre toute violation de seuil. Des événements appropriés sont générés pour les violations du seuil de santé et vous pouvez prendre des mesures préventives en fonction de ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de meilleures pratiques pour les seuils qui s'appliquent à tous les volumes surveillés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

La plupart des options de seuil ont des valeurs par défaut pour une meilleure surveillance. Cependant, vous pouvez modifier les valeurs pour les adapter aux exigences de votre environnement.

Notez que lorsque la croissance automatique est activée sur un volume, les seuils de capacité sont considérés comme dépassés en fonction de la taille de volume maximale définie par la croissance automatique, et non en fonction de la taille du volume d'origine.



La valeur par défaut de 1 000 copies Snapshot s'applique uniquement aux volumes FlexVol lorsque la version ONTAP est 9.4 ou supérieure, et aux volumes FlexGroup lorsque la version ONTAP est 9.8 ou supérieure. Pour les clusters installés avec des versions plus anciennes du logiciel ONTAP, le nombre maximal est de 250 copies Snapshot par volume. Pour ces versions plus anciennes, Unified Manager interprète ce nombre 1000 (et tout nombre compris entre 1000 et 250) comme 250 ; ce qui signifie que vous continuerez à recevoir des événements lorsque le nombre de copies Snapshot atteint 250. Si vous souhaitez définir ce seuil à moins de 250 pour ces anciennes versions, vous devez définir le seuil à 250 ou moins ici, dans la vue Santé : Tous les volumes ou dans la page Détails du volume/santé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Seuils d'événement > Volume**.
2. Configurez les valeurs de seuil appropriées pour la capacité, les copies instantanées, les quotas qtree, la croissance du volume et les inodes.
3. Cliquez sur **Enregistrer**.

Informations connexes

["Ajout d'utilisateurs"](#)

Configurer les valeurs de seuil de santé globales de Qtree

Vous pouvez configurer les valeurs de seuil de santé globales pour tous les qtrees afin de suivre toute violation de seuil. Des événements appropriés sont générés pour les violations du seuil de santé et vous pouvez prendre des mesures préventives en fonction de ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de meilleures pratiques pour les seuils qui s'appliquent à tous les qtrees surveillés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Les options de seuil ont des valeurs par défaut pour une meilleure surveillance. Cependant, vous pouvez modifier les valeurs en fonction des exigences de votre environnement.

Les événements sont générés pour un qtree uniquement lorsqu'un quota Qtree ou un quota par défaut a été défini sur le qtree. Les événements ne sont pas générés si l'espace défini dans un quota d'utilisateur ou de groupe a dépassé le seuil.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Seuils d'événement > Qtree**.
2. Configurez les valeurs de seuil de capacité appropriées.
3. Cliquez sur **Enregistrer**.

Configurer les paramètres de seuil de décalage pour les relations de protection non gérées

Vous pouvez modifier les paramètres globaux de seuil d'avertissement de décalage et d'erreur par défaut pour les relations de protection non gérées afin que les événements soient générés à des intervalles adaptés à vos besoins.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Le temps de latence ne doit pas dépasser l'intervalle de planification de transfert défini. Par exemple, si le calendrier de transfert est horaire, le temps de latence ne doit pas dépasser une heure. Le seuil de décalage spécifie un pourcentage que le temps de décalage ne doit pas dépasser. En prenant l'exemple d'une heure, si le seuil de décalage est défini à 150 %, vous recevrez un événement lorsque le temps de décalage sera supérieur à 1,5 heure.

Les paramètres décrits dans cette tâche sont appliqués globalement à toutes les relations de protection non gérées. Les paramètres ne peuvent pas être spécifiés et appliqués exclusivement à une relation de protection non gérée.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Seuils d'événement > Relation**.
2. Augmentez ou diminuez le pourcentage de temps de latence d'avertissement ou d'erreur global par défaut selon les besoins.
3. Pour désactiver le déclenchement d'un événement d'avertissement ou d'erreur à partir de n'importe quel seuil de décalage, décochez la case en regard de **Activé**.
4. Cliquez sur **Enregistrer**.

Informations connexes

["Ajout d'utilisateurs"](#)

Modifier les paramètres de seuil de santé agrégés individuels

Vous pouvez modifier les paramètres de seuil de santé pour la capacité globale, la croissance et les copies instantanées d'un ou plusieurs agrégats. Lorsqu'un seuil est franchi, des alertes sont générées et vous recevez des notifications. Ces notifications vous aident à prendre des mesures préventives en fonction de l'événement généré.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

En fonction des modifications apportées aux valeurs seuils, les événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Lorsque la croissance automatique est activée sur les volumes qui résident sur l'agrégat, les seuils de capacité agrégée sont considérés comme dépassés en fonction de la taille de volume maximale définie par la croissance automatique, et non en fonction de la taille de volume d'origine.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Dans la vue **Santé : Tous les agrégats**, sélectionnez un ou plusieurs agrégats, puis cliquez sur **Modifier les seuils**.
3. Dans la boîte de dialogue **Modifier les seuils agrégés**, modifiez les paramètres de seuil de l'un des éléments suivants : capacité, croissance ou copies instantanées en sélectionnant la case à cocher appropriée, puis en modifiant les paramètres.
4. Cliquez sur **Enregistrer**.

Informations connexes

["Ajout d'utilisateurs"](#)

Modifier les paramètres de seuil de santé de volume individuels

Vous pouvez modifier les paramètres de seuil de santé pour la capacité du volume, la croissance, le quota et la réserve d'espace d'un ou plusieurs volumes. Lorsqu'un seuil est franchi, des alertes sont générées et vous recevez des notifications. Ces notifications vous aident à prendre des mesures préventives en fonction de l'événement généré.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

En fonction des modifications apportées aux valeurs seuils, les événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Notez que lorsque la croissance automatique est activée sur un volume, les seuils de capacité sont considérés comme dépassés en fonction de la taille de volume maximale définie par la croissance automatique, et non en fonction de la taille du volume d'origine.



La valeur par défaut de 1 000 copies Snapshot s'applique uniquement aux volumes FlexVol lorsque la version ONTAP est 9.4 ou supérieure, et aux volumes FlexGroup lorsque la version ONTAP est 9.8 ou supérieure. Pour les clusters installés avec des versions plus anciennes du logiciel ONTAP, le nombre maximal est de 250 copies Snapshot par volume. Pour ces versions plus anciennes, Unified Manager interprète ce nombre 1000 (et tout nombre compris entre 1000 et 250) comme 250 ; ce qui signifie que vous continuerez à recevoir des événements lorsque le nombre de copies Snapshot atteint 250. Si vous souhaitez définir ce seuil à moins de 250 pour ces anciennes versions, vous devez définir le seuil à 250 ou moins ici, dans la vue Santé : Tous les volumes ou dans la page Détails du volume/santé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans la vue **Santé : tous les volumes**, sélectionnez un ou plusieurs volumes, puis cliquez sur **Modifier les seuils**.
3. Dans la boîte de dialogue **Modifier les seuils de volume**, modifiez les paramètres de seuil de l'un des éléments suivants : capacité, copies d'instantanés, quota qtree, croissance ou inodes en sélectionnant la case à cocher appropriée, puis en modifiant les paramètres.
4. Cliquez sur **Enregistrer**.

Informations connexes

["Ajout d'utilisateurs"](#)

Modifier les paramètres de seuil de santé individuels de Qtree

Vous pouvez modifier les paramètres de seuil de santé pour la capacité qtree pour un ou plusieurs qtrees. Lorsqu'un seuil est franchi, des alertes sont générées et vous recevez des notifications. Ces notifications vous aident à prendre des mesures préventives en fonction de l'événement généré.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

En fonction des modifications apportées aux valeurs seuils, les événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Qtrees**.
2. Dans la vue **Capacité : Tous les Qtrees**, sélectionnez un ou plusieurs qtrees, puis cliquez sur **Modifier les seuils**.
3. Dans la boîte de dialogue **Modifier les seuils Qtree**, modifiez les seuils de capacité pour le ou les qtrees sélectionnés et cliquez sur **Enregistrer**.



Vous pouvez également définir des seuils Qtree individuels à partir de l'onglet Qtrees sur la page Détails de la machine virtuelle de stockage / Santé.

Gérer les objectifs de sécurité du cluster

Unified Manager fournit un tableau de bord qui identifie le niveau de sécurité de vos clusters ONTAP , de vos machines virtuelles de stockage (SVM) et de vos volumes en fonction des recommandations définies dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9*.

L'objectif du tableau de bord de sécurité est d'afficher les zones dans lesquelles vos clusters ONTAP ne sont pas conformes aux directives recommandées par NetApp afin que vous puissiez résoudre ces problèmes potentiels. Dans la plupart des cas, vous résoudrez les problèmes à l'aide ONTAP System Manager ou de l'ONTAP CLI. Il est possible que votre organisation ne suive pas toutes les recommandations. Dans certains cas, vous n'aurez donc pas besoin d'apporter de modifications.

Voir le ["Guide de renforcement de la sécurité NetApp pour ONTAP 9"](#) (TR-4569) pour des recommandations et

des résolutions détaillées.

En plus de signaler l'état de sécurité, Unified Manager génère également des événements de sécurité pour tout cluster ou SVM présentant des violations de sécurité. Vous pouvez suivre ces problèmes dans la page d'inventaire de gestion des événements et vous pouvez configurer des alertes pour ces événements afin que votre administrateur de stockage soit averti lorsque de nouveaux événements de sécurité se produisent.

Pour plus d'informations, voir ["Quels critères de sécurité sont évalués"](#).

Quels critères de sécurité sont évalués

En général, les critères de sécurité de vos clusters ONTAP , machines virtuelles de stockage (SVM) et volumes sont évalués par rapport aux recommandations définies dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9*.

Certains des contrôles de sécurité comprennent :

- si un cluster utilise une méthode d'authentification sécurisée, telle que SAML
- si les clusters appairés ont leur communication cryptée
- si le journal d'audit d'une machine virtuelle de stockage est activé
- si vos volumes ont un cryptage logiciel ou matériel activé

Consultez les rubriques sur les catégories de conformité et les ["Guide de renforcement de la sécurité NetApp pour ONTAP 9"](#) pour des informations détaillées.



Les événements de mise à niveau signalés par la plateforme Active IQ sont également considérés comme des événements de sécurité. Ces événements identifient les problèmes pour lesquels la résolution nécessite la mise à niveau du logiciel ONTAP , du micrologiciel du nœud ou du logiciel du système d'exploitation (pour les avis de sécurité). Ces événements ne sont pas affichés dans le panneau Sécurité, mais ils sont disponibles à partir de la page d'inventaire Gestion des événements.

Pour plus d'informations, voir ["Gestion des objectifs de sécurité des clusters"](#).

Catégories de conformité des clusters

Ce tableau décrit les paramètres de conformité de sécurité du cluster évalués par Unified Manager, la recommandation NetApp et si le paramètre affecte la détermination globale de la conformité ou non du cluster.

La présence de SVM non conformes sur un cluster affectera la valeur de conformité du cluster. Ainsi, dans certains cas, vous devrez peut-être résoudre des problèmes de sécurité avec une SVM avant que la sécurité de votre cluster ne soit considérée comme conforme.

Notez que tous les paramètres répertoriés ci-dessous n'apparaissent pas pour toutes les installations. Par exemple, si vous n'avez pas de clusters appairés ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments Cluster Peering ou AutoSupport HTTPS Transport dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Affecte la conformité du cluster
FIPS mondial	Indique si le mode de conformité Global FIPS (Federal Information Processing Standard) 140-2 est activé ou désactivé. Lorsque FIPS est activé, TLSv1 et SSLv3 sont désactivés et seuls TLSv1.1 et TLSv1.2 sont autorisés.	Activé	Oui
Telnet	Indique si l'accès Telnet au système est activé ou désactivé. NetApp recommande Secure Shell (SSH) pour un accès à distance sécurisé.	Désactivées	Oui
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Non	Oui
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs accédant au système.	Activé	Oui
Appairage de cluster	Indique si la communication entre les clusters homologues est chiffrée ou non chiffrée. Le chiffrement doit être configuré sur les clusters source et de destination pour que ce paramètre soit considéré comme conforme.	Crypté	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Protocole de temps réseau	Indique si le cluster dispose d'un ou plusieurs serveurs NTP configurés. Pour la redondance et un meilleur service, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	Configuré	Oui
Protocole OCSP	À partir de la version 9.14.1, Active IQ Unified Manager fournit des informations sur l'état du protocole OCSP (Online Certificate Status Protocol) au niveau de la machine virtuelle de stockage (SVM, anciennement appelée Vserver). Cela signifie que la validation OCSP est appliquée à toutes les connexions SSL/TLS établies avec le SVM et garantit l'intégrité et la validité des certificats utilisés dans ces connexions.	Activé	Non
Journalisation d'audit à distance	Indique si la transmission du journal (Syslog) est chiffrée ou non.	Crypté	Oui
Transport HTTPS AutoSupport	Indique si HTTPS est utilisé comme protocole de transport par défaut pour l'envoi de messages AutoSupport au support NetApp .	Activé	Oui
Utilisateur administrateur par défaut	Indique si l'utilisateur administrateur par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tous les comptes intégrés inutiles.	Désactivées	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Utilisateurs SAML	Indique si SAML est configuré. SAML vous permet de configurer l'authentification multifacteur (MFA) comme méthode de connexion pour l'authentification unique.	Non	Non
Utilisateurs Active Directory	Indique si Active Directory est configuré. Active Directory et LDAP sont les mécanismes d'authentification préférés pour les utilisateurs accédant aux clusters.	Non	Non
Utilisateurs LDAP	Indique si LDAP est configuré. Active Directory et LDAP sont les mécanismes d'authentification préférés des utilisateurs gérant des clusters par rapport aux utilisateurs locaux.	Non	Non
Utilisateurs de certificats	Indique si un utilisateur de certificat est configuré pour se connecter au cluster.	Non	Non
Utilisateurs locaux	Indique si les utilisateurs locaux sont configurés pour se connecter au cluster.	Non	Non
Shell distant	Indique si RSH est activé. Pour des raisons de sécurité, RSH doit être désactivé. Le Secure Shell (SSH) pour un accès distant sécurisé est privilégié.	Désactivées	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
MD5 en cours d'utilisation	Indique si les comptes d'utilisateur ONTAP utilisent une fonction de hachage MD5 moins sécurisée. La migration des comptes utilisateurs hachés MD5 vers la fonction de hachage cryptographique plus sécurisée comme SHA-512 est préférée.	Non	Oui
Type d'émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé par une autorité de certification	Non

Catégories de conformité des machines virtuelles de stockage

Ce tableau décrit les critères de conformité de sécurité de la machine virtuelle de stockage (SVM) évalués par Unified Manager, la recommandation NetApp et si le paramètre affecte la détermination globale de la conformité ou non de la SVM.

Paramètre	Description	Recommandation	Affecte la conformité SVM
Journal d'audit	Indique si la journalisation d'audit est activée ou désactivée.	Activé	Oui
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par <code>cbc*</code> .	Non	Oui
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs accédant aux SVM sur le système.	Activé	Oui
Cryptage LDAP	Indique si le cryptage LDAP est activé ou désactivé.	Activé	Non

Paramètre	Description	Recommandation	Affecte la conformité SVM
Authentification NTLM	Indique si l'authentification NTLM est activée ou désactivée.	Activé	Non
Signature de charge utile LDAP	Indique si la signature de charge utile LDAP est activée ou désactivée.	Activé	Non
Paramètres CHAP	Indique si CHAP est activé ou désactivé.	Activé	Non
Kerberos V5	Indique si l'authentification Kerberos V5 est activée ou désactivée.	Activé	Non
Authentification NIS	Indique si l'utilisation de l'authentification NIS est configurée.	Désactivées	Non
Statut de la politique FPolicy actif	Indique si FPolicy est créé ou non.	Oui	Non
Cryptage SMB activé	Indique si la signature et le scellement SMB ne sont pas activés.	Oui	Non
Signature SMB activée	Indique si la signature SMB n'est pas activée.	Oui	Non

Catégories de conformité en termes de volume

Ce tableau décrit les paramètres de chiffrement de volume qu'Unified Manager évalue pour déterminer si les données de vos volumes sont correctement protégées contre l'accès par des utilisateurs non autorisés.

Notez que les paramètres de chiffrement du volume n'affectent pas la conformité du cluster ou de la machine virtuelle de stockage.

Paramètre	Description
Logiciel crypté	Affiche le nombre de volumes protégés à l'aide des solutions de chiffrement logiciel NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).

Paramètre	Description
Matériel crypté	Affiche le nombre de volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
Logiciel et matériel cryptés	Affiche le nombre de volumes protégés par un chiffrement logiciel et matériel.
Non crypté	Affiche le nombre de volumes qui ne sont pas chiffrés.

Que signifie « non conforme »

Les clusters et les machines virtuelles de stockage (SVM) sont considérés comme non conformes lorsque l'un des critères de sécurité évalués par rapport aux recommandations définies dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9* n'est pas respecté. De plus, un cluster est considéré comme non conforme lorsqu'un SVM est signalé comme n'étant pas conforme.

Les icônes d'état dans les cartes de sécurité ont les significations suivantes par rapport à leur conformité :

-  - Le paramètre est configuré comme recommandé.
-  - Le paramètre n'est pas configuré comme recommandé.
-  - Soit la fonctionnalité n'est pas activée sur le cluster, soit le paramètre n'est pas configuré comme recommandé, mais ce paramètre ne contribue pas à la conformité de l'objet.

Notez que l'état de chiffrement du volume ne contribue pas à déterminer si le cluster ou le SVM sont considérés comme conformes.

Afficher l'état de sécurité des clusters et des machines virtuelles de stockage

Active IQ Unified Manager vous permet d'afficher l'état de sécurité des objets de stockage dans votre environnement à partir de différents points de l'interface. Vous pouvez collecter et analyser des informations et des rapports en fonction de paramètres définis et détecter des comportements suspects ou des modifications système non autorisées sur les clusters surveillés et les machines virtuelles de stockage.

Pour les recommandations de sécurité, voir le ["Guide de renforcement de la sécurité NetApp pour ONTAP 9"](#)

Afficher l'état de sécurité au niveau de l'objet sur la page Sécurité

En tant qu'administrateur système, vous pouvez utiliser la page **Sécurité** pour obtenir une visibilité sur le niveau de sécurité de vos clusters ONTAP et de vos machines virtuelles de stockage aux niveaux du centre de données et du site. Les objets pris en charge sont les clusters, les machines virtuelles de stockage et les volumes. Suivez ces étapes :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. Selon que vous souhaitez afficher l'état de sécurité de tous les clusters surveillés ou d'un seul cluster,

sélectionnez **Tous les clusters** ou sélectionnez un seul cluster dans le menu déroulant.

3. Cliquez sur la flèche droite dans le panneau **Sécurité**. La page Sécurité s'affiche.

En cliquant sur les graphiques à barres, les nombres et **View Reports** les liens vous amènent à la page **Volumes**, **Clusters** ou **Machines virtuelles de stockage** pour vous permettre d'afficher les détails correspondants ou de générer des rapports, selon vos besoins.

La page Sécurité affiche les panneaux suivants :

- **Conformité du cluster** : l'état de sécurité (nombre de clusters conformes ou non conformes) de tous les clusters d'un centre de données
- **Conformité des machines virtuelles de stockage** : l'état de sécurité (nombre de machines virtuelles de stockage conformes ou non conformes) pour toutes les machines virtuelles de stockage de votre centre de données
- **Chiffrement du volume** : l'état de chiffrement du volume (nombre de volumes chiffrés ou non chiffrés) de tous les volumes de votre environnement
- **Statut anti-ransomware du volume** : l'état de sécurité (nombre de volumes avec anti-ransomware activé ou désactivé) de tous les volumes de votre environnement
- **Authentification et certificats de cluster** : le nombre de clusters utilisant chaque type de méthode d'authentification, comme SAML, Active Directory ou via des certificats et une authentification locale. Le panneau affiche également le nombre de clusters dont les certificats ont expiré ou sont sur le point d'expirer dans 60 jours.

Afficher les détails de sécurité de tous les clusters sur la page Clusters

La page de détails **Clusters / Sécurité** vous permet d'afficher l'état de conformité de la sécurité au niveau du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Sélectionnez **Affichage > Sécurité > Tous les clusters**.

Les paramètres de sécurité par défaut, tels que Global FIPS, Telnet, les paramètres SSH non sécurisés, la bannière de connexion, le protocole de temps réseau, AutoSupport HTTPS Transport et l'état d'expiration du certificat de cluster sont affichés.

Vous pouvez cliquer sur le  Cliquez sur le bouton Plus d'options et choisissez d'afficher les détails de sécurité sur la page **Sécurité** d'Unified Manager ou sur System Manager. Vous devez disposer d'informations d'identification valides pour afficher les détails sur le Gestionnaire système.



Si un cluster a un certificat expiré, vous pouvez cliquer sur **expired** sous **Validité du certificat de cluster** et renouvelez-le à partir du Gestionnaire système (9.10.1 et versions ultérieures). Vous ne pouvez pas cliquer **expired** si l'instance du Gestionnaire système est d'une version antérieure à 9.10.1.

Afficher les détails de sécurité de tous les clusters à partir de la page des machines virtuelles de stockage

La page de détails **VM de stockage / Sécurité** vous permet d'afficher l'état de conformité de la sécurité au niveau de la machine virtuelle de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Machines virtuelles de stockage**.
2. Sélectionnez **Affichage > Sécurité > Toutes les machines virtuelles de stockage**. Une liste de clusters avec les paramètres de sécurité s'affiche.

Vous pouvez avoir une vue par défaut de la conformité de sécurité des machines virtuelles de stockage en vérifiant les paramètres de sécurité, tels que les machines virtuelles de stockage, le cluster, la bannière de connexion, le journal d'audit et les paramètres SSH non sécurisés.

Vous pouvez cliquer sur le  Cliquez sur le bouton Plus d'options et choisissez d'afficher les détails de sécurité sur la page **Sécurité** d'Unified Manager ou sur System Manager. Vous devez disposer d'informations d'identification valides pour afficher les détails sur le Gestionnaire système.

Pour plus de détails sur la sécurité anti-ransomware pour les volumes et les machines virtuelles de stockage, voir ["Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage"](#).

Afficher les événements de sécurité pouvant nécessiter des mises à jour de logiciels ou de micrologiciels

Certains événements de sécurité ont une zone d'impact de « Mise à niveau ». Ces événements sont signalés à partir de la plateforme Active IQ et identifient les problèmes pour lesquels la résolution nécessite la mise à niveau du logiciel ONTAP, du micrologiciel du nœud ou du logiciel du système d'exploitation (pour les avis de sécurité).

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous souhaitez peut-être effectuer une action corrective immédiate pour certains de ces problèmes, tandis que d'autres problèmes pourront attendre votre prochaine maintenance programmée. Vous pouvez afficher tous ces événements et les attribuer à des utilisateurs capables de résoudre les problèmes. De plus, s'il existe certains événements de mise à niveau de sécurité dont vous ne souhaitez pas être informé, cette liste peut vous aider à identifier ces événements afin que vous puissiez les désactiver.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

Par défaut, tous les événements actifs (nouveaux et reconnus) sont affichés sur la page d'inventaire de gestion des événements.

2. Dans le menu Affichage, sélectionnez **Événements de mise à niveau**.

La page affiche tous les événements de sécurité de mise à niveau actifs.

Afficher comment l'authentification des utilisateurs est gérée sur tous les clusters

La page Sécurité affiche les types d'authentification utilisés pour authentifier les utilisateurs sur chaque cluster, ainsi que le nombre d'utilisateurs qui accèdent au cluster à l'aide de chaque type. Cela vous permet de vérifier que l'authentification des utilisateurs est effectuée de manière sécurisée, comme défini par votre organisation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.

2. En haut du tableau de bord, sélectionnez **Tous les clusters** dans le menu déroulant.
3. Cliquez sur la flèche droite dans le panneau **Sécurité** et la page **Sécurité** s'affiche.
4. Consultez la carte **Authentification de cluster** pour voir le nombre d'utilisateurs qui accèdent au système à l'aide de chaque type d'authentification.
5. Consultez la carte **Sécurité du cluster** pour afficher les mécanismes d'authentification utilisés pour authentifier les utilisateurs sur chaque cluster.

Si certains utilisateurs accèdent au système à l'aide d'une méthode non sécurisée ou d'une méthode non recommandée par NetApp, vous pouvez désactiver la méthode.

Afficher l'état de chiffrement de tous les volumes

Vous pouvez afficher une liste de tous les volumes et leur état de chiffrement actuel afin de déterminer si les données de vos volumes sont correctement protégées contre tout accès par des utilisateurs non autorisés.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Les types de cryptage qui peuvent être appliqués à un volume sont :

- Logiciel - Volumes protégés à l'aide des solutions de chiffrement logiciel NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
- Matériel - Volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
- Logiciel et matériel - Volumes protégés par un cryptage logiciel et matériel.
- Aucun - Volumes qui ne sont pas chiffrés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Santé > Chiffrement des volumes**.
3. Dans la vue **Santé : Chiffrement des volumes**, triez sur le champ **Type de chiffrement** ou utilisez le filtre pour afficher les volumes qui ont un type de chiffrement spécifique ou qui ne sont pas chiffrés (type de chiffrement « Aucun »).

Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage

Vous pouvez afficher une liste de tous les volumes et machines virtuelles de stockage (SVM) et leur état anti-ransomware actuel afin de déterminer si les données sur vos volumes et SVM sont correctement protégées contre les attaques de ransomware.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Pour plus d'informations sur les différents statuts anti-ransomware, consultez ["ONTAP: Activer l'anti-ransomware"](#).

Afficher les détails de sécurité de tous les volumes avec détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Santé > Sécurité > Anti-ransomware**
3. Dans la vue **Sécurité : Anti-ransomware**, vous pouvez trier selon les différents champs ou utiliser le filtre.



L'anti-ransomware n'est pas pris en charge pour les volumes hors ligne, les volumes restreints, les volumes SnapLock , les volumes FlexGroup , les volumes FlexCache , les volumes SAN uniquement, les volumes de machines virtuelles de stockage arrêtées, les volumes racine de machines virtuelles de stockage ou les volumes de protection des données.

Afficher les détails de sécurité de toutes les machines virtuelles de stockage avec détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Machines virtuelles de stockage**.
2. Sélectionnez **Affichage > Sécurité > Anti-ransomware**. Une liste des SVM avec le statut anti-ransomware s'affiche.



La surveillance anti-ransomware n'est pas prise en charge sur les machines virtuelles de stockage sur lesquelles le protocole NAS n'est pas activé.

Afficher tous les événements de sécurité actifs

Vous pouvez afficher tous les événements de sécurité actifs, puis attribuer chacun d'eux à un utilisateur capable de résoudre le problème. De plus, si vous ne souhaitez pas recevoir certains événements de sécurité, cette liste peut vous aider à identifier les événements que vous souhaitez désactiver.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

Par défaut, les événements nouveaux et reconnus sont affichés sur la page d'inventaire de gestion des événements.

2. Dans le menu Affichage, sélectionnez **Événements de sécurité actifs**.

La page affiche tous les événements de sécurité nouveaux et reconnus qui ont été générés au cours des 7 derniers jours.

Ajouter des alertes pour les événements de sécurité

Vous pouvez configurer des alertes pour des événements de sécurité individuels, comme pour tout autre événement reçu par Unified Manager. De plus, si vous souhaitez traiter tous les événements de sécurité de la même manière et envoyer un e-mail à la même personne, vous pouvez créer une alerte unique pour vous avertir lorsque des événements de sécurité sont déclenchés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

L'exemple ci-dessous montre comment créer une alerte pour l'événement de sécurité « Protocole Telnet activé ». Cela enverra une alerte si l'accès Telnet est configuré pour l'accès administratif à distance au cluster. Vous pouvez utiliser cette même méthodologie pour créer des alertes pour tous les événements de sécurité.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et sélectionnez le cluster ou le cluster sur lequel vous souhaitez activer cette alerte.
5. Cliquez sur **Événements** et effectuez les actions suivantes :
 - a. Dans la liste Gravité de l'événement, sélectionnez **Avertissement**.
 - b. Dans la liste des événements correspondants, sélectionnez **Protocole Telnet activé**.
6. Cliquez sur **Actions** puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
7. Configurez toutes les autres options sur cette page pour la fréquence de notification, l'émission de taps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Désactiver des événements de sécurité spécifiques

Tous les événements sont activés par défaut. Vous pouvez désactiver des événements spécifiques pour empêcher la génération de notifications pour les événements qui ne sont pas importants dans votre environnement. Vous pouvez activer les événements désactivés si vous souhaitez reprendre la réception des notifications les concernant.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous désactivez les événements, les événements précédemment générés dans le système sont marqués comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications pour ces événements sont générées à partir du prochain cycle de surveillance.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des événements**.
2. Dans la page de configuration **Événement**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Si vous voulez...	Alors fais ceci...
Désactiver les événements	a. Cliquez sur Désactiver. b. Dans la boîte de dialogue Désactiver les événements, sélectionnez la gravité Avertissement. Il s'agit de la catégorie pour tous les événements de sécurité. c. Dans la colonne Événements correspondants, sélectionnez les événements de sécurité que vous souhaitez désactiver, puis cliquez sur la flèche droite pour déplacer ces événements vers la colonne Désactiver les événements. d. Cliquez sur Enregistrer et fermer. e. Vérifiez que les événements que vous avez désactivés s'affichent dans la vue de liste de la page Configuration des événements.
Activer les événements	a. Dans la liste des événements désactivés, cochez la case correspondant à l'événement ou aux événements que vous souhaitez réactiver. b. Cliquez sur Activer.

Événements de sécurité

Les événements de sécurité vous fournissent des informations sur l'état de sécurité des clusters ONTAP , des machines virtuelles de stockage (SVM) et des volumes en fonction des paramètres définis dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9*. Ces événements vous informent des problèmes potentiels afin que vous puissiez évaluer leur gravité et résoudre le problème si nécessaire.

Les événements de sécurité sont regroupés par type de source et incluent le nom de l'événement et de l'interruption, le niveau d'impact et la gravité. Ces événements apparaissent dans les catégories d'événements de cluster et de machine virtuelle de stockage.

Gérer les opérations de sauvegarde et de restauration

Vous pouvez créer des sauvegardes d' Active IQ Unified Manager et utiliser la fonction de restauration pour restaurer la sauvegarde sur le même système (local) ou sur un nouveau système (distant) en cas de panne du système ou de perte de données.

Il existe trois méthodes de sauvegarde et de restauration en fonction du système d'exploitation sur lequel vous avez installé Unified Manager et du nombre de clusters et de nœuds gérés :

Système opérateur	Taille du déploiement	Méthode de sauvegarde recommandée
VMware vSphere	N'importe lequel	Instantané VMware de l'appliance virtuelle Unified Manager
Red Hat Enterprise Linux	Petit	Vidage de la base de données MySQL d'Unified Manager
	Grand	Instantané NetApp de la base de données Unified Manager
Microsoft Windows	Petit	Vidage de la base de données MySQL d'Unified Manager
	Grand	Instantané NetApp de la base de données Unified Manager avec le protocole iSCSI

Ces différentes méthodes sont décrites dans les sections qui suivent.

Sauvegarde et restauration pour Unified Manager sur un appareil virtuel

Le modèle de sauvegarde et de restauration d'Unified Manager lorsqu'il est installé sur une appliance virtuelle consiste à capturer et à restaurer une image de l'application virtuelle complète.

Les tâches suivantes vous permettent d'effectuer une sauvegarde de l'appliance virtuelle :

1. Mettez la machine virtuelle hors tension et prenez un instantané VMware de l'appliance virtuelle Unified Manager.
2. Créez une copie de l'instantané NetApp sur le magasin de données pour capturer l'instantané VMware.

Si la banque de données n'est pas hébergée sur un système exécutant le logiciel ONTAP , suivez les instructions du fournisseur de stockage pour créer une sauvegarde de l'instantané VMware.

3. Répliquez la copie NetApp Snapshot, ou l'équivalent snapshot, sur un stockage alternatif.
4. Supprimez le snapshot VMware.

Vous devez implémenter une planification de sauvegarde à l'aide de ces tâches pour garantir que l'appliance virtuelle Unified Manager est protégée en cas de problème.

Pour restaurer la machine virtuelle, vous pouvez utiliser l'instantané VMware que vous avez créé pour restaurer la machine virtuelle à l'état de sauvegarde du moment précis.

Sauvegarde et restauration à l'aide d'un vidage de base de données MySQL

Une sauvegarde de vidage de base de données MySQL est une copie de la base de données Active IQ Unified Manager et des fichiers de configuration que vous pouvez utiliser en cas de panne du système ou de perte de données. Vous pouvez planifier une

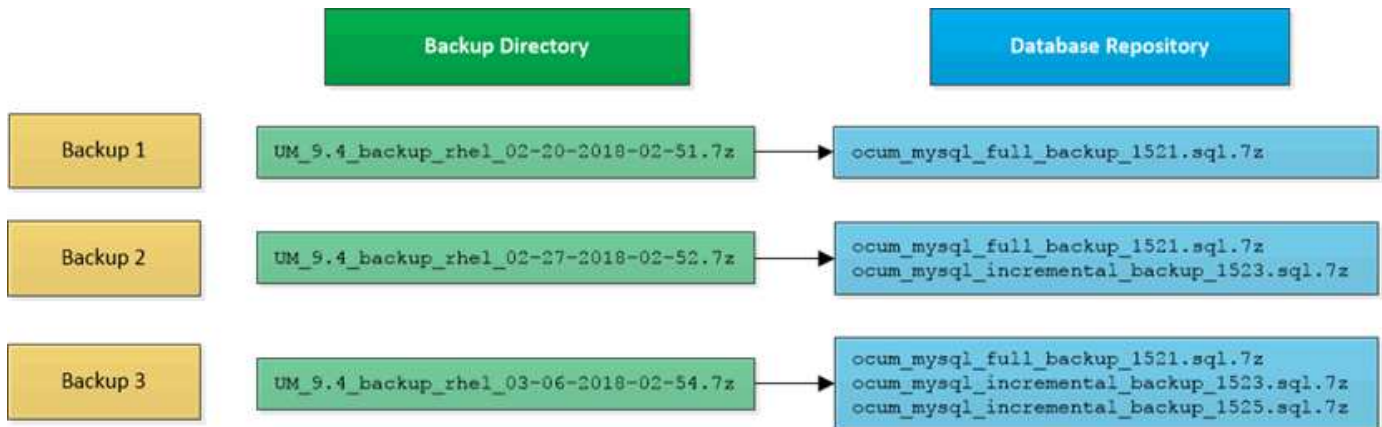
sauvegarde à écrire vers une destination locale ou vers une destination distante. Il est fortement recommandé de définir un emplacement distant externe au système hôte Active IQ Unified Manager .



Le vidage de la base de données MySQL est le mécanisme de sauvegarde par défaut lorsque Unified Manager est installé sur un serveur Linux et Windows. Toutefois, si Unified Manager gère un grand nombre de clusters et de nœuds, ou si vos sauvegardes MySQL prennent plusieurs heures, vous pouvez effectuer des sauvegardes à l'aide de copies Snapshot. Cette fonctionnalité est disponible sur Red Hat Enterprise Linux et Windows.

Une sauvegarde de vidage de base de données se compose d'un seul fichier dans le répertoire de sauvegarde et d'un ou plusieurs fichiers dans le répertoire du référentiel de base de données. Le fichier dans le répertoire de sauvegarde est très petit car il contient uniquement un pointeur vers les fichiers situés dans le répertoire du référentiel de base de données qui sont nécessaires pour recréer la sauvegarde.

La première fois que vous générez une sauvegarde de base de données, un seul fichier est créé dans le répertoire de sauvegarde et un fichier de sauvegarde complet est créé dans le répertoire du référentiel de base de données. La prochaine fois que vous générez une sauvegarde, un seul fichier est créé dans le répertoire de sauvegarde et un fichier de sauvegarde incrémentielle est créé dans le répertoire du référentiel de base de données qui contient les différences par rapport au fichier de sauvegarde complet. Ce processus se poursuit à mesure que vous créez des sauvegardes supplémentaires, jusqu'au paramètre de rétention maximal, comme illustré dans la figure suivante.



Ne renommez ni ne supprimez aucun des fichiers de sauvegarde dans ces deux répertoires, sinon toute opération de restauration ultérieure échouera.

Si vous écrivez vos fichiers de sauvegarde sur le système local, vous devez lancer un processus pour copier les fichiers de sauvegarde vers un emplacement distant afin qu'ils soient disponibles en cas de problème système nécessitant une restauration complète.

Avant de commencer une opération de sauvegarde, Active IQ Unified Manager effectue une vérification d'intégrité pour vérifier que tous les fichiers et répertoires de sauvegarde requis existent et sont accessibles en écriture. Il vérifie également qu'il y a suffisamment d'espace sur le système pour créer le fichier de sauvegarde.

Configurer la destination et la planification des sauvegardes de vidage de base de données

Vous pouvez configurer les paramètres de sauvegarde de vidage de base de données Unified Manager pour définir le chemin de sauvegarde de la base de données, le nombre

de rétentions et la planification de sauvegarde. Vous pouvez activer des sauvegardes planifiées quotidiennes ou hebdomadaires. Par défaut, les sauvegardes planifiées sont désactivées, mais vous devez définir une planification de sauvegarde.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez disposer d'un minimum de 150 Go d'espace disponible à l'emplacement que vous définissez comme chemin de sauvegarde.

Il est recommandé d'utiliser un emplacement distant externe au système hôte Unified Manager.

- Lorsque Unified Manager est installé sur un système Linux et que vous utilisez la sauvegarde MySQL, assurez-vous que les autorisations et propriétés suivantes sont définies sur le répertoire de sauvegarde.

Autorisations : 0750, Propriété : jboss:maintenance

- Lorsque Unified Manager est installé sur un système Windows et que vous utilisez la sauvegarde MySQL, assurez-vous que seul l'administrateur a accès au répertoire de sauvegarde.

La première sauvegarde nécessite plus de temps que les sauvegardes suivantes, car la première sauvegarde est une sauvegarde complète. Une sauvegarde complète peut dépasser 1 Go et prendre trois à quatre heures. Les sauvegardes ultérieures sont incrémentielles et nécessitent moins de temps.



- Si vous trouvez que le nombre de fichiers de sauvegarde incrémentielle est trop important pour l'espace que vous avez alloué aux sauvegardes, vous pouvez effectuer périodiquement une sauvegarde complète pour remplacer l'ancienne sauvegarde et ses fichiers incrémentiels. Comme autre option, vous pouvez effectuer une sauvegarde en utilisant des copies instantanées.
- La sauvegarde effectuée au cours des 15 premiers jours suivant l'ajout d'un nouveau cluster peut ne pas être suffisamment précise pour obtenir les données de performances historiques.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Sauvegarde de la base de données**.
2. Dans la page **Sauvegarde de la base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Configurez les valeurs appropriées pour un chemin de sauvegarde, un nombre de rétentions et une planification.

La valeur par défaut du nombre de rétentions est 10 ; vous pouvez utiliser 0 pour créer des sauvegardes illimitées.

4. Sélectionnez le bouton **Planifié quotidiennement** ou **Planifié chaque semaine**, puis spécifiez les détails de la planification.
5. Cliquez sur **Appliquer**.

Les fichiers de sauvegarde de vidage de base de données sont créés en fonction de la planification. Vous pouvez voir les fichiers de sauvegarde disponibles dans la page Sauvegarde de la base de données.

Qu'est-ce qu'une restauration de base de données

Une restauration de base de données MySQL est le processus de restauration d'un

fichier de sauvegarde Unified Manager existant sur le même serveur Unified Manager ou sur un serveur Unified Manager différent. Vous effectuez l'opération de restauration à partir de la console de maintenance Unified Manager.

Si vous effectuez une opération de restauration sur le même système (local) et que les fichiers de sauvegarde sont tous stockés localement, vous pouvez exécuter l'option de restauration en utilisant l'emplacement par défaut. Si vous effectuez une opération de restauration sur un autre système Unified Manager (un système distant), vous devez copier le ou les fichiers de sauvegarde du stockage secondaire vers le disque local avant d'exécuter l'option de restauration.

Pendant le processus de restauration, vous êtes déconnecté d'Unified Manager. Vous pouvez vous connecter au système une fois le processus de restauration terminé.

Si vous restaurez l'image de sauvegarde sur un nouveau serveur, une fois l'opération de restauration terminée, vous devez générer un nouveau certificat de sécurité HTTPS et redémarrer le serveur Unified Manager. Vous devrez également reconfigurer les paramètres d'authentification SAML, s'ils sont nécessaires, lors de la restauration de l'image de sauvegarde sur un nouveau serveur.



Les anciens fichiers de sauvegarde ne peuvent pas être utilisés pour restaurer une image après la mise à niveau d'Unified Manager vers une version plus récente du logiciel. Pour économiser de l'espace, tous les anciens fichiers de sauvegarde, à l'exception du fichier le plus récent, sont supprimés automatiquement lorsque vous mettez à niveau Unified Manager.

Informations connexes

["Générer un certificat de sécurité HTTPS"](#)

["Activation de l'authentification SAML"](#)

["Authentification avec Active Directory ou OpenLDAP"](#)

Restaurer une sauvegarde de base de données MySQL sous Windows

En cas de perte ou de corruption de données, vous pouvez utiliser la fonction de restauration pour restaurer Unified Manager à l'état stable précédent avec une perte minimale. Vous pouvez restaurer la base de données MySQL d'Unified Manager sur un système Windows local ou un système Windows distant à l'aide de la console de maintenance d'Unified Manager.

Avant de commencer

- Vous devez disposer des privilèges d'administrateur Windows.
- Vous devez avoir copié le fichier de sauvegarde d'Unified Manager et le contenu du répertoire du référentiel de base de données sur le système sur lequel vous effectuerez l'opération de restauration.

Il est recommandé de copier le fichier de sauvegarde dans le répertoire par défaut

`\ProgramData\NetApp\OnCommandAppData\ocum\backup`. Les fichiers du référentiel de base de données doivent être copiés dans le `\database_dumps_repo` sous-répertoire sous le `\backup` annuaire.

- Les fichiers de sauvegarde doivent être de `.7z` taper.

La fonctionnalité de restauration est spécifique à la plate-forme et à la version. Vous pouvez restaurer une

sauvegarde MySQL d'Unified Manager uniquement sur la même version d'Unified Manager, et une sauvegarde Windows ne peut être restaurée que sur une plate-forme Windows.



Si les noms de dossier contiennent un espace, vous devez inclure le chemin absolu ou le chemin relatif du fichier de sauvegarde entre guillemets.

Étapes

1. Si vous effectuez une restauration sur un nouveau serveur, après l'installation d'Unified Manager, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification une fois l'installation terminée. Le fichier de sauvegarde renseigne ces informations pendant le processus de restauration.
2. Connectez-vous au système Unified Manager avec les informations d'identification d'administrateur.
3. Lancez PowerShell ou l'invite de commande en tant qu'administrateur Windows.
4. Entrez la commande `maintenance_console` et appuyez sur Entrée.
5. Dans la console de maintenance **Menu principal**, entrez le numéro de l'option **Restauration de sauvegarde**.
6. Entrez le numéro pour la **Restauration de la sauvegarde MySQL**.
7. Lorsque vous y êtes invité, entrez le chemin absolu du fichier de sauvegarde.

```
Bundle to restore from:
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
kup_windows_02-20-2020-02-51.7z
```

Une fois l'opération de restauration terminée, vous pouvez vous connecter à Unified Manager.

Après avoir restauré la sauvegarde, si le serveur OnCommand Workflow Automation ne fonctionne pas, procédez comme suit :

1. Sur le serveur Workflow Automation, modifiez l'adresse IP du serveur Unified Manager pour qu'elle pointe vers la dernière machine.
2. Sur le serveur Unified Manager, réinitialisez le mot de passe de la base de données si l'acquisition échoue à l'étape 1.

Sauvegarde et restauration à l'aide de NetApp Snapshots

Une copie NetApp Snapshot crée une image ponctuelle de la base de données Unified Manager et des fichiers de configuration que vous pouvez utiliser pour restaurer en cas de panne du système ou de perte de données. Vous planifiez l'écriture périodique d'une copie Snapshot sur un volume de l'un de vos clusters ONTAP afin de toujours disposer d'une copie à jour.



Cette fonctionnalité n'est pas disponible pour Active IQ Unified Manager installé sur une appliance virtuelle.

Si votre Active IQ Unified Manager est installé sur une machine Linux, vous pouvez décider de configurer votre sauvegarde et votre restauration à l'aide de NetApp Snapshots.

Les copies instantanées prennent très peu de temps, généralement quelques minutes seulement, et la base de données Unified Manager est verrouillée pendant une très courte période, ce qui entraîne très peu de perturbations dans votre installation. L'image consomme un espace de stockage minimal et entraîne une surcharge de performances négligeable, car elle enregistre uniquement les modifications apportées aux fichiers depuis la dernière copie instantanée. Étant donné que le snapshot est créé sur un cluster ONTAP, vous pouvez tirer parti d'autres fonctionnalités NetApp telles que SnapMirror pour créer une protection secondaire, si nécessaire.

Avant de commencer une opération de sauvegarde, Unified Manager effectue un contrôle d'intégrité pour vérifier que le système de destination est disponible.



- Vous ne pouvez restaurer une copie instantanée que sur la même version d'Active IQ Unified Manager.

Par exemple, si vous avez créé une sauvegarde sur Unified Manager 9.16, la sauvegarde ne peut être restaurée que sur les systèmes Unified Manager 9.16.

- Si une modification est apportée à la configuration de l'instantané, l'instantané peut devenir invalide.

Configurer l'emplacement de la copie de l'instantané

Vous pouvez configurer le volume sur lequel les copies Snapshot seront stockées sur l'un de vos clusters ONTAP à l'aide d'ONTAP System Manager ou de l'interface de ligne de commande ONTAP.

Avant de commencer

Le cluster, la machine virtuelle de stockage et le volume doivent répondre aux exigences suivantes :

- Exigences du cluster :
 - ONTAP 9.3 ou supérieur doit être installé
 - Il doit être géographiquement proche du serveur Unified Manager
 - Il peut être surveillé par Unified Manager, mais ce n'est pas obligatoire
- Exigences relatives à la machine virtuelle de stockage :
 - Le commutateur de nom et le mappage de nom doivent être définis pour utiliser « fichiers »
 - Utilisateurs locaux créés pour correspondre aux utilisateurs côté client
 - Assurez-vous que tous les accès en lecture/écriture sont sélectionnés
 - Assurez-vous que l'accès superutilisateur est défini sur « any » dans la politique d'exportation
 - NFS pour NetApp Snapshot pour Linux
 - NFSv4 doit être activé sur le serveur NFS et le domaine d'ID NFSv4 spécifié sur le client et la machine virtuelle de stockage
 - Le volume doit être au moins le double de la taille du répertoire Unified Manager/opt/netapp/data

Utilisez la commande du `-sh /opt/netapp/data/` pour vérifier la taille actuelle.

- Exigences de volume :
 - Le volume doit être au moins le double de la taille du répertoire Unified Manager `/opt/netapp/data`
 - Le style de sécurité doit être défini sur UNIX
 - La politique de capture instantanée locale doit être désactivée
 - La taille automatique du volume doit être activée
 - Le niveau de service de performance doit être défini sur une politique avec des IOPS élevées et une faible latence, telle que « Extrême »

Pour les étapes détaillées de création du volume NFS, voir ["Comment configurer NFSv4 dans ONTAP 9"](#) et le ["Guide de configuration express NFS ONTAP 9"](#).

Spécifiez l'emplacement de destination des copies instantanées

Vous devez configurer l'emplacement de destination des copies Active IQ Unified Manager Snapshot sur un volume que vous avez déjà configuré dans l'un de vos clusters ONTAP. Vous devez utiliser la console de maintenance pour définir l'emplacement.

- Vous devez disposer des informations d'identification de l'utilisateur root pour l'hôte Linux sur lequel Active IQ Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez disposer de l'adresse IP de gestion du cluster, du nom de la machine virtuelle de stockage, du nom du volume, ainsi que du nom d'utilisateur et du mot de passe du système de stockage.
- Vous devez avoir monté le volume sur l'hôte Active IQ Unified Manager et vous devez disposer du chemin de montage.

Étapes

1. Utilisez Secure Shell pour vous connecter à l'adresse IP ou au nom de domaine complet du système Active IQ Unified Manager.
2. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de maintenance (umadmin).
3. Entrez la commande `maintenance_console` et appuyez sur Entrée.
4. Dans la console de maintenance **Menu principal**, entrez le numéro de l'option **Restauration de sauvegarde**.
5. Saisissez le numéro pour ***Configurer la sauvegarde instantanée NetApp ***.
6. Entrez le numéro pour configurer NFS.
7. Vérifiez les informations que vous devrez fournir, puis saisissez le numéro pour **Entrer les détails de configuration de sauvegarde**.
8. Pour identifier le volume sur lequel le snapshot sera écrit, entrez l'adresse IP de l'interface de gestion de cluster, le nom de la machine virtuelle de stockage, le nom du volume, le nom du LUN, le nom d'utilisateur et le mot de passe du système de stockage, ainsi que le chemin de montage.
9. Vérifiez ces informations et entrez `y`.

Le système effectue les tâches suivantes :

- Établit la connexion au cluster
- Arrête tous les services
- Crée un nouveau répertoire dans le volume et copie les fichiers de configuration de la base de données Active IQ Unified Manager
- Supprime les fichiers d' Active IQ Unified Manager et crée un lien symbolique vers le nouveau répertoire de base de données
- Redémarre tous les services

10. Quittez la console de maintenance et lancez l'interface Active IQ Unified Manager pour créer une planification pour la copie Snapshot si vous ne l'avez pas déjà fait.

Configurer la sauvegarde sur Windows

Active IQ Unified Manager prend en charge la sauvegarde et la restauration à l'aide de NetApp Snapshots sur le système d'exploitation Windows à l'aide de LUN utilisant le protocole iSCSI.

Une sauvegarde basée sur des instantanés peut être effectuée pendant que tous les services Unified Manager sont en cours d'exécution. Un état cohérent de la base de données est capturé dans le cadre du snapshot, car la sauvegarde place un verrou de lecture global sur l'ensemble de la base de données qui empêche toute écriture simultanée. Pour que votre système Unified Manager installé sur le système d'exploitation Windows puisse effectuer une sauvegarde et une restauration à l'aide de snapshots NetApp , vous devez d'abord configurer la sauvegarde d'Unified Manager sur la base de snapshots à l'aide de la console de maintenance.

Avant de configurer Unified Manager pour la création de copies Snapshot, vous devez effectuer les tâches de configuration suivantes.

- Configurer le cluster ONTAP
- Configurer la machine hôte Windows

Configurer l'emplacement de sauvegarde pour Windows

Vous devez configurer le volume pour stocker les copies Snapshot après avoir sauvegardé Unified Manager sous Windows.

Avant de commencer

Le cluster, la machine virtuelle de stockage et le volume doivent répondre aux exigences suivantes :

- Exigences du cluster :
 - ONTAP 9.3 ou supérieur doit être installé
 - Il doit être géographiquement proche du serveur Unified Manager
 - Il est surveillé par Unified Manager
- Exigences relatives à la machine virtuelle de stockage :
 - Connectivité iSCSI sur le cluster ONTAP
 - Le protocole iSCSI doit être activé pour la machine configurée
 - Vous devez disposer d'un volume et d'un LUN dédiés à la configuration de la sauvegarde. Le volume sélectionné ne doit contenir qu'un seul LUN et rien d'autre.
 - La taille du LUN doit être au moins deux fois supérieure à la taille des données devant être gérées

dans Active IQ Unified Manager 9.9.

Cela définit également la même exigence de taille en termes de volume.

- Assurez-vous que tous les accès en lecture/écriture sont sélectionnés
- Assurez-vous que l'accès superutilisateur est défini sur « any » dans la politique d'exportation
- Exigences en matière de volume et de LUN :
 - Le volume doit être au moins le double de la taille du répertoire de données MySQL d'Unified Manager.
 - Le style de sécurité doit être défini sur Windows
 - La politique de capture instantanée locale doit être désactivée
 - La taille automatique du volume doit être activée
 - Le niveau de service de performance doit être défini sur une politique avec des IOPS élevées et une faible latence, telle que « Extrême »

Configurer le cluster ONTAP

Vous devez effectuer quelques étapes de préconfiguration sur les clusters ONTAP avant de pouvoir sauvegarder et restaurer Active IQ Unified Manager à l'aide d'une copie Snapshot sur les systèmes Windows.

Vous pouvez configurer le cluster ONTAP à l'aide de l'invite de commande ou de l'interface utilisateur du Gestionnaire système. La configuration du cluster ONTAP implique la configuration des LIF de données pour qu'ils puissent être attribués en tant que LIF iSCSI à la machine virtuelle de stockage. L'étape suivante consiste à configurer une machine virtuelle de stockage compatible iSCSI à l'aide de l'interface utilisateur du gestionnaire de système. Vous devrez configurer un itinéraire réseau statique pour cette machine virtuelle de stockage afin de contrôler la manière dont les LIF utilisent le réseau pour le trafic sortant.



Vous devez disposer d'un volume dédié et d'un LUN pour la configuration de sauvegarde. Le volume sélectionné ne doit inclure qu'un seul LUN. La taille du LUN doit être au moins deux fois supérieure à la taille des données que Active IQ Unified Manager est censé gérer.

Vous devez effectuer la configuration suivante :

Étapes

1. Configurez une machine virtuelle de stockage compatible iSCSI ou utilisez une machine virtuelle de stockage existante dotée de la même configuration.
2. Configurez un itinéraire réseau pour la machine virtuelle de stockage configurée.
3. Configurez un volume de capacité appropriée et un seul LUN à l'intérieur en vous assurant que le volume est dédié uniquement à ce LUN.



Dans un scénario où le LUN est créé sur le Gestionnaire système, le démappage du LUN peut supprimer le groupe i et la restauration peut échouer. Pour éviter ce scénario, assurez-vous que lors de la création d'un LUN, celui-ci est créé explicitement et n'est pas supprimé lorsque le LUN est démappé.

4. Configurez un groupe d'initiateurs dans la machine virtuelle de stockage.
5. Configurer un ensemble de ports.

6. Intégrez l'igroup avec le portset.
7. Mappez le LUN au igroup.

Configurer la machine hôte Windows

Vous devez configurer votre machine hôte Windows avant de pouvoir utiliser NetApp Snapshot pour sauvegarder et restaurer Active IQ Unified Manager. Pour démarrer l'initiateur Microsoft iSCSI sur une machine hôte Windows, saisissez « iscsi » dans la barre de recherche et cliquez sur **Initiateur iSCSI**.

Avant de commencer

Vous devez nettoyer toutes les configurations précédentes sur la machine hôte.

Si vous essayez de démarrer l'initiateur iSCSI sur une nouvelle installation de Windows, vous êtes invité à confirmer et, après confirmation, la boîte de dialogue Propriétés iSCSI s'affiche. S'il s'agit d'une installation Windows existante, la boîte de dialogue Propriétés iSCSI s'affiche avec une cible inactive ou essayant de se connecter. Vous devrez donc vous assurer que toutes les configurations précédentes sur l'hôte Windows sont supprimées.

Étapes

1. Nettoyez toutes les configurations précédentes sur la machine hôte.
2. Découvrez le portail cible.
3. Connectez-vous au portail cible.
4. Connectez-vous via multipath au portail cible.
5. Découvrez les deux LIF.
6. Découvrez le LUN configuré sur la machine Windows en tant que périphérique.
7. Configurez le LUN découvert comme un nouveau lecteur de volume dans Windows.

Spécifier l'emplacement de destination des copies instantanées sous Windows

Vous devez configurer l'emplacement de destination des copies Active IQ Unified Manager Snapshot sur un volume que vous avez déjà configuré dans l'un de vos clusters ONTAP . Vous devez utiliser la console de maintenance pour définir l'emplacement.

- Vous devez disposer du privilège administrateur pour l'hôte Windows sur lequel Active IQ Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez disposer de l'adresse IP de gestion du cluster, du nom de la machine virtuelle de stockage, du nom du volume, du nom du LUN, ainsi que du nom d'utilisateur et du mot de passe du système de stockage.
- Vous devez avoir monté le volume en tant que lecteur réseau sur l'hôte Active IQ Unified Manager et vous devez disposer du lecteur de montage.

Étapes

1. À l'aide de Power Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Active IQ Unified Manager .

2. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de maintenance (umadmin).
3. Entrez la commande `maintenance_console` et appuyez sur Entrée.
4. Dans la console de maintenance **Menu principal**, entrez le numéro de l'option **Restauration de sauvegarde**.
5. Saisissez le numéro pour *Configurer la sauvegarde instantanée NetApp *.
6. Entrez le numéro pour configurer iSCSI.
7. Vérifiez les informations que vous devrez fournir, puis saisissez le numéro pour **Entrer les détails de configuration de sauvegarde**.
8. Pour identifier le volume sur lequel le snapshot sera écrit, entrez l'adresse IP de l'interface de gestion de cluster, le nom de la machine virtuelle de stockage, le nom du volume, le nom du LUN, le nom d'utilisateur et le mot de passe du système de stockage, ainsi que le lecteur de montage.
9. Vérifiez ces informations et entrez `y` .

Le système effectue les tâches suivantes :

- La machine virtuelle de stockage est validée
 - Le volume est validé
 - Montez le lecteur et l'état est validé
 - Existence et état du LUN
 - Existence d'un lecteur réseau
 - L'existence d'un espace recommandé (plus de deux fois le répertoire de données MySQL) sur le volume monté est validée
 - Chemin LUN correspondant au LUN dédié dans le volume
 - nom du groupe `i`
 - GUID du volume sur lequel le lecteur réseau est monté
 - Initiateur iSCSI utilisé pour communiquer avec ONTAP
10. Quittez la console de maintenance et lancez l'interface Active IQ Unified Manager pour créer une planification pour les copies Snapshot.

Configurer la sauvegarde par copie instantanée à partir de la console de maintenance

Pour effectuer une sauvegarde d' Active IQ Unified Manager à l'aide d'une copie Snapshot, vous devez effectuer quelques étapes de configuration à partir de la console de maintenance.

Avant de commencer

Vous devriez avoir les détails suivants pour votre système :

- Adresse IP du cluster
- Nom du VM de stockage
- Nom du volume
- Nom du LUN
- Chemin de montage

- Informations d'identification du système de stockage

Étapes

1. Accédez à la console de maintenance d'Unified Manager.
2. Entrez 4 pour sélectionner **Sauvegarde et restauration**.
3. Entrez 2 pour sélectionner **Sauvegarder et restaurer à l'aide de NetApp Snapshot**.



Si vous souhaitez modifier la configuration de sauvegarde, saisissez 3 pour sélectionner *Mettre à jour la configuration de sauvegarde des instantanés NetApp *. Vous ne pouvez mettre à jour que le mot de passe.

4. Dans le menu, entrez 1 pour sélectionner *Configurer la sauvegarde instantanée NetApp *.
5. Entrez 1 pour fournir les informations requises.
6. Fournissez le nom d'utilisateur et le mot de passe pour la console de maintenance, puis fournissez la confirmation que le LUN est monté sur l'hôte.

Le processus vérifie ensuite que le répertoire de données, le chemin LUN, la machine virtuelle de stockage, les volumes, la disponibilité de l'espace, le lecteur, etc. fournis par vous sont corrects. Les opérations qui se déroulent en arrière-plan sont :

- Les services sont arrêtés
- Le répertoire de la base de données est déplacé vers le stockage monté
- Le répertoire de la base de données est supprimé et les liens symboliques sont établis
- Les services sont redémarrés. Une fois la configuration terminée dans l'interface Active IQ Unified Manager , le type de sauvegarde est modifié en NetApp Snapshot et se reflète dans l'interface utilisateur comme Sauvegarde de base de données (basée sur Snapshot).

Avant de commencer une opération de sauvegarde, vous devez vérifier s'il y a un changement dans la configuration du snapshot, car cela pourrait entraîner l'invalidation du snapshot. Supposons que vous ayez configuré une sauvegarde sur le lecteur G et qu'un instantané ait été pris. Vous avez ensuite reconfiguré la sauvegarde sur le lecteur E et les données sont enregistrées sur le lecteur E conformément à la nouvelle configuration. Si vous essayez de restaurer un instantané pris alors qu'il se trouvait sur le lecteur G, cela échoue avec l'erreur indiquant que le lecteur G n'existe pas.

Définir un calendrier de sauvegarde pour Linux et Windows

Vous pouvez configurer la planification selon laquelle les copies d'instantanés d'Unified Manager sont créées à l'aide de l'interface utilisateur d'Unified Manager.

Avant de commencer

- Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré les paramètres de création de copies Snapshot à partir de la console de maintenance pour identifier la destination où les snapshots seront créés.

Les copies instantanées sont créées en quelques minutes seulement et la base de données Unified Manager n'est verrouillée que pendant quelques secondes.



La sauvegarde effectuée au cours des 15 premiers jours suivant l'ajout d'un nouveau cluster peut ne pas être suffisamment précise pour obtenir les données de performances historiques.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Sauvegarde de la base de données**.
2. Dans la page **Sauvegarde de la base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Saisissez le nombre maximal de copies Snapshot que vous souhaitez conserver dans le champ **Nombre de rétention**.

La valeur par défaut du nombre de rétentions est 10. Le nombre maximal de copies Snapshot est déterminé par la version du logiciel ONTAP sur le cluster. Vous pouvez laisser ce champ vide pour implémenter la valeur maximale quelle que soit la version ONTAP .
4. Sélectionnez le bouton **Planifié quotidiennement** ou **Planifié chaque semaine**, puis spécifiez les détails de la planification.
5. Cliquez sur **Appliquer**.

Des copies instantanées sont créées en fonction de la planification. Vous pouvez voir les fichiers de sauvegarde disponibles dans la page Sauvegarde de la base de données.

En raison de l'importance de ce volume et des instantanés, vous souhaitez peut-être créer une ou deux alertes pour ce volume afin d'être averti lorsque :

- L'espace volumique est rempli à 90 %. Utilisez l'événement **Volume Espace Plein** pour configurer l'alerte.

Vous pouvez ajouter de la capacité au volume à l'aide ONTAP System Manager ou de l'interface de ligne de commande ONTAP afin que la base de données Unified Manager ne manque pas d'espace.

- Le nombre d'instantanés est proche d'atteindre le nombre maximum. Utilisez l'événement **Trop de copies d'instantanés** pour configurer l'alerte.

Vous pouvez supprimer les anciens snapshots à l'aide ONTAP System Manager ou de l'interface de ligne de commande ONTAP afin qu'il y ait toujours de la place pour de nouvelles copies de snapshots.

Vous configurez les alertes dans la page Configuration des alertes.

Restaurer Unified Manager à l'aide de copies instantanées

En cas de perte ou de corruption de données, vous pouvez restaurer Unified Manager à l'état stable précédent avec une perte minimale de données. Vous pouvez restaurer la base de données Unified Manager Snapshot sur un système d'exploitation local ou distant à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez disposer des informations d'identification de l'utilisateur root pour l'hôte Linux et des privilèges d'administration pour la machine hôte Windows sur laquelle Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

La fonctionnalité de restauration est spécifique à la plate-forme et à la version. Vous ne pouvez restaurer une sauvegarde Unified Manager que sur la même version d'Unified Manager.

Étapes

1. Connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager.

- Linux : Shell sécurisé
- Windows : Power Shell

2. Connectez-vous au système avec les informations d'identification de l'utilisateur root.
3. Entrez la commande `maintenance_console` et appuyez sur Entrée.
4. Dans la console de maintenance **Menu principal**, entrez 4 pour l'option **Restauration de sauvegarde**.
5. Saisissez 2 pour sélectionner **Sauvegarder et restaurer à l'aide de NetApp Snapshot**.

Si vous effectuez une restauration sur un nouveau serveur, après l'installation d'Unified Manager, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification une fois l'installation terminée. Saisissez 1 pour sélectionner *Configurer la sauvegarde instantanée NetApp * et configurez les paramètres des copies instantanées telles qu'elles se trouvent sur le système d'origine.

6. Saisissez 3 pour sélectionner **Restaurer à l'aide de NetApp Snapshot**.
7. Sélectionnez la copie instantanée à partir de laquelle vous souhaitez restaurer Unified Manager. Appuyez sur **Entrée**.
8. Une fois le processus de restauration terminé, connectez-vous à l'interface utilisateur d'Unified Manager.

Après avoir restauré la sauvegarde, si le serveur Workflow Automation ne fonctionne pas, procédez comme suit :

1. Sur le serveur Workflow Automation, modifiez l'adresse IP du serveur Unified Manager pour qu'elle pointe vers la dernière machine.
2. Sur le serveur Unified Manager, réinitialisez le mot de passe de la base de données si l'acquisition échoue à l'étape 1.

Modifier le type de sauvegarde

Si vous souhaitez modifier le type de sauvegarde de votre système Active IQ Unified Manager , vous pouvez utiliser les options de la console de maintenance. L'option **Déconfigurer la sauvegarde NetApp Snapshot** vous permet de revenir à la sauvegarde basée sur MySQL.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez 4 dans le **Menu principal** pour la sauvegarde et la restauration.
3. Sélectionnez 2 dans le menu **Sauvegarde et restauration**.
4. Sélectionnez 4 pour *Déconfigurer la sauvegarde instantanée NetApp *.

Les actions effectuées sont affichées : arrêter les services, rompre le lien symbolique, déplacer les données du stockage vers le répertoire, puis redémarrer les services.

Une fois la méthode de sauvegarde modifiée, le mécanisme de sauvegarde passe de la copie instantanée à la sauvegarde MySQL par défaut. Cette modification apparaît dans la section Sauvegarde de la base de

données des paramètres généraux.

Sauvegarde à la demande pour Unified Manager

Vous pouvez utiliser l'interface utilisateur Active IQ Unified Manager pour générer une sauvegarde à la demande chaque fois que nécessaire. La sauvegarde à la demande vous permet de créer instantanément une sauvegarde en utilisant la méthode de sauvegarde existante. La sauvegarde à la demande ne fait pas de distinction entre la sauvegarde basée sur MySQL ou NetApp Snapshot.

Vous pouvez effectuer une sauvegarde à la demande en utilisant le bouton **Sauvegarder maintenant** sur la page de sauvegarde de la base de données. La sauvegarde à la demande ne dépend pas des planifications que vous avez configurées pour Active IQ Unified Manager.

Migrer une appliance virtuelle Unified Manager vers un système Linux

Vous pouvez restaurer une sauvegarde de vidage de base de données MySQL Unified Manager à partir d'une appliance virtuelle vers un système Red Hat Enterprise Linux si vous souhaitez modifier le système d'exploitation hôte sur lequel Unified Manager s'exécute.

Avant de commencer

- Sur l'appareil virtuel :
 - Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.
 - Vous devez connaître le nom de l'utilisateur de maintenance Unified Manager pour l'opération de restauration.
- Sur le système Linux :
 - Vous devez avoir installé Unified Manager sur un serveur Linux en suivant les instructions de ["Installation d'Unified Manager sur les systèmes Linux"](#).
 - La version d'Unified Manager sur ce serveur doit être la même que la version sur l'appliance virtuelle à partir de laquelle vous utilisez le fichier de sauvegarde.
 - Ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification sur le système Linux après l'installation. Le fichier de sauvegarde renseigne ces informations pendant le processus de restauration.
 - Vous devez disposer des informations d'identification de l'utilisateur root pour l'hôte Linux.

Ces étapes décrivent comment créer un fichier de sauvegarde sur l'appliance virtuelle, copier les fichiers de sauvegarde sur Red Hat Enterprise Linux, puis restaurer la sauvegarde de la base de données sur le nouveau système.

Étapes

1. Sur l'appliance virtuelle, cliquez sur **Gestion > Sauvegarde de la base de données**.
2. Dans la page **Sauvegarde de la base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Modifiez le chemin de sauvegarde vers `/jail/support`.
4. Dans la section Planification, sélectionnez **Planifié quotidiennement** et saisissez une heure quelques minutes après l'heure actuelle afin que la sauvegarde soit créée rapidement.

5. Cliquez sur **Appliquer**.
6. Attendez quelques heures que la sauvegarde soit générée.

Une sauvegarde complète peut dépasser 1 Go et prendre trois à quatre heures.

7. Connectez-vous en tant qu'utilisateur root à l'hôte Linux sur lequel Unified Manager est installé et copiez les fichiers de sauvegarde depuis /support sur l'appliance virtuelle à l'aide de
SCP.root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

Assurez-vous d'avoir copié le fichier de sauvegarde .7z et tous les fichiers du référentiel .7z dans le sous-répertoire /database-dumps-repo.

8. À l'invite de commande, restaurez la sauvegarde :um backup restore -f
/<backup_file_path>/<backup_file_name>

```
um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
```

9. Une fois l'opération de restauration terminée, connectez-vous à l'interface Web d'Unified Manager.

Vous devez effectuer les tâches suivantes :

- Générez un nouveau certificat de sécurité HTTPS et redémarrez le serveur Unified Manager.
- Modifiez le chemin de sauvegarde vers le paramètre par défaut de votre système Linux (/data/ocum-backup), ou vers un nouveau chemin de votre choix, car il n'y a pas de chemin /jail/support sur le système Linux.
- Reconfigurez les deux côtés de votre connexion Workflow Automation, si WFA est utilisé.
- Reconfigurez les paramètres d'authentification SAML, si vous utilisez SAML.

Après avoir vérifié que tout fonctionne comme prévu sur votre système Linux, vous pouvez arrêter et supprimer l'appliance virtuelle Unified Manager.

Gérer les scripts

Vous pouvez utiliser des scripts pour modifier ou mettre à jour automatiquement plusieurs objets de stockage dans Unified Manager. Le script est associé à une alerte. Lorsqu'un événement déclenche une alerte, le script est exécuté. Vous pouvez télécharger des scripts personnalisés et tester leur exécution lorsqu'une alerte est générée.

La possibilité de télécharger des scripts sur Unified Manager et de les exécuter est activée par défaut. Si votre organisation ne souhaite pas autoriser cette fonctionnalité pour des raisons de sécurité, vous pouvez la désactiver depuis **Gestion du stockage > Paramètres des fonctionnalités**.

Comment fonctionnent les scripts avec les alertes

Vous pouvez associer une alerte à votre script afin que le script soit exécuté lorsqu'une alerte est déclenchée pour un événement dans Unified Manager. Vous pouvez utiliser les scripts pour résoudre les problèmes liés aux objets de stockage ou identifier les objets de stockage qui génèrent les événements.

Lorsqu'une alerte est générée pour un événement dans Unified Manager, un e-mail d'alerte est envoyé aux destinataires spécifiés. Si vous avez associé une alerte à un script, le script est exécuté. Vous pouvez obtenir les détails des arguments transmis au script à partir de l'e-mail d'alerte.



Si vous avez créé un script personnalisé et l'avez associé à une alerte pour un type d'événement spécifique, les actions sont effectuées en fonction de votre script personnalisé pour ce type d'événement, et les actions **Corriger** ne sont pas disponibles par défaut sur la page Actions de gestion ou sur le tableau de bord Unified Manager.

Le script utilise les arguments suivants pour l'exécution :

- -eventID
- -eventName
- -eventSeverity
- -eventSourceID
- -eventSourceName
- -eventSourceType
- -eventState
- -eventArgs

Vous pouvez utiliser les arguments dans vos scripts et collecter des informations sur les événements associés ou modifier les objets de stockage.

Exemple d'obtention d'arguments à partir de scripts

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Lorsqu'une alerte est générée, ce script est exécuté et la sortie suivante s'affiche :

```
-eventID : 290
-eventSourceID : 4138
```

Ajouter des scripts

Vous pouvez ajouter des scripts dans Unified Manager et associer les scripts à des alertes. Ces scripts sont exécutés automatiquement lorsqu'une alerte est générée et vous permettent d'obtenir des informations sur les objets de stockage pour lesquels l'événement est généré.

Avant de commencer

- Vous devez avoir créé et enregistré les scripts que vous souhaitez ajouter au serveur Unified Manager.
- Les formats de fichiers pris en charge pour les scripts sont Perl, Shell, PowerShell, Python et .bat fichiers.

Plateforme sur laquelle Unified Manager est installé	Langues prises en charge
VMware	Scripts Perl et Shell
Linux	Scripts Perl, Python et Shell
Windows	Scripts PowerShell, Perl, Python et .bat

- Pour les scripts Perl, Perl doit être installé sur le serveur Unified Manager. Pour les installations VMware, Perl 5 est installé par défaut et les scripts prendront en charge uniquement ce que Perl 5 prend en charge. Si Perl a été installé après Unified Manager, vous devez redémarrer le serveur Unified Manager.
- Pour les scripts PowerShell, la stratégie d'exécution PowerShell appropriée doit être définie sur le serveur Windows afin que les scripts puissent être exécutés.



Si votre script crée des fichiers journaux pour suivre la progression du script d'alerte, vous devez vous assurer que les fichiers journaux ne sont créés nulle part dans le dossier d'installation d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez télécharger des scripts personnalisés et collecter des détails sur l'événement concernant l'alerte.



Si vous ne voyez pas cette fonctionnalité disponible dans l'interface utilisateur, c'est parce que la fonctionnalité a été désactivée par votre administrateur. Si nécessaire, vous pouvez activer cette fonctionnalité depuis **Gestion du stockage > Paramètres des fonctionnalités**.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Scripts**.
2. Dans la page **Scripts**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un script**, cliquez sur **Parcourir** pour sélectionner votre fichier de script.
4. Saisissez une description pour le script que vous sélectionnez.
5. Cliquez sur **Ajouter**.

Supprimer les scripts

Vous pouvez supprimer un script d'Unified Manager lorsque le script n'est plus nécessaire ou valide.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Le script ne doit pas être associé à une alerte.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Scripts**.
2. Dans la page **Scripts**, sélectionnez le script que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Exécution du script de test

Vous pouvez vérifier que votre script est exécuté correctement lorsqu'une alerte est générée pour un objet de stockage.

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir téléchargé un script dans le format de fichier pris en charge sur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Scripts**.
2. Dans la page Scripts, ajoutez votre script de test.
3. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration des alertes**.
4. Dans la page **Configuration des alertes**, effectuez l'une des actions suivantes :

À...	Fais ceci...
Ajouter une alerte	a. Cliquez sur Ajouter. b. Dans la section Actions, associez l'alerte à votre script de test.
Modifier une alerte	a. Sélectionnez une alerte, puis cliquez sur Modifier. b. Dans la section Actions, associez l'alerte à votre script de test.

5. Cliquez sur **Enregistrer**.
6. Dans la page **Configuration des alertes**, sélectionnez l'alerte que vous avez ajoutée ou modifiée, puis cliquez sur **Tester**.

Le script est exécuté avec l'argument « -test » et une alerte de notification est envoyée aux adresses e-mail spécifiées lors de la création de l'alerte.

Gérer et surveiller les groupes

Vous pouvez créer des groupes dans Unified Manager pour gérer les objets de stockage.

Comprendre les groupes

Vous pouvez créer des groupes dans Unified Manager pour gérer les objets de stockage. Comprendre les concepts relatifs aux groupes et la manière dont les règles de groupe vous permettent d'ajouter des objets de stockage à un groupe vous aidera à gérer les objets de stockage dans votre environnement.

Qu'est-ce qu'un groupe

Un groupe est une collection dynamique d'objets de stockage hétérogènes (clusters, SVM ou volumes). Vous pouvez créer des groupes dans Unified Manager pour gérer facilement un ensemble d'objets de stockage. Les membres d'un groupe peuvent changer en fonction des objets de stockage surveillés par Unified Manager à un moment donné.

- Chaque groupe a un nom unique.
- Vous devez configurer au moins une règle de groupe pour chaque groupe.
- Vous pouvez associer un groupe à plusieurs règles de groupe.
- Chaque groupe peut inclure plusieurs types d'objets de stockage tels que des clusters, des SVM ou des volumes.
- Les objets de stockage sont ajoutés dynamiquement à un groupe en fonction du moment où une règle de groupe est créée ou lorsque Unified Manager termine un cycle de surveillance.
- Vous pouvez appliquer simultanément des actions sur tous les objets de stockage d'un groupe, comme la définition de seuils pour les volumes.

Comment fonctionnent les règles de groupe pour les groupes

Une règle de groupe est un critère que vous définissez pour permettre aux objets de stockage (volumes, clusters ou SVM) d'être inclus dans un groupe spécifique. Vous pouvez utiliser des groupes de conditions ou des conditions pour définir une règle de groupe pour un groupe.

- Vous devez associer une règle de groupe à un groupe.
- Vous devez associer un type d'objet pour une règle de groupe ; un seul type d'objet est associé pour une règle de groupe.
- Les objets de stockage sont ajoutés ou supprimés du groupe après chaque cycle de surveillance ou lorsqu'une règle est créée, modifiée ou supprimée.
- Une règle de groupe peut avoir un ou plusieurs groupes de conditions, et chaque groupe de conditions peut avoir une ou plusieurs conditions.
- Les objets de stockage peuvent appartenir à plusieurs groupes en fonction des règles de groupe que vous créez.

Conditions

Vous pouvez créer plusieurs groupes de conditions, et chaque groupe de conditions peut avoir une ou plusieurs conditions. Vous pouvez appliquer tous les groupes de conditions définis dans une règle de groupe pour les groupes afin de spécifier quels objets de stockage sont inclus dans le groupe.

Les conditions au sein d'un groupe de conditions sont exécutées à l'aide de la fonction ET logique. Toutes les conditions d'un groupe de conditions doivent être remplies. Lorsque vous créez ou modifiez une règle de groupe, une condition est créée qui applique, sélectionne et regroupe uniquement les objets de stockage qui satisfont toutes les conditions du groupe de conditions. Vous pouvez utiliser plusieurs conditions au sein d'un groupe de conditions lorsque vous souhaitez restreindre la portée des objets de stockage à inclure dans un groupe.

Vous pouvez créer des conditions avec des objets de stockage en utilisant les opérandes et l'opérateur

suivants et en spécifiant la valeur requise.

Type d'objet de stockage	Opérandes applicables
Volume	• Nom de l'objet • Nom du cluster propriétaire • Nom de SVM propriétaire • Annotations
SVM	• Nom de l'objet • Nom du cluster propriétaire • Annotations
Cluster	• Nom de l'objet • Annotations

Lorsque vous sélectionnez une annotation comme opérande pour un objet de stockage, l'opérateur « Est » est disponible. Pour tous les autres opérandes, vous pouvez sélectionner « Est » ou « Contient » comme opérateur.

- Opérande

La liste des opérandes dans Unified Manager change en fonction du type d'objet sélectionné. La liste inclut le nom de l'objet, le nom du cluster propriétaire, le nom de la SVM propriétaire et les annotations que vous définissez dans Unified Manager.

- Opérateur

La liste des opérateurs change en fonction de l'opérande sélectionné pour une condition. Les opérateurs pris en charge dans Unified Manager sont « Est » et « Contient ».

Lorsque vous sélectionnez l'opérateur « Est », la condition est évaluée pour une correspondance exacte de la valeur de l'opérande avec la valeur fournie pour l'opérande sélectionné.

Lorsque vous sélectionnez l'opérateur « Contient », la condition est évaluée pour répondre à l'un des critères suivants :

- La valeur de l'opérande correspond exactement à la valeur fournie pour l'opérande sélectionné
- La valeur de l'opérande contient la valeur fournie pour l'opérande sélectionné

- Valeur

Le champ de valeur change en fonction de l'opérande sélectionné.

Exemple de règle de groupe avec conditions

Considérons un groupe de conditions pour un volume avec les deux conditions suivantes :

- Le nom contient « vol »
- Le nom de la SVM est « data_svm »

Ce groupe de conditions sélectionne tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur des SVM portant le nom « data_svm ».

Groupes de conditions

Les groupes de conditions sont exécutés à l'aide de la fonction OU logique, puis appliqués aux objets de stockage. Les objets de stockage doivent satisfaire à l'un des groupes de conditions pour être inclus dans un groupe. Les objets de stockage de tous les groupes de conditions sont combinés. Vous pouvez utiliser des groupes de conditions pour augmenter la portée des objets de stockage à inclure dans un groupe.

Exemple de règle de groupe avec des groupes de conditions

Considérez deux groupes de conditions pour un volume, chaque groupe contenant les deux conditions suivantes :

- Groupe de conditions 1
 - Le nom contient « vol »
 - Le nom SVM est « data_svm ». Le groupe de conditions 1 sélectionne tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur des SVM portant le nom « data_svm ».
- Groupe de conditions 2
 - Le nom contient « vol »
 - La valeur d'annotation de data-priority est « critical ». Le groupe de conditions 2 sélectionne tous les volumes qui incluent « vol » dans leurs noms et qui sont annotés avec la valeur d'annotation data-priority « critical ».

Lorsqu'une règle de groupe contenant ces deux groupes de conditions est appliquée sur des objets de stockage, les objets de stockage suivants sont ajoutés à un groupe sélectionné :

- Tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur le SVM avec le nom « data_svm ».
- Tous les volumes qui incluent « vol » dans leur nom et qui sont annotés avec la valeur d'annotation de priorité des données « critical ».

Comment fonctionnent les actions de groupe sur les objets de stockage

Une action de groupe est une opération effectuée sur tous les objets de stockage d'un groupe. Par exemple, vous pouvez configurer l'action du groupe de seuil de volume pour modifier simultanément les valeurs de seuil de volume de tous les volumes d'un groupe.

Les groupes prennent en charge des types d'actions de groupe uniques. Vous pouvez avoir un groupe avec un seul type d'action de groupe de seuil de santé de volume. Cependant, vous pouvez configurer un autre type d'action de groupe, si disponible, pour le même groupe. Le rang d'une action de groupe détermine l'ordre dans lequel l'action est appliquée aux objets de stockage. La page de détails d'un objet de stockage fournit des informations sur l'action de groupe appliquée à l'objet de stockage.

Exemple d'actions de groupe uniques

Considérez un volume A qui appartient aux groupes G1 et G2, et les actions de groupe de seuil d'intégrité de volume suivantes sont configurées pour ces groupes :

- `Change\_capacity\_threshold` action de groupe de rang 1, pour configurer la capacité du volume

- `Change\_snapshot\_copies` action de groupe de rang 2, pour configurer les copies Snapshot du volume

Le `Change_capacity_threshold` l'action de groupe a toujours la priorité sur la `Change_snapshot_copies` action de groupe et est appliquée au volume A. Lorsque Unified Manager termine un cycle de surveillance, les événements liés au seuil de santé du volume A sont réévalués conformément à la `Change_capacity_threshold` action de groupe. Vous ne pouvez pas configurer un autre type de seuil de volume d'action de groupe pour le groupe G1 ou G2.

Ajouter des groupes

Vous pouvez créer des groupes pour combiner des clusters, des volumes et des machines virtuelles de stockage (SVM) pour faciliter la gestion.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez définir des règles de groupe pour ajouter ou supprimer des membres du groupe et pour modifier les actions du groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Groupes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un groupe**, saisissez un nom et une description pour le groupe.
4. Cliquez sur **Ajouter**.

Modifier les groupes

Vous pouvez modifier le nom et la description d'un groupe que vous avez créé dans Unified Manager.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous modifiez un groupe pour mettre à jour le nom, vous devez spécifier un nom unique ; vous ne pouvez pas utiliser un nom de groupe existant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Groupes**, sélectionnez le groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le groupe**, modifiez le nom, la description ou les deux du groupe.
4. Cliquez sur **Enregistrer**.

Supprimer des groupes

Vous pouvez supprimer un groupe d'Unified Manager lorsque le groupe n'est plus nécessaire.

Avant de commencer

- Aucun des objets de stockage (clusters, SVM ou volumes) ne doit être associé à une règle de groupe

associée au groupe que vous souhaitez supprimer.

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Groupes**, sélectionnez le groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

La suppression d'un groupe ne supprime pas les actions de groupe associées au groupe. Cependant, ces actions de groupe ne seront pas mappées une fois le groupe supprimé.

Ajouter des règles de groupe

Vous pouvez créer des règles de groupe pour qu'un groupe ajoute dynamiquement des objets de stockage tels que des volumes, des clusters ou des machines virtuelles de stockage (SVM) au groupe. Vous devez configurer au moins un groupe de conditions avec au moins une condition pour créer une règle de groupe.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Les objets de stockage actuellement surveillés sont ajoutés dès que la règle de groupe est créée. Les nouveaux objets ne sont ajoutés qu'une fois le cycle de surveillance terminé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Règles de groupe**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle de groupe**, spécifiez un nom pour la règle de groupe.
4. Dans le champ **Type d'objet cible**, sélectionnez le type d'objet de stockage que vous souhaitez regrouper.
5. Dans le champ **Groupe**, sélectionnez le groupe requis pour lequel vous souhaitez créer des règles de groupe.
6. Dans la section **Conditions**, procédez comme suit pour créer une condition, un groupe de conditions ou les deux :

Créer....	Fais ceci...
Une condition	a. Sélectionnez un opérande dans la liste des opérandes. b. Sélectionnez Contient ou Est comme opérateur. c. Saisissez une valeur ou sélectionnez une valeur dans la liste disponible.

Créer....	Fais ceci...
Un groupe de conditions	- Cliquez sur Ajouter un groupe de conditions - Sélectionnez un opérande dans la liste des opérandes. - Sélectionnez Contient ou Est comme opérateur. - Saisissez une valeur ou sélectionnez une valeur dans la liste disponible. - Cliquez sur Ajouter une condition pour créer d'autres conditions si nécessaire et répétez les étapes a à d pour chaque condition.

7. Cliquez sur **Ajouter**.

Exemple de création d'une règle de groupe

Effectuez les étapes suivantes dans la boîte de dialogue Ajouter une règle de groupe pour créer une règle de groupe, y compris la configuration d'une condition et l'ajout d'un groupe de conditions :

Étapes

- Spécifiez un nom pour la règle de groupe.
- Sélectionnez le type d'objet comme machine virtuelle de stockage (SVM).
- Sélectionnez un groupe dans la liste des groupes.
- Dans la section Conditions, sélectionnez **Nom de l'objet** comme opérande.
- Sélectionnez **Contient** comme opérateur.
- Entrez la valeur comme `svm_data`.
- Cliquez sur **Ajouter un groupe de conditions**.
- Sélectionnez **Nom de l'objet** comme opérande.
- Sélectionnez **Contient** comme opérateur.
- Entrez la valeur comme `vol`.
- Cliquez sur **Ajouter une condition**.
- Répétez les étapes 8 à 10 en sélectionnant **data-priority** comme opérande à l'étape 8, **Is** comme opérateur à l'étape 9 et **critical** comme valeur à l'étape 10.
- Cliquez sur **Ajouter** pour créer la condition pour la règle de groupe.

Modifier les règles du groupe

Vous pouvez modifier les règles de groupe pour modifier les groupes de conditions et les conditions au sein d'un groupe de conditions pour ajouter ou supprimer des objets de stockage vers ou depuis un groupe spécifique.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Règles de groupe**, sélectionnez la règle de groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier la règle de groupe**, modifiez le nom de la règle de groupe, le nom du groupe associé, les groupes de conditions et les conditions selon vos besoins.



Vous ne pouvez pas modifier le type d'objet cible pour une règle de groupe.

4. Cliquez sur **Enregistrer**.

Supprimer les règles du groupe

Vous pouvez supprimer une règle de groupe d'Active IQ Unified Manager lorsque la règle de groupe n'est plus nécessaire.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsqu'une règle de groupe est supprimée, les objets de stockage associés sont supprimés du groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Règles de groupe**, sélectionnez la règle de groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Ajouter des actions de groupe

Vous pouvez configurer les actions de groupe que vous souhaitez appliquer aux objets de stockage d'un groupe. La configuration des actions pour un groupe vous permet de gagner du temps, car vous n'avez pas besoin d'ajouter ces actions à chaque objet individuellement.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Actions de groupe**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une action de groupe**, saisissez un nom et une description pour l'action.
4. Dans le menu **Groupe**, sélectionnez un groupe pour lequel vous souhaitez configurer l'action.
5. Dans le menu **Type d'action**, sélectionnez un type d'action.

La boîte de dialogue s'agrandit, vous permettant de configurer le type d'action sélectionné avec les paramètres requis.

6. Saisissez les valeurs appropriées pour les paramètres requis pour configurer une action de groupe.
7. Cliquez sur **Ajouter**.

Modifier les actions du groupe

Vous pouvez modifier les paramètres d'action de groupe que vous avez configurés dans Unified Manager, tels que le nom de l'action de groupe, la description, le nom du groupe associé et les paramètres du type d'action.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Actions de groupe**, sélectionnez l'action de groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier l'action de groupe**, modifiez le nom de l'action de groupe, la description, le nom du groupe associé et les paramètres du type d'action, selon vos besoins.
4. Cliquez sur **Enregistrer**.

Configurer les seuils de santé du volume pour les groupes

Vous pouvez configurer des seuils d'intégrité de volume au niveau du groupe pour la capacité, les copies instantanées, les quotas qtree, la croissance et les inodes.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Le type d'action de groupe de seuil de santé du volume est appliqué uniquement aux volumes d'un groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Actions de groupe**, cliquez sur **Ajouter**.
3. Saisissez un nom et une description pour l'action de groupe.
4. Dans la liste déroulante **Groupe**, sélectionnez un groupe pour lequel vous souhaitez configurer une action de groupe.
5. Sélectionnez **Type d'action** comme seuil de santé du volume.
6. Sélectionnez la catégorie pour laquelle vous souhaitez définir le seuil.
7. Saisissez les valeurs requises pour le seuil de santé.
8. Cliquez sur **Ajouter**.

Supprimer les actions de groupe

Vous pouvez supprimer une action de groupe d'Unified Manager lorsque l'action de groupe n'est plus nécessaire.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous supprimez l'action de groupe pour le seuil d'intégrité du volume, les seuils globaux sont appliqués aux objets de stockage de ce groupe. Les seuils de santé au niveau de l'objet définis sur l'objet de stockage ne sont pas affectés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Actions de groupe**, sélectionnez l'action de groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Réorganiser les actions de groupe

Vous pouvez modifier l'ordre des actions de groupe qui doivent être appliquées aux objets de stockage d'un groupe. Les actions de groupe sont appliquées aux objets de stockage de manière séquentielle en fonction de leur rang. Le rang le plus bas est attribué à l'action de groupe que vous avez configurée en dernier. Vous pouvez modifier le rang de l'action de groupe en fonction de vos besoins.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez sélectionner une seule ligne ou plusieurs lignes, puis effectuer plusieurs opérations de glisser-déposer pour modifier le rang des actions de groupe. Cependant, vous devez enregistrer les modifications pour que la repriorisation soit reflétée dans la grille des actions du groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Groupes**.
2. Dans l'onglet **Actions de groupe**, cliquez sur **Réorganiser**.
3. Dans la boîte de dialogue **Réorganiser les actions de groupe**, faites glisser et déposez les lignes pour réorganiser la séquence des actions de groupe selon vos besoins.
4. Cliquez sur **Enregistrer**.

Prioriser les événements des objets de stockage à l'aide d'annotations

Vous pouvez créer et appliquer des règles d'annotation aux objets de stockage afin de pouvoir identifier et filtrer ces objets en fonction du type d'annotation appliqué et de sa priorité.

En savoir plus sur les annotations

Comprendre les concepts relatifs aux annotations vous aide à gérer les événements liés aux objets de stockage dans votre environnement.

Que sont les annotations

Une annotation est une chaîne de texte (le nom) qui est attribuée à une autre chaîne de texte (la valeur). Chaque paire nom-valeur d'annotation peut être associée

dynamiquement à des objets de stockage à l'aide de règles d'annotation. Lorsque vous associez des objets de stockage à des annotations prédéfinies, vous pouvez filtrer et afficher les événements qui leur sont liés. Vous pouvez appliquer des annotations aux clusters, aux volumes et aux machines virtuelles de stockage (SVM).

Chaque nom d'annotation peut avoir plusieurs valeurs ; chaque paire nom-valeur peut être associée à un objet de stockage via des règles.

Par exemple, vous pouvez créer une annotation nommée « data-center » avec les valeurs « Boston » et « Canada ». Vous pouvez ensuite appliquer l'annotation « data-center » avec la valeur « Boston » au volume v1. Lorsqu'une alerte est générée pour un événement sur un volume v1 annoté avec « data-center », l'e-mail généré indique l'emplacement du volume, « Boston », ce qui vous permet de hiérarchiser et de résoudre le problème.

Comment fonctionnent les règles d'annotation dans Unified Manager

Une règle d'annotation est un critère que vous définissez pour annoter des objets de stockage (volumes, clusters ou machines virtuelles de stockage (SVM)). Vous pouvez utiliser des groupes de conditions ou des conditions pour définir des règles d'annotation.

- Vous devez associer une règle d'annotation à une annotation.
- Vous devez associer un type d'objet pour une règle d'annotation ; un seul type d'objet peut être associé pour une règle d'annotation.
- Unified Manager ajoute ou supprime des annotations des objets de stockage après chaque cycle de surveillance ou lorsqu'une règle est créée, modifiée, supprimée ou réorganisée.
- Une règle d'annotation peut avoir un ou plusieurs groupes de conditions, et chaque groupe de conditions peut avoir une ou plusieurs conditions.
- Les objets de stockage peuvent avoir plusieurs annotations. Une règle d'annotation pour une annotation particulière peut également utiliser différentes annotations dans les conditions de règle pour ajouter une autre annotation à des objets déjà annotés.

Conditions

Vous pouvez créer plusieurs groupes de conditions, et chaque groupe de conditions peut avoir une ou plusieurs conditions. Vous pouvez appliquer tous les groupes de conditions définis dans une règle d'annotation d'une annotation afin d'annoter des objets de stockage.

Les conditions au sein d'un groupe de conditions sont exécutées à l'aide de la fonction ET logique. Toutes les conditions d'un groupe de conditions doivent être remplies. Lorsque vous créez ou modifiez une règle d'annotation, une condition est créée qui applique, sélectionne et annote uniquement les objets de stockage qui répondent à toutes les conditions du groupe de conditions. Vous pouvez utiliser plusieurs conditions au sein d'un groupe de conditions lorsque vous souhaitez restreindre la portée des objets de stockage à annoter.

Vous pouvez créer des conditions avec des objets de stockage en utilisant les opérandes et l'opérateur suivants et en spécifiant la valeur requise.

Type d'objet de stockage	Opérandes applicables
Volume	• Nom de l'objet • Nom du cluster propriétaire • Nom de SVM propriétaire • Annotations
SVM	• Nom de l'objet • Nom du cluster propriétaire • Annotations
Cluster	• Nom de l'objet • Annotations

Lorsque vous sélectionnez une annotation comme opérande pour un objet de stockage, l'opérateur « Is » est disponible. Pour tous les autres opérandes, vous pouvez sélectionner « Est » ou « Contient » comme opérateur. Lorsque vous sélectionnez l'opérateur « Est », la condition est évaluée pour une correspondance exacte de la valeur de l'opérande avec la valeur fournie pour l'opérande sélectionné. Lorsque vous sélectionnez l'opérateur « Contient », la condition est évaluée pour répondre à l'un des critères suivants :

- La valeur de l'opérande correspond exactement à la valeur de l'opérande sélectionné.
- La valeur de l'opérande contient la valeur fournie pour l'opérande sélectionné.

Exemple de règle d'annotation avec conditions

Considérez une règle d'annotation avec un groupe de conditions pour un volume avec les deux conditions suivantes :

- Le nom contient « vol »
- Le nom de la SVM est « data_svm »

Cette règle d'annotation annote tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur des SVM portant le nom « data_svm » avec l'annotation sélectionnée et le type d'annotation.

Groupes de conditions

Les groupes de conditions sont exécutés à l'aide de la fonction OU logique, puis appliqués aux objets de stockage. Les objets de stockage doivent répondre aux exigences de l'un des groupes de conditions pour être annotés. Les objets de stockage qui répondent aux conditions de tous les groupes de conditions sont annotés. Vous pouvez utiliser des groupes de conditions pour augmenter la portée des objets de stockage à annoter.

Exemple de règle d'annotation avec des groupes de conditions

Considérez une règle d'annotation avec deux groupes de conditions pour un volume ; chaque groupe contient les deux conditions suivantes :

- Groupe de conditions 1
 - Le nom contient « vol »

- Le nom SVM est « data_svm ». Ce groupe de conditions annote tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur des SVM portant le nom « data_svm ».
- Groupe de conditions 2
 - Le nom contient « vol »
 - La valeur d'annotation de data-priority est « critical ». Ce groupe de conditions annote tous les volumes qui incluent « vol » dans leurs noms et qui sont annotés avec la valeur d'annotation data-priority comme « critical ».

Lorsqu'une règle d'annotation contenant ces deux groupes de conditions est appliquée aux objets de stockage, les objets de stockage suivants sont annotés :

- Tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur SVM avec le nom « data_svm ».
- Tous les volumes qui incluent « vol » dans leur nom et qui sont annotés avec la valeur d'annotation de priorité des données « critical ».

Description des valeurs d'annotation prédéfinies

Data-priority est une annotation prédéfinie qui possède les valeurs Mission critique, Élevé et Faible. Ces valeurs vous permettent d'annoter les objets de stockage en fonction de la priorité des données qu'ils contiennent. Vous ne pouvez pas modifier ou supprimer les valeurs d'annotation prédéfinies.

- **Priorité des données : critique pour la mission**

Cette annotation s'applique aux objets de stockage contenant des données critiques. Par exemple, les objets contenant des applications de production peuvent être considérés comme critiques pour la mission.

- **Priorité des données : élevée**

Cette annotation est appliquée aux objets de stockage contenant des données hautement prioritaires. Par exemple, les objets qui hébergent des applications métier peuvent être considérés comme hautement prioritaires.

- **Priorité des données : faible**

Cette annotation est appliquée aux objets de stockage contenant des données de faible priorité. Par exemple, les objets qui se trouvent sur un stockage secondaire, tels que les destinations de sauvegarde et de miroir, peuvent être de faible priorité.

Ajouter des annotations de manière dynamique

Lorsque vous créez des annotations personnalisées, Unified Manager associe dynamiquement des clusters, des machines virtuelles de stockage (SVM) et des volumes aux annotations à l'aide de règles. Ces règles attribuent automatiquement les annotations aux objets de stockage.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans la page **Annotations**, cliquez sur **Ajouter une annotation**.
3. Dans la boîte de dialogue **Ajouter une annotation**, saisissez un nom et une description pour l'annotation.
4. Facultatif : dans la section **Valeurs d'annotation**, cliquez sur **Ajouter** pour ajouter des valeurs à l'annotation.
5. Cliquez sur **Enregistrer**.

Ajouter des valeurs aux annotations

Vous pouvez ajouter des valeurs aux annotations, puis associer des objets de stockage à une paire nom-valeur d'annotation particulière. L'ajout de valeurs aux annotations vous aide à gérer les objets de stockage plus efficacement.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous ne pouvez pas ajouter de valeurs aux annotations prédéfinies.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans la page **Annotations**, sélectionnez l'annotation à laquelle vous souhaitez ajouter une valeur, puis cliquez sur **Ajouter** dans la section **Valeurs**.
3. Dans la boîte de dialogue **Ajouter une valeur d'annotation**, spécifiez une valeur pour l'annotation.

La valeur que vous spécifiez doit être unique pour l'annotation sélectionnée.

4. Cliquez sur **Ajouter**.

Supprimer les annotations

Vous pouvez supprimer les annotations personnalisées et leurs valeurs lorsqu'elles ne sont plus nécessaires.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Les valeurs d'annotation ne doivent pas être utilisées dans d'autres annotations ou règles de groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Annotations**, sélectionnez l'annotation que vous souhaitez supprimer.

Les détails de l'annotation sélectionnée sont affichés.

3. Cliquez sur **Actions > Supprimer** pour supprimer l'annotation sélectionnée et sa valeur.
4. Dans la boîte de dialogue d'avertissement, cliquez sur **Oui** pour confirmer la suppression.

Afficher la liste des annotations et les détails

Vous pouvez afficher la liste des annotations associées dynamiquement aux clusters, aux volumes et aux machines virtuelles de stockage (SVM). Vous pouvez également afficher des détails tels que la description, la personne créée, la date de création, les valeurs, les règles et les objets associés à l'annotation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Annotations**, cliquez sur le nom de l'annotation pour afficher les détails associés.

Supprimer les valeurs des annotations

Vous pouvez supprimer les valeurs associées aux annotations personnalisées lorsque cette valeur ne s'applique plus à l'annotation.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- La valeur d'annotation ne doit pas être associée à des règles d'annotation ou à des règles de groupe.

Vous ne pouvez pas supprimer les valeurs des annotations prédéfinies.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans la liste des annotations de l'onglet **Annotations**, sélectionnez l'annotation dont vous souhaitez supprimer une valeur.
3. Dans la zone **Valeurs** de l'onglet **Annotations**, sélectionnez la valeur que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
4. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

La valeur est supprimée et n'est plus affichée dans la liste des valeurs de l'annotation sélectionnée.

Créer des règles d'annotation

Vous pouvez créer des règles d'annotation qu'Unified Manager utilise pour annoter dynamiquement des objets de stockage tels que des volumes, des clusters ou des machines virtuelles de stockage (SVM).

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Les objets de stockage actuellement surveillés sont annotés dès que la règle d'annotation est créée. Les nouveaux objets ne sont annotés qu'une fois le cycle de surveillance terminé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Règles d'annotation**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle d'annotation**, spécifiez un nom pour la règle d'annotation.

4. Dans le champ **Type d'objet cible**, sélectionnez le type d'objet de stockage que vous souhaitez annoter.
5. Dans les champs **Appliquer l'annotation**, sélectionnez l'annotation et la valeur d'annotation que vous souhaitez utiliser.
6. Dans la section Conditions, effectuez l'action appropriée pour créer une condition, un groupe de conditions ou les deux :

Pour créer...	Fais ceci...
Une condition	a. Sélectionnez un opérande dans la liste des opérandes. b. Sélectionnez Contient ou Est comme opérateur. c. Saisissez une valeur ou sélectionnez une valeur dans la liste disponible.
Un groupe de conditions	a. Cliquez sur Ajouter un groupe de conditions. b. Sélectionnez un opérande dans la liste des opérandes. c. Sélectionnez Contient ou Est comme opérateur. d. Saisissez une valeur ou sélectionnez une valeur dans la liste disponible. e. Cliquez sur Ajouter une condition pour créer d'autres conditions si nécessaire et répétez les étapes a à d pour chaque condition.

7. Cliquez sur **Ajouter**.

Exemple de création d'une règle d'annotation

Effectuez les étapes suivantes dans la boîte de dialogue Ajouter une règle d'annotation pour créer une règle d'annotation, y compris la configuration d'une condition et l'ajout d'un groupe de conditions :

Étapes

1. Spécifiez un nom pour la règle d'annotation.
2. Sélectionnez le type d'objet cible comme machine virtuelle de stockage (SVM).
3. Sélectionnez une annotation dans la liste des annotations et spécifiez une valeur.
4. Dans la section Conditions, sélectionnez **Nom de l'objet** comme opérande.
5. Sélectionnez **Contient** comme opérateur.
6. Entrez la valeur comme `svm_data`.
7. Cliquez sur **Ajouter un groupe de conditions**.
8. Sélectionnez **Nom de l'objet** comme opérande.
9. Sélectionnez **Contient** comme opérateur.
10. Entrez la valeur comme `vol`.

11. Cliquez sur **Ajouter une condition**.
12. Répétez les étapes 8 à 10 en sélectionnant **data-priority** comme opérande à l'étape 8, **Is** comme opérateur à l'étape 9 et **mission-critical** comme valeur à l'étape 10.
13. Cliquez sur **Ajouter**.

Ajouter manuellement des annotations à des objets de stockage individuels

Vous pouvez annoter manuellement les volumes, clusters et SVM sélectionnés sans utiliser de règles d'annotation. Vous pouvez annoter un seul objet de stockage ou plusieurs objets de stockage et spécifier la combinaison de paires nom-valeur requise pour l'annotation.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Accédez aux objets de stockage que vous souhaitez annoter :

Pour ajouter une annotation à...	Fais ceci...
Groupes	a. Cliquez sur Stockage > Clusters. b. Sélectionnez un ou plusieurs clusters.
Volumes	a. Cliquez sur Stockage > Volumes. b. Sélectionnez un ou plusieurs volumes.
SVM	a. Cliquez sur Stockage > SVM. b. Sélectionnez un ou plusieurs SVM.

2. Cliquez sur **Annoter** et sélectionnez une paire nom-valeur.
3. Cliquez sur **Appliquer**.

Modifier les règles d'annotation

Vous pouvez modifier les règles d'annotation pour modifier les groupes de conditions et les conditions au sein du groupe de conditions afin d'ajouter ou de supprimer des annotations des objets de stockage.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Les annotations sont dissociées des objets de stockage lorsque vous modifiez les règles d'annotation associées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Règles d'annotation**, sélectionnez la règle d'annotation que vous souhaitez modifier, puis

cliquez sur **Actions > Modifier**.

3. Dans la boîte de dialogue **Modifier la règle d'annotation**, modifiez le nom de la règle, le nom et la valeur de l'annotation, les groupes de conditions et les conditions selon vos besoins.

Vous ne pouvez pas modifier le type d'objet cible pour une règle d'annotation.

4. Cliquez sur **Enregistrer**.

Configurer les conditions des règles d'annotation

Vous pouvez configurer une ou plusieurs conditions pour créer des règles d'annotation qu'Unified Manager applique aux objets de stockage. Les objets de stockage qui satisfont la règle d'annotation sont annotés avec la valeur spécifiée dans la règle.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Règles d'annotation**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle d'annotation**, saisissez un nom pour la règle.
4. Sélectionnez un type d'objet dans la liste Type d'objet cible, puis sélectionnez un nom et une valeur d'annotation dans la liste.
5. Dans la section **Conditions** de la boîte de dialogue, sélectionnez un opérande et un opérateur dans la liste et entrez une valeur de condition, ou cliquez sur **Ajouter une condition** pour créer une nouvelle condition.
6. Cliquez sur **Enregistrer et ajouter**.

Exemple de configuration d'une condition pour une règle d'annotation

Considérez une condition pour le type d'objet SVM, où le nom de l'objet contient « svm_data ».

Effectuez les étapes suivantes dans la boîte de dialogue Ajouter une règle d'annotation pour configurer la condition :

Étapes

1. Saisissez un nom pour la règle d'annotation.
2. Sélectionnez le type d'objet cible comme SVM.
3. Sélectionnez une annotation dans la liste des annotations et une valeur.
4. Dans le champ **Conditions**, sélectionnez **Nom de l'objet** comme opérande.
5. Sélectionnez **Contient** comme opérateur.
6. Entrez la valeur comme svm_data .
7. Cliquez sur **Ajouter**.

Supprimer les règles d'annotation

Vous pouvez supprimer les règles d'annotation d'Active IQ Unified Manager lorsque les règles ne sont plus nécessaires.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous supprimez une règle d'annotation, l'annotation est dissociée et supprimée des objets de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Règles d'annotation**, sélectionnez la règle d'annotation que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui** pour confirmer la suppression.

Réorganiser les règles d'annotation

Vous pouvez modifier l'ordre dans lequel Unified Manager applique les règles d'annotation aux objets de stockage. Les règles d'annotation sont appliquées aux objets de stockage de manière séquentielle en fonction de leur rang. Lorsque vous configurez une règle d'annotation, le rang est le plus bas. Mais vous pouvez modifier le rang de la règle d'annotation en fonction de vos besoins.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez sélectionner une seule ligne ou plusieurs lignes et effectuer de nombreuses opérations de glisser-déposer pour modifier le rang des règles d'annotation. Cependant, vous devez enregistrer les modifications pour que la repriorisation soit affichée dans l'onglet Règles d'annotation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Annotations**.
2. Dans l'onglet **Règles d'annotation**, cliquez sur **Réorganiser**.
3. Dans la boîte de dialogue **Réorganiser la règle d'annotation**, faites glisser et déposez une ou plusieurs lignes pour réorganiser la séquence des règles d'annotation.
4. Cliquez sur **Enregistrer**.

Vous devez enregistrer les modifications pour que la réorganisation soit affichée.

Envoyer un package d'assistance via l'interface Web et la console de maintenance

Vous devez envoyer un dossier d'assistance lorsque le problème que vous rencontrez nécessite un diagnostic et un dépannage plus détaillés que ceux fournis par un message AutoSupport . Vous pouvez envoyer un package d'assistance au support technique à l'aide de l'interface Web et de la console de maintenance d'Unified Manager.

Unified Manager stocke un maximum de deux bundles de support complet et trois bundles de support léger à la fois.

Informations connexes

["Rôles et capacités des utilisateurs d'Unified Manager"](#)

Envoyer des messages AutoSupport et des packages d'assistance au support technique

La page AutoSupport vous permet d'envoyer des messages AutoSupport prédéfinis et à la demande à votre équipe de support technique pour assurer le bon fonctionnement de votre environnement et vous aider à maintenir l'intégrité de votre environnement.

AutoSupport est activé par défaut et ne doit pas être désactivé pour que vous puissiez bénéficier des avantages de NetAppActive IQ.

Vous pouvez envoyer des informations de diagnostic du système et des données détaillées sur le serveur Unified Manager dans un message selon vos besoins, planifier l'envoi périodique d'un message ou même générer et envoyer des lots d'assistance à l'équipe d'assistance technique.



Un utilisateur disposant d'un rôle d'administrateur de stockage peut générer et envoyer des messages AutoSupport à la demande et des groupes d'assistance au support technique. Cependant, seul un administrateur ou un utilisateur de maintenance peut activer ou désactiver AutoSupport périodique et configurer les paramètres HTTP comme décrit dans la section Configuration du serveur proxy HTTP. Dans un environnement qui doit utiliser un serveur proxy HTTP, la configuration doit être terminée avant qu'un administrateur de stockage puisse envoyer des messages AutoSupport à la demande et des bundles d'assistance au support technique.

Envoyer des messages AutoSupport à la demande

Vous pouvez générer et envoyer un message à la demande au support technique, à un destinataire de courrier électronique spécifié ou aux deux.

Étapes

1. Accédez à **Général** > * AutoSupport* et effectuez l'une ou les deux actions suivantes :
2. Si vous souhaitez envoyer le message AutoSupport au support technique, cochez la case **Envoyer au support technique**.
3. Si vous souhaitez envoyer le message AutoSupport à un destinataire de courrier électronique spécifique, cochez la case **Envoyer au destinataire de courrier électronique** et saisissez l'adresse électronique du destinataire.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **Générer et envoyer AutoSupport**.

Activer AutoSupport périodique

Vous pouvez envoyer périodiquement des messages spécifiques et prédéfinis au support technique pour diagnostiquer et résoudre les problèmes. Cette fonctionnalité est activée par défaut. Si cette option est désactivée, un administrateur ou un utilisateur de maintenance peut activer les paramètres.

Étapes

1. Accédez à **Général** > * AutoSupport*.
2. Dans la section AutoSupport périodique, cochez la case **Activer l'envoi périodique des données AutoSupport à Active IQ**.
3. Si nécessaire, définissez le nom, le port et les informations d'authentification du serveur proxy HTTP comme décrit dans la section Configuration du serveur proxy HTTP.
4. Cliquez sur **Enregistrer**.

Télécharger le pack d'assistance à la demande

Vous pouvez générer et envoyer un package d'assistance au support technique en fonction des besoins de dépannage. Unified Manager stocke uniquement les deux bundles de support les plus récemment générés. Les anciens packs de support sont supprimés du système.

Étant donné que certains types de données de support peuvent utiliser une grande quantité de ressources de cluster ou prendre beaucoup de temps à s'exécuter, lorsque vous sélectionnez le bundle de support complet, vous pouvez inclure ou exclure des types de données spécifiques pour réduire la taille du bundle de support. Vous avez également la possibilité de créer un pack de support léger contenant seulement 30 jours de journaux et d'enregistrements de base de données de configuration. Il exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

Étapes

1. Accédez à **Général** > * AutoSupport*.
2. Dans la section Pack d'assistance à la demande, cliquez sur **Générer et envoyer un pack d'assistance**.
3. Pour envoyer un pack d'assistance léger au support technique, dans la fenêtre contextuelle Générer et envoyer un pack d'assistance, cochez la case **Générer un pack d'assistance léger**.
4. Alternativement, pour envoyer un pack d'assistance complet, cochez la case **Générer un pack d'assistance complet**. Sélectionnez les types de données spécifiques à inclure ou à exclure dans le pack de support.



Même si vous ne sélectionnez aucun type de données, le bundle de support est toujours généré avec d'autres données Unified Manager.

5. Cochez la case **Envoyer le bundle au support technique** pour générer et envoyer le bundle au support technique. Si vous ne cochez pas cette case, le bundle est généré et stocké localement sur le serveur Unified Manager. Le bundle de support généré est disponible pour une utilisation ultérieure dans le répertoire /support sur les systèmes VMware, dans /opt/netapp/data/support/ sur les systèmes Linux et dans ProgramData\NetApp\OnCommandAppData\ocum\support sur les systèmes Windows.
6. Cliquez sur **Envoyer**.

Configurer un serveur proxy HTTP

Vous pouvez désigner un proxy pour fournir l'accès Internet afin d'envoyer du contenu AutoSupport au support si votre environnement ne fournit pas d'accès direct depuis le serveur Unified Manager. Cette section est disponible uniquement pour les administrateurs et les utilisateurs de maintenance.

• Utiliser un proxy HTTP

Cochez cette case pour identifier le serveur utilisé comme proxy HTTP.

Saisissez le nom d'hôte ou l'adresse IP du serveur proxy, ainsi que le numéro de port utilisé pour se connecter au serveur.

• Utiliser l'authentification

Cochez cette case si vous devez fournir des informations d'authentification pour accéder au serveur utilisé comme proxy HTTP.

Saisissez le nom d'utilisateur et le mot de passe requis pour vous authentifier auprès du proxy HTTP.



Les proxys HTTP qui fournissent uniquement une authentification de base ne sont pas pris en charge.

Accéder à la console de maintenance

Si l'interface utilisateur d'Unified Manager n'est pas opérationnelle ou si vous devez exécuter des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour gérer votre système Unified Manager.

Avant de commencer

Vous devez avoir installé et configuré Unified Manager.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.



Lors de l'installation sur VMware, si vous êtes déjà connecté en tant qu'utilisateur de maintenance via la console VMware, vous ne pouvez pas vous connecter simultanément à l'aide de Secure Shell.

Étape

1. Suivez ces étapes pour accéder à la console de maintenance :

Sur ce système d'exploitation...	Suivez ces étapes...
VMware	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. b. Connectez-vous à la console de maintenance en utilisant votre nom d'utilisateur et votre mot de passe de maintenance.
Linux	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager. b. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de maintenance (umadmin). c. Entrez la commande <code>maintenance_console</code> et appuyez sur Entrée.
Windows	a. Connectez-vous au système Unified Manager avec les informations d'identification d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Entrez la commande <code>maintenance_console</code> et appuyez sur Entrée.

Le menu de la console de maintenance d'Unified Manager s'affiche.

Générer et télécharger un pack de support

Vous pouvez générer un ensemble de support contenant des informations de diagnostic afin de pouvoir l'envoyer au support technique pour obtenir de l'aide en cas de problème.

À partir d'Unified Manager 9.8, si votre serveur Unified Manager est connecté à Internet, vous pouvez également télécharger le pack de support sur NetApp à partir de la console de maintenance.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu'utilisateur de maintenance.

Étant donné que certains types de données de support peuvent utiliser une grande quantité de ressources de cluster ou prendre beaucoup de temps à s'exécuter, lorsque vous sélectionnez le bundle de support complet, vous pouvez spécifier les types de données à inclure ou à exclure pour réduire la taille du bundle de support. Vous avez également la possibilité de créer un pack de support léger contenant seulement 30 jours de journaux et d'enregistrements de base de données de configuration. Il exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

Unified Manager stocke uniquement les deux bundles de support les plus récemment générés. Les anciens packs de support sont supprimés du système.

Étapes

1. Dans la console de maintenance **Menu principal**, sélectionnez **Support/Diagnostics**.
2. Sélectionnez **Générer un pack d'assistance léger** ou **Générer un pack d'assistance** en fonction du niveau de détails que vous souhaitez avoir dans le pack d'assistance.
3. Si vous choisissez le pack de support complet, sélectionnez ou désélectionnez les types de données suivants à inclure ou à exclure dans le pack de support :

- **vidage de la base de données**

Un vidage de la base de données du serveur MySQL.

- **décharge de tas**

Un instantané de l'état des principaux processus du serveur Unified Manager. Cette option est désactivée par défaut et ne doit être sélectionnée que lorsque le support client le demande.

- **enregistrements d'acquisition**

Un enregistrement de toutes les communications entre Unified Manager et les clusters surveillés.



Si vous désélectionnez tous les types de données, le bundle de support est toujours généré avec d'autres données Unified Manager.

4. Taper **g** , puis appuyez sur Entrée pour générer le pack de support.

Étant donné que la génération d'un bundle de support est une opération gourmande en mémoire, vous êtes invité à vérifier que vous souhaitez vraiment générer le bundle de support à ce stade.

5. Taper **y** , puis appuyez sur Entrée pour générer le pack de support.

Si vous ne souhaitez pas générer le pack de support à ce stade, saisissez **n** , puis appuyez sur Entrée.

6. Si vous avez inclus des fichiers de vidage de base de données dans le pack de support complet, vous êtes invité à spécifier la période pour laquelle vous souhaitez que les statistiques de performances soient incluses. L'inclusion de statistiques de performances peut prendre beaucoup de temps et d'espace, vous pouvez donc également vider la base de données sans inclure les statistiques de performances :

a. Saisissez la date de début au format AAAAMMJJ.

Par exemple, entrez 20210101 pour le 1er janvier 2021. Entrer `n` si vous ne souhaitez pas que les statistiques de performances soient incluses.

b. Saisissez le nombre de jours de statistiques à inclure, à partir de minuit à la date de début spécifiée.

Vous pouvez saisir un nombre compris entre 1 et 10.

Si vous incluez des statistiques de performances, le système affiche la période pendant laquelle les statistiques de performances seront collectées.

7. Une fois le pack de support créé, vous êtes invité à indiquer si vous souhaitez le télécharger sur NetApp. Taper `y` , puis appuyez sur Entrée.

Vous êtes invité à saisir votre numéro de dossier d'assistance.

8. Si vous avez déjà un numéro de dossier, saisissez-le et appuyez sur Entrée. Sinon, appuyez simplement sur Entrée.

Le pack de support est téléchargé sur NetApp.

Si votre serveur Unified Manager n'est pas connecté à Internet ou si vous ne parvenez pas à télécharger le pack d'assistance pour une autre raison, vous pouvez le récupérer et l'envoyer manuellement. Vous pouvez le récupérer à l'aide d'un client SFTP ou en utilisant les commandes CLI UNIX ou Linux. Sur les installations Windows, vous pouvez utiliser le Bureau à distance (RDP) pour récupérer le pack de support.

Le bundle de support généré réside dans le répertoire `/support` sur les systèmes VMware, dans `/opt/netapp/data/support/` sur les systèmes Linux et dans `ProgramData\NetApp\OnCommandAppData\ocum\support` sur les systèmes Windows.

Informations connexes

["Rôles et capacités des utilisateurs d'Unified Manager"](#)

Récupérer le pack de support à l'aide d'un client Windows

Si vous êtes un utilisateur Windows, vous pouvez télécharger et installer un outil pour récupérer le pack de support à partir de votre serveur Unified Manager. Vous pouvez envoyer le dossier d'assistance au support technique pour un diagnostic plus détaillé d'un problème. Filezilla ou WinSCP sont des exemples d'outils que vous pouvez utiliser.

Avant de commencer

Vous devez être l'utilisateur de maintenance pour effectuer cette tâche.

Vous devez utiliser un outil prenant en charge SCP ou SFTP.

Étapes

1. Téléchargez et installez un outil pour récupérer le pack de support.
2. Ouvrez l'outil.
3. Connectez-vous à votre serveur de gestion Unified Manager via SFTP.

L'outil affiche le contenu du répertoire /support et vous pouvez visualiser tous les bundles de support existants.

4. Sélectionnez le répertoire de destination du bundle de support que vous souhaitez copier.
5. Sélectionnez le pack de support que vous souhaitez copier et utilisez l'outil pour copier le fichier du serveur Unified Manager vers votre système local.

Récupérer le pack de support à l'aide d'un client UNIX ou Linux

Si vous êtes un utilisateur UNIX ou Linux, vous pouvez récupérer le pack de support de votre vApp à l'aide de l'interface de ligne de commande (CLI) sur votre serveur client Linux. Vous pouvez utiliser SCP ou SFTP pour récupérer le bundle de support.

Avant de commencer

Vous devez être l'utilisateur de maintenance pour effectuer cette tâche.

Vous devez avoir généré un bundle de support à l'aide de la console de maintenance et disposer du nom du bundle de support.

Étapes

1. Accédez à la CLI via Telnet ou la console, en utilisant votre serveur client Linux.
2. Accéder au/support annuaire.
3. Récupérez le bundle de support et copiez-le dans le répertoire local à l'aide de la commande suivante :

Si vous utilisez...	Ensuite, utilisez la commande suivante...
SCP	<code>scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>
SFTP	<code>sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory></code>

Le nom du bundle de support vous est fourni lorsque vous le générez à l'aide de la console de maintenance.

4. Entrez le mot de passe de l'utilisateur de maintenance.

Exemples

L'exemple suivant utilise SCP pour récupérer le bundle de support :

```
`$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: ``
support_bundle_20160216_145359.7z 100% 119MB 11.9MB/s 00:10
```

L'exemple suivant utilise SFTP pour récupérer le bundle de support :

```
`$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: ``
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

Envoyer un dossier d'assistance au support technique

Lorsqu'un problème nécessite des informations de diagnostic et de dépannage plus détaillées que celles fournies par un message AutoSupport , vous pouvez envoyer un dossier d'assistance au support technique.

Avant de commencer

Vous devez avoir accès au pack d'assistance pour l'envoyer au support technique.

Vous devez disposer d'un numéro de dossier généré via le site Web de support technique.

Étapes

1. Connectez-vous au site de support NetApp .
2. Téléchargez le fichier.

["Comment télécharger un fichier sur NetApp"](#)

Tâches et informations liées à plusieurs flux de travail

Certaines tâches et certains textes de référence qui peuvent vous aider à comprendre et à terminer un workflow sont communs à de nombreux workflows dans Unified Manager, notamment l'ajout et la révision de notes sur un événement, l'attribution d'un événement, la reconnaissance et la résolution d'événements, ainsi que les détails sur les volumes, les machines virtuelles de stockage (SVM), les agrégats, etc.

Composants de cluster et pourquoi ils peuvent être en conflit

Vous pouvez identifier les problèmes de performances du cluster lorsqu'un composant du cluster entre en conflit. Les performances des charges de travail qui utilisent le composant ralentissent et leur temps de réponse (latence) aux demandes des clients

augmente, ce qui déclenche un événement dans Unified Manager.

Un composant en conflit ne peut pas fonctionner à un niveau optimal. Ses performances ont diminué et les performances des autres composants et charges de travail du cluster, appelés *victimes*, pourraient avoir une latence accrue. Pour sortir un composant de la compétition, vous devez réduire sa charge de travail ou augmenter sa capacité à gérer davantage de travail, afin que les performances puissent revenir à des niveaux normaux. Étant donné qu'Unified Manager collecte et analyse les performances de la charge de travail à des intervalles de cinq minutes, il détecte uniquement lorsqu'un composant de cluster est systématiquement surutilisé. Les pics transitoires de surconsommation qui ne durent que peu de temps dans l'intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être en conflit car une ou plusieurs charges de travail sur celui-ci sont en concurrence pour que leurs demandes d'E/S soient satisfaites. D'autres charges de travail sur l'agrégat peuvent être affectées, ce qui entraîne une diminution de leurs performances. Pour réduire la quantité d'activité sur l'agrégat, vous pouvez prendre différentes mesures, telles que déplacer une ou plusieurs charges de travail vers un agrégat ou un nœud moins occupé, afin de réduire la demande de charge de travail globale sur l'agrégat actuel. Pour un groupe de politiques QoS, vous pouvez ajuster la limite de débit ou déplacer les charges de travail vers un autre groupe de politiques, afin que les charges de travail ne soient plus limitées.

Unified Manager surveille les composants de cluster suivants pour vous alerter lorsqu'ils sont en conflit :

- **Réseau**

Représente le temps d'attente des demandes d'E/S par les protocoles réseau externes sur le cluster. Le temps d'attente est le temps passé à attendre que les transactions « transfert prêt » se terminent avant que le cluster puisse répondre à une demande d'E/S. Si le composant réseau est en conflit, cela signifie qu'un temps d'attente élevé au niveau de la couche de protocole a un impact sur la latence d'une ou plusieurs charges de travail.

- **Traitement réseau**

Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre la couche de protocole et le cluster. Le traitement du réseau de gestion des nœuds a peut-être changé depuis la détection de l'événement. Si le composant de traitement réseau est en conflit, cela signifie qu'une utilisation élevée au niveau du nœud de traitement réseau a un impact sur la latence d'une ou plusieurs charges de travail.

Lorsque vous utilisez un cluster All SAN Array dans une configuration active-active, la valeur de latence de traitement réseau s'affiche pour les deux nœuds afin que vous puissiez vérifier que les nœuds partagent la charge de manière égale.

- **Limite QoS Max**

Représente le paramètre de débit maximal (pic) du groupe de politiques de qualité de service (QoS) de stockage attribué à la charge de travail. Si le composant du groupe de stratégies est en conflit, cela signifie que toutes les charges de travail du groupe de stratégies sont limitées par la limite de débit définie, ce qui a un impact sur la latence d'une ou plusieurs de ces charges de travail.

- **Limite QoS minimale**

Représente la latence d'une charge de travail provoquée par le paramètre de débit QoS minimum (attendu) attribué à d'autres charges de travail. Si le minimum de QoS défini sur certaines charges de travail utilise la majorité de la bande passante pour garantir le débit promis, d'autres charges de travail seront limitées et verront plus de latence.

- **Interconnexion de cluster**

Représente les câbles et les adaptateurs avec lesquels les nœuds en cluster sont physiquement connectés. Si le composant d'interconnexion du cluster est en conflit, cela signifie que le temps d'attente élevé pour les demandes d'E/S au niveau de l'interconnexion du cluster a un impact sur la latence d'une ou plusieurs charges de travail.

- *** Data Processing***

Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient la charge de travail. Le nœud gérant le traitement des données peut avoir changé depuis la détection de l'événement. Si le composant de traitement des données est en conflit, cela signifie qu'une utilisation élevée au niveau du nœud de traitement des données a un impact sur la latence d'une ou plusieurs charges de travail.

- **Activation du volume**

Représente le processus qui suit l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1 000 volumes sont actifs, ce processus suit le nombre de volumes critiques qui doivent accéder aux ressources via le nœud en même temps. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques subiront une latence comme indiqué ici.

- *** Ressources MetroCluster ***

Représente les ressources MetroCluster, y compris la NVRAM et les liaisons inter-commutateurs (ISL), utilisées pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster est en conflit, cela signifie que le débit d'écriture est élevé à partir des charges de travail sur le cluster local ou qu'un problème d'intégrité de la liaison affecte la latence d'une ou plusieurs charges de travail sur le cluster local. Si le cluster n'est pas dans une configuration MetroCluster, cette icône ne s'affiche pas.

- **Opérations d'agrégation ou d'agrégation SSD**

Représente l'agrégat de stockage sur lequel les charges de travail s'exécutent. Si le composant agrégé est en conflit, cela signifie qu'une utilisation élevée de l'agrégat a un impact sur la latence d'une ou plusieurs charges de travail. Un agrégat se compose de tous les disques durs, ou d'un mélange de disques durs et de SSD (un agrégat Flash Pool), ou d'un mélange de disques durs et d'un niveau cloud (un agrégat FabricPool). Un « agrégat SSD » se compose de tous les SSD (un agrégat entièrement flash) ou d'un mélange de SSD et d'un niveau cloud (un agrégat FabricPool).

- **Latence du cloud**

Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et le niveau cloud sur lequel les données utilisateur sont stockées. Si le composant de latence du cloud est en conflit, cela signifie qu'une grande quantité de lectures provenant de volumes hébergés sur le niveau cloud a un impact sur la latence d'une ou plusieurs charges de travail.

- **Synchroniser SnapMirror**

Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur du volume principal vers le volume secondaire dans une relation synchrone SnapMirror. Si le composant de synchronisation SnapMirror est en conflit, cela signifie que l'activité des opérations synchrones SnapMirror a un impact sur la latence d'une ou plusieurs charges de travail.

Page de détails sur le volume/la santé

Vous pouvez utiliser la page Détails Volume/Santé pour afficher des informations détaillées sur un volume sélectionné, telles que la capacité, l'efficacité du stockage, la configuration, la protection, l'annotation et les événements générés. Vous pouvez également afficher des informations sur les objets associés et les alertes associées à ce volume.

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour le volume sélectionné :

- **Passer à la vue Performances**

Vous permet d'accéder à la page des détails Volume / Performance.

- **Actes**

- Ajouter une alerte

Vous permet d'ajouter une alerte au volume sélectionné.

- Modifier les seuils

Vous permet de modifier les paramètres de seuil pour le volume sélectionné.

- Annoter

Vous permet d'annoter le volume sélectionné.

- Protéger

Vous permet de créer des relations SnapMirror ou SnapVault pour le volume sélectionné.

- Relation

Vous permet d'exécuter les opérations de relation de protection suivantes :

- Modifier

Lance la boîte de dialogue Modifier la relation qui vous permet de modifier les stratégies, les planifications et les taux de transfert maximum SnapMirror existants pour une relation de protection existante.

- Avorter

Annule les transferts en cours pour une relation sélectionnée. En option, il vous permet de supprimer le point de contrôle de redémarrage pour les transferts autres que le transfert de base. Vous ne pouvez pas supprimer le point de contrôle pour un transfert de base.

- Mettre au repos

Désactive temporairement les mises à jour programmées pour une relation sélectionnée. Les

transferts déjà en cours doivent être terminés avant que la relation ne soit interrompue.

- **Casser**

Rompt la relation entre les volumes source et de destination et modifie la destination en un volume en lecture-écriture.

- **Retirer**

Supprime définitivement la relation entre la source et la destination sélectionnées. Les volumes ne sont pas détruits et les copies Snapshot sur les volumes ne sont pas supprimées. Cette opération ne peut pas être annulée.

- **CV**

Active les transferts planifiés pour une relation suspendue. Lors du prochain intervalle de transfert planifié, un point de contrôle de redémarrage est utilisé, s'il existe.

- **Resynchroniser**

Vous permet de resynchroniser une relation précédemment rompue.

- **Initialiser/Mettre à jour**

Vous permet d'effectuer un premier transfert de référence sur une nouvelle relation de protection ou d'effectuer une mise à jour manuelle si la relation est déjà initialisée.

- **Resynchronisation inversée**

Vous permet de rétablir une relation de protection précédemment rompue, en inversant la fonction de la source et de la destination en faisant de la source une copie de la destination d'origine. Le contenu de la source est écrasé par le contenu de la destination et toutes les données plus récentes que les données de la copie Snapshot commune sont supprimées.

- **Restaurer**

Vous permet de restaurer des données d'un volume vers un autre volume. Pour plus d'informations, voir "[Restauration des données à l'aide de la page Détails du volume/de l'état de santé](#)".



Les boutons Restaurer et Relation ne sont pas disponibles pour les volumes qui sont dans des relations de protection synchrones.

- **Voir les volumes**

Vous permet d'accéder à la vue Santé : Tous les volumes.

Onglet Capacité

L'onglet Capacité affiche des détails sur le volume sélectionné, tels que sa capacité physique, sa capacité logique, ses paramètres de seuil, sa capacité de quota et des informations sur toute opération de déplacement de volume :

- **Capacité physique**

Détaille la capacité physique du volume :

- Dépassement de capacité d'instantané

Affiche l'espace de données consommé par les copies Snapshot.

- Utilisé

Affiche l'espace utilisé par les données dans le volume.

- Avertissement

Indique que l'espace dans le volume est presque plein. Si ce seuil est dépassé, l'événement Espace presque plein est généré.

- Erreur

Indique que l'espace dans le volume est plein. Si ce seuil est dépassé, l'événement Espace plein est généré.

- Inutilisable

Indique que l'événement d'espace de volume à provisionnement fin est généré et que l'espace dans le volume à provisionnement fin est à risque en raison de problèmes de capacité globale. La capacité inutilisable s'affiche uniquement pour les volumes à provisionnement fin.

- Graphique de données

Affiche la capacité totale de données et la capacité de données utilisée du volume.

Si la croissance automatique est activée, le graphique de données affiche également l'espace disponible dans l'agrégat. Le graphique de données affiche l'espace de stockage effectif qui peut être utilisé par les données du volume, qui peut être l'un des suivants :

- Capacité réelle des données du volume pour les conditions suivantes :
 - La croissance automatique est désactivée.
 - Le volume activé pour la croissance automatique a atteint la taille maximale.
 - Un volume provisionné de manière dense et compatible avec la croissance automatique ne peut pas croître davantage.
- Capacité de données du volume après prise en compte de la taille maximale du volume (pour les volumes à provisionnement fin et pour les volumes à provisionnement épais lorsque l'agrégat dispose d'espace pour que le volume atteigne sa taille maximale)
- Capacité de données du volume après avoir pris en compte la prochaine taille de croissance automatique possible (pour les volumes fortement provisionnés qui ont un seuil de pourcentage de croissance automatique)

- Graphique des copies instantanées

Ce graphique s'affiche uniquement lorsque la capacité Snapshot utilisée ou la réserve Snapshot n'est pas nulle.

Les deux graphiques affichent la capacité par laquelle la capacité de Snapshot dépasse la réserve de Snapshot si la capacité de Snapshot utilisée dépasse la réserve de Snapshot.

- **Capacité logique**

Affiche les caractéristiques de l'espace logique du volume. L'espace logique indique la taille réelle des données stockées sur le disque sans appliquer les économies réalisées grâce aux technologies d'efficacité de stockage ONTAP .

- **Rapports d'espace logique**

Affiche si le volume dispose d'un rapport d'espace logique configuré. La valeur peut être activée, désactivée ou non applicable. « Non applicable » s'affiche pour les volumes sur des versions plus anciennes d' ONTAP ou sur des volumes qui ne prennent pas en charge les rapports d'espace logique.

- **Utilisé**

Affiche la quantité d'espace logique utilisée par les données du volume et le pourcentage d'espace logique utilisé en fonction de la capacité totale des données.

- **Application de l'espace logique**

Affiche si l'application de l'espace logique est configurée pour les volumes à provisionnement fin. Lorsque cette option est définie sur Activé, la taille logique utilisée du volume ne peut pas être supérieure à la taille du volume physique actuellement définie.

- **Croissance automatique**

Affiche si le volume augmente automatiquement lorsqu'il n'y a plus d'espace.

- **Garantie d'espace**

Affiche le contrôle de réglage du FlexVol volume lorsqu'un volume supprime des blocs libres d'un agrégat. Ces blocs sont alors garantis comme étant disponibles pour les écritures dans les fichiers du volume. La garantie d'espace peut être définie sur l'une des valeurs suivantes :

- **Aucune**

Aucune garantie d'espace n'est configurée pour le volume.

- **Déposer**

La taille complète des fichiers peu écrits (par exemple, les LUN) est garantie.

- **Volume**

La taille complète du volume est garantie.

- **Partiel**

Le volume FlexCache réserve de l'espace en fonction de sa taille. Si la taille du volume FlexCache est de 100 Mo ou plus, l'espace minimum garanti est défini sur 100 Mo par défaut. Si la taille du volume FlexCache est inférieure à 100 Mo, l'espace minimum garanti est défini sur la taille du volume FlexCache . Si la taille du volume FlexCache augmente ultérieurement, la garantie d'espace minimum n'est pas incrémentée.



La garantie d'espace est partielle lorsque le volume est de type Data-Cache.

- **Détails (physiques)**

Affiche les caractéristiques physiques du volume.

- **Capacité totale**

Affiche la capacité physique totale du volume.

- **Capacité de données**

Affiche la quantité d'espace physique utilisée par le volume (capacité utilisée) et la quantité d'espace physique encore disponible (capacité libre) dans le volume. Ces valeurs sont également affichées sous forme de pourcentage de la capacité physique totale.

Lorsque l'événement d'espace de volume à provisionnement fin à risque est généré pour les volumes à provisionnement fin, la quantité d'espace utilisée par le volume (capacité utilisée) et la quantité d'espace disponible dans le volume mais qui ne peut pas être utilisée (capacité inutilisable) en raison de problèmes de capacité globale s'affichent.

- **Réserve instantanée**

Affiche la quantité d'espace utilisée par les copies Snapshot (capacité utilisée) et la quantité d'espace disponible pour les copies Snapshot (capacité libre) dans le volume. Ces valeurs sont également affichées sous forme de pourcentage de la réserve totale de snapshots.

Lorsque l'événement Espace de volume à provisionnement dynamique à risque est généré pour les volumes à provisionnement dynamique, la quantité d'espace utilisée par les copies Snapshot (capacité utilisée) et la quantité d'espace disponible dans le volume mais qui ne peut pas être utilisée pour créer des copies Snapshot (capacité inutilisable) en raison de problèmes de capacité globale s'affichent.

- **Seuils de volume**

Affiche les seuils de capacité de volume suivants :

- Seuil presque plein

Spécifie le pourcentage auquel un volume est presque plein.

- Seuil complet

Spécifie le pourcentage auquel un volume est plein.

- **Autres détails**

- Autogrow Taille maximale

Affiche la taille maximale jusqu'à laquelle le volume peut croître automatiquement. La valeur par défaut est de 120 % de la taille du volume lors de la création. Ce champ s'affiche uniquement lorsque la croissance automatique est activée pour le volume.

- Capacité engagée du quota Qtree

Affiche l'espace réservé dans les quotas.

- Capacité surengagée du quota Qtree

Affiche la quantité d'espace pouvant être utilisée avant que le système ne génère l'événement Volume Qtree Quota Overcommitted.

- Réserve fractionnaire

Contrôle la taille de la réserve d'écrasement. Par défaut, la réserve fractionnaire est définie sur 100, ce qui indique que 100 % de l'espace réservé requis est réservé afin que les objets soient entièrement protégés contre les écrasements. Si la réserve fractionnaire est inférieure à 100 %, l'espace réservé pour tous les fichiers d'espace réservé dans ce volume est réduit au pourcentage de réserve fractionnaire.

- Instantané du taux de croissance quotidien

Affiche le changement (en pourcentage, ou en Ko, Mo, Go, etc.) qui se produit toutes les 24 heures dans les copies Snapshot du volume sélectionné.

- Instantané Jours à Plein

Affiche le nombre estimé de jours restants avant que l'espace réservé aux copies Snapshot dans le volume n'atteigne le seuil spécifié.

Le champ Jours d'instantané jusqu'à achèvement affiche une valeur Non applicable lorsque le taux de croissance des copies d'instantané dans le volume est nul ou négatif, ou lorsqu'il n'y a pas suffisamment de données pour calculer le taux de croissance.

- Suppression automatique des instantanés

Spécifie si les copies instantanées sont automatiquement supprimées pour libérer de l'espace lorsqu'une écriture sur un volume échoue en raison d'un manque d'espace dans l'ensemble.

- Copies instantanées

Affiche des informations sur les copies Snapshot dans le volume.

Le nombre de copies Snapshot dans le volume est affiché sous forme de lien. Cliquer sur le lien ouvre la boîte de dialogue Copies d'instantanés sur un volume, qui affiche les détails des copies d'instantanés.

Le nombre de copies d'instantanés est mis à jour environ toutes les heures ; cependant, la liste des copies d'instantanés est mise à jour au moment où vous cliquez sur l'icône. Cela peut entraîner une différence entre le nombre de copies d'instantanés affiché dans la topologie et le nombre de copies d'instantanés répertoriées lorsque vous cliquez sur l'icône.

- **Déplacement du volume**

Affiche l'état de l'opération de déplacement de volume en cours ou de la dernière opération effectuée sur le volume, ainsi que d'autres détails, tels que la phase actuelle de l'opération de déplacement de volume en cours, l'agrégat source, l'agrégat de destination, l'heure de début, l'heure de fin et l'heure de fin estimée.

Affiche également le nombre d'opérations de déplacement de volume effectuées sur le volume sélectionné. Vous pouvez afficher plus d'informations sur les opérations de déplacement de volume en cliquant sur le lien **Historique de déplacement de volume**.

Onglet Configuration

L'onglet Configuration affiche les détails du volume sélectionné, tels que la politique d'exportation, le type de RAID, la capacité et les fonctionnalités liées à l'efficacité du stockage du volume :

• Aperçu

- Nom et prénom

Affiche le nom complet du volume.

- Agrégats

Affiche le nom de l'agrégat sur lequel réside le volume ou le nombre d'agrégats sur lesquels réside le volume FlexGroup .

- Politique de hiérarchisation

Affiche la stratégie de hiérarchisation définie pour le volume ; si le volume est déployé sur un agrégat compatible FabricPool. La politique peut être Aucune, Instantané uniquement, Sauvegarde, Automatique ou Tout.

- Machine virtuelle de stockage

Affiche le nom du SVM qui contient le volume.

- Chemin de jonction

Affiche l'état du chemin, qui peut être actif ou inactif. Le chemin dans le SVM sur lequel le volume est monté est également affiché. Vous pouvez cliquer sur le lien **Historique** pour afficher les cinq modifications les plus récentes apportées au chemin de jonction.

- Politique d'exportation

Affiche le nom de la politique d'exportation créée pour le volume. Vous pouvez cliquer sur le lien pour afficher les détails sur les politiques d'exportation, les protocoles d'authentification et l'accès activés sur les volumes appartenant au SVM.

- Style

Affiche le style du volume. Le style de volume peut être FlexVol ou FlexGroup.

- Type

Affiche le type du volume sélectionné. Le type de volume peut être Lecture-écriture, Partage de charge, Protection des données, Cache de données ou Temporaire.

- Type RAID

Affiche le type RAID du volume sélectionné. Le type RAID peut être RAID0, RAID4, RAID-DP ou RAID-TEC.



Plusieurs types de RAID peuvent s'afficher pour les volumes FlexGroup , car les volumes constitutifs des FlexGroups peuvent se trouver sur des agrégats de types différents.

- Type de SnapLock

Affiche le type SnapLock de l'agrégat qui contient le volume.

- Expiration de SnapLock

Affiche la date d'expiration du volume SnapLock .

- **Capacité**

- Provisionnement léger

Affiche si le provisionnement léger est configuré pour le volume.

- Auto-croissance

Affiche si le volume flexible augmente automatiquement au sein d'un agrégat.

- Suppression automatique des instantanés

Spécifie si les copies instantanées sont automatiquement supprimées pour libérer de l'espace lorsqu'une écriture sur un volume échoue en raison d'un manque d'espace dans l'ensemble.

- Quotas

Spécifie si les quotas sont activés pour le volume.

- **Efficacité**

- Compression

Spécifie si la compression est activée ou désactivée.

- Déduplication

Spécifie si la déduplication est activée ou désactivée.

- Mode de déduplication

Spécifie si l'opération de déduplication activée sur un volume est une opération manuelle, planifiée ou basée sur une stratégie. Si le mode est défini sur Planifié, le calendrier de fonctionnement s'affiche et si le mode est défini sur une stratégie, le nom de la stratégie s'affiche.

- Type de déduplication

Spécifie le type d'opération de déduplication exécutée sur le volume. Si le volume est dans une relation SnapVault , le type affiché est SnapVault. Pour tout autre volume, le type est affiché comme Régulier.

- Politique d'efficacité du stockage

Spécifie le nom de la stratégie d'efficacité de stockage qui a été attribuée via Unified Manager à ce volume. Cette politique peut contrôler les paramètres de compression et de déduplication.

- **Protection**

- Copies instantanées

Spécifie si les copies automatiques d'instantanés sont activées ou désactivées.

Onglet Protection

L'onglet Protection affiche les détails de protection sur le volume sélectionné, tels que les informations de décalage, le type de relation et la topologie de la relation.

• Résumé

Affiche les propriétés des relations de protection (SnapMirror, SnapVault ou Storage VM DR) pour un volume sélectionné. Pour tout autre type de relation, seule la propriété Type de relation est affichée. Si un volume principal est sélectionné, seules les stratégies de copie de snapshots gérés et locaux sont affichées. Les propriétés affichées pour les relations SnapMirror et SnapVault incluent les suivantes :

- Volume source

Affiche le nom de la source du volume sélectionné si le volume sélectionné est une destination.

- État de décalage

Affiche l'état de décalage de mise à jour ou de transfert pour une relation de protection. Le statut peut être Erreur, Avertissement ou Critique.

Le statut de décalage n'est pas applicable aux relations synchrones.

- Durée du décalage

Affiche le temps pendant lequel les données sur le miroir sont en retard par rapport à la source.

- Dernière mise à jour réussie

Affiche la date et l'heure de la dernière mise à jour de protection réussie.

La dernière mise à jour réussie n'est pas applicable aux relations synchrones.

- Membre du service de stockage

Affiche Oui ou Non pour indiquer si le volume appartient ou non à un service de stockage et est géré par celui-ci.

- Version Réplication flexible

Affiche soit Oui, Oui avec option de sauvegarde, soit Aucun. Oui indique que la réplication SnapMirror est possible même si les volumes source et de destination exécutent des versions différentes du logiciel ONTAP . Oui avec l'option de sauvegarde indique la mise en œuvre de la protection SnapMirror avec la possibilité de conserver plusieurs versions de copies de sauvegarde sur la destination. Aucun indique que la réplication flexible de version n'est pas activée.

- Capacité relationnelle

Indique les capacités ONTAP disponibles pour la relation de protection.

- Service de protection

Affiche le nom du service de protection si la relation est gérée par une application partenaire de protection.

- Type de relation

Affiche tout type de relation, y compris Miroir asynchrone, Coffre asynchrone, Miroir asynchroneVault, StrictSync et Synchronisation.

- État de la relation

Affiche l'état de la relation SnapMirror ou SnapVault . L'état peut être non initialisé, SnapMirrored ou cassé. Si un volume source est sélectionné, l'état de la relation n'est pas applicable et n'est pas affiché.

- Statut du transfert

Affiche l'état de transfert pour la relation de protection. Le statut du transfert peut être l'un des suivants :

- Avortement

Les transferts SnapMirror sont activés ; cependant, une opération d'abandon de transfert qui pourrait inclure la suppression du point de contrôle est en cours.

- Vérification

Le volume de destination subit une vérification de diagnostic et aucun transfert n'est en cours.

- Finalisation

Les transferts SnapMirror sont activés. Le volume est actuellement en phase de post-transfert pour les transferts SnapVault incrémentiels.

- Inactif

Les transferts sont activés et aucun transfert n'est en cours.

- Synchronisé

Les données des deux volumes dans la relation synchrone sont synchronisées.

- Désynchronisé

Les données du volume de destination ne sont pas synchronisées avec le volume source.

- Préparation

Les transferts SnapMirror sont activés. Le volume est actuellement en phase de pré-transfert pour les transferts SnapVault incrémentiels.

- En file d'attente

Les transferts SnapMirror sont activés. Aucun transfert n'est en cours.

- Au repos

Les transferts SnapMirror sont désactivés. Aucun transfert n'est en cours.

- Mise au repos

Un transfert SnapMirror est en cours. Les transferts supplémentaires sont désactivés.

- Transfert

Les transferts SnapMirror sont activés et un transfert est en cours.

- Transition

Le transfert asynchrone des données du volume source vers le volume de destination est terminé et la transition vers le fonctionnement synchrone a commencé.

- En attendant

Un transfert SnapMirror a été lancé, mais certaines tâches associées attendent d'être mises en file d'attente.

- Taux de transfert maximal

Affiche le taux de transfert maximal pour la relation. Le débit de transfert maximal peut être une valeur numérique en kilooctets par seconde (Kbps), en mégaoctets par seconde (Mbps), en gigaoctets par seconde (Gbps) ou en téraoctets par seconde (Tbps). Si Aucune limite n'est affichée, le transfert de base entre les relations est illimité.

- Politique SnapMirror

Affiche la politique de protection du volume. DPDefault indique la politique de protection du miroir asynchrone par défaut, XDPDefault indique la politique de coffre-fort asynchrone par défaut et DPSyncDefault indique la politique de MirrorVault asynchrone par défaut. StrictSync indique la politique de protection synchrone stricte par défaut et Sync indique la politique synchrone par défaut. Vous pouvez cliquer sur le nom de la politique pour afficher les détails associés à cette politique, y compris les informations suivantes :

- Priorité de transfert
- Ignorer le paramètre de temps d'accès
- Limite d'essais
- Commentaires
- Étiquettes SnapMirror
- Paramètres de conservation
- Copies instantanées réelles
- Conserver les copies instantanées
- Seuil d'avertissement de rétention
- Copies instantanées sans paramètres de conservation Dans une relation SnapVault en cascade où la source est un volume de protection des données (DP), seule la règle « sm_created » s'applique.

- Calendrier de mise à jour

Affiche la planification SnapMirror attribuée à la relation. En positionnant votre curseur sur l'icône d'information, vous affichez les détails du planning.

- Politique d'instantané local

Affiche la politique de copie d'instantané pour le volume. La politique est Par défaut, Aucune ou tout nom donné à une politique personnalisée.

- Protégé par

Affiche le type de protection utilisé pour le volume sélectionné. Par exemple, si un volume est protégé par les relations de volume du groupe de cohérence et de SnapMirror , ce champ affiche à la fois

SnapMirror et du groupe de cohérence. Ce champ fournit également un lien qui vous redirige vers la page Relations pour afficher l'état de la relation unifiée. Le lien s'applique uniquement aux relations constitutives.

- Groupe de cohérence

Pour les volumes protégés par les relations de synchronisation active SnapMirror, cette colonne affiche le groupe de cohérence du volume.

• Vues

Affiche la topologie de protection du volume sélectionné. La topologie comprend des représentations graphiques de tous les volumes liés au volume sélectionné. Le volume sélectionné est indiqué par une bordure gris foncé et les lignes entre les volumes dans la topologie indiquent le type de relation de protection. La direction des relations dans la topologie est affichée de gauche à droite, avec la source de chaque relation à gauche et la destination à droite.

Les lignes doubles en gras spécifient une relation de miroir asynchrone, une ligne simple en gras spécifie une relation de coffre-fort asynchrone, les lignes doubles en gras spécifient une relation de coffre-fort miroir asynchrone et une ligne en gras et une ligne non grasse spécifient une relation synchrone. Le tableau ci-dessous indique si la relation synchrone est StrictSync ou Sync.

Un clic droit sur un volume affiche un menu à partir duquel vous pouvez choisir de protéger le volume ou de restaurer les données qu'il contient. Un clic droit sur une relation affiche un menu à partir duquel vous pouvez choisir de modifier, d'abandonner, de suspendre, d'interrompre, de supprimer ou de reprendre une relation.

Les menus ne s'afficheront pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action, par exemple, si vous ne disposez que des privilèges d'opérateur
- Si le volume est dans une relation de protection synchrone
- Lorsque l'ID de volume est inconnu, par exemple lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert, cliquer sur un autre volume dans la topologie sélectionne et affiche les informations de ce volume. Un point d'interrogation (?) dans le coin supérieur gauche d'un volume indique que le volume est manquant ou qu'il n'a pas encore été découvert. Cela peut également indiquer que les informations sur la capacité sont manquantes. En positionnant votre curseur sur le point d'interrogation, vous affichez des informations supplémentaires, notamment des suggestions de mesures correctives.

La topologie affiche des informations sur la capacité du volume, le décalage, les copies instantanées et le dernier transfert de données réussi s'il est conforme à l'un des nombreux modèles de topologie courants. Si une topologie n'est pas conforme à l'un de ces modèles, les informations sur le décalage du volume et le dernier transfert de données réussi sont affichées dans une table de relations sous la topologie. Dans ce cas, la ligne en surbrillance dans le tableau indique le volume sélectionné et, dans la vue topologique, les lignes en gras avec un point bleu indiquent la relation entre le volume sélectionné et son volume source.

Les vues topologiques incluent les informations suivantes :

• Capacité

Affiche la quantité totale de capacité utilisée par le volume. Le positionnement de votre curseur sur un volume dans la topologie affiche les paramètres d'avertissement et de seuil critique actuels pour ce volume dans la boîte de dialogue Paramètres de seuil actuels. Vous pouvez également modifier les paramètres de

seuil en cliquant sur le lien **Modifier les seuils** dans la boîte de dialogue Paramètres de seuil actuels. La désactivation de la case à cocher **Capacité** masque toutes les informations de capacité pour tous les volumes de la topologie.

- **Décalage**

Affiche la durée du décalage et l'état du décalage des relations de protection entrantes. La désactivation de la case à cocher **Lag** masque toutes les informations de décalage pour tous les volumes de la topologie. Lorsque la case à cocher **Lag** est grisée, les informations de décalage pour le volume sélectionné s'affichent dans le tableau des relations sous la topologie, ainsi que les informations de décalage pour tous les volumes associés.

- **Instantané**

Affiche le nombre de copies Snapshot disponibles pour un volume. La désactivation de la case à cocher **Snapshot** masque toutes les informations de copie Snapshot pour tous les volumes de la topologie. En cliquant sur une icône de copie d'instantané () affiche la liste des copies instantanées pour un volume. Le nombre de copies d'instantanés affiché à côté de l'icône est mis à jour environ toutes les heures ; cependant, la liste des copies d'instantanés est mise à jour au moment où vous cliquez sur l'icône. Cela peut entraîner une différence entre le nombre de copies d'instantanés affiché dans la topologie et le nombre de copies d'instantanés répertoriées lorsque vous cliquez sur l'icône.

- **Dernier transfert réussi**

Affiche le montant, la durée, l'heure et la date du dernier transfert de données réussi. Lorsque la case à cocher **Dernier transfert réussi** est grisée, les dernières informations de transfert réussi pour le volume sélectionné s'affichent dans le tableau des relations sous la topologie, ainsi que les dernières informations de transfert réussi pour tous les volumes associés.

- **Histoire**

Affiche dans un graphique l'historique des relations de protection SnapMirror et SnapVault entrantes pour le volume sélectionné. Trois graphiques d'historique sont disponibles : durée du décalage de la relation entrante, durée du transfert de la relation entrante et taille du transfert de la relation entrante. Les informations d'historique s'affichent uniquement lorsque vous sélectionnez un volume de destination. Si vous sélectionnez un volume principal, les graphiques sont vides et le message Aucune donnée trouvée s'affiche. Si les volumes sont protégés par des relations synchrones de groupe de cohérence et de SnapMirror, les informations relatives à la durée et à la taille du transfert de relation ne s'affichent pas.

Vous pouvez sélectionner un type de graphique dans la liste déroulante en haut du volet Historique. Vous pouvez également afficher les détails d'une période spécifique en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques d'historique peuvent vous aider à identifier les tendances : par exemple, si de grandes quantités de données sont transférées au même moment de la journée ou de la semaine, ou si le seuil d'avertissement ou d'erreur de décalage est constamment dépassé, vous pouvez prendre les mesures appropriées. De plus, vous pouvez cliquer sur le bouton **Exporter** pour créer un rapport au format CSV pour le graphique que vous visualisez.

Les graphiques de l'historique de protection affichent les informations suivantes :

- **Durée du décalage relationnel**

Affiche les secondes, les minutes ou les heures sur l'axe vertical (y) et affiche les jours, les mois ou les années sur l'axe horizontal (x), selon la période de durée sélectionnée. La valeur supérieure sur l'axe des

y indique la durée de décalage maximale atteinte dans la période indiquée sur l'axe des x. La ligne orange horizontale sur le graphique représente le seuil d'erreur de décalage et la ligne jaune horizontale représente le seuil d'avertissement de décalage. En positionnant votre curseur sur ces lignes, vous affichez le réglage du seuil. La ligne bleue horizontale représente la durée du décalage. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone d'intérêt.

- **Durée du transfert de relation**

Affiche les secondes, les minutes ou les heures sur l'axe vertical (y) et affiche les jours, les mois ou les années sur l'axe horizontal (x), selon la période de durée sélectionnée. La valeur supérieure sur l'axe des y indique la durée de transfert maximale atteinte dans la période indiquée sur l'axe des x. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur la zone d'intérêt.



Ce graphique n'est pas disponible pour les volumes qui sont dans des relations de protection synchrones.

- **Taille de la relation transférée**

Affiche les octets, les kilo-octets, les mégaoctets, etc., sur l'axe vertical (y) en fonction de la taille du transfert, et affiche les jours, les mois ou les années sur l'axe horizontal (x) en fonction de la période sélectionnée. La valeur supérieure sur l'axe des y indique la taille de transfert maximale atteinte au cours de la période indiquée sur l'axe des x. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone d'intérêt.



Ce graphique n'est pas disponible pour les volumes qui sont dans des relations de protection synchrones.

Espace historique

La zone Historique affiche des graphiques qui fournissent des informations sur la capacité et les réservations d'espace du volume sélectionné. De plus, vous pouvez cliquer sur le bouton **Exporter** pour créer un rapport au format CSV pour le graphique que vous visualisez.

Les graphiques peuvent être vides et le message Aucune donnée trouvée s'affiche lorsque les données ou l'état du volume restent inchangés pendant une période donnée.

Vous pouvez sélectionner un type de graphique dans la liste déroulante en haut du volet Historique. Vous pouvez également afficher les détails d'une période spécifique en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques d'historique peuvent vous aider à identifier les tendances : par exemple, si l'utilisation du volume dépasse systématiquement le seuil presque plein, vous pouvez prendre les mesures appropriées.

Les graphiques d'historique affichent les informations suivantes :

- **Capacité de volume utilisée**

Affiche la capacité utilisée dans le volume et la tendance d'utilisation de la capacité du volume en fonction de l'historique d'utilisation, sous forme de graphiques linéaires en octets, kilo-octets, mégaoctets, etc., sur l'axe vertical (y). La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Capacité du volume utilisé, la ligne du graphique Capacité du volume utilisé est masquée.

- **Capacité de volume utilisée par rapport au total**

Affiche la tendance d'utilisation de la capacité du volume en fonction de l'historique d'utilisation, ainsi que la capacité utilisée, la capacité totale et les détails des économies d'espace grâce à la déduplication et à la compression, sous forme de graphiques linéaires, en octets, kilo-octets, mégaoctets, etc., sur l'axe vertical (y). La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Capacité de tendance utilisée, la ligne du graphique Capacité de tendance utilisée est masquée.

- **Capacité de volume utilisée (%)**

Affiche la capacité utilisée dans le volume et la tendance d'utilisation de la capacité du volume en fonction de l'historique d'utilisation, sous forme de graphiques linéaires, en pourcentage, sur l'axe vertical (y). La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Capacité du volume utilisé, la ligne du graphique Capacité du volume utilisé est masquée.

- **Capacité d'instantané utilisée (%)**

Affiche la réserve de Snapshot et le seuil d'avertissement de Snapshot sous forme de graphiques linéaires, ainsi que la capacité utilisée par les copies de Snapshot sous forme de graphique en aires, en pourcentage, sur l'axe vertical (y). Le débordement de Snapshot est représenté avec différentes couleurs. La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Réserve d'instantané, la ligne du graphique Réserve d'instantané est masquée.

Liste des événements

La liste des événements affiche des détails sur les événements nouveaux et reconnus :

- **Gravité**

Affiche la gravité de l'événement.

- **Événement**

Affiche le nom de l'événement.

- **Heure déclenchée**

Affiche le temps écoulé depuis que l'événement a été généré. Si le temps écoulé dépasse une semaine, l'horodatage auquel l'événement a été généré est affiché.

Volet Annotations associées

Le volet Annotations associées vous permet d'afficher les détails des annotations associées au volume sélectionné. Les détails incluent le nom de l'annotation et les valeurs d'annotation appliquées au volume. Vous pouvez également supprimer les annotations manuelles du volet Annotations associées.

Volet Appareils associés

Le volet Périphériques associés vous permet d'afficher et de naviguer vers les SVM, les agrégats, les qtrees, les LUN et les copies Snapshot associés au volume :

- **Machine virtuelle de stockage**

Affiche la capacité et l'état de santé du SVM qui contient le volume sélectionné.

- **Agrégat**

Affiche la capacité et l'état de santé de l'agrégat qui contient le volume sélectionné. Pour les volumes FlexGroup , le nombre d'agrégats qui composent le FlexGroup est répertorié.

- **Volumes dans l'ensemble**

Affiche le nombre et la capacité de tous les volumes appartenant à l'agrégat parent du volume sélectionné. L'état de santé des volumes est également affiché, en fonction du niveau de gravité le plus élevé. Par exemple, si un agrégat contient dix volumes, dont cinq affichent l'état Avertissement et les cinq autres l'état Critique, alors l'état affiché est Critique. Ce composant n'apparaît pas pour les volumes FlexGroup .

- **Qtrees**

Affiche le nombre de qtrees que contient le volume sélectionné et la capacité des qtrees avec quota que contient le volume sélectionné. La capacité des qtrees avec quota est affichée par rapport à la capacité des données de volume. L'état de santé des qtrees est également affiché, en fonction du niveau de gravité le plus élevé. Par exemple, si un volume comporte dix qtrees, cinq avec un statut Avertissement et les cinq autres avec un statut Critique, alors le statut affiché est Critique.

- **Actions NFS**

Affiche le nombre et l'état des partages NFS associés au volume.

- **Actions PME**

Affiche le nombre et l'état des partages SMB/CIFS.

- **LUN**

Affiche le nombre et la taille totale de tous les LUN dans le volume sélectionné. L'état de santé des LUN est également affiché, en fonction du niveau de gravité le plus élevé.

- **Quotas d'utilisateurs et de groupes**

Affiche le nombre et l'état des quotas d'utilisateur et de groupe d'utilisateurs associés au volume et à ses qtrees.

- * Volumes FlexClone *

Affiche le nombre et la capacité de tous les volumes clonés du volume sélectionné. Le nombre et la capacité ne s'affichent que si le volume sélectionné contient des volumes clonés.

- **Volume parent**

Affiche le nom et la capacité du volume parent d'un volume FlexClone sélectionné. Le volume parent s'affiche uniquement si le volume sélectionné est un volume FlexClone .

Volet Groupes associés

Le volet Groupes associés vous permet d'afficher la liste des groupes associés au volume sélectionné.

Volet Alertes associées

Le volet Alertes associées vous permet d'afficher la liste des alertes créées pour le volume sélectionné. Vous pouvez également ajouter une alerte en cliquant sur le lien Ajouter une alerte ou modifier une alerte existante en cliquant sur le nom de l'alerte.

Page de détails sur la santé de la machine virtuelle de stockage

Vous pouvez utiliser la page Détails de la machine virtuelle de stockage / Santé pour afficher des informations détaillées sur la machine virtuelle de stockage sélectionnée, telles que son état de santé, sa capacité, sa configuration, ses stratégies de données, ses interfaces logiques (LIF), ses LUN, ses qtrees, son utilisateur, ses quotas de groupe d'utilisateurs et ses détails de protection. Vous pouvez également afficher des informations sur les objets associés et les alertes associées pour la machine virtuelle de stockage.



Vous ne pouvez surveiller que la machine virtuelle de stockage de données.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour la machine virtuelle de stockage sélectionnée :

- **Passer à la vue Performances**

Vous permet d'accéder à la page Détails de la machine virtuelle de stockage / Performances.

- **Actes**

- Ajouter une alerte

Vous permet d'ajouter une alerte à la machine virtuelle de stockage sélectionnée.

- Annoter

Vous permet d'annoter la machine virtuelle de stockage sélectionnée.

- **Afficher les machines virtuelles de stockage**

Vous permet d'accéder à la vue Santé : toutes les machines virtuelles de stockage.

Onglet Santé

L'onglet Santé affiche des informations détaillées sur la disponibilité des données, la capacité des données et les problèmes de protection de divers objets tels que les volumes, les agrégats, les LIF NAS, les LIF SAN, les LUN, les protocoles, les services, les partages NFS et les partages CIFS.

Vous pouvez cliquer sur le graphique d'un objet pour afficher la liste filtrée des objets. Par exemple, vous pouvez cliquer sur le graphique de capacité du volume qui affiche les avertissements pour afficher la liste des volumes qui présentent des problèmes de capacité avec une gravité d'avertissement.

- **Problèmes de disponibilité**

Affiche, sous forme de graphique, le nombre total d'objets, y compris les objets présentant des problèmes de disponibilité et les objets ne présentant aucun problème lié à la disponibilité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations sous le graphique fournissent des détails sur les problèmes de disponibilité qui peuvent avoir un impact ou ont déjà eu un impact sur la disponibilité des données dans la machine virtuelle de stockage. Par exemple, des informations sont affichées sur les LIF NAS et les LIF SAN qui sont en panne et sur les volumes qui sont hors ligne.

Vous pouvez également afficher des informations sur les protocoles et services associés actuellement en cours d'exécution, ainsi que le nombre et l'état des partages NFS et CIFS.

- **Problèmes de capacité**

Affiche, sous forme de graphique, le nombre total d'objets, y compris les objets présentant des problèmes de capacité et les objets ne présentant aucun problème lié à la capacité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations sous le graphique fournissent des détails sur les problèmes de capacité qui peuvent avoir un impact ou ont déjà eu un impact sur la capacité des données dans la machine virtuelle de stockage. Par exemple, des informations sont affichées sur les agrégats susceptibles de dépasser les valeurs seuils définies.

- **Problèmes de protection**

Fournit un aperçu rapide de l'état de santé lié à la protection des machines virtuelles de stockage en affichant, sous forme de boîte de dialogue de champ, le nombre total de relations, y compris les relations qui présentent des problèmes de protection et les relations qui n'en présentent aucun. Vous pouvez également afficher l'état de la relation DR de la machine virtuelle de stockage pour la machine virtuelle de stockage sélectionnée. Les événements des relations DR des machines virtuelles de stockage sont affichés ici et en cliquant sur les événements, vous accédez à la page des détails de l'événement. Lorsque des volumes non protégés existent, cliquer sur le lien vous amène à la vue Santé : Tous les volumes où vous pouvez afficher une liste filtrée des volumes non protégés sur la machine virtuelle de stockage. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Cliquer sur un graphique vous amène à la vue Relation : Toutes les relations, où vous pouvez afficher une liste filtrée des détails des relations de protection. Les informations sous le graphique fournissent des détails sur les problèmes de protection qui peuvent avoir un impact ou ont déjà eu un impact sur la protection des données dans la machine virtuelle de stockage. Par exemple, des informations sont affichées sur les volumes dont la réserve de copie Snapshot est presque pleine ou sur les problèmes de décalage de relation SnapMirror .

Onglet Capacité

L'onglet Capacité affiche des informations détaillées sur la capacité de données du SVM sélectionné.

Les informations suivantes sont affichées pour une machine virtuelle de stockage avec un FlexVol volume ou un volume FlexGroup :

- **Capacité**

La zone Capacité affiche des détails sur la capacité utilisée et disponible allouée à partir de tous les volumes :

- **Capacité totale**

Affiche la capacité totale de la machine virtuelle de stockage.

- Utilisé

Affiche l'espace utilisé par les données dans les volumes appartenant à la machine virtuelle de stockage.

- Disponible garanti

Affiche l'espace disponible garanti pour les données disponibles pour les volumes dans la machine virtuelle de stockage.

- Non garanti

Affiche l'espace disponible restant pour les données allouées aux volumes à provisionnement fin dans la machine virtuelle de stockage.

- **Volumes avec problèmes de capacité**

La liste des volumes présentant des problèmes de capacité affiche, sous forme de tableau, des détails sur les volumes présentant des problèmes de capacité :

- Statut

Indique que le volume présente un problème de capacité d'une gravité indiquée.

Vous pouvez déplacer le pointeur sur l'état pour afficher plus d'informations sur l'événement ou les événements liés à la capacité générés pour le volume.

Si l'état du volume est déterminé par un événement unique, vous pouvez afficher des informations telles que le nom de l'événement, l'heure et la date de déclenchement de l'événement, le nom de l'administrateur auquel l'événement est attribué et la cause de l'événement. Vous pouvez utiliser le bouton **Afficher les détails** pour afficher plus d'informations sur l'événement.

Si l'état du volume est déterminé par plusieurs événements de même gravité, les trois principaux événements sont affichés avec des informations telles que le nom de l'événement, l'heure et la date de déclenchement des événements et le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également cliquer sur le lien **Afficher tous les événements** pour afficher la liste des événements générés.



Un volume peut avoir plusieurs événements de la même gravité ou de gravités différentes. Cependant, seule la gravité la plus élevée est affichée. Par exemple, si un volume comporte deux événements avec des niveaux de gravité Erreur et Avertissement, seule la gravité Erreur est affichée.

- Volume

Affiche le nom du volume.

- Capacité de données utilisée

Affiche, sous forme de graphique, des informations sur l'utilisation de la capacité volumique (en pourcentage).

- Jours à remplir

Affiche le nombre estimé de jours restants avant que le volume n'atteigne sa pleine capacité.

- Provisionnement léger

Affiche si la garantie d'espace est définie pour le volume sélectionné. Les valeurs valides sont Oui et Non.

- Agrégats

Pour les volumes FlexVol , affiche le nom de l'agrégat qui contient le volume. Pour les volumes FlexGroup , affiche le nombre d'agrégats utilisés dans le FlexGroup.

Onglet Configuration

L'onglet Configuration affiche les détails de configuration de la machine virtuelle de stockage sélectionnée, tels que son cluster, son volume racine, le type de volumes qu'elle contient (volumes FlexVol), les politiques et la protection créées sur la machine virtuelle de stockage :

- **Aperçu**

- Cluster

Affiche le nom du cluster auquel appartient la machine virtuelle de stockage.

- Type de volume autorisé

Affiche le type de volumes pouvant être créés dans la machine virtuelle de stockage. Le type peut être FlexVol ou FlexVol/ FlexGroup.

- Volume racinaire

Affiche le nom du volume racine de la machine virtuelle de stockage.

- Protocoles autorisés

Affiche le type de protocoles pouvant être configurés sur la machine virtuelle de stockage. Indique également si un protocole est en cours d'exécution (●), vers le bas (●), ou n'est pas configuré (●).

- **Interfaces réseau de données**

- NAS

Affiche le nombre d'interfaces NAS associées à la machine virtuelle de stockage. Indique également si les interfaces sont actives (●) ou vers le bas (●).

- SAN

Affiche le nombre d'interfaces SAN associées à la machine virtuelle de stockage. Indique également si les interfaces sont actives (●) ou vers le bas (●).

- FC-NVMe

Affiche le nombre d'interfaces FC-NVMe associées à la machine virtuelle de stockage. Indique également si les interfaces sont actives (●) ou vers le bas (●).

- **Interfaces réseau de gestion**

- Disponibilité

Affiche le nombre d'interfaces de gestion associées à la machine virtuelle de stockage. Indique également si les interfaces de gestion sont opérationnelles () ou vers le bas ().

• Politiques

- Snapshots

Affiche le nom de la stratégie de snapshot créée sur la machine virtuelle de stockage.

- Politiques d'exportation

Affiche soit le nom de la politique d'exportation si une seule politique est créée, soit le nombre de politiques d'exportation si plusieurs politiques sont créées.

• Protection

- Stockage VM DR

Affiche si la machine virtuelle de stockage sélectionnée est protégée, de destination ou non protégée et le nom de la destination sur laquelle la machine virtuelle de stockage est protégée. Si la machine virtuelle de stockage sélectionnée est la destination, les détails de la machine virtuelle de stockage source sont affichés. En cas de déploiement, ce champ affiche le nombre total de machines virtuelles de stockage de destination sur lesquelles la machine virtuelle de stockage est protégée. Le lien de comptage vous amène à la grille de relations de la machine virtuelle de stockage filtrée sur la machine virtuelle de stockage source.

- Volumes protégés

Affiche le nombre de volumes protégés sur la machine virtuelle de stockage sélectionnée par rapport au nombre total de volumes. Si vous visualisez une machine virtuelle de stockage de destination, le lien numérique concerne les volumes de destination de la machine virtuelle de stockage sélectionnée.

- Volumes non protégés

Affiche le nombre de volumes non protégés sur la machine virtuelle de stockage sélectionnée.

• Services

- Type

Affiche le type de service configuré sur la machine virtuelle de stockage. Le type peut être Domain Name System (DNS) ou Network Information Service (NIS).

- État

Affiche l'état du service, qui peut être Up (), Vers le bas (), ou non configuré ().

- Nom de domaine

Affiche les noms de domaine complets (FQDN) du serveur DNS pour les services DNS ou du serveur NIS pour les services NIS. Lorsque le serveur NIS est activé, le FQDN actif du serveur NIS s'affiche. Lorsque le serveur NIS est désactivé, la liste de tous les noms de domaine complets s'affiche.

- Adresse IP

Affiche les adresses IP du serveur DNS ou NIS. Lorsque le serveur NIS est activé, l'adresse IP active du serveur NIS s'affiche. Lorsque le serveur NIS est désactivé, la liste de toutes les adresses IP s'affiche.

Onglet Interfaces réseau

L'onglet Interfaces réseau affiche des détails sur les interfaces réseau de données (LIF) créées sur la machine virtuelle de stockage sélectionnée :

- **Interface réseau**

Affiche le nom de l'interface créée sur la machine virtuelle de stockage sélectionnée.

- **Statut opérationnel**

Affiche l'état opérationnel de l'interface, qui peut être Up (👆), Vers le bas (👇), ou Inconnu (❓). L'état opérationnel d'une interface est déterminé par l'état de ses ports physiques.

- **Statut administratif**

Affiche l'état administratif de l'interface, qui peut être Up (👆), Vers le bas (👇), ou Inconnu (❓). L'état administratif d'une interface est contrôlé par l'administrateur de stockage pour apporter des modifications à la configuration ou à des fins de maintenance. Le statut administratif peut être différent du statut opérationnel. Cependant, si l'état administratif d'une interface est Down, l'état opérationnel est Down par défaut.

- **Adresse IP / WWPN**

Affiche l'adresse IP des interfaces Ethernet et le nom de port mondial (WWPN) pour les LIF FC.

- **Protocoles**

Affiche la liste des protocoles de données spécifiés pour l'interface, tels que CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe et FlexCache.

- **Rôle**

Affiche le rôle de l'interface. Les rôles peuvent être des données ou de la gestion.

- **Port d'attache**

Affiche le port physique auquel l'interface était initialement associée.

- **Port actuel**

Affiche le port physique auquel l'interface est actuellement associée. Si l'interface est migrée, le port actuel peut être différent du port d'origine.

- **Ensemble de ports**

Affiche l'ensemble de ports sur lequel l'interface est mappée.

- **Politique de basculement**

Affiche la stratégie de basculement configurée pour l'interface. Pour les interfaces NFS, CIFS et FlexCache, la stratégie de basculement par défaut est Suivant disponible. La politique de basculement

n'est pas applicable aux interfaces FC et iSCSI.

- **Groupes de routage**

Affiche le nom du groupe de routage. Vous pouvez afficher plus d'informations sur les itinéraires et la passerelle de destination en cliquant sur le nom du groupe de routage.

Les groupes de routage ne sont pas pris en charge pour ONTAP 8.3 ou version ultérieure et, par conséquent, une colonne vide s'affiche pour ces clusters.

- **Groupe de basculement**

Affiche le nom du groupe de basculement.

Onglet Qtrees

L'onglet Qtrees affiche des détails sur les qtrees et leurs quotas. Vous pouvez cliquer sur le bouton **Modifier les seuils** si vous souhaitez modifier les paramètres de seuil de santé pour la capacité qtree pour un ou plusieurs qtrees.

Utilisez le bouton **Exporter** pour créer un fichier de valeurs séparées par des virgules (.csv) contenant les détails de tous les qtrees surveillés. Lors de l'exportation vers un fichier CSV, vous pouvez choisir de créer un rapport qtrees pour la machine virtuelle de stockage actuelle, pour toutes les machines virtuelles de stockage du cluster actuel ou pour toutes les machines virtuelles de stockage de tous les clusters de votre centre de données. Certains champs qtrees supplémentaires apparaissent dans le fichier CSV exporté.

- **Statut**

Affiche l'état actuel du qtree. Le statut peut être Critique (❌), Erreur (⚠️), Avertissement (⚠️), ou Normal (✅).

Vous pouvez déplacer le pointeur sur l'icône d'état pour afficher plus d'informations sur l'événement ou les événements générés pour le qtree.

Si l'état du qtree est déterminé par un seul événement, vous pouvez afficher des informations telles que le nom de l'événement, l'heure et la date de déclenchement de l'événement, le nom de l'administrateur à qui l'événement est attribué et la cause de l'événement. Vous pouvez utiliser **Afficher les détails** pour afficher plus d'informations sur l'événement.

Si l'état du qtree est déterminé par plusieurs événements de même gravité, les trois principaux événements sont affichés avec des informations telles que le nom de l'événement, l'heure et la date de déclenchement des événements et le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également utiliser **Afficher tous les événements** pour afficher la liste des événements générés.



Un qtree peut avoir plusieurs événements de la même gravité ou de gravités différentes. Cependant, seule la gravité la plus élevée est affichée. Par exemple, si un qtree comporte deux événements avec des gravités d'erreur et d'avertissement, seule la gravité d'erreur est affichée.

- **Qtree**

Affiche le nom du qtree.

- **Grappe**

Affiche le nom du cluster contenant le qtree. Apparaît uniquement dans le fichier CSV exporté.

- **Machine virtuelle de stockage**

Affiche le nom de la machine virtuelle de stockage (SVM) contenant le qtree. Apparaît uniquement dans le fichier CSV exporté.

- **Volume**

Affiche le nom du volume qui contient le qtree.

Vous pouvez déplacer le pointeur sur le nom du volume pour afficher plus d'informations sur le volume.

- **Quota défini**

Indique si un quota est activé ou désactivé sur le qtree.

- **Type de quota**

Spécifie si le quota est destiné à un utilisateur, à un groupe d'utilisateurs ou à un qtree. Apparaît uniquement dans le fichier CSV exporté.

- **Utilisateur ou groupe**

Affiche le nom de l'utilisateur ou du groupe d'utilisateurs. Il y aura plusieurs lignes pour chaque utilisateur et groupe d'utilisateurs. Lorsque le type de quota est qtree ou si le quota n'est pas défini, la colonne est vide. Apparaît uniquement dans le fichier CSV exporté.

- **Disque utilisé %**

Affiche le pourcentage d'espace disque utilisé. Si une limite matérielle du disque est définie, cette valeur est basée sur la limite matérielle du disque. Si le quota est défini sans limite de disque dur, la valeur est basée sur l'espace de données du volume. Si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree, alors « Non applicable » s'affiche dans la page de grille et le champ est vide dans les données d'exportation CSV.

- **Limite du disque dur**

Affiche la quantité maximale d'espace disque allouée au qtree. Unified Manager génère un événement critique lorsque cette limite est atteinte et qu'aucune autre écriture sur disque n'est autorisée. La valeur est affichée comme « Illimité » dans les conditions suivantes : si le quota est défini sans limite de disque dur, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree.

- **Limite logicielle du disque**

Affiche la quantité d'espace disque allouée au qtree avant qu'un événement d'avertissement ne soit généré. La valeur est affichée comme « Illimité » dans les conditions suivantes : si le quota est défini sans limite logicielle de disque, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

- **Seuil de disque**

Affiche la valeur seuil définie sur l'espace disque. La valeur s'affiche comme « Illimité » dans les conditions suivantes : si le quota est défini sans limite de seuil de disque, si le quota n'est pas défini ou si les quotas

sont désactivés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

- **Fichiers utilisés %**

Affiche le pourcentage de fichiers utilisés dans le qtree. Si la limite stricte du fichier est définie, cette valeur est basée sur la limite stricte du fichier. Aucune valeur n'est affichée si le quota est défini sans limite stricte de fichier. Si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree, alors « Non applicable » s'affiche dans la page de grille et le champ est vide dans les données d'exportation CSV.

- **Limite stricte du fichier**

Affiche la limite stricte du nombre de fichiers autorisés sur les qtrees. La valeur est affichée comme « Illimité » dans les conditions suivantes : si le quota est défini sans limite stricte de fichier, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree.

- **Limite souple du fichier**

Affiche la limite souple pour le nombre de fichiers autorisés sur les qtrees. La valeur est affichée comme « Illimité » dans les conditions suivantes : si le quota est défini sans limite logicielle de fichier, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

Onglet Quotas d'utilisateurs et de groupes

Affiche les détails sur les quotas d'utilisateur et de groupe d'utilisateurs pour la machine virtuelle de stockage sélectionnée. Vous pouvez afficher des informations telles que l'état du quota, le nom de l'utilisateur ou du groupe d'utilisateurs, les limites souples et strictes définies sur les disques et les fichiers, la quantité d'espace disque et le nombre de fichiers utilisés, ainsi que la valeur du seuil du disque. Vous pouvez également modifier l'adresse e-mail associée à un utilisateur ou à un groupe d'utilisateurs.

- **Bouton de commande Modifier l'adresse e-mail**

Ouvre la boîte de dialogue Modifier l'adresse e-mail, qui affiche l'adresse e-mail actuelle de l'utilisateur ou du groupe d'utilisateurs sélectionné. Vous pouvez modifier l'adresse email. Si le champ **Modifier l'adresse e-mail** est vide, la règle par défaut est utilisée pour générer une adresse e-mail pour l'utilisateur ou le groupe d'utilisateurs sélectionné.

Si plusieurs utilisateurs ont le même quota, les noms des utilisateurs sont affichés sous forme de valeurs séparées par des virgules. De plus, la règle par défaut n'est pas utilisée pour générer l'adresse e-mail ; par conséquent, vous devez fournir l'adresse e-mail requise pour que les notifications soient envoyées.

- **Bouton de commande Configurer les règles de messagerie**

Vous permet de créer ou de modifier des règles pour générer une adresse e-mail pour les quotas d'utilisateur ou de groupe d'utilisateurs configurés sur la machine virtuelle de stockage. Une notification est envoyée à l'adresse e-mail spécifiée en cas de dépassement de quota.

- **Statut**

Affiche l'état actuel du quota. Le statut peut être Critique (❌), Avertissement (⚠️), ou Normal (✅).

Vous pouvez déplacer le pointeur sur l'icône d'état pour afficher plus d'informations sur l'événement ou les événements générés pour le quota.

Si l'état du quota est déterminé par un seul événement, vous pouvez afficher des informations telles que le nom de l'événement, l'heure et la date de déclenchement de l'événement, le nom de l'administrateur à qui l'événement est attribué et la cause de l'événement. Vous pouvez utiliser **Afficher les détails** pour afficher plus d'informations sur l'événement.

Si l'état du quota est déterminé par plusieurs événements de même gravité, les trois principaux événements sont affichés avec des informations telles que le nom de l'événement, l'heure et la date de déclenchement des événements et le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également utiliser **Afficher tous les événements** pour afficher la liste des événements générés.



Un quota peut avoir plusieurs événements de la même gravité ou de gravités différentes. Cependant, seule la gravité la plus élevée est affichée. Par exemple, si un quota comporte deux événements avec des niveaux de gravité Erreur et Avertissement, seule la gravité Erreur est affichée.

- **Utilisateur ou groupe**

Affiche le nom de l'utilisateur ou du groupe d'utilisateurs. Si plusieurs utilisateurs ont le même quota, les noms des utilisateurs sont affichés sous forme de valeurs séparées par des virgules.

La valeur s'affiche comme « Inconnu » lorsque ONTAP ne fournit pas de nom d'utilisateur valide en raison d'erreurs SecD.

- **Taper**

Spécifie si le quota est destiné à un utilisateur ou à un groupe d'utilisateurs.

- **Volume ou Qtree**

Affiche le nom du volume ou du qtree sur lequel le quota d'utilisateur ou de groupe d'utilisateurs est spécifié.

Vous pouvez déplacer le pointeur sur le nom du volume ou du qtree pour afficher plus d'informations sur le volume ou le qtree.

- **Disque utilisé %**

Affiche le pourcentage d'espace disque utilisé. La valeur s'affiche comme « Non applicable » si le quota est défini sans limite de disque dur.

- **Limite du disque dur**

Affiche la quantité maximale d'espace disque allouée pour le quota. Unified Manager génère un événement critique lorsque cette limite est atteinte et qu'aucune autre écriture sur disque n'est autorisée. La valeur est affichée comme « Illimité » si le quota est défini sans limite de disque dur.

- **Limite logicielle du disque**

Affiche la quantité d'espace disque allouée au quota avant qu'un événement d'avertissement ne soit généré. La valeur est affichée comme « Illimité » si le quota est défini sans limite logicielle de disque. Par défaut, cette colonne est masquée.

- **Seuil de disque**

Affiche la valeur seuil définie sur l'espace disque. La valeur s'affiche comme « Illimité » si le quota est défini sans limite de seuil de disque. Par défaut, cette colonne est masquée.

- **Fichiers utilisés %**

Affiche le pourcentage de fichiers utilisés dans le qtree. La valeur est affichée comme « Non applicable » si le quota est défini sans limite stricte de fichier.

- **Limite stricte du fichier**

Affiche la limite stricte du nombre de fichiers autorisés sur le quota. La valeur est affichée comme « Illimité » si le quota est défini sans limite stricte de fichier.

- **Limite souple du fichier**

Affiche la limite souple pour le nombre de fichiers autorisés sur le quota. La valeur est affichée comme « Illimité » si le quota est défini sans limite logicielle de fichier. Par défaut, cette colonne est masquée.

- **Adresse email**

Affiche l'adresse e-mail de l'utilisateur ou du groupe d'utilisateurs auquel les notifications sont envoyées en cas de dépassement des quotas.

Onglet Partages NFS

L'onglet Partages NFS affiche des informations sur les partages NFS telles que leur état, le chemin associé au volume (volumes FlexGroup ou volumes FlexVol), les niveaux d'accès des clients aux partages NFS et la politique d'exportation définie pour les volumes exportés. Les partages NFS ne seront pas affichés dans les conditions suivantes : si le volume n'est pas monté ou si les protocoles associés à la stratégie d'exportation du volume ne contiennent pas de partages NFS.

- **Statut**

Affiche l'état actuel des partages NFS. Le statut peut être Erreur (❗) ou Normal (✅).

- **Chemin de jonction**

Affiche le chemin sur lequel le volume est monté. Si une politique d'exportation NFS explicite est appliquée à un qtree, la colonne affiche le chemin du volume via lequel le qtree est accessible.

- **Chemin de jonction actif**

Affiche si le chemin d'accès au volume monté est actif ou inactif.

- **Volume ou Qtree**

Affiche le nom du volume ou du qtree auquel la stratégie d'exportation NFS est appliquée. Si une stratégie d'exportation NFS est appliquée à un qtree dans le volume, la colonne affiche à la fois les noms du volume et du qtree.

Vous pouvez cliquer sur le lien pour afficher les détails de l'objet dans la page de détails correspondante. Si l'objet est un qtree, les liens sont affichés à la fois pour le qtree et pour le volume.

- **État du volume**

Affiche l'état du volume en cours d'exportation. L'état peut être Hors ligne, En ligne, Restreint ou Mixte.

- Hors ligne

L'accès en lecture ou en écriture au volume n'est pas autorisé.

- En ligne

L'accès en lecture et en écriture au volume est autorisé.

- Limité

Des opérations limitées, telles que la reconstruction de parité, sont autorisées, mais l'accès aux données n'est pas autorisé.

- Mixte

Les constituants d'un volume FlexGroup ne sont pas tous dans le même état.

- **Style de sécurité**

Affiche l'autorisation d'accès pour les volumes exportés. Le style de sécurité peut être UNIX, Unifié, NTFS ou Mixte.

- UNIX (clients NFS)

Les fichiers et répertoires du volume ont des autorisations UNIX.

- Unifié

Les fichiers et répertoires du volume ont un style de sécurité unifié.

- NTFS (clients CIFS)

Les fichiers et répertoires du volume disposent d'autorisations Windows NTFS.

- Mixte

Les fichiers et répertoires du volume peuvent avoir des autorisations UNIX ou des autorisations Windows NTFS.

- **Autorisation UNIX**

Affiche les bits d'autorisation UNIX dans un format de chaîne octale, défini pour les volumes exportés. Il est similaire aux bits d'autorisation de style UNIX.

- **Politique d'exportation**

Affiche les règles qui définissent l'autorisation d'accès pour les volumes exportés. Vous pouvez cliquer sur le lien pour afficher les détails des règles associées à la politique d'exportation, telles que les protocoles d'authentification et l'autorisation d'accès.

Onglet Partages PME

Affiche des informations sur les partages SMB sur la machine virtuelle de stockage sélectionnée. Vous pouvez afficher des informations telles que l'état du partage SMB, le nom du partage, le chemin associé à la machine

virtuelle de stockage, l'état du chemin de jonction du partage, l'objet conteneur, l'état du volume conteneur, les données de sécurité du partage et les stratégies d'exportation définies pour le partage. Vous pouvez également déterminer si un chemin NFS équivalent pour le partage SMB existe.



Les partages dans les dossiers ne sont pas affichés dans l'onglet Partages SMB.

- **Bouton de commande Afficher le mappage des utilisateurs**

Lance la boîte de dialogue Mappage des utilisateurs.

Vous pouvez afficher les détails du mappage utilisateur pour la machine virtuelle de stockage.

- **Afficher le bouton de commande ACL**

Lance la boîte de dialogue Contrôle d'accès pour le partage.

Vous pouvez afficher les détails de l'utilisateur et des autorisations pour le partage sélectionné.

- **Statut**

Affiche l'état actuel du partage. Le statut peut être Normal (✅) ou Erreur (❗).

- **Nom de partage**

Affiche le nom du partage SMB.

- **Chemin**

Affiche le chemin de jonction sur lequel le partage est créé.

- **Chemin de jonction actif**

Affiche si le chemin d'accès au partage est actif ou inactif.

- **Objet contenant**

Affiche le nom de l'objet contenant auquel appartient le partage. L'objet contenant peut être un volume ou un qtree.

En cliquant sur le lien, vous pouvez afficher les détails sur l'objet contenant dans la page Détails correspondante. Si l'objet contenant est un qtree, les liens sont affichés à la fois pour le qtree et le volume.

- **État du volume**

Affiche l'état du volume en cours d'exportation. L'état peut être Hors ligne, En ligne, Restreint ou Mixte.

- Hors ligne

L'accès en lecture ou en écriture au volume n'est pas autorisé.

- En ligne

L'accès en lecture et en écriture au volume est autorisé.

- Limité

Des opérations limitées, telles que la reconstruction de parité, sont autorisées, mais l'accès aux données n'est pas autorisé.

- Mixte

Les constituants d'un volume FlexGroup ne sont pas tous dans le même état.

• Sécurité

Affiche l'autorisation d'accès pour les volumes exportés. Le style de sécurité peut être UNIX, Unifié, NTFS ou Mixte.

- UNIX (clients NFS)

Les fichiers et répertoires du volume ont des autorisations UNIX.

- Unifié

Les fichiers et répertoires du volume ont un style de sécurité unifié.

- NTFS (clients CIFS)

Les fichiers et répertoires du volume disposent d'autorisations Windows NTFS.

- Mixte

Les fichiers et répertoires du volume peuvent avoir des autorisations UNIX ou des autorisations Windows NTFS.

• Politique d'exportation

Affiche le nom de la politique d'exportation applicable au partage. Si aucune politique d'exportation n'est spécifiée pour la machine virtuelle de stockage, la valeur s'affiche comme Non activée.

Vous pouvez cliquer sur le lien pour afficher les détails des règles associées à la politique d'exportation, telles que les protocoles d'accès et les autorisations. Le lien est désactivé si la politique d'exportation est désactivée pour la machine virtuelle de stockage sélectionnée.

• Équivalent NFS

Spécifie s'il existe un équivalent NFS pour le partage.

Onglet SAN

Affiche les détails sur les LUN, les groupes d'initiateurs et les initiateurs de la machine virtuelle de stockage sélectionnée. Par défaut, la vue LUN est affichée. Vous pouvez afficher les détails sur les groupes d'initiateurs dans l'onglet Groupes d'initiateurs et les détails sur les initiateurs dans l'onglet Initiateurs.

• Onglet LUN

Affiche les détails sur les LUN appartenant à la machine virtuelle de stockage sélectionnée. Vous pouvez afficher des informations telles que le nom du LUN, l'état du LUN (en ligne ou hors ligne), le nom du système de fichiers (volume ou qtree) qui contient le LUN, le type de système d'exploitation hôte, la capacité totale de données et le numéro de série du LUN. La colonne Performances LUN fournit un lien vers la page Détails LUN/Performances.

Vous pouvez également afficher des informations indiquant si le provisionnement léger est activé sur le LUN et si le LUN est mappé à un groupe d'initiateurs. S'il est mappé à un initiateur, vous pouvez afficher les groupes d'initiateurs et les initiateurs mappés au LUN sélectionné.

- **Onglet Groupes d'initiateurs**

Affiche les détails sur les groupes initiateurs. Vous pouvez afficher des détails tels que le nom du groupe d'initiateurs, l'état d'accès, le type de système d'exploitation hôte utilisé par tous les initiateurs du groupe et le protocole pris en charge. Lorsque vous cliquez sur le lien dans la colonne État d'accès, vous pouvez afficher l'état d'accès actuel du groupe initiateur.

- **Normale**

Le groupe initiateur est connecté à plusieurs chemins d'accès.

- **Chemin unique**

Le groupe initiateur est connecté à un seul chemin d'accès.

- **Pas de chemins**

Il n'y a aucun chemin d'accès connecté au groupe initiateur.

Vous pouvez voir si les groupes d'initiateurs sont mappés à toutes les interfaces ou à des interfaces spécifiques via un ensemble de ports. Lorsque vous cliquez sur le lien de comptage dans la colonne Interfaces mappées, toutes les interfaces sont affichées ou des interfaces spécifiques pour un ensemble de ports sont affichées. Les interfaces mappées via le portail cible ne sont pas affichées. Le nombre total d'initiateurs et de LUN mappés à un groupe d'initiateurs s'affiche.

Vous pouvez également afficher les LUN et les initiateurs mappés au groupe d'initiateurs sélectionné.

- **Onglet Initiateurs**

Affiche le nom et le type de l'initiateur ainsi que le nombre total de groupes d'initiateurs mappés à cet initiateur pour la machine virtuelle de stockage sélectionnée.

```
initiator groups that are mapped to the selected initiator group.
```

Volet Annotations associées

Le volet Annotations associées vous permet d'afficher les détails d'annotation associés à la machine virtuelle de stockage sélectionnée. Les détails incluent le nom de l'annotation et les valeurs d'annotation appliquées à la machine virtuelle de stockage. Vous pouvez également supprimer les annotations manuelles du volet Annotations associées.

Volet Appareils associés

Le volet Périphériques associés vous permet d'afficher le cluster, les agrégats et les volumes associés à la machine virtuelle de stockage :

- **Grappe**

Affiche l'état de santé du cluster auquel appartient la machine virtuelle de stockage.

- **Agrégats**

Affiche le nombre d'agrégats appartenant à la machine virtuelle de stockage sélectionnée. L'état de santé des agrégats est également affiché, en fonction du niveau de gravité le plus élevé. Par exemple, si une machine virtuelle de stockage contient dix agrégats, dont cinq affichent l'état Avertissement et les cinq autres l'état Critique, l'état affiché est Critique.

- **Agrégats attribués**

Affiche le nombre d'agrégats attribués à une machine virtuelle de stockage. L'état de santé des agrégats est également affiché, en fonction du niveau de gravité le plus élevé.

- **Volumes**

Affiche le nombre et la capacité des volumes appartenant à la machine virtuelle de stockage sélectionnée. L'état de santé des volumes est également affiché, en fonction du niveau de gravité le plus élevé. Lorsqu'il existe des volumes FlexGroup dans la machine virtuelle de stockage, le décompte inclut également les FlexGroups ; il n'inclut pas les constituants FlexGroup .

Volet Groupes associés

Le volet Groupes associés vous permet d'afficher la liste des groupes associés à la machine virtuelle de stockage sélectionnée.

Volet Alertes associées

Le volet Alertes associées vous permet d'afficher la liste des alertes créées pour la machine virtuelle de stockage sélectionnée. Vous pouvez également ajouter une alerte en cliquant sur le lien **Ajouter une alerte** ou modifier une alerte existante en cliquant sur le nom de l'alerte.

Page de détails sur les clusters/la santé

La page Détails du cluster/de l'état de santé fournit des informations détaillées sur un cluster sélectionné, telles que l'état de santé, la capacité et les détails de configuration. Vous pouvez également afficher des informations sur les interfaces réseau (LIF), les nœuds, les disques, les périphériques associés et les alertes associées pour le cluster.

L'état à côté du nom du cluster, par exemple (Bon), représente l'état de communication ; si Unified Manager peut communiquer avec le cluster. Il ne représente pas l'état de basculement ou l'état global du cluster.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour le cluster sélectionné :

- **Passer à la vue Performances**

Vous permet d'accéder à la page Détails du cluster / Performances.

- **Actes**

- Ajouter une alerte : ouvre la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter une alerte au cluster sélectionné.
- Redécouvrir : lance une actualisation manuelle du cluster, ce qui permet à Unified Manager de

découvrir les modifications récentes apportées au cluster.

Si Unified Manager est associé à OnCommand Workflow Automation, l'opération de redécouverte réacquiert également les données mises en cache de WFA, le cas échéant.

Une fois l'opération de redécouverte lancée, un lien vers les détails du travail associé s'affiche pour permettre le suivi de l'état du travail.

- Annoter : vous permet d'annoter le cluster sélectionné.

• Voir les clusters

Vous permet d'accéder à la vue Santé : Tous les clusters.

Onglet Santé

Affiche des informations détaillées sur la disponibilité des données et les problèmes de capacité des données de divers objets de cluster tels que les nœuds, les SVM et les agrégats. Les problèmes de disponibilité sont liés à la capacité de service de données des objets du cluster. Les problèmes de capacité sont liés à la capacité de stockage des données des objets du cluster.

Vous pouvez cliquer sur le graphique d'un objet pour afficher une liste filtrée des objets. Par exemple, vous pouvez cliquer sur le graphique de capacité SVM qui affiche les avertissements pour afficher une liste filtrée des SVM. Cette liste contient les SVM qui ont des volumes ou des qtrees présentant des problèmes de capacité avec un niveau de gravité d'avertissement. Vous pouvez également cliquer sur le graphique de disponibilité des SVM qui affiche les avertissements pour afficher la liste des SVM présentant des problèmes de disponibilité avec un niveau de gravité d'avertissement.

Problèmes de disponibilité

Affiche graphiquement le nombre total d'objets, y compris les objets présentant des problèmes de disponibilité et les objets ne présentant aucun problème de disponibilité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations sous le graphique fournissent des détails sur les problèmes de disponibilité qui peuvent avoir un impact ou ont déjà eu un impact sur la disponibilité des données dans le cluster. Par exemple, des informations sont affichées sur les étagères de disques qui sont en panne et les agrégats qui sont hors ligne.



Les données affichées pour le graphique à barres SFO sont basées sur l'état HA des nœuds. Les données affichées pour tous les autres graphiques à barres sont calculées en fonction des événements générés.

Problèmes de capacité

Affiche graphiquement le nombre total d'objets, y compris les objets présentant des problèmes de capacité et les objets ne présentant aucun problème lié à la capacité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations sous le graphique fournissent des détails sur les problèmes de capacité qui peuvent avoir un impact ou ont déjà eu un impact sur la capacité des données du cluster. Par exemple, des informations sont affichées sur les agrégats susceptibles de dépasser les valeurs seuils définies.

Onglet Capacité

Affiche des informations détaillées sur la capacité du cluster sélectionné.

Capacité

Affiche le graphique de capacité des données concernant la capacité utilisée et la capacité disponible de tous les agrégats alloués :

- Espace logique utilisé

La taille réelle des données stockées sur tous les agrégats de ce cluster sans appliquer les économies réalisées grâce à l'utilisation des technologies d'efficacité de stockage ONTAP . Cela n'inclut pas les copies instantanées.

- Réduction des données

Affiche le ratio sans copies d'instantanés et avec deux chiffres significatifs, par exemple, 1,8 à 1. Ce ratio est basé sur les paramètres d'efficacité de stockage ONTAP configurés.

- Utilisé

La capacité physique utilisée par les données sur tous les agrégats. Cela n'inclut pas la capacité utilisée pour la parité, le dimensionnement optimal et la réservation.

- disponible

Affiche la capacité disponible pour les données.

- Pièces de rechange

Affiche la capacité de stockage disponible pour le stockage sur tous les disques de rechange.

- Provisionné

Affiche la capacité provisionnée pour tous les volumes sous-jacents.

Détails

Affiche des informations détaillées sur la capacité utilisée et disponible. Le calcul exclut les données agrégées de la racine.

- Capacité totale

Affiche la capacité totale du cluster. Cela n'inclut pas la capacité attribuée à la parité.

- Utilisé

Affiche la capacité utilisée par les données. Cela n'inclut pas la capacité utilisée pour la parité, le dimensionnement optimal et la réservation.

- disponible

Affiche la capacité disponible pour les données.

- Provisionné

Affiche la capacité provisionnée pour tous les volumes sous-jacents.

- Pièces de rechange

Affiche la capacité de stockage disponible pour le stockage sur tous les disques de rechange.

Niveau Cloud

Affiche la capacité totale de niveau cloud utilisée et la capacité utilisée pour chaque niveau cloud connecté pour les agrégats compatibles FabricPool sur le cluster. Un FabricPool peut être sous licence ou sans licence.

Répartition de la capacité physique par type de disque

La zone Répartition de la capacité physique par type de disque affiche des informations détaillées sur la capacité de disque des différents types de disques du cluster. En cliquant sur le type de disque, vous pouvez afficher plus d'informations sur le type de disque à partir de l'onglet Disques.

- Capacité totale utilisable

Affiche la capacité disponible et la capacité de réserve des disques de données.

- Disque dur

Affiche graphiquement la capacité utilisée et la capacité disponible de tous les disques de données HDD du cluster. La ligne pointillée représente la capacité de réserve des disques de données du disque dur.

- Éclair

- SSD Data

Affiche graphiquement la capacité utilisée et la capacité disponible des disques de données SSD du cluster.

- Cache SSD

Affiche graphiquement la capacité de stockage des disques de cache SSD du cluster.

- SSD de rechange

Affiche graphiquement la capacité de réserve des disques SSD, de données et de cache du cluster.

- Disques non attribués

Affiche le nombre de disques non attribués dans le cluster.

Liste des agrégats présentant des problèmes de capacité

Affiche sous forme de tableau les détails sur la capacité utilisée et la capacité disponible des agrégats présentant des problèmes de risque de capacité.

- Statut

Indique que l'agrégat présente un problème de capacité d'une certaine gravité.

Vous pouvez déplacer le pointeur sur l'état pour afficher plus d'informations sur l'événement ou les événements générés pour l'agrégat.

Si l'état de l'agrégat est déterminé par un seul événement, vous pouvez afficher des informations telles que le nom de l'événement, l'heure et la date de déclenchement de l'événement, le nom de l'administrateur auquel l'événement est attribué et la cause de l'événement. Vous pouvez cliquer sur le bouton **Afficher les détails** pour afficher plus d'informations sur l'événement.

Si l'état de l'agrégat est déterminé par plusieurs événements de même gravité, les trois principaux événements sont affichés avec des informations telles que le nom de l'événement, l'heure et la date de déclenchement des événements et le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également cliquer sur le lien **Afficher tous les événements** pour afficher la liste des événements générés.



Un agrégat peut avoir plusieurs événements liés à la capacité de la même gravité ou de gravités différentes. Cependant, seule la gravité la plus élevée est affichée. Par exemple, si un agrégat comporte deux événements avec des niveaux de gravité Erreur et Critique, seule la gravité Critique est affichée.

- Agrégat

Affiche le nom de l'agrégat.

- Capacité de données utilisée

Affiche graphiquement des informations sur l'utilisation globale de la capacité (en pourcentage).

- Jours à remplir

Affiche le nombre estimé de jours restants avant que l'agrégat n'atteigne sa pleine capacité.

Onglet Configuration

Affiche les détails du cluster sélectionné, tels que l'adresse IP, le contact et l'emplacement :

Présentation du cluster

- Interface de gestion

Affiche le LIF de gestion de cluster qu'Unified Manager utilise pour se connecter au cluster. L'état opérationnel de l'interface est également affiché.

- Nom d'hôte ou adresse IP

Affiche le nom de domaine complet, le nom court ou l'adresse IP du LIF de gestion de cluster qu'Unified Manager utilise pour se connecter au cluster.

- Nom de domaine complet

Affiche le nom de domaine complet (FQDN) du cluster.

- Version du système d'exploitation

Affiche la version ONTAP exécutée par le cluster. Si les nœuds du cluster exécutent différentes versions d'ONTAP, la version ONTAP la plus ancienne est affichée.

- Contact

Affiche les détails sur l'administrateur que vous devez contacter en cas de problèmes avec le cluster.

- Pays

Affiche l'emplacement du cluster.

- Personnalité

Identifie s'il s'agit d'un cluster configuré avec All SAN Array.

Présentation du cluster distant

Fournit des détails sur le cluster distant dans une configuration MetroCluster . Ces informations s'affichent uniquement pour les configurations MetroCluster .

- Cluster

Affiche le nom du cluster distant. Vous pouvez cliquer sur le nom du cluster pour accéder à la page de détails du cluster.

- Nom d'hôte ou adresse IP

Affiche le nom de domaine complet, le nom court ou l'adresse IP du cluster distant.

- Pays

Affiche l'emplacement du cluster distant.

Présentation de MetroCluster

Fournit des détails sur le cluster local dans une configuration MetroCluster sur FC ou MetroCluster sur IP. Ces informations s'affichent uniquement pour les configurations MetroCluster sur FC ou IP.

- Type

Affiche si le type MetroCluster est à deux ou quatre nœuds. Pour MetroCluster sur IP, seuls quatre nœuds sont pris en charge.

- Configuration

Affiche la configuration MetroCluster sur FC et IP, qui peut avoir les valeurs suivantes :

Pour FC

- Configuration extensible avec câbles SAS
- Configuration extensible avec pont FC-SAS
- Configuration de la structure avec des commutateurs FC



Pour un MetroCluster à quatre nœuds, seule la configuration Fabric avec des commutateurs FC est prise en charge.

Pour IP

- Configuration IP avec commutateurs Ethernet (L2 ou L3, selon la configuration du cluster)
 - Commutation automatisée non planifiée (AUSO)

Affiche si le basculement automatique non planifié est activé pour le cluster local. Par défaut, AUSO est activé pour tous les clusters dans une configuration MetroCluster à deux nœuds dans Unified Manager. Vous pouvez utiliser l'interface de ligne de commande pour modifier le paramètre AUSO. Ceci est pris en charge uniquement pour MetroCluster sur FC.

- Mode de commutation

Affiche le mode de commutation pour la configuration MetroCluster sur IP. Les valeurs disponibles sont : `Active`, `Negotiated Switchover`, et `Automatic Unplanned Switchover`.

Nœuds

- Disponibilité

Affiche le nombre de nœuds en activité (●) ou vers le bas (●) dans le cluster.

- Versions du système d'exploitation

Affiche les versions ONTAP exécutées par les nœuds ainsi que le nombre de nœuds exécutant une version particulière d'ONTAP. Par exemple, 9.6 (2), 9.3 (1) spécifie que deux nœuds exécutent ONTAP 9.6 et qu'un nœud exécute ONTAP 9.3.

Machines virtuelles de stockage

- Disponibilité

Affiche le nombre de SVM en activité (●) ou vers le bas (●) dans le cluster.

Interfaces réseau

- Disponibilité

Affiche le nombre de LIF non-données qui sont en service (●) ou vers le bas (●) dans le cluster.

- Interfaces de gestion de cluster

Affiche le nombre de LIF de gestion de cluster.

- Interfaces de gestion des nœuds

Affiche le nombre de LIF de gestion de nœuds.

- Interfaces de cluster

Affiche le nombre de LIF de cluster.

- Interfaces interclusters

Affiche le nombre de LIF interclusters.

Protocoles

- Protocoles de données

Affiche la liste des protocoles de données sous licence activés pour le cluster. Les protocoles de données incluent iSCSI, CIFS, NFS, NVMe et FC/FCoE.

Protection

- Médiateurs

Affiche si le cluster prend en charge les médiateurs et l'état de connectivité du médiateur. Il indique si le médiateur est configuré et, s'il est configuré, il affiche l'état des médiateurs.

- Non applicable

S'affiche lorsque le cluster ne prend pas en charge les médiateurs.

- Non configuré

S'affiche lorsque le cluster prend en charge les médiateurs, mais que le médiateur n'est pas configuré.

- Adresse IP

S'affiche lorsque le cluster prend en charge les médiateurs et que le médiateur est configuré. Le statut du médiateur est indiqué par la couleur. La couleur verte indique que le statut du médiateur est accessible. La couleur rouge indique que le statut du médiateur est inaccessible.

Niveaux de cloud

Répertorie les noms des niveaux de cloud auxquels ce cluster est connecté. Il répertorie également le type (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage ou StorageGRID) et les états des niveaux de cloud (disponible ou indisponible).

Onglet Connectivité MetroCluster

Affiche les problèmes et l'état de connectivité des composants du cluster dans la configuration MetroCluster sur FC. Un cluster s'affiche dans une case rouge lorsque le partenaire de reprise après sinistre du cluster rencontre des problèmes.



L'onglet Connectivité MetroCluster s'affiche uniquement pour les clusters qui se trouvent dans une configuration MetroCluster sur FC.

Vous pouvez accéder à la page de détails d'un cluster distant en cliquant sur le nom du cluster distant. Vous pouvez également afficher les détails des composants en cliquant sur le lien de comptage d'un composant. Par exemple, cliquer sur le lien de comptage du nœud dans le cluster affiche l'onglet du nœud dans la page de détails du cluster. Cliquer sur le lien de comptage des disques du cluster distant affiche l'onglet disque dans la page de détails du cluster distant.



Lors de la gestion d'une configuration MetroCluster à huit nœuds, cliquer sur le lien de comptage du composant Étagères de disques affiche uniquement les étagères locales de la paire HA par défaut. De plus, il n'existe aucun moyen d'afficher les étagères locales sur l'autre paire HA.

Vous pouvez déplacer le pointeur sur les composants pour afficher les détails et l'état de connectivité des clusters en cas de problème et pour afficher plus d'informations sur l'événement ou les événements générés pour le problème.

Si l'état du problème de connectivité entre les composants est déterminé par un seul événement, vous pouvez afficher des informations telles que le nom de l'événement, l'heure et la date de déclenchement de l'événement, le nom de l'administrateur auquel l'événement est attribué et la cause de l'événement. Le bouton **Afficher les détails** fournit plus d'informations sur l'événement.

Si l'état du problème de connectivité entre les composants est déterminé par plusieurs événements de même gravité, les trois principaux événements sont affichés avec des informations telles que le nom de l'événement, l'heure et la date de déclenchement des événements et le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également cliquer sur le lien **Afficher tous les événements** pour afficher la liste des événements générés.

Onglet Réplication MetroCluster

Affiche l'état des données en cours de réplication dans une configuration MetroCluster sur FC. Vous pouvez utiliser l'onglet Réplication MetroCluster pour garantir la protection des données en mettant en miroir de manière synchrone les données avec les clusters déjà appariés. Un cluster s'affiche dans une case rouge lorsque le partenaire de reprise après sinistre du cluster rencontre des problèmes.



L'onglet Réplication MetroCluster s'affiche uniquement pour les clusters qui se trouvent dans une configuration MetroCluster sur FC.

Dans un environnement MetroCluster, vous pouvez utiliser cet onglet pour vérifier les connexions logiques et le peering du cluster local avec le cluster distant. Vous pouvez visualiser la représentation objective des composants du cluster avec leurs connexions logiques. Cela permet d'identifier les problèmes qui peuvent survenir lors de la mise en miroir des métadonnées et des données.

Dans l'onglet Réplication MetroCluster, le cluster local fournit la représentation graphique détaillée du cluster sélectionné et le partenaire MetroCluster fait référence au cluster distant.

Onglet Interfaces réseau

Affiche les détails sur tous les LIF non liés aux données créés sur le cluster sélectionné.

Interface réseau

Affiche le nom du LIF créé sur le cluster sélectionné.

État opérationnel

Affiche l'état opérationnel de l'interface, qui peut être Up (🟢), Vers le bas (🔴), ou Inconnu (🔵). L'état opérationnel d'une interface réseau est déterminé par l'état de ses ports physiques.

Statut administratif

Affiche l'état administratif de l'interface, qui peut être Up (🟢), Vers le bas (🔴), ou Inconnu (🔵). Vous pouvez contrôler l'état administratif d'une interface lorsque vous apportez des modifications à la configuration ou pendant la maintenance. Le statut administratif peut être différent du statut opérationnel. Cependant, si le statut administratif d'un LIF est en panne, le statut opérationnel est en panne par défaut.

Adresse IP

Affiche l'adresse IP de l'interface.

Rôle

Affiche le rôle de l'interface. Les rôles possibles sont les LIF de gestion de cluster, les LIF de gestion de nœud, les LIF de cluster et les LIF intercluster.

Port d'attache

Affiche le port physique auquel l'interface était initialement associée.

Port actuel

Affiche le port physique auquel l'interface est actuellement associée. Après la migration LIF, le port actuel peut être différent du port d'origine.

Politique de basculement

Affiche la stratégie de basculement configurée pour l'interface.

Groupes de routage

Affiche le nom du groupe de routage. Vous pouvez afficher plus d'informations sur les itinéraires et la passerelle de destination en cliquant sur le nom du groupe de routage.

Les groupes de routage ne sont pas pris en charge pour ONTAP 8.3 ou version ultérieure et, par conséquent, une colonne vide s'affiche pour ces clusters.

Groupe de basculement

Affiche le nom du groupe de basculement.

Onglet Nœuds

Affiche des informations sur les nœuds du cluster sélectionné. Vous pouvez afficher des informations détaillées sur les paires HA, les étagères de disques et les ports :

Détails HA

Fournit une représentation graphique de l'état HA et de l'état de santé des nœuds de la paire HA. L'état de santé du nœud est indiqué par les couleurs suivantes :

- **Vert**

Le nœud est en état de fonctionnement.

- **Jaune**

Le nœud a pris le contrôle du nœud partenaire ou le nœud est confronté à des problèmes environnementaux.

- **Rouge**

Le nœud est en panne.

Vous pouvez consulter les informations sur la disponibilité de la paire HA et prendre les mesures nécessaires pour éviter tout risque. Par exemple, dans le cas d'une éventuelle opération de reprise, le message suivant s'affiche : Basculement de stockage possible.

Vous pouvez afficher une liste des événements liés à la paire HA et à son environnement, tels que les ventilateurs, les blocs d'alimentation, la batterie NVRAM, les cartes flash, le processeur de service et la connectivité des étagères de disques. Vous pouvez également afficher l'heure à laquelle les événements ont été déclenchés.

Vous pouvez afficher d'autres informations liées au nœud, telles que le numéro de modèle.

S'il existe des clusters à nœud unique, vous pouvez également afficher les détails sur les nœuds.

Étagères à disques

Affiche des informations sur les étagères de disques dans la paire HA.

Vous pouvez également afficher les événements générés pour les étagères de disques et les composants environnementaux, ainsi que l'heure à laquelle les événements ont été déclenchés.

- **ID d'étagère**

Affiche l'ID de l'étagère où se trouve le disque.

- **État du composant**

Affiche les détails environnementaux des étagères de disques, tels que les blocs d'alimentation, les ventilateurs, les capteurs de température, les capteurs de courant, la connectivité du disque et les capteurs de tension. Les détails environnementaux sont affichés sous forme d'icônes dans les couleurs suivantes :

- **Vert**

Les composants environnementaux fonctionnent correctement.

- **Gris**

Aucune donnée n'est disponible pour les composants environnementaux.

- **Rouge**

Certains composants environnementaux sont en panne.

- **État**

Affiche l'état de l'étagère de disque. Les états possibles sont Hors ligne, En ligne, Aucun statut, Initialisation requise, Manquant et Inconnu.

- **Modèle**

Affiche le numéro de modèle de l'étagère de disque.

- **Étagère de disque local**

Indique si l'étagère de disques est située sur le cluster local ou sur le cluster distant. Cette colonne

s'affiche uniquement pour les clusters dans une configuration MetroCluster .

- **ID unique**

Affiche l'identifiant unique de l'étagère de disque.

- **Version du micrologiciel**

Affiche la version du micrologiciel de l'étagère de disque.

Ports

Affiche des informations sur les ports FC, FCoE et Ethernet associés. Vous pouvez afficher les détails sur les ports et les LIF associés en cliquant sur les icônes de port.

Vous pouvez également visualiser les événements générés pour les ports.

Vous pouvez afficher les détails du port suivants :

- **ID du port**

Affiche le nom du port. Par exemple, les noms de port peuvent être e0M, e0a et e0b.

- **Rôle**

Affiche le rôle du port. Les rôles possibles sont Cluster, Données, Intercluster, Gestion des nœuds et Non défini.

- **Type**

Affiche le protocole de couche physique utilisé pour le port. Les types possibles sont Ethernet, Fibre Channel et FCoE.

- **WWPN**

Affiche le nom du port mondial (WWPN) du port.

- **Révision du micrologiciel**

Affiche la révision du firmware du port FC/FCoE.

- **Statut**

Affiche l'état actuel du port. Les états possibles sont Haut, Bas, Lien non connecté ou Inconnu (?).

Vous pouvez consulter les événements liés au port à partir de la liste des événements. Vous pouvez également afficher les détails LIF associés, tels que le nom LIF, l'état opérationnel, l'adresse IP ou WWPN, les protocoles, le nom du SVM associé au LIF, le port actuel, la politique de basculement et le groupe de basculement.

Onglet Disques

Affiche les détails sur les disques du cluster sélectionné. Vous pouvez afficher des informations relatives aux disques, telles que le nombre de disques utilisés, de disques de rechange, de disques cassés et de disques non attribués. Vous pouvez également afficher d'autres détails tels que le nom du disque, le type de disque et

le nœud propriétaire du disque.

Résumé du pool de disques

Affiche le nombre de disques, classés par types effectifs (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN et VMDISK) et l'état des disques. Vous pouvez également afficher d'autres détails, tels que le nombre d'agrégats, de disques partagés, de disques de rechange, de disques cassés, de disques non attribués et de disques non pris en charge. Si vous cliquez sur le lien de comptage du type de disque effectif, les disques de l'état sélectionné et du type effectif s'affichent. Par exemple, si vous cliquez sur le lien de comptage pour l'état du disque Cassé et le type effectif SAS, tous les disques avec l'état du disque Cassé et le type effectif SAS sont affichés.

Disque

Affiche le nom du disque.

Groupe RAID

Affiche le nom du groupe RAID.

Nœud propriétaire

Affiche le nom du nœud auquel appartient le disque. Si le disque n'est pas attribué, aucune valeur n'est affichée dans cette colonne.

État

Affiche l'état du disque : agrégé, partagé, de secours, cassé, non attribué, non pris en charge ou inconnu. Par défaut, cette colonne est triée pour afficher les états dans l'ordre suivant : Cassé, Non attribué, Non pris en charge, De secours, Agrégé et Partagé.

Disque local

Affiche Oui ou Non pour indiquer si le disque est situé sur le cluster local ou le cluster distant. Cette colonne s'affiche uniquement pour les clusters dans une configuration MetroCluster .

Position

Affiche la position du disque en fonction de son type de conteneur : par exemple, Copie, Données ou Parité. Par défaut, cette colonne est masquée.

Agrégats impactés

Affiche le nombre d'agrégats impactés en raison du disque défaillant. Vous pouvez déplacer le pointeur sur le lien de comptage pour afficher les agrégats impactés, puis cliquer sur le nom de l'agrégat pour afficher les détails de l'agrégat. Vous pouvez également cliquer sur le nombre total d'agrégats pour afficher la liste des agrégats impactés dans la vue Santé : Tous les agrégats.

Aucune valeur n'est affichée dans cette colonne pour les cas suivants :

- Pour les disques cassés lorsqu'un cluster contenant de tels disques est ajouté à Unified Manager
- Lorsqu'il n'y a pas de disques défaillants

Piscine de stockage

Affiche le nom du pool de stockage auquel appartient le SSD. Vous pouvez déplacer le pointeur sur le nom du pool de stockage pour afficher les détails du pool de stockage.

Capacité de stockage

Affiche la capacité du disque disponible pour utilisation.

Capacité brute

Affiche la capacité du disque brut non formaté avant le dimensionnement et la configuration RAID. Par défaut, cette colonne est masquée.

Type

Affiche les types de disques : par exemple, ATA, SATA, FCAL ou VMDISK.

Type efficace

Affiche le type de disque attribué par ONTAP.

Certains types de disques ONTAP sont considérés comme équivalents aux fins de création et d'ajout d'agrégats et de gestion des disques de secours. ONTAP attribue un type de disque effectif à chaque type de disque.

Blocs de rechange consommés %

Affiche en pourcentage les blocs de rechange consommés dans le disque SSD. Cette colonne est vide pour les disques autres que les disques SSD.

Durée de vie nominale utilisée %

Affiche en pourcentage une estimation de la durée de vie du SSD utilisé, basée sur l'utilisation réelle du SSD et la prévision du fabricant concernant la durée de vie du SSD. Une valeur supérieure à 99 indique que l'endurance estimée a été consommée, mais peut ne pas indiquer une défaillance du SSD. Si la valeur est inconnue, le disque est omis.

Micrologiciel

Affiche la version du firmware du disque.

tr/min

Affiche les tours par minute (RPM) du disque. Par défaut, cette colonne est masquée.

Modèle

Affiche le numéro de modèle du disque. Par défaut, cette colonne est masquée.

Fournisseur

Affiche le nom du fournisseur du disque. Par défaut, cette colonne est masquée.

ID d'étagère

Affiche l'ID de l'étagère où se trouve le disque.

Compartiment

Affiche l'ID de la baie où se trouve le disque.

Volet Annotations associées

Vous permet d'afficher les détails d'annotation associés au cluster sélectionné. Les détails incluent le nom de l'annotation et les valeurs d'annotation appliquées au cluster. Vous pouvez également supprimer les annotations manuelles du volet Annotations associées.

Volet Appareils associés

Vous permet d'afficher les détails des périphériques associés au cluster sélectionné.

Les détails incluent les propriétés du périphérique connecté au cluster, telles que le type de périphérique, la taille, le nombre et l'état de santé. Vous pouvez cliquer sur le lien de comptage pour une analyse plus approfondie sur cet appareil particulier.

Vous pouvez utiliser le volet Partenaire MetroCluster pour obtenir le nombre et les détails sur le partenaire MetroCluster distant ainsi que ses composants de cluster associés tels que les nœuds, les agrégats et les SVM. Le volet Partenaire MetroCluster s'affiche uniquement pour les clusters dans une configuration MetroCluster .

Le volet Périphériques associés vous permet d'afficher et de naviguer vers les nœuds, les SVM et les agrégats associés au cluster :

Partenaire MetroCluster

Affiche l'état de santé du partenaire MetroCluster . À l'aide du lien de comptage, vous pouvez naviguer plus loin et obtenir des informations sur l'état et la capacité des composants du cluster.

Nœuds

Affiche le nombre, la capacité et l'état de santé des nœuds appartenant au cluster sélectionné. La capacité indique la capacité totale utilisable par rapport à la capacité disponible.

Machines virtuelles de stockage

Affiche le nombre de SVM appartenant au cluster sélectionné.

Agrégats

Affiche le nombre, la capacité et l'état de santé des agrégats appartenant au cluster sélectionné.

Volet Groupes associés

Vous permet d'afficher la liste des groupes qui incluent le cluster sélectionné.

Volet Alertes associées

Le volet Alertes associées vous permet d'afficher la liste des alertes pour le cluster sélectionné. Vous pouvez

également ajouter une alerte en cliquant sur le lien [Ajouter une alerte](#) ou modifier une alerte existante en cliquant sur le nom de l'alerte.

Informations connexes

["Page des volumes"](#) ["Affichage de la liste et des détails des clusters"](#)

Page de détails sur l'agrégat / la santé

Vous pouvez utiliser la page Détails de l'agrégat / de l'état de santé pour afficher des informations détaillées sur l'agrégat sélectionné, telles que la capacité, les informations sur le disque, les détails de configuration et les événements générés. Vous pouvez également afficher des informations sur les objets associés et les alertes associées pour cet agrégat.

Boutons de commande



Lors de la surveillance d'un agrégat compatible FabricPool, les valeurs engagées et surengagées sur cette page ne concernent que la capacité locale ou de niveau de performance. La quantité d'espace disponible dans le niveau cloud n'est pas reflétée dans les valeurs surengagées. De même, les valeurs seuils agrégées ne concernent que le niveau de performance local.

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour l'agrégat sélectionné :

- **Passer à la vue Performances**

Vous permet d'accéder à la page Détails de l'agrégat / des performances.

- **Actes**

- Ajouter une alerte

Vous permet d'ajouter une alerte à l'agrégat sélectionné.

- Modifier les seuils

Vous permet de modifier les paramètres de seuil pour l'agrégat sélectionné.

- **Voir les agrégats**

Vous permet d'accéder à la vue Santé : Tous les agrégats.

Onglet Capacité

L'onglet Capacité affiche des informations détaillées sur l'agrégat sélectionné, telles que sa capacité, ses seuils et son taux de croissance quotidien.

Par défaut, les événements de capacité ne sont pas générés pour les agrégats racine. De plus, les valeurs de seuil utilisées par Unified Manager ne s'appliquent pas aux agrégats de racines de nœuds. Seul un représentant du support technique peut modifier les paramètres pour que ces événements soient générés. Lorsque les paramètres sont modifiés par un représentant du support technique, les valeurs de seuil sont appliquées à l'agrégat racine du nœud.

- **Capacité**

Affiche le graphique de capacité des données et le graphique des copies d'instantanés, qui affichent les détails de capacité de l'agrégat :

- Espace logique utilisé

La taille réelle des données stockées dans l'agrégat sans appliquer les économies réalisées grâce à l'utilisation des technologies d'efficacité de stockage ONTAP .

- Utilisé

La capacité physique utilisée par les données dans leur ensemble.

- Surengagé

Lorsque l'espace dans l'agrégat est surengagé, le graphique affiche un indicateur avec le montant surengagé.

- Avertissement

Affiche une ligne pointillée à l'emplacement où le seuil d'avertissement est défini ; ce qui signifie que l'espace dans l'agrégat est presque plein. Si ce seuil est dépassé, l'événement Espace presque plein est généré.

- Erreur

Affiche une ligne continue à l'emplacement où le seuil d'erreur est défini ; ce qui signifie que l'espace dans l'agrégat est plein. Si ce seuil est dépassé, l'événement Espace plein est généré.

- Graphique des copies instantanées

Ce graphique s'affiche uniquement lorsque la capacité Snapshot utilisée ou la réserve Snapshot n'est pas nulle.

Les deux graphiques affichent la capacité par laquelle la capacité de Snapshot dépasse la réserve de Snapshot si la capacité de Snapshot utilisée dépasse la réserve de Snapshot.

- **Niveau Cloud**

Affiche l'espace utilisé par les données dans le niveau cloud pour les agrégats compatibles FabricPool. Un FabricPool peut être sous licence ou sans licence.

Lorsque le niveau cloud est mis en miroir sur un autre fournisseur cloud (le « niveau miroir »), les deux niveaux cloud sont affichés ici.

- **Détails**

Affiche des informations détaillées sur la capacité.

- Capacité totale

Affiche la capacité totale dans l'ensemble.

- Capacité de données

Affiche la quantité d'espace utilisée par l'agrégat (capacité utilisée) et la quantité d'espace disponible dans l'agrégat (capacité libre).

- Réserve instantanée

Affiche la capacité Snapshot utilisée et libre de l'agrégat.

- Capacité surengagée

Affiche le surengagement global. Le surengagement global vous permet de fournir plus de stockage que ce qui est réellement disponible à partir d'un agrégat donné, à condition que la totalité de ce stockage ne soit pas actuellement utilisée. Lorsque le provisionnement léger est utilisé, la taille totale des volumes de l'agrégat peut dépasser la capacité totale de l'agrégat.



Si vous avez surchargé votre agrégat, vous devez surveiller attentivement son espace disponible et ajouter du stockage si nécessaire pour éviter les erreurs d'écriture dues à un espace insuffisant.

- Niveau Cloud

Affiche l'espace utilisé par les données dans le niveau cloud pour les agrégats compatibles FabricPool. Un FabricPool peut être sous licence ou sans licence. Lorsque le niveau cloud est mis en miroir sur un autre fournisseur de cloud (le niveau miroir), les deux niveaux cloud sont affichés ici

- Espace cache total

Affiche l'espace total des disques SSD ou des unités d'allocation ajoutés à un agrégat Flash Pool. Si vous avez activé Flash Pool pour un agrégat mais n'avez ajouté aucun SSD, l'espace de cache s'affiche comme 0 Ko.



Ce champ est masqué si Flash Pool est désactivé pour un agrégat.

- Seuils agrégés

Affiche les seuils de capacité globale suivants :

- Seuil presque plein

Spécifie le pourcentage auquel un agrégat est presque plein.

- Seuil complet

Spécifie le pourcentage auquel un agrégat est plein.

- Seuil de quasi-dépassement d'engagement

Spécifie le pourcentage auquel un agrégat est presque sur-engagé.

- Seuil de surengagement

Spécifie le pourcentage auquel un agrégat est surengagé.

- Autres détails : Taux de croissance quotidien

Affiche l'espace disque utilisé dans l'ensemble si le taux de changement entre les deux derniers

échantillons se poursuit pendant 24 heures.

Par exemple, si un agrégat utilise 10 Go d'espace disque à 14 h et 12 Go à 18 h, le taux de croissance quotidien (Go) de cet agrégat est de 2 Go.

- Déplacement du volume

Affiche le nombre d'opérations de déplacement de volume actuellement en cours :

- Volumes sortis

Affiche le nombre et la capacité des volumes qui sont déplacés hors de l'agrégat.

Vous pouvez cliquer sur le lien pour afficher plus de détails, tels que le nom du volume, l'agrégat vers lequel le volume est déplacé, l'état de l'opération de déplacement du volume et l'heure de fin estimée.

- Volumes en

Affiche le nombre et la capacité restante des volumes qui sont déplacés vers l'agrégat.

Vous pouvez cliquer sur le lien pour afficher plus de détails, tels que le nom du volume, l'agrégat à partir duquel le volume est déplacé, l'état de l'opération de déplacement du volume et l'heure de fin estimée.

- Capacité utilisée estimée après le déplacement du volume

Affiche la quantité estimée d'espace utilisé (en pourcentage et en Ko, Mo, Go, etc.) dans l'ensemble une fois les opérations de déplacement de volume terminées.

- **Aperçu des capacités - Volumes**

Affiche des graphiques qui fournissent des informations sur la capacité des volumes contenus dans l'agrégat. La quantité d'espace utilisée par le volume (capacité utilisée) et la quantité d'espace disponible (capacité libre) dans le volume sont affichées. Lorsque l'événement d'espace de volume à provisionnement fin à risque est généré pour les volumes à provisionnement fin, la quantité d'espace utilisée par le volume (capacité utilisée) et la quantité d'espace disponible dans le volume mais qui ne peut pas être utilisée (capacité inutilisable) en raison de problèmes de capacité globale s'affichent.

Vous pouvez sélectionner le graphique que vous souhaitez afficher dans les listes déroulantes. Vous pouvez trier les données affichées dans le graphique pour afficher des détails tels que la taille utilisée, la taille provisionnée, la capacité disponible, le taux de croissance quotidien le plus rapide et le taux de croissance le plus lent. Vous pouvez filtrer les données en fonction des machines virtuelles de stockage (SVM) qui contiennent les volumes dans l'agrégat. Vous pouvez également afficher les détails des volumes provisionnés de manière fine. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur la zone d'intérêt. Par défaut, le graphique affiche les 30 premiers volumes filtrés dans l'ensemble.

Onglet Informations sur le disque

Affiche des informations détaillées sur les disques de l'agrégat sélectionné, y compris le type et la taille du RAID, ainsi que le type de disques utilisés dans l'agrégat. L'onglet affiche également graphiquement les groupes RAID et les types de disques utilisés (tels que SAS, ATA, FCAL, SSD ou VMDISK). Vous pouvez afficher plus d'informations, telles que la baie du disque, l'étagère et la vitesse de rotation, en positionnant votre curseur sur les disques de parité et les disques de données.

- **Données**

Affiche graphiquement les détails sur les disques de données dédiés, les disques de données partagés ou les deux. Lorsque les disques de données contiennent des disques partagés, les détails graphiques des disques partagés sont affichés. Lorsque les disques de données contiennent des disques dédiés et des disques partagés, les détails graphiques des disques de données dédiés et des disques de données partagés sont affichés.

- **Détails du RAID**

Les détails RAID ne sont affichés que pour les disques dédiés.

- Type

Affiche le type de RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

- Taille du groupe

Affiche le nombre maximal de disques autorisés dans le groupe RAID.

- Groupes

Affiche le nombre de groupes RAID dans l'ensemble.

- **Disques utilisés**

- Type efficace

Affiche les types de disques de données (par exemple, ATA, SATA, FCAL, SSD ou VMDISK) dans l'ensemble.

- Disques de données

Affiche le nombre et la capacité des disques de données attribués à un agrégat. Les détails du disque de données ne s'affichent pas lorsque l'agrégat contient uniquement des disques partagés.

- Disques de parité

Affiche le nombre et la capacité des disques de parité attribués à un agrégat. Les détails du disque de parité ne s'affichent pas lorsque l'agrégat contient uniquement des disques partagés.

- Disques partagés

Affiche le nombre et la capacité des disques de données partagés attribués à un agrégat. Les détails du disque partagé s'affichent uniquement lorsque l'agrégat contient des disques partagés.

- **Disques de rechange**

Affiche le type effectif de disque, le nombre et la capacité des disques de données de rechange disponibles pour le nœud dans l'agrégat sélectionné.



Lorsqu'un agrégat est basculé vers le nœud partenaire, Unified Manager n'affiche pas tous les disques de rechange compatibles avec l'agrégat.

- **Cache SSD**

Fournit des détails sur les disques SSD à cache dédié et les disques SSD à cache partagé.

Les détails suivants concernant les disques SSD à cache dédié sont affichés :

- **Détails du RAID**

- Type

- Affiche le type RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

- Taille du groupe

- Affiche le nombre maximal de disques autorisés dans le groupe RAID.

- Groupes

- Affiche le nombre de groupes RAID dans l'ensemble.

- **Disques utilisés**

- Type efficace

- Indique que les disques utilisés pour le cache dans l'ensemble sont de type SSD.

- Disques de données

- Affiche le nombre et la capacité des disques de données attribués à un agrégat pour le cache.

- Disques de parité

- Affiche le nombre et la capacité des disques de parité attribués à un agrégat pour le cache.

- **Disques de rechange**

Affiche le type effectif de disque, le nombre et la capacité des disques de rechange disponibles pour le nœud dans l'agrégat sélectionné pour le cache.



Lorsqu'un agrégat est basculé vers le nœud partenaire, Unified Manager n'affiche pas tous les disques de rechange compatibles avec l'agrégat.

Fournit les détails suivants pour le cache partagé :

- **Piscine de stockage**

Affiche le nom du pool de stockage. Vous pouvez déplacer le pointeur sur le nom du pool de stockage pour afficher les détails suivants :

- Statut

- Affiche l'état du pool de stockage, qui peut être sain ou non.

- Total des allocations

- Affiche le nombre total d'unités d'allocation et la taille du pool de stockage.

- Taille de l'unité d'allocation

- Affiche la quantité minimale d'espace dans le pool de stockage qui peut être allouée à un agrégat.

- **Disques**

Affiche le nombre de disques utilisés pour créer le pool de stockage. Si le nombre de disques dans la colonne du pool de stockage et le nombre de disques affichés dans l'onglet Informations sur le disque pour ce pool de stockage ne correspondent pas, cela indique qu'un ou plusieurs disques sont défectueux et que le pool de stockage n'est pas sain.

- **Allocation utilisée**

Affiche le nombre et la taille des unités d'allocation utilisées par les agrégats. Vous pouvez cliquer sur le nom de l'agrégat pour afficher les détails de l'agrégat.

- **Allocation disponible**

Affiche le nombre et la taille des unités d'allocation disponibles pour les nœuds. Vous pouvez cliquer sur le nom du nœud pour afficher les détails agrégés.

- **Cache alloué**

Affiche la taille des unités d'allocation utilisées par l'agrégat.

- **Unités d'allocation**

Affiche le nombre d'unités d'allocation utilisées par l'agrégat.

- **Disques**

Affiche le nombre de disques contenus dans le pool de stockage.

- **Détails**

- **Piscine de stockage**

Affiche le nombre de pools de stockage.

- **Taille totale**

Affiche la taille totale des pools de stockage.

- **Niveau Cloud**

Affiche le nom du niveau cloud, si vous avez configuré un agrégat compatible FabricPool, et affiche l'espace total utilisé. Lorsque le niveau cloud est mis en miroir sur un autre fournisseur de cloud (le niveau miroir), les détails des deux niveaux cloud sont affichés ici

Onglet Configuration

L'onglet Configuration affiche des détails sur l'agrégat sélectionné, tels que son nœud de cluster, son type de bloc, son type de RAID, sa taille et son nombre de groupes RAID :

- **Aperçu**

- **Nœud**

Affiche le nom du nœud qui contient l'agrégat sélectionné.

- Type de bloc

Affiche le format de bloc de l'agrégat : 32 bits ou 64 bits.

- Type RAID

Affiche le type de RAID (RAID0, RAID4, RAID-DP, RAID-TEC ou RAID mixte).

- Taille de la RAID

Affiche la taille du groupe RAID.

- Groupes RAID

Affiche le nombre de groupes RAID dans l'ensemble.

- Type de SnapLock

Affiche le type SnapLock de l'agrégat.

- **Niveau Cloud**

S'il s'agit d'un agrégat compatible FabricPool, les détails du niveau cloud sont affichés. Certains champs sont différents selon le fournisseur de stockage. Lorsque le niveau cloud est mis en miroir sur un autre fournisseur cloud (le « niveau miroir »), les deux niveaux cloud sont affichés ici.

- Fournisseur

Affiche le nom du fournisseur de stockage, par exemple, StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage ou Alibaba Cloud Object Storage.

- Nom

Affiche le nom du niveau cloud lors de sa création par ONTAP.

- Serveur

Affiche le nom de domaine complet du niveau cloud.

- Port

Le port utilisé pour communiquer avec le fournisseur de cloud.

- Clé d'accès ou compte

Affiche la clé d'accès ou le compte pour le niveau cloud.

- Nom du conteneur

Affiche le nom du bucket ou du conteneur du niveau cloud.

- SSL

Affiche si le cryptage SSL est activé pour le niveau cloud.

Espace historique

La zone Historique affiche des graphiques qui fournissent des informations sur la capacité de l'agrégat sélectionné. De plus, vous pouvez cliquer sur le bouton **Exporter** pour créer un rapport au format CSV pour le graphique que vous visualisez.

Vous pouvez sélectionner un type de graphique dans la liste déroulante en haut du volet Historique. Vous pouvez également afficher les détails d'une période spécifique en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques d'historique peuvent vous aider à identifier les tendances : par exemple, si l'utilisation globale dépasse systématiquement le seuil presque plein, vous pouvez prendre les mesures appropriées.

Les graphiques d'historique affichent les informations suivantes :

- **Capacité globale utilisée (%)**

Affiche la capacité utilisée dans l'ensemble et la tendance d'utilisation de la capacité globale en fonction de l'historique d'utilisation sous forme de graphiques linéaires, en pourcentage, sur l'axe vertical (y). La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Capacité utilisée, la ligne du graphique Capacité utilisée est masquée.

- **Capacité globale utilisée par rapport à la capacité totale**

Affiche la tendance d'utilisation de la capacité globale en fonction de l'historique d'utilisation, ainsi que la capacité utilisée et la capacité totale, sous forme de graphiques linéaires, en octets, kilo-octets, mégaoctets, etc., sur l'axe vertical (y). La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Capacité de tendance utilisée, la ligne du graphique Capacité de tendance utilisée est masquée.

- **Capacité globale utilisée (%) par rapport à la capacité engagée (%)**

Affiche la tendance d'utilisation de la capacité globale en fonction de l'historique d'utilisation, ainsi que l'espace engagé sous forme de graphiques linéaires, en pourcentage, sur l'axe vertical (y). La période de temps est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Espace engagé, la ligne du graphique Espace engagé est masquée.

Liste des événements

La liste des événements affiche des détails sur les événements nouveaux et reconnus :

- **Gravité**

Affiche la gravité de l'événement.

- **Événement**

Affiche le nom de l'événement.

- **Heure déclenchée**

Affiche le temps écoulé depuis que l'événement a été généré. Si le temps écoulé dépasse une semaine, l'horodatage de la génération de l'événement est affiché.

Volet Appareils associés

Le volet Périphériques associés vous permet d'afficher le nœud de cluster, les volumes et les disques associés à l'agrégat :

- **Nœud**

Affiche la capacité et l'état de santé du nœud qui contient l'agrégat. La capacité indique la capacité totale utilisable par rapport à la capacité disponible.

- **Agrégats dans le nœud**

Affiche le nombre et la capacité de tous les agrégats dans le nœud de cluster qui contient l'agrégat sélectionné. L'état de santé des agrégats est également affiché, en fonction du niveau de gravité le plus élevé. Par exemple, si un nœud de cluster contient dix agrégats, dont cinq affichent l'état Avertissement et les cinq autres l'état Critique, l'état affiché est Critique.

- **Volumes**

Affiche le nombre et la capacité des volumes FlexVol et des volumes FlexGroup dans l'ensemble ; le nombre n'inclut pas les constituants FlexGroup . L'état de santé des volumes est également affiché, en fonction du niveau de gravité le plus élevé.

- **Réserve de ressources**

Affiche les pools de ressources liés à l'agrégat.

- **Disques**

Affiche le nombre de disques dans l'agrégat sélectionné.

Volet Alertes associées

Le volet Alertes associées vous permet d'afficher la liste des alertes créées pour l'agrégat sélectionné. Vous pouvez également ajouter une alerte en cliquant sur le lien Ajouter une alerte ou modifier une alerte existante en cliquant sur le nom de l'alerte.

Informations connexes

["Affichage des détails du pool de stockage"](#)

Protéger et restaurer les données

Créer, surveiller et dépanner les relations de protection

Unified Manager vous permet de créer des relations de protection, de surveiller et de dépanner la protection miroir et la protection du coffre de sauvegarde des données stockées sur des clusters gérés, et de restaurer les données lorsqu'elles sont écrasées ou perdues.

Types de protection SnapMirror

Selon le déploiement de votre topologie de stockage de données, Unified Manager vous permet de configurer plusieurs types de relations de protection SnapMirror. Toutes les variantes de la protection SnapMirror offrent une protection de reprise après sinistre en cas de basculement, mais offrent des capacités différentes en termes de performances, de flexibilité de version et de protection contre les copies de sauvegarde multiples.

Relations de protection asynchrones SnapMirror traditionnelles

La protection asynchrone SnapMirror traditionnelle fournit une protection de miroir de réplication de blocs entre les volumes source et de destination.

Dans les relations SnapMirror traditionnelles, les opérations de miroir s'exécutent plus rapidement que dans les relations SnapMirror alternatives, car l'opération de miroir est basée sur la réplication de blocs. Cependant, la protection SnapMirror traditionnelle nécessite que le volume de destination s'exécute sous la même version mineure ou une version ultérieure du logiciel ONTAP que le volume source dans la même version majeure (par exemple, version 8.x à 8.x ou 9.x à 9.x). La réplication d'une source 9.1 vers une destination 9.0 n'est pas prise en charge car la destination exécute une version majeure antérieure.

Protection asynchrone SnapMirror avec réplication flexible en fonction des versions

La protection asynchrone SnapMirror avec réplication flexible en fonction des versions fournit une protection de miroir de réplication logique entre les volumes source et de destination, même si ces volumes s'exécutent sous différentes versions du logiciel ONTAP 8.3 ou ultérieure (par exemple, version 8.3 à 8.3.1, ou 8.3 à 9.1, ou 9.2.2 à 9.2).

Dans les relations SnapMirror avec réplication flexible en fonction des versions, les opérations de mise en miroir ne s'exécutent pas aussi rapidement qu'elles le feraient dans les relations SnapMirror traditionnelles.

En raison d'une exécution plus lente, SnapMirror avec protection de réplication flexible en fonction des versions n'est pas adapté à la mise en œuvre dans l'une ou l'autre des circonstances suivantes :

- L'objet source contient plus de 10 millions de fichiers à protéger.
- L'objectif du point de récupération pour les données protégées est de deux heures ou moins. (C'est-à-dire que la destination doit toujours contenir des données en miroir récupérables qui ne sont pas plus anciennes de deux heures que les données de la source.)

Dans l'une ou l'autre des circonstances répertoriées, l'exécution plus rapide basée sur la réplication de blocs de la protection SnapMirror par défaut est requise.

Protection asynchrone SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions

La protection asynchrone SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions offre une protection miroir entre les volumes source et de destination et la possibilité de stocker plusieurs copies des données en miroir à la destination.

L'administrateur de stockage peut spécifier quelles copies Snapshot sont mises en miroir de la source vers la destination et peut également spécifier la durée de conservation de ces copies à la destination, même si elles sont supprimées à la source.

Dans les relations SnapMirror avec option de réplication et de sauvegarde flexible en fonction des versions, les opérations de mise en miroir ne s'exécutent pas aussi rapidement qu'elles le feraient dans les relations SnapMirror traditionnelles.

Réplication unifiée SnapMirror (miroir et coffre-fort)

La réplication unifiée SnapMirror vous permet de configurer la reprise après sinistre et l'archivage sur le même volume de destination. Comme avec SnapMirror, la protection unifiée des données effectue un transfert de base la première fois que vous l'appellez. Un transfert de base sous la politique de protection des données unifiée par défaut « MirrorAndVault » effectue une copie instantanée du volume source, puis transfère cette copie et les blocs de données auxquels elle fait référence vers le volume de destination. Comme SnapVault, la protection unifiée des données n'inclut pas les anciennes copies Snapshot dans la ligne de base.

SnapMirror Protection synchrone avec synchronisation stricte

La protection synchrone SnapMirror avec synchronisation « stricte » garantit que les volumes principal et secondaire sont toujours une copie conforme l'un de l'autre. Si une erreur de réplication se produit lors de la tentative d'écriture de données sur le volume secondaire, les E/S client sur le volume principal sont interrompues.

SnapMirror Protection synchrone avec synchronisation régulière

La protection synchrone SnapMirror avec synchronisation « régulière » ne nécessite pas que le volume principal et le volume secondaire soient toujours une copie conforme l'un de l'autre, garantissant ainsi la disponibilité du volume principal. Si une erreur de réplication se produit lors de la tentative d'écriture de données sur le volume secondaire, les volumes principal et secondaire ne sont plus synchronisés et les E/S client continuent vers le volume principal.



Le bouton Restaurer et les boutons d'opération Relation ne sont pas disponibles lors de la surveillance des relations de protection synchrones à partir de la vue Santé : Tous les volumes ou de la page Détails Volume/Santé.

Synchronisation active de SnapMirror

La fonctionnalité de synchronisation active SnapMirror est disponible avec ONTAP 9.8 et versions ultérieures, et vous pouvez l'utiliser pour protéger les applications avec des LUN, permettant aux applications de basculer de manière transparente, garantissant ainsi la continuité des activités en cas de sinistre.

Il vous permet de découvrir et de surveiller les relations SnapMirror synchrones pour les groupes de cohérence (CG) disponibles sur les clusters et les machines virtuelles de stockage à partir d'Unified Manager. La synchronisation active SnapMirror est prise en charge sur les clusters AFF ou All SAN Array (ASA), où les clusters principal et secondaire peuvent être AFF ou ASA. SnapMirror Active Sync protège les applications avec des LUN iSCSI ou FCP.

Lorsque vous affichez les volumes et les LUN protégés par la relation de synchronisation active SnapMirror , vous pouvez obtenir une vue unifiée des relations de protection, des groupes de cohérence dans l'inventaire des volumes, afficher la topologie de protection pour les relations de groupe de cohérence, afficher les données historiques pour les relations de groupe de cohérence jusqu'à un an. Vous pouvez également télécharger le rapport. Vous pouvez également afficher le résumé des relations du groupe de cohérence, rechercher de l'aide pour les relations du groupe de cohérence et obtenir des informations sur les volumes protégés par le groupe de cohérence.

Sur la page Relations, vous pouvez également trier, filtrer et étendre la protection des objets de stockage source et de destination et de leur relation qui sont protégés par le groupe de cohérence.

Pour en savoir plus sur la synchronisation active de SnapMirror , reportez-vous à "[Documentation ONTAP 9 pour Snapmirror Active Sync \(anciennement SM-BC\)](#)".

Configurer les relations de protection dans Unified Manager

Vous devez effectuer plusieurs étapes pour utiliser Unified Manager et OnCommand Workflow Automation afin de configurer les relations SnapMirror et SnapVault afin de protéger vos données.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir établi des relations homologues entre deux clusters ou deux machines virtuelles de stockage (SVM).
- OnCommand Workflow Automation doit être intégré à Unified Manager :
 - "[Configurer OnCommand Workflow Automation](#)".
 - "[Vérification de la mise en cache des sources de données d'Unified Manager dans Workflow Automation](#)".

Étapes

1. Selon le type de relation de protection que vous souhaitez créer, effectuez l'une des opérations suivantes :
 - "[Créer une relation de protection SnapMirror](#)".
 - "[Créer une relation de protection SnapVault](#)".
2. Si vous souhaitez créer une politique pour la relation, en fonction du type de relation que vous créez, effectuez l'une des opérations suivantes :
 - "[Créer une politique SnapVault](#)".
 - "[Créer une politique SnapMirror](#)".
3. "[Créer une planification SnapMirror ou SnapVault](#)".

Configurer une connexion entre Workflow Automation et Unified Manager

Vous pouvez configurer une connexion sécurisée entre OnCommand Workflow Automation (WFA) et Unified Manager. La connexion à Workflow Automation vous permet d'utiliser des fonctionnalités de protection telles que les workflows de configuration SnapMirror et SnapVault , ainsi que des commandes de gestion des relations SnapMirror

Avant de commencer

- La version installée de Workflow Automation doit être 5.1.1P6 ou supérieure.



Le « pack WFA pour la gestion des Data ONTAP » est inclus dans WFA 5.1.1P6. Il n'est donc pas nécessaire de télécharger ce pack depuis NetAppStorage Automation Store et de l'installer séparément sur votre serveur WFA comme cela était requis par le passé. "[Pack WFA pour la gestion ONTAP](#)"

- Vous devez disposer du nom de l'utilisateur de base de données que vous avez créé dans Unified Manager pour prendre en charge les connexions WFA et Unified Manager.

Cet utilisateur de base de données doit avoir reçu le rôle d'utilisateur de schéma d'intégration.

- Vous devez disposer du rôle d'administrateur ou du rôle d'architecte dans Workflow Automation.
- Vous devez disposer de l'adresse de l'hôte, du numéro de port 443, du nom d'utilisateur et du mot de passe pour la configuration de Workflow Automation.
- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Automatisation du flux de travail**.
2. Dans la zone **Utilisateur de base de données** de la page **Automatisation du flux de travail**, sélectionnez le nom et entrez le mot de passe de l'utilisateur de base de données que vous avez créé pour prendre en charge les connexions Unified Manager et Workflow Automation.
3. Dans la zone **Informations d'identification d'automatisation du flux de travail** de la page, saisissez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6), ainsi que le nom d'utilisateur et le mot de passe pour la configuration d'automatisation du flux de travail.

Vous devez utiliser le port du serveur Unified Manager (port 443).

4. Cliquez sur **Enregistrer**.
5. Si vous utilisez un certificat auto-signé, cliquez sur **Oui** pour autoriser le certificat de sécurité.

La page Automatisation du flux de travail s'affiche.

6. Cliquez sur **Oui** pour recharger l'interface utilisateur Web et ajouter les fonctionnalités d'automatisation du flux de travail.

Informations connexes

["Documentation NetApp : OnCommand Workflow Automation \(versions actuelles\)"](#)

Vérifier la mise en cache des sources de données d'Unified Manager dans Workflow Automation

Vous pouvez déterminer si la mise en cache de la source de données Unified Manager fonctionne correctement en vérifiant si l'acquisition de la source de données réussit dans Workflow Automation. Vous pouvez le faire lorsque vous intégrez Workflow Automation à Unified Manager pour garantir que la fonctionnalité Workflow Automation est disponible après l'intégration.

Avant de commencer

Vous devez disposer du rôle d'administrateur ou du rôle d'architecte dans Workflow Automation pour effectuer cette tâche.

Étapes

1. Depuis l'interface utilisateur d'automatisation du flux de travail, sélectionnez **Exécution > Sources de données**.
2. Cliquez avec le bouton droit sur le nom de la source de données Unified Manager, puis sélectionnez **Acquérir maintenant**.
3. Vérifiez que l'acquisition réussit sans erreur.

Les erreurs d'acquisition doivent être résolues pour que l'intégration de Workflow Automation avec Unified Manager réussisse.

Que se passe-t-il lorsque OnCommand Workflow Automation est réinstallé ou mis à niveau

Avant de réinstaller ou de mettre à niveau OnCommand Workflow Automation, vous devez d'abord supprimer la connexion entre OnCommand Workflow Automation et Unified Manager et vous assurer que tous les travaux OnCommand Workflow Automation en cours d'exécution ou planifiés sont arrêtés.

Vous devez également supprimer manuellement Unified Manager d' OnCommand Workflow Automation.

Après avoir réinstallé ou mis à niveau OnCommand Workflow Automation, vous devez reconfigurer la connexion avec Unified Manager.

Supprimer la configuration OnCommand Workflow Automation d'Unified Manager

Vous pouvez supprimer la configuration d' OnCommand Workflow Automation d'Unified Manager lorsque vous ne souhaitez plus utiliser Workflow Automation.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général > Automatisation du flux de travail** dans le menu Configuration de gauche.
2. Sur la page **Automatisation du flux de travail**, cliquez sur **Supprimer la configuration**.

Effectuer un basculement et une restauration de la relation de protection

Lorsqu'un volume source de votre relation de protection est désactivé en raison d'une panne matérielle ou d'un sinistre, vous pouvez utiliser les fonctionnalités de relation de protection dans Unified Manager pour rendre la destination de protection accessible en lecture/écriture et basculer vers ce volume jusqu'à ce que la source soit à nouveau en ligne ; vous pouvez ensuite revenir à la source d'origine lorsqu'elle est disponible pour diffuser des données.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

- Vous devez avoir configuré OnCommand Workflow Automation pour effectuer cette opération.

Étapes

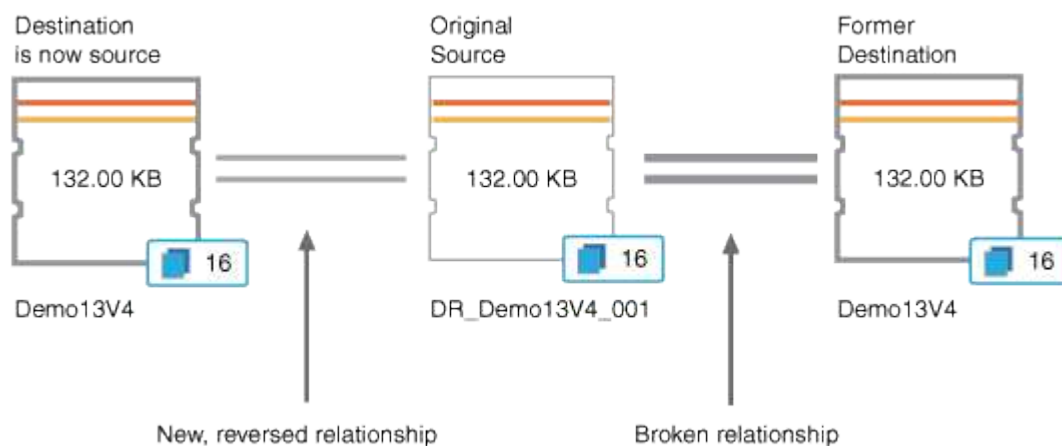
1. "Rompre la relation SnapMirror".

Vous devez rompre la relation avant de pouvoir convertir la destination d'un volume de protection des données en volume de lecture/écriture, et avant de pouvoir inverser la relation.

2. "Inverser la relation de protection".

Lorsque le volume source d'origine est à nouveau disponible, vous pouvez décider de rétablir la relation de protection d'origine en restaurant le volume source. Avant de pouvoir restaurer la source, vous devez la synchroniser avec les données écrites sur l'ancienne destination. Vous utilisez l'opération de resynchronisation inverse pour créer une nouvelle relation de protection en inversant les rôles de la relation d'origine et en synchronisant le volume source avec l'ancienne destination. Une nouvelle copie d'instantané de base est créée pour la nouvelle relation.

La relation inversée ressemble à une relation en cascade :



3. "Rompre la relation inversée SnapMirror".

Lorsque le volume source d'origine est resynchronisé et peut à nouveau diffuser des données, utilisez l'opération break pour rompre la relation inversée.

4. "Supprimer la relation".

Lorsque la relation inversée n'est plus nécessaire, vous devez supprimer cette relation avant de rétablir la relation d'origine.

5. "Resynchroniser la relation".

Utilisez l'opération de resynchronisation pour synchroniser les données de la source vers la destination et pour rétablir la relation d'origine.

Rompre une relation SnapMirror à partir de la page de détails Volume/Santé

Vous pouvez rompre une relation de protection à partir de la page Détails Volume/Santé et arrêter les transferts de données entre un volume source et un volume de destination dans une relation SnapMirror . Vous pouvez rompre une relation lorsque vous souhaitez

migrer des données, pour une reprise après sinistre ou pour des tests d'application. Le volume de destination est modifié en volume de lecture-écriture. Vous ne pouvez pas rompre une relation SnapVault .

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez rompre.
2. Cliquez avec le bouton droit sur la destination et sélectionnez **Pause** dans le menu.

La boîte de dialogue Rompre la relation s'affiche.

3. Cliquez sur **Continuer** pour rompre la relation.
4. Dans la topologie, vérifiez que la relation est rompue.

Relations de protection inverse à partir de la page Détails Volume/Santé

Lorsqu'un sinistre désactive le volume source dans votre relation de protection, vous pouvez utiliser le volume de destination pour diffuser des données en le convertissant en lecture/écriture pendant que vous réparez ou remplacez la source. Lorsque la source est à nouveau disponible pour recevoir des données, vous pouvez utiliser l'opération de resynchronisation inverse pour établir la relation dans le sens inverse, en synchronisant les données sur la source avec les données sur la destination de lecture/écriture.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- La relation ne doit pas être une relation SnapVault .
- Une relation de protection doit déjà exister.
- La relation de protection doit être rompue.
- La source et la destination doivent être en ligne.
- La source ne doit pas être la destination d'un autre volume de protection des données.
- Lorsque vous effectuez cette tâche, les données de la source qui sont plus récentes que les données de la copie Snapshot commune sont supprimées.
- Les politiques et les planifications créées sur la relation de resynchronisation inverse sont les mêmes que celles de la relation de protection d'origine.

Si les politiques et les calendriers n'existent pas, ils sont créés.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, recherchez dans la topologie la relation SnapMirror sur laquelle vous souhaitez inverser la source et la destination, puis cliquez dessus avec le bouton droit de la souris.

2. Sélectionnez **Resynchronisation inverse** dans le menu.

La boîte de dialogue Resynchronisation inversée s'affiche.

3. Vérifiez que la relation affichée dans la boîte de dialogue **Resynchronisation inverse** est celle pour laquelle vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Soumettre**.

La boîte de dialogue Resynchronisation inversée est fermée et un lien de tâche s'affiche en haut de la page Détails du volume/de l'état de santé.

4. **Facultatif** : cliquez sur **Afficher les tâches** sur la page de détails **Volume/Santé** pour suivre l'état de chaque tâche de resynchronisation inverse.

Une liste filtrée de tâches s'affiche.

5. **Facultatif** : cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

L'opération de resynchronisation inverse est terminée lorsque toutes les tâches sont terminées avec succès.

Supprimer une relation de protection de la page Détails du volume/de la santé

Vous pouvez supprimer une relation de protection pour supprimer définitivement une relation existante entre la source et la destination sélectionnées : par exemple, lorsque vous souhaitez créer une relation à l'aide d'une destination différente. Cette opération supprime toutes les métadonnées et ne peut pas être annulée.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez supprimer.
2. Cliquez avec le bouton droit sur le nom de la destination et sélectionnez **Supprimer** dans le menu.

La boîte de dialogue Supprimer la relation s'affiche.

3. Cliquez sur **Continuer** pour supprimer la relation.

La relation est supprimée de la page Détails Volume / Santé.

Resynchroniser les relations de protection à partir de la page Détails du volume/de la santé

Vous pouvez resynchroniser les données sur une relation SnapMirror ou SnapVault qui a été rompue, puis la destination a été rendue en lecture/écriture afin que les données de la source correspondent aux données de la destination. Vous pouvez également resynchroniser lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, ce qui entraîne l'échec des mises à jour de SnapMirror ou de SnapVault .

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, recherchez dans la topologie la relation de protection que vous souhaitez resynchroniser et cliquez dessus avec le bouton droit de la souris.
2. Sélectionnez **Resynchroniser** dans le menu.

Alternativement, dans le menu **Actions**, sélectionnez **Relation > Resynchroniser** pour resynchroniser la relation dont vous consultez actuellement les détails.

La boîte de dialogue Resynchroniser s'affiche.

3. Dans l'onglet **Options de resynchronisation**, sélectionnez une priorité de transfert et le débit de transfert maximal.
4. Cliquez sur **Copies d'instantanés source** ; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

La boîte de dialogue Sélectionner la copie d'instantané source s'affiche.

5. Si vous souhaitez spécifier une copie d'instantané existante plutôt que de transférer la copie d'instantané par défaut, cliquez sur **Copie d'instantané existante** et sélectionnez une copie d'instantané dans la liste.
6. Cliquez sur **Soumettre**.

Vous revenez à la boîte de dialogue Resynchroniser.

7. Si vous avez sélectionné plusieurs sources à resynchroniser, cliquez sur **Par défaut** pour la source suivante pour laquelle vous souhaitez spécifier une copie instantanée existante.
8. Cliquez sur **Soumettre** pour commencer le travail de resynchronisation.

La tâche de resynchronisation est démarrée, vous revenez à la page des détails Volume / Santé et un lien vers les tâches s'affiche en haut de la page.

9. **Facultatif** : cliquez sur **Afficher les tâches** sur la page **Détails du volume/de l'état** pour suivre l'état de chaque tâche de resynchronisation.

Une liste filtrée de tâches s'affiche.

10. **Facultatif** : cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

Le travail de resynchronisation est terminé lorsque toutes les tâches sont terminées avec succès.

Résoudre un échec de tâche de protection

Ce workflow fournit un exemple de la manière dont vous pouvez identifier et résoudre un échec de tâche de protection à partir du tableau de bord Unified Manager.

Avant de commencer

Étant donné que certaines tâches de ce flux de travail nécessitent que vous vous connectiez à l'aide du rôle

Administrateur, vous devez être familiarisé avec les rôles requis pour utiliser diverses fonctionnalités.

Dans ce scénario, vous accédez à la page Tableau de bord pour voir s'il existe des problèmes avec vos tâches de protection. Dans la zone Incident de protection, vous remarquez qu'il existe un incident de tâche terminée, indiquant une erreur d'échec de tâche de protection sur un volume. Vous examinez cette erreur pour déterminer la cause possible et la résolution potentielle.

Étapes

1. Dans le panneau Incidents de protection de la zone Incidents et risques non résolus du tableau de bord, cliquez sur l'événement **Échec de la tâche de protection**.



Le texte lié à l'événement est écrit sous la forme `object_name:/object_name - Error Name`, tel que `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

La page Détails de l'événement pour la tâche de protection ayant échoué s'affiche.

2. Consultez le message d'erreur dans le champ Cause de la zone **Résumé** pour déterminer le problème et évaluer les actions correctives potentielles.

Voir ["Identifier le problème et effectuer des actions correctives en cas d'échec d'une tâche de protection"](#).

Identifier le problème et effectuer des actions correctives pour une tâche de protection ayant échoué

Vous examinez le message d'erreur d'échec de la tâche dans le champ Cause de la page Détails de l'événement et déterminez que la tâche a échoué en raison d'une erreur de copie d'instantané. Vous accédez ensuite à la page Détails Volume / Santé pour recueillir plus d'informations.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Le message d'erreur fourni dans le champ Cause de la page Détails de l'événement contient le texte suivant concernant la tâche ayant échoué :

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Ce message fournit les informations suivantes :

- Une tâche de sauvegarde ou de mise en miroir n'a pas été effectuée avec succès.

Le travail impliquait une relation de protection entre le volume source `cluster2_src_vol2` sur le serveur virtuel `cluster2_src_svm` et le volume de destination `managed_svc2_vol3` sur le serveur virtuel

nommé `cluster3_dst_svm`.

- Une tâche de copie d'instantané a échoué pour `0426cluster2_src_vol2snap` sur le volume source `cluster2_src_svm:/cluster2_src_vol2`.

Dans ce scénario, vous pouvez identifier la cause et les actions correctives potentielles de l'échec du travail. Cependant, la résolution de l'échec nécessite que vous accédiez à l'interface utilisateur Web du gestionnaire de système ou aux commandes CLI ONTAP.

Étapes

1. Vous examinez le message d'erreur et déterminez qu'une tâche de copie d'instantané a échoué sur le volume source, ce qui indique qu'il y a probablement un problème avec votre volume source.

Vous pouvez également cliquer sur le lien **Détails du travail** à la fin du message d'erreur, mais dans le cadre de ce scénario, vous choisissez de ne pas le faire.

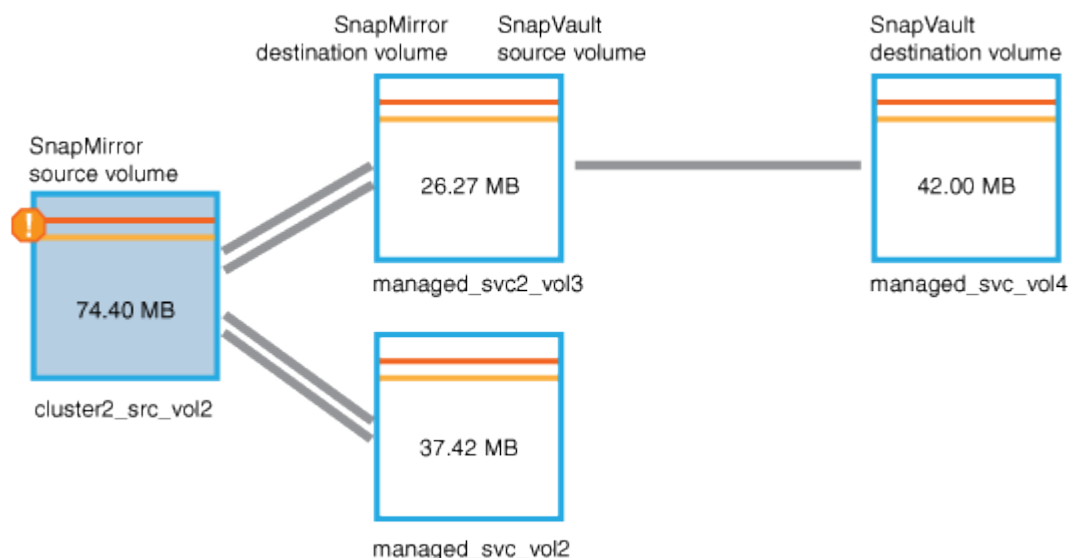
2. Vous décidez que vous souhaitez essayer de résoudre l'événement, vous procédez donc comme suit :
 - a. Cliquez sur le bouton **Attribuer à** et sélectionnez **Moi** dans le menu.
 - b. Cliquez sur le bouton **Accuser réception** pour ne plus recevoir de notifications d'alerte répétées, si des alertes ont été définies pour l'événement.
 - c. En option, vous pouvez également ajouter des notes sur l'événement.
3. Cliquez sur le champ **Source** dans le volet **Résumé** pour voir les détails sur le volume source.

Le champ **Source** contient le nom de l'objet source : dans ce cas, le volume sur lequel le travail de copie de snapshot a été planifié.

La page de détails Volume / Santé s'affiche pour `cluster2_src_vol2`, montrant le contenu de l'onglet Protection.

4. En regardant le graphique de topologie de protection, vous voyez une icône d'erreur associée au premier volume de la topologie, qui est le volume source de la relation SnapMirror.

Vous voyez également les barres horizontales dans l'icône du volume source, indiquant les seuils d'avertissement et d'erreur définis pour ce volume.



5. Vous placez votre curseur sur l'icône d'erreur pour voir la boîte de dialogue contextuelle qui affiche les paramètres de seuil et constatez que le volume a dépassé le seuil d'erreur, indiquant un problème de capacité.
6. Cliquez sur l'onglet **Capacité**.

Informations sur la capacité concernant le volume `cluster2_src_vol2` affiche.

7. Dans le panneau **Capacité**, vous voyez qu'il y a une icône d'erreur dans le graphique à barres, indiquant à nouveau que la capacité du volume a dépassé le niveau de seuil défini pour le volume.
8. Sous le graphique de capacité, vous voyez que la croissance automatique du volume a été désactivée et qu'une garantie d'espace de volume a été définie.

Vous pouvez décider d'activer la croissance automatique, mais dans le cadre de ce scénario, vous décidez d'enquêter davantage avant de prendre une décision sur la manière de résoudre le problème de capacité.

9. Faites défiler la liste jusqu'à la liste **Événements** et constatez que les événements Échec du travail de protection, Jours du volume jusqu'à saturation et Espace du volume plein ont été générés.
10. Dans la liste **Événements**, cliquez sur l'événement **Espace volume plein** pour obtenir plus d'informations, après avoir décidé que cet événement semble le plus pertinent pour votre problème de capacité.

La page Détails de l'événement affiche l'événement Espace volume plein pour le volume source.

11. Dans la zone **Résumé**, vous lisez le champ Cause de l'événement : `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Sous la zone Résumé, vous voyez les actions correctives suggérées.



Les actions correctives suggérées s'affichent uniquement pour certains événements. Vous ne voyez donc pas cette zone pour tous les types d'événements.

Vous cliquez sur la liste des actions suggérées que vous pouvez effectuer pour résoudre l'événement d'espace de volume plein :

- Activer la croissance automatique sur ce volume.
- Redimensionner le volume.
- Activez et exécutez la déduplication sur ce volume.
- Activer et exécuter la compression sur ce volume.

13. Vous décidez d'activer la croissance automatique sur le volume, mais pour ce faire, vous devez déterminer l'espace libre disponible sur l'agrégat parent et le taux de croissance actuel du volume :
 - a. Regardez l'agrégat parent, `cluster2_src_aggr1`, dans le volet **Périphériques associés**.



Vous pouvez cliquer sur le nom de l'agrégat pour obtenir plus de détails sur l'agrégat.

Vous déterminez que l'agrégat dispose de suffisamment d'espace pour permettre la croissance automatique du volume.

- b. En haut de la page, regardez l'icône indiquant un incident critique et examinez le texte sous l'icône.

Vous déterminez que « Jours jusqu'à épuisement : moins d'un jour | Taux de croissance quotidien : 5,4 % ».

14. Accédez au Gestionnaire de système ou à l'interface de ligne de commande ONTAP pour activer le `volume autogrow option`.



Notez les noms du volume et de l'agrégat afin de les avoir à disposition lors de l'activation de la croissance automatique.

15. Après avoir résolu le problème de capacité, revenez à la page des détails de l'événement Unified Manager **Événement** et marquez l'événement comme résolu.

Résoudre les problèmes de décalage

Ce flux de travail fournit un exemple de la manière dont vous pouvez résoudre un problème de décalage. Dans ce scénario, vous êtes un administrateur ou un opérateur accédant à la page Tableau de bord d'Unified Manager pour voir s'il existe des problèmes avec vos relations de protection et, s'ils existent, pour trouver des solutions.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Dans la page Tableau de bord, vous examinez la zone Incidents et risques non résolus et voyez une erreur de décalage SnapMirror dans le volet Protection sous Risques de protection.

Étapes

1. Dans le volet **Protection** de la page **Tableau de bord**, recherchez l'erreur de décalage de relation SnapMirror et cliquez dessus.

La page Détails de l'événement pour l'événement d'erreur de décalage s'affiche.

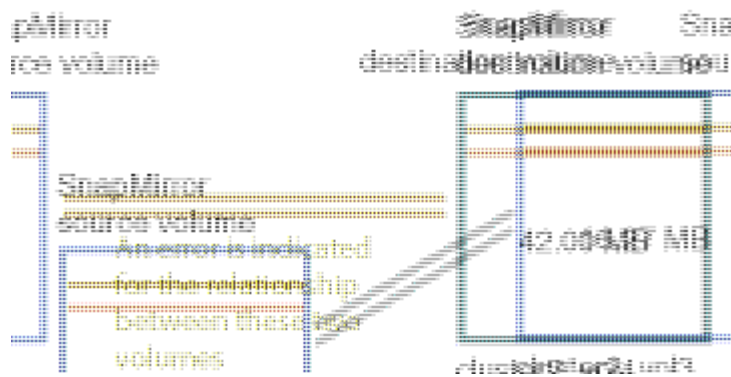
2. À partir de la page de détails de l'**Événement**, vous pouvez effectuer une ou plusieurs des tâches suivantes :
 - Consultez le message d'erreur dans le champ Cause de la zone Résumé pour déterminer s'il existe une action corrective suggérée.
 - Cliquez sur le nom de l'objet, dans ce cas un volume, dans le champ Source de la zone Résumé pour obtenir des détails sur le volume.
 - Recherchez des notes qui pourraient avoir été ajoutées à propos de cet événement.
 - Ajoutez une note à l'événement.
 - Affecter l'événement à un utilisateur spécifique.
 - Reconnaître ou résoudre l'événement.

3. Dans ce scénario, vous cliquez sur le nom de l'objet (dans ce cas, un volume) dans le champ Source de la zone **Résumé** pour obtenir des détails sur le volume.

L'onglet Protection de la page Détails Volume / Santé s'affiche.

4. Dans l'onglet **Protection**, vous regardez le diagramme de topologie.

Vous constatez que le volume avec l'erreur de décalage est le dernier volume d'une cascade SnapMirror à trois volumes. Le volume que vous avez sélectionné est entouré en gris foncé et une double ligne orange provenant du volume source indique une erreur de relation SnapMirror .



5. Cliquez sur chacun des volumes de la cascade SnapMirror .

Lorsque vous sélectionnez chaque volume, les informations de protection dans les zones Résumé, Topologie, Historique, Événements, Périphériques associés et Alertes associées changent pour afficher les détails relatifs au volume sélectionné.

6. Vous regardez la zone **Résumé** et positionnez votre curseur sur l'icône d'informations dans le champ **Calendrier de mise à jour** pour chaque volume.

Dans ce scénario, vous remarquez que la stratégie SnapMirror est DPDefault et que la planification SnapMirror est mise à jour toutes les heures, cinq minutes après l'heure. Vous réalisez que tous les volumes de la relation tentent d'effectuer un transfert SnapMirror en même temps.

7. Pour résoudre le problème de décalage, vous modifiez les planifications de deux des volumes en cascade afin que chaque destination commence un transfert SnapMirror une fois que sa source a terminé un transfert.

Gérer et surveiller les relations de protection

Active IQ Unified Manager vous permet de créer des relations de protection, de surveiller et de dépanner les relations SnapMirror et SnapVault sur les clusters gérés et de restaurer les données lorsqu'elles sont écrasées ou perdues.

Pour les opérations SnapMirror , il existe deux types de réplication :

- Asynchrone

La réplication du volume principal vers le volume secondaire est déterminée par une planification.

- Synchronne

La réplication est effectuée simultanément sur le volume principal et secondaire.

Vous pouvez effectuer jusqu'à 10 tâches de protection simultanément sans impact sur les performances. Vous pourriez constater un impact sur les performances lorsque vous exécutez entre 11 et 30 tâches simultanément. Il n'est pas recommandé d'exécuter plus de 30 tâches simultanément.

Afficher l'état de protection du volume

La page Protection des données présente une vue holistique des détails de protection des données pour tous les volumes protégés d'un seul cluster ou de tous les clusters

d'un centre de données.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. Selon que vous souhaitez afficher l'état de protection des données pour tous les clusters surveillés ou pour un seul cluster, sélectionnez **Tous les clusters** ou sélectionnez un seul cluster dans le menu déroulant.
3. Cliquez sur la flèche droite en haut du panneau Protection des données. La page **Protection des données** s'affiche.

Selon que vous avez sélectionné un seul ou tous les clusters de votre centre de données, cette page affiche l'état de protection des données des volumes protégés par des copies Snapshot ou des stratégies SnapMirror, ainsi que le nombre de volumes non protégés.

La sélection d'un cluster dans la liste **Cluster individuel** affiche l'état de la relation de protection Snapshot et SnapMirror des volumes protégés dans ce cluster.

En cliquant sur les événements sur cette page, vous accédez à la page Détails de l'événement. Vous pouvez cliquer sur le lien **Afficher tout** pour afficher tous les événements de protection actifs dans la page d'inventaire de gestion des événements. Vous pouvez passer votre souris pour afficher les décomptes et légendes respectifs. Vous pouvez cliquer sur :

- Les graphiques à barres pour les volumes non protégés et les volumes protégés par des copies Snapshot permettent d'accéder à la page Volumes et d'afficher les détails.
- Les graphiques à barres de toutes les relations accèdent à la page Relations, où les détails sont filtrés par le cluster source.

Afficher l'état de protection des volumes protégés par des copies instantanées

Présentation des copies instantanées : Un aperçu des volumes protégés par des copies instantanées, tels que :

- Le nombre total de volumes protégés et non protégés par des copies Snapshot.
- Le nombre total de volumes qui utilisent ou dépassent l'espace réservé pour les copies Snapshot.

Analyse des copies instantanées détaille les informations suivantes :

- Événements individuels pour les copies Snapshot, y compris les événements générés au cours des dernières 24 heures.
- Tableau détaillé des volumes protégés et non protégés par des copies Snapshot.
- Volumes utilisant, n'utilisant pas et dépassant la capacité de copie Snapshot réservée.
- Répartition des volumes en fonction du nombre de copies Snapshot.

Points à noter pour les copies instantanées

- Pour compter les volumes protégés par des copies Snapshot, les volumes source et de destination sont pris en compte.
- Le nombre de copies Snapshot renvoyées concerne uniquement les volumes qui sont en ligne et disponibles.
- La plage graphique pour le nombre de copies d'instantanés est dynamique. Il est généré en fonction du nombre d'instantanés présents dans le cluster sélectionné.

- Pour considérer un volume comme protégé, la planification de la copie instantanée du volume doit être activée.
- La valeur de l'espace de réserve pour les copies Snapshot est importante pour visualiser la quantité d'espace disque utilisé ou pour calculer l'espace qui peut être récupéré si une ou plusieurs copies Snapshot sont supprimées.

Afficher l'état de protection des relations SnapMirror

- Présentation de SnapMirror * : un aperçu des volumes protégés par les politiques SnapMirror , tels que :
 - Le nombre de volumes protégés par les politiques SnapMirror respectives, telles que les relations de volume SnapMirror , la reprise après sinistre de la machine virtuelle de stockage (SVM-DR) et leurs combinaisons.
 - Nombre total de relations SnapMirror subissant un décalage de l'objectif de point de récupération (RPO) en fonction de l'état du décalage.
 - SnapMirror Analysis* détaille les informations suivantes :
 - Événements individuels générés pour les relations SnapMirror , y compris les événements générés au cours des dernières 24 heures
 - Le nombre de volumes protégés par chaque type de politique SnapMirror .
 - Nombre de relations protégées par les types de relations SnapMirror , tels que Miroir asynchrone, Coffre asynchrone, MirrorVault asynchrone, StricxtSync, Groupe de cohérence de synchronisation active SnapMirror et Synchronisation.
 - Le nombre de relations saines et malsaines.
 - Rupture du rapport volume-compte. Vous pouvez basculer les graphiques en fonction du temps de latence et du statut RPO.
 -
- Seuils de décalage pour les relations non gérées. Vous pouvez cliquer sur l'icône des paramètres () pour configurer les paramètres de seuil de décalage. Pour plus d'informations, voir "[Configuration des paramètres de seuil de latence pour les relations de protection non gérées](#)".

Points à noter pour les relations SnapMirror

- Pour compter les relations SnapMirror , les volumes sources, qui sont activés pour la lecture et l'écriture, sont comptés. Les volumes de destination et racine ne sont pas pris en compte.
- Pour la relation SnapMirror , les événements sont affichés pour le cluster source.
- Le nombre de relations SnapMirror inclut le nombre de volumes avec des sources et des destinations sur le même cluster ou sur des clusters différents.
- La durée du décalage RPO dans la réplication des données est basée sur la relation SnapMirror . Le statut est classé comme `ok` , `warning` , ou `error` , en fonction du seuil de relation défini. Vous pouvez consulter l'état pour déterminer si les paramètres fonctionnent comme prévu ou si vous devez résoudre un problème.
- Si un volume possède plusieurs relations SnapMirror , chaque type de relation est comptabilisé pour le décalage RPO.
- Les relations de volume sont considérées comme non saines s'il existe des problèmes de réplication des données entre la source et la destination, par exemple lorsque la relation est rompue.

Afficher les clusters protégés par la configuration MetroCluster

Le panneau * MetroCluster Protection* de la page **Data Protection** affiche le nombre de clusters protégés ou non protégés par MetroCluster via la configuration FC ou IP sur votre site. En cliquant sur les graphiques à barres de ce panneau, vous accédez à la page Clusters où les détails du cluster sont filtrés en fonction des clusters protégés ou non protégés. Pour plus d'informations sur la surveillance de votre configuration MetroCluster , consultez "[Surveillance des configurations MetroCluster](#)" .

Afficher les relations de protection du volume

À partir de la vue Relation : Toutes les relations et de la page Relations de volume, vous pouvez afficher l'état des relations de volume SnapMirror et SnapVault existantes. Vous pouvez également examiner les détails des relations de protection, notamment l'état du transfert et du décalage, les détails de la source et de la destination, les informations de planification et de politique, etc.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez également lancer des commandes de relation à partir de cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Toutes les relations**.

La vue Relation : Toutes les relations s'affiche.

3. Choisissez l'une des méthodes suivantes pour afficher les détails de la protection du volume :
 - Pour afficher les informations actuelles sur toutes les relations de volume, restez sur la page par défaut **Toutes les relations**.
 - Pour afficher des informations détaillées sur les tendances de transfert de volume sur une période donnée, dans le menu Affichage, sélectionnez Relation : Affichage État du transfert du dernier mois.
 - Pour afficher des informations détaillées sur l'activité de transfert de volume au quotidien, dans le menu Affichage, sélectionnez Relation : Taux de transfert du dernier mois.



Les vues de transfert de volume affichent des informations pour les volumes dans des relations asynchrones uniquement - les volumes dans des relations synchrones ne sont pas affichés.

Surveiller les LUN dans une relation de groupe de cohérence

Si votre environnement ONTAP prend en charge la synchronisation active SnapMirror pour protéger les applications avec des LUN, vous pouvez afficher et surveiller ces LUN sur Active IQ Unified Manager.

La synchronisation active de SnapMirror garantit un objectif de temps de récupération (RTO) nul lors du basculement dans les environnements SAN. Dans un déploiement typique prenant en charge la synchronisation active SnapMirror , les LUN sur les volumes sont protégés par des relations de groupe de cohérence.

Ces LUN primaires et secondaires sont des LUN composites ou une paire de LUN répliquées avec le même UUID et le même numéro de série. Les opérations d'E/S (lecture et écriture) sont multiplexées sur les sites source et de destination sur ces LUN composites, garantissant ainsi la transparence.

Pour afficher les LUN composites, les clusters principaux et secondaires avec les LUN qui font partie de la relation de groupe de cohérence doivent être ajoutés et découverts sur Unified Manager. Seuls les LUN iSCSI et FCP sont pris en charge.

Pour plus d'informations sur la synchronisation active de SnapMirror, consultez "[Documentation ONTAP 9 pour SnapMirror Active Sync \(anciennement SM-BC\)](#)".

Pour afficher les LUN composites dans votre environnement, procédez comme suit :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > LUN**.
2. Dans le menu Affichage, sélectionnez **Relation > Tous les LUN**.

La vue Relation : Tous les LUN s'affiche.

Vous pouvez afficher les détails du LUN, tels que le nom du LUN, le volume, la machine virtuelle de stockage hébergeant le LUN, le cluster, le groupe de cohérence et le LUN partenaire. Vous pouvez cliquer sur chacun de ces composants pour accéder à une vue détaillée. En cliquant sur le groupe de cohérence, vous accédez à la page Relations.

Cliquer sur le LUN partenaire vous permet d'afficher ses détails de configuration dans l'onglet SAN de la page Détails de la machine virtuelle de stockage pour la machine virtuelle de stockage sur laquelle le LUN partenaire est hébergé. Des informations telles que les initiateurs et les groupes d'initiateurs ainsi que d'autres aspects du LUN partenaire sont affichées.

Vous pouvez exécuter les fonctions standard au niveau de la grille de tri, de filtrage, de génération et de téléchargement de rapports pour les LUN protégés dans votre environnement.

Créer une relation de protection SnapVault à partir de la vue Santé : Tous les volumes

Vous pouvez utiliser la vue Santé : tous les volumes pour créer des relations SnapVault pour un ou plusieurs volumes sur la même machine virtuelle de stockage afin d'activer les sauvegardes de données à des fins de protection.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Le menu **Protéger** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action : par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans la vue **Santé : Tous les volumes**, sélectionnez un volume que vous souhaitez protéger et cliquez sur **Protéger**.

Alternativement, pour créer plusieurs relations de protection sur la même machine virtuelle de stockage (SVM), sélectionnez un ou plusieurs volumes dans la vue Santé : tous les volumes, puis cliquez sur **Protéger** dans la barre d'outils.

3. Sélectionnez * SnapVault* dans le menu.

La boîte de dialogue Configurer la protection s'ouvre.

4. Cliquez sur * SnapVault* pour afficher l'onglet * SnapVault* et configurer les informations du volume secondaire.
5. Cliquez sur **Avancé** pour définir la déduplication, la compression, la croissance automatique et la garantie d'espace selon vos besoins, puis cliquez sur **Appliquer**.
6. Remplissez la zone **Informations de destination** et la zone **Paramètres de relation** dans l'onglet * SnapVault*.
7. Cliquez sur **Appliquer**.

Vous êtes renvoyé à la vue Santé : Tous les volumes.

8. Cliquez sur le lien de la tâche de configuration de la protection en haut de la vue **Santé : tous les volumes**.

Si vous créez une seule relation de protection, la page Détails du travail s'affiche. Toutefois, si vous créez plusieurs relations de protection, une liste filtrée de tous les travaux associés à l'opération de protection s'affiche.

9. Effectuez l'une des opérations suivantes :

- Si vous n'avez qu'une seule tâche, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et pour déterminer quand la tâche est terminée.
- Si vous avez plus d'un emploi :
 - i. Cliquez sur un travail dans la liste des travaux.
 - ii. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection et pour déterminer quand le travail est terminé.
 - iii. Utilisez le bouton **Retour** pour revenir à la liste filtrée et afficher un autre travail.

Créer une relation de protection SnapVault à partir de la page Détails du volume/de l'état de santé

Vous pouvez créer une relation SnapVault à l'aide de la page Détails Volume/Santé afin que les sauvegardes de données soient activées à des fins de protection sur les volumes.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail pour effectuer cette tâche.

Le menu **Protéger** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action : par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, cliquez avec le bouton droit sur un volume dans la vue topologique que vous souhaitez protéger.
2. Sélectionnez **Protéger** > * SnapVault* dans le menu.

La boîte de dialogue Configurer la protection s'ouvre.

3. Cliquez sur * SnapVault* pour afficher l'onglet * SnapVault* et configurer les informations sur la ressource secondaire.
4. Cliquez sur **Avancé** pour définir la déduplication, la compression, la croissance automatique et la garantie d'espace selon vos besoins, puis cliquez sur **Appliquer**.
5. Remplissez la zone **Informations de destination** et la zone **Paramètres de relation** dans la boîte de dialogue **Configurer la protection**.
6. Cliquez sur **Appliquer**.

Vous êtes renvoyé à la page des détails Volume / Santé.

7. Cliquez sur le lien de configuration de la protection en haut de la page de détails **Volume / Santé**.

La page Détails du travail s'affiche.

8. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection et pour déterminer quand le travail est terminé.

Une fois les tâches terminées, les nouvelles relations s'affichent dans la vue topologique de la page Détails Volume/Santé.

Créer une relation de protection SnapMirror à partir de la vue Santé : Tous les volumes

L'utilisation de la vue Santé : tous les volumes vous permet de créer plusieurs relations de protection SnapMirror à la fois en sélectionnant plusieurs volumes sur la même machine virtuelle de stockage.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Le menu **Protéger** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action : par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le

cluster de destination n'a pas encore été découvert

Étapes

1. Dans la vue **Santé : tous les volumes**, sélectionnez un volume que vous souhaitez protéger.

Alternativement, pour créer plusieurs relations de protection sur la même SVM, sélectionnez un ou plusieurs volumes dans la vue Santé : tous les volumes, puis cliquez sur **Protéger** > * SnapMirror* dans la barre d'outils.

La boîte de dialogue Configurer la protection s'affiche.

2. Cliquez sur * SnapMirror* pour afficher l'onglet * SnapMirror* et configurer les informations de destination.
3. Cliquez sur **Avancé** pour définir la garantie d'espace, selon vos besoins, puis cliquez sur **Appliquer**.
4. Remplissez la zone **Informations de destination** et la zone **Paramètres de relation** dans l'onglet * SnapMirror*.
5. Cliquez sur **Appliquer**.

Vous êtes renvoyé à la vue Santé : Tous les volumes.

6. Cliquez sur le lien de configuration de la protection en haut de la vue **Santé : Tous les volumes**.

Si vous créez une seule relation de protection, la page Détails du travail s'affiche. Toutefois, si vous créez plusieurs relations de protection, une liste de tous les travaux associés à l'opération de protection s'affiche.

7. Effectuez l'une des opérations suivantes :

- Si vous n'avez qu'une seule tâche, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et pour déterminer quand la tâche est terminée.
- Si vous avez plus d'un emploi :
 - i. Cliquez sur un travail dans la liste des travaux.
 - ii. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection et pour déterminer quand le travail est terminé.
 - iii. Utilisez le bouton **Retour** pour revenir à la liste filtrée et afficher un autre travail.

Selon la SVM de destination que vous avez spécifiée lors de la configuration ou les options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut être l'une des plusieurs variantes possibles :

- Si vous avez spécifié une SVM de destination qui s'exécute sous la même version ou une version plus récente d' ONTAP par rapport à celle du volume source, une relation SnapMirror basée sur la réplication de blocs est le résultat par défaut.
- Si vous avez spécifié une SVM de destination qui s'exécute sous la même version ou une version plus récente d' ONTAP par rapport à celle du volume source, mais que vous avez activé la réplication flexible en fonction des versions dans les paramètres avancés, une relation SnapMirror avec la réplication flexible en fonction des versions est le résultat.
- Si vous avez spécifié une SVM de destination qui s'exécute sous une version d' ONTAP antérieure à celle du volume source et que la version antérieure prend en charge la réplication flexible en fonction des versions, une relation SnapMirror avec réplication flexible en fonction des versions est le résultat automatique.

Créer une relation de protection SnapMirror à partir de la page Détails du volume/de l'état de santé

Vous pouvez utiliser la page Détails Volume/Santé pour créer une relation SnapMirror afin que la réplication des données soit activée à des fins de protection. La réplication SnapMirror vous permet de restaurer les données du volume de destination en cas de perte de données sur la source.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Le menu **Protéger** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action : par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Vous pouvez effectuer jusqu'à 10 tâches de protection simultanément sans impact sur les performances. Vous pourriez constater un impact sur les performances lorsque vous exécutez entre 11 et 30 tâches simultanément. Il n'est pas recommandé d'exécuter plus de 30 tâches simultanément.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, cliquez avec le bouton droit dans la vue topologique sur le nom d'un volume que vous souhaitez protéger.
2. Sélectionnez **Protéger** > * SnapMirror* dans le menu.

La boîte de dialogue Configurer la protection s'affiche.

3. Cliquez sur * SnapMirror* pour afficher l'onglet * SnapMirror* et configurer les informations de destination.
4. Cliquez sur **Avancé** pour définir la garantie d'espace, selon vos besoins, puis cliquez sur **Appliquer**.
5. Remplissez la zone **Informations de destination** et la zone **Paramètres de relation** dans la boîte de dialogue **Configurer la protection**.
6. Cliquez sur **Appliquer**.

Vous êtes renvoyé à la page des détails Volume / Santé.

7. Cliquez sur le lien de configuration de la protection en haut de la page de détails **Volume / Santé**.

Les tâches et les détails du travail sont affichés dans la page Détails du travail.

8. Dans la page des détails du **Tâche**, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et pour déterminer quand la tâche est terminée.
9. Une fois les tâches terminées, cliquez sur **Retour** sur votre navigateur pour revenir à la page de détails **Volume / Santé**.

La nouvelle relation s'affiche dans la vue topologique de la page Détails Volume/Santé.

Selon la SVM de destination que vous avez spécifiée lors de la configuration ou les options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut être l'une des plusieurs variantes possibles :

- Si vous avez spécifié une SVM de destination qui s'exécute sous la même version ou une version plus récente d' ONTAP par rapport à celle du volume source, une relation SnapMirror basée sur la réplication de blocs est le résultat par défaut.
- Si vous avez spécifié une SVM de destination qui s'exécute sous la même version ou une version plus récente d' ONTAP par rapport à celle du volume source, mais que vous avez activé la réplication flexible en fonction des versions dans les paramètres avancés, une relation SnapMirror avec la réplication flexible en fonction des versions est le résultat.
- Si vous avez spécifié une SVM de destination qui s'exécute sous une version antérieure d' ONTAP ou une version supérieure à celle du volume source et que la version antérieure prend en charge la réplication flexible en fonction des versions, une relation SnapMirror avec réplication flexible en fonction des versions est le résultat automatique.

Créer une relation SnapMirror avec une réplication flexible en fonction des versions

Vous pouvez créer une relation SnapMirror avec une réplication flexible en termes de version. La réplication flexible en fonction des versions vous permet d'implémenter la protection SnapMirror même si les volumes source et de destination s'exécutent sous différentes versions d' ONTAP.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- Les SVM source et de destination doivent chacune avoir une licence SnapMirror activée.
- Les SVM source et de destination doivent chacune s'exécuter sous une version du logiciel ONTAP qui prend en charge la réplication flexible en fonction des versions.

SnapMirror avec réplication flexible en fonction des versions vous permet d'implémenter la protection SnapMirror même dans des environnements de stockage hétérogènes dans lesquels tout le stockage ne s'exécute pas sous une seule version d' ONTAP; cependant, les opérations de miroir effectuées sous SnapMirror avec réplication flexible en fonction des versions ne s'exécutent pas aussi rapidement qu'elles le feraient sous la réplication de blocs traditionnelle SnapMirror.

Étapes

1. Affichez la boîte de dialogue **Configurer la protection** pour le volume que vous souhaitez protéger.
 - Si vous consultez l'onglet Protection de la page Détails du volume/de l'état de santé, cliquez avec le bouton droit de la souris dans la vue topologique portant le nom du volume que vous souhaitez protéger et sélectionnez **Protéger** > * SnapMirror* dans le menu.
 - Si vous consultez la vue Santé : Tous les volumes, recherchez un volume que vous souhaitez protéger et cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Protéger** > * SnapMirror* dans le menu. La boîte de dialogue Configurer la protection s'affiche.
2. Cliquez sur * SnapMirror* pour afficher l'onglet * SnapMirror*.
3. Remplissez la zone **Informations de destination** et la zone **Paramètres de relation** dans la boîte de dialogue **Configurer la protection**.

Si vous spécifiez une SVM de destination qui s'exécute sous une version d' ONTAP antérieure à celle du volume source que vous protégez, et si cette version antérieure prend en charge la réplication flexible en fonction des versions, cette tâche configure automatiquement SnapMirror avec la réplication flexible en fonction des versions.

4. Si vous spécifiez une SVM de destination qui s'exécute sous la même version d' ONTAP que celle du volume source, mais que vous souhaitez toujours configurer SnapMirror avec une réplication flexible en fonction des versions, cliquez sur **Avancé** pour activer la réplication flexible en fonction des versions, puis cliquez sur **Appliquer**.

5. Cliquez sur **Appliquer**.

Vous êtes renvoyé à la page des détails Volume / Santé.

6. Cliquez sur le lien de configuration de la protection en haut de la page de détails **Volume / Santé**.

Les tâches et les détails des tâches sont affichés dans la page Détails de la tâche.

7. Dans la page des détails du **Tâche**, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et pour déterminer quand la tâche est terminée.

8. Une fois les tâches terminées, cliquez sur **Retour** sur votre navigateur pour revenir à la page de détails **Volume / Santé**.

La nouvelle relation s'affiche dans la vue topologique de la page Détails Volume/Santé.

Créer des relations SnapMirror avec une réplication flexible en fonction des versions avec option de sauvegarde

Vous pouvez créer une relation SnapMirror avec une capacité de réplication et de sauvegarde flexible en fonction des versions. La fonctionnalité d'option de sauvegarde vous permet d'implémenter la protection SnapMirror et de conserver également plusieurs versions de copies de sauvegarde à l'emplacement de destination.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- Les SVM source et de destination doivent chacune avoir une licence SnapMirror activée.
- Les SVM source et de destination doivent chacune avoir une licence SnapVault activée.
- Les SVM source et de destination doivent chacune s'exécuter sous une version du logiciel ONTAP qui prend en charge la réplication flexible en fonction des versions.

La configuration de SnapMirror avec la capacité d'option de sauvegarde vous permet de protéger vos données avec les capacités de récupération après sinistre de SnapMirror , telles que la capacité de basculement de volume, et en même temps de fournir des fonctionnalités SnapVault , telles que la protection contre plusieurs copies de sauvegarde.

Étapes

1. Affichez la boîte de dialogue **Configurer la protection** pour le volume que vous souhaitez protéger.
 - Si vous consultez l'onglet Protection de la page Détails du volume/de l'état de santé, cliquez avec le bouton droit de la souris dans la vue topologique sur le nom d'un volume que vous souhaitez protéger

et sélectionnez **Protéger** > * SnapMirror* dans le menu.

- Si vous consultez la vue Santé : Tous les volumes, recherchez un volume que vous souhaitez protéger et cliquez dessus avec le bouton droit de la souris, puis sélectionnez **Protéger** > * SnapMirror* dans le menu. La boîte de dialogue Configurer la protection s'affiche.

2. Cliquez sur * SnapMirror* pour afficher l'onglet * SnapMirror*.
3. Remplissez la zone **Informations de destination** et la zone **Paramètres de relation** dans la boîte de dialogue **Configurer la protection**.
4. Cliquez sur **Avancé** pour afficher la boîte de dialogue **Paramètres de destination avancés**.
5. Si la case à cocher **Réplication flexible de version** n'est pas déjà sélectionnée, sélectionnez-la maintenant.
6. Cochez la case **Avec option de sauvegarde** pour activer la fonction d'option de sauvegarde ; puis cliquez sur **Appliquer**.
7. Cliquez sur **Appliquer**.

Vous êtes renvoyé à la page des détails Volume / Santé.

8. Cliquez sur le lien de configuration de la protection en haut de la page de détails **Volume / Santé**.

Les tâches et les détails des tâches sont affichés dans la page Détails de la tâche.

9. Dans la page des détails du **Tâche**, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et pour déterminer quand la tâche est terminée.
10. Une fois les tâches terminées, cliquez sur **Retour** sur votre navigateur pour revenir à la page de détails **Volume / Santé**.

La nouvelle relation s'affiche dans la vue topologique de la page Détails Volume/Santé.

Configurer les paramètres d'efficacité de destination

Vous pouvez configurer les paramètres d'efficacité de destination tels que la déduplication, la compression, la croissance automatique et la garantie d'espace sur une destination de protection à l'aide de la boîte de dialogue Paramètres de destination avancés. Vous utilisez ces paramètres lorsque vous souhaitez optimiser l'utilisation de l'espace sur un volume de destination ou secondaire.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Par défaut, les paramètres d'efficacité correspondent à ceux du volume source, à l'exception des paramètres de compression dans une relation SnapVault , qui sont désactivés par défaut.

Étapes

1. Cliquez sur l'onglet * SnapMirror* ou sur l'onglet * SnapVault* dans la boîte de dialogue **Configurer la protection**, selon le type de relation que vous configurez.
2. Cliquez sur **Avancé** dans la zone **Informations sur la destination**.

La boîte de dialogue Paramètres de destination avancés s'ouvre.

3. Activez ou désactivez les paramètres d'efficacité pour la déduplication, la compression, la croissance automatique et la garantie d'espace, selon vos besoins.
4. Cliquez sur **Appliquer** pour enregistrer vos sélections et revenir à la boîte de dialogue **Configurer la protection**.

Créer des planifications SnapMirror et SnapVault

Vous pouvez créer des planifications SnapMirror et SnapVault de base ou avancées pour activer les transferts automatiques de protection des données sur un volume source ou principal afin que les transferts aient lieu plus ou moins fréquemment, selon la fréquence à laquelle les données changent sur vos volumes.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez déjà avoir complété la zone Informations de destination dans la boîte de dialogue Configurer la protection.
- Vous devez avoir configuré l'automatisation du flux de travail pour effectuer cette tâche.

Étapes

1. Dans l'onglet * SnapMirror* ou * SnapVault* de la boîte de dialogue **Configurer la protection**, cliquez sur le lien **Créer une planification** dans la zone **Paramètres de relation**.

La boîte de dialogue Créer une planification s'affiche.

2. Dans le champ **Nom du planning**, saisissez le nom que vous souhaitez donner au planning.
3. Sélectionnez l'une des options suivantes :

- **Basique**

Sélectionnez si vous souhaitez créer un programme de type intervalle de base.

- **Avancé**

Sélectionnez si vous souhaitez créer une planification de type cron.

4. Cliquez sur **Créer**.

La nouvelle planification s'affiche dans la liste déroulante Planification SnapMirror ou Planification SnapVault .

Créer des relations en cascade ou en éventail pour étendre la protection à partir d'une relation de protection existante

Vous pouvez étendre la protection d'une relation existante en créant soit une distribution à partir du volume source, soit une cascade à partir du volume de destination d'une relation existante. Vous pouvez le faire lorsque vous devez copier des données d'un site vers plusieurs sites ou pour fournir une protection supplémentaire en créant davantage de sauvegardes.

Vous pouvez étendre la protection aux volumes à l'aide d'un groupe de cohérence, qui est un conteneur

contenant plusieurs volumes afin que vous puissiez gérer tous les volumes comme une seule entité. Vous pouvez afficher le groupe de cohérence de synchronisation active SnapMirror et la relation du groupe de cohérence synchrone dans la page Relations d'Unified Manager.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Cliquez sur **Protection > Relations**. Vous pouvez également consulter les relations à partir de la page Détails du volume.
2. À partir de la page **Relations de volume**, sélectionnez la relation SnapMirror à partir de laquelle vous souhaitez étendre la protection.
3. Dans la barre d'action, cliquez sur **Étendre la protection**.
4. Dans le menu, sélectionnez **Depuis la source** ou **Depuis la destination**, selon que vous créez une relation de diffusion à partir de la source ou une relation en cascade à partir de la destination.
5. Sélectionnez **Avec SnapMirror** ou **Avec SnapVault** selon le type de relation de protection que vous créez.

La boîte de dialogue **Configurer la protection** s'affiche.



Cela peut être réalisé à partir de la page de détails de la relation unifiée / Relation de volume et Volume / Santé.

6. Complétez les informations comme indiqué dans la boîte de dialogue **Configurer la protection**.

Modifier les relations de protection à partir de la page Relations de volume

Vous pouvez modifier les relations de protection existantes pour modifier le taux de transfert maximal, la politique de protection ou la planification de protection. Vous pouvez modifier une relation pour réduire la bande passante utilisée pour les transferts ou pour augmenter la fréquence des transferts planifiés, car les données changent souvent.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Les volumes sélectionnés doivent être des destinations de relation de protection. Vous ne pouvez pas modifier les relations lorsque des volumes sources, des volumes de partage de charge ou des volumes qui ne sont pas la destination d'une relation SnapMirror ou SnapVault sont sélectionnés.

Étapes

1. À partir de la page **Relations de volume**, sélectionnez dans la liste des volumes un ou plusieurs volumes dans la même SVM pour lesquels vous souhaitez modifier les paramètres de relation, puis sélectionnez **Modifier** dans la barre d'outils.

La boîte de dialogue Modifier la relation s'affiche.

2. Dans la boîte de dialogue **Modifier la relation**, modifiez le taux de transfert maximal, la politique de protection ou la planification de protection, selon vos besoins.
3. Cliquez sur **Appliquer**.

Les modifications sont appliquées aux relations sélectionnées.

Modifier les relations de protection à partir de la page Détails du volume/de la santé

Vous pouvez modifier les relations de protection existantes pour modifier le taux de transfert maximal actuel, la politique de protection ou la planification de protection. Vous pouvez modifier une relation pour réduire la bande passante utilisée pour les transferts ou pour augmenter la fréquence des transferts planifiés, car les données changent souvent.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir installé et configuré Workflow Automation.

Les volumes sélectionnés doivent être des destinations de relation de protection. Vous ne pouvez pas modifier les relations lorsque des volumes sources, des volumes de partage de charge ou des volumes qui ne sont pas la destination d'une relation SnapMirror ou SnapVault sont sélectionnés.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, recherchez dans la topologie la relation de protection que vous souhaitez modifier et cliquez dessus avec le bouton droit de la souris.
2. Sélectionnez **Modifier** dans le menu.

Alternativement, à partir du menu **Actions**, sélectionnez **Relation > Modifier** pour modifier la relation dont vous consultez actuellement les détails.

La boîte de dialogue **Modifier la relation** s'affiche.

3. Dans la boîte de dialogue Modifier la relation, modifiez le taux de transfert maximal, la stratégie de protection ou la planification de protection, selon vos besoins.
4. Cliquez sur **Appliquer**.

Les modifications sont appliquées aux relations sélectionnées.

Créez une politique SnapMirror pour maximiser l'efficacité du transfert

Vous pouvez créer une stratégie SnapMirror pour spécifier la priorité de transfert SnapMirror pour les relations de protection. Les stratégies SnapMirror vous permettent de maximiser l'efficacité du transfert de la source vers la destination en attribuant des priorités afin que les transferts de priorité inférieure soient planifiés pour s'exécuter après les transferts de priorité normale.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- Cette tâche suppose que vous avez déjà complété la zone Informations de destination dans la boîte de dialogue Configurer la protection.

Étapes

1. Dans l'onglet * SnapMirror* de la boîte de dialogue **Configurer la protection**, cliquez sur le lien **Créer une stratégie** dans la zone **Paramètres de relation**.

La boîte de dialogue Créer une stratégie SnapMirror s'affiche.

2. Dans le champ **Nom de la politique**, saisissez le nom que vous souhaitez donner à la politique.
3. Dans le champ **Priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la politique.
4. Dans le champ **Commentaire**, saisissez un commentaire facultatif pour la politique.
5. Cliquez sur **Créer**.

La nouvelle politique s'affiche dans la liste déroulante Politique SnapMirror .

Créez une politique SnapVault pour maximiser l'efficacité du transfert

Vous pouvez créer une nouvelle politique SnapVault pour définir la priorité d'un transfert SnapVault . Vous utilisez des politiques pour maximiser l'efficacité des transferts du primaire au secondaire dans une relation de protection.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- Vous devez déjà avoir complété la zone Informations de destination dans la boîte de dialogue Configurer la protection.

Étapes

1. Dans l'onglet * SnapVault* de la boîte de dialogue **Configurer la protection**, cliquez sur le lien **Créer une stratégie** dans la zone **Paramètres de relation**.

L'onglet SnapVault s'affiche.

2. Dans le champ **Nom de la politique**, saisissez le nom que vous souhaitez donner à la politique.
3. Dans le champ **Priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la politique.
4. **Facultatif** : dans le champ **Commentaire**, saisissez un commentaire pour la politique.
5. Dans la zone **Étiquette de réplication**, ajoutez ou modifiez une étiquette de réplication, si nécessaire.
6. Cliquez sur **Créer**.

La nouvelle politique s'affiche dans la liste déroulante Créer une politique.

Annuler un transfert de protection des données actif à partir de la page Relations de volume

Vous pouvez interrompre un transfert de protection des données actif lorsque vous souhaitez arrêter une réplication SnapMirror en cours. Vous pouvez également effacer le point de contrôle de redémarrage pour les transferts ultérieurs au transfert de base. Vous

pouvez interrompre un transfert lorsqu'il entre en conflit avec une autre opération, comme un déplacement de volume.



Vous ne pouvez pas interrompre les relations entre les volumes protégés par le groupe de cohérence.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

L'action d'abandon ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action : par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Vous ne pouvez pas effacer le point de contrôle de redémarrage pour un transfert de base.

Étapes

1. Pour interrompre les transferts pour une ou plusieurs relations de protection, à partir de la page **Relations de volume**, sélectionnez un ou plusieurs volumes et, dans la barre d'outils, cliquez sur **Annuler**.

La boîte de dialogue Abandonner le transfert s'affiche.

2. Si vous souhaitez effacer le point de contrôle de redémarrage pour un transfert qui n'est pas un transfert de base, sélectionnez **Effacer les points de contrôle**.
3. Cliquez sur **Continuer**.

La boîte de dialogue Abandonner le transfert est fermée et l'état de la tâche d'abandon s'affiche en haut de la page Relations de volume, ainsi qu'un lien vers les détails de la tâche.

4. **Facultatif** : cliquez sur le lien **Afficher les détails** pour accéder à la page de détails du **travail** pour obtenir des détails supplémentaires et pour afficher la progression du travail.

Annuler un transfert de protection des données actif à partir de la page Détails du volume/de la santé

Vous pouvez interrompre un transfert de protection des données actif lorsque vous souhaitez arrêter une réplication SnapMirror en cours. Vous pouvez également effacer le point de contrôle de redémarrage pour un transfert s'il ne s'agit pas d'un transfert de base. Vous pouvez interrompre un transfert lorsqu'il entre en conflit avec une autre opération, comme un déplacement de volume.



Vous ne pouvez pas interrompre les relations entre les volumes protégés par le groupe de cohérence.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

- Vous devez avoir configuré l'automatisation du flux de travail.

L'action d'abandon ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action : par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Vous ne pouvez pas effacer le point de contrôle de redémarrage pour un transfert de base.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, cliquez avec le bouton droit sur la relation dans la vue topologique pour le transfert de données que vous souhaitez interrompre et sélectionnez **Annuler**.

La boîte de dialogue Abandonner le transfert s'affiche.

2. Si vous souhaitez effacer le point de contrôle de redémarrage pour un transfert qui n'est pas un transfert de base, sélectionnez **Effacer les points de contrôle**.
3. Cliquez sur **Continuer**.

La boîte de dialogue Abandonner le transfert est fermée et l'état de l'opération d'abandon s'affiche en haut de la page Détails du volume/de l'état avec un lien vers les détails de la tâche.

4. **Facultatif** : cliquez sur le lien **Afficher les détails** pour accéder à la page de détails du **travail** pour obtenir des détails supplémentaires et pour afficher la progression du travail.
5. Cliquez sur chaque tâche pour afficher ses détails.
6. Cliquez sur la flèche Retour de votre navigateur pour revenir à la page de détails **Volume / Santé**.

L'opération d'abandon est terminée lorsque toutes les tâches sont terminées avec succès.

Suspendre une relation de protection à partir de la page Relations de volume

À partir de la page Relations de volume, vous pouvez suspendre une relation de protection pour empêcher temporairement les transferts de données. Vous pouvez suspendre une relation lorsque vous souhaitez créer une copie Snapshot d'un volume de destination SnapMirror contenant une base de données et que vous souhaitez vous assurer que son contenu est stable pendant l'opération de copie Snapshot.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

L'action de mise en veille ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action ; par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu ; par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

- Lorsque vous n'avez pas associé Workflow Automation et Unified Manager

Étapes

1. Pour suspendre les transferts pour une ou plusieurs relations de protection, à partir de la page **Relations de volume**, sélectionnez un ou plusieurs volumes et, dans la barre d'outils, cliquez sur **Suspendre**.

La boîte de dialogue Quiesce s'affiche.

2. Cliquez sur **Continuer**.

L'état de la tâche de mise en veille est affiché en haut de la page des détails Volume / Santé, avec un lien vers les détails de la tâche.

3. Cliquez sur le lien **Afficher les détails** pour accéder à la page de détails du **Travail** pour obtenir des détails supplémentaires et la progression du travail.
4. **Facultatif** : cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

La tâche de mise en veille est terminée lorsque toutes les tâches sont terminées avec succès.

Suspendre une relation de protection à partir de la page de détails Volume/Santé

Vous pouvez suspendre une relation de protection pour empêcher temporairement les transferts de données. Vous pouvez suspendre une relation lorsque vous souhaitez créer une copie Snapshot d'un volume de destination SnapMirror contenant une base de données et que vous souhaitez vous assurer que son contenu est stable pendant la copie Snapshot.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

L'action de mise en veille ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action, par exemple, si vous ne disposez que des privilèges d'opérateur
- Lorsque l'ID de volume est inconnu, par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert
- Lorsque vous n'avez pas associé Workflow Automation et Unified Manager

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, cliquez avec le bouton droit de la souris sur la relation dans la vue topologique pour la relation de protection que vous souhaitez suspendre.
2. Sélectionnez **Quiesce** dans le menu.
3. Cliquez sur **Oui** pour continuer.

L'état de la tâche de mise en veille est affiché en haut de la page des détails Volume / Santé, avec un lien vers les détails de la tâche.

4. Cliquez sur le lien **Afficher les détails** pour accéder à la page de détails du **Travail** pour obtenir des détails supplémentaires et la progression du travail.

5. **Facultatif** : cliquez sur la flèche Retour de votre navigateur pour revenir à la page de détails **Volume / Santé**.

La tâche de mise en veille est terminée lorsque toutes les tâches sont terminées avec succès.

Rompre une relation SnapMirror à partir de la page Relations de volume

Vous pouvez rompre une relation de protection pour arrêter les transferts de données entre un volume source et un volume de destination dans une relation SnapMirror . Vous pouvez rompre une relation lorsque vous souhaitez migrer des données, pour une reprise après sinistre ou pour des tests d'application. Le volume de destination est modifié en volume de lecture/écriture. Vous ne pouvez pas rompre une relation SnapVault .

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Dans la page **Relations de volume**, sélectionnez un ou plusieurs volumes avec des relations de protection pour lesquels vous souhaitez arrêter les transferts de données et, dans la barre d'outils, cliquez sur **Interrompre**.

La boîte de dialogue Rompre la relation s'affiche.

2. Cliquez sur **Continuer** pour rompre la relation.
3. Dans la page **Relations de volume**, vérifiez dans la colonne **État de la relation** que la relation est rompue.

La colonne État de la relation est masquée par défaut, vous devrez donc peut-être la sélectionner dans la liste des colonnes afficher/masquer  .

Supprimer une relation de protection de la page Relations de volume

À partir de la page Relations de volume, vous pouvez supprimer une relation de protection pour supprimer définitivement une relation existante entre la source et la destination sélectionnées : par exemple, lorsque vous souhaitez créer une relation à l'aide d'une destination différente. Cette opération supprime toutes les métadonnées et ne peut pas être annulée.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Dans la page **Relations de volume**, sélectionnez un ou plusieurs volumes avec des relations de protection que vous souhaitez supprimer et, dans la barre d'outils, cliquez sur **Supprimer**.

La boîte de dialogue Supprimer la relation s'affiche.

2. Cliquez sur **Continuer** pour supprimer la relation.

La relation est supprimée de la page Relations de volume.

Reprendre les transferts programmés sur une relation suspendue à partir de la page Relations de volume

Une fois que vous avez suspendu une relation pour empêcher les transferts planifiés de se produire, vous pouvez utiliser **Reprendre** pour réactiver les transferts planifiés afin que les données sur le volume source ou principal soient protégées. Les transferts reprennent à partir d'un point de contrôle, s'il existe, au prochain intervalle de transfert planifié.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Vous ne pouvez pas sélectionner plus de 10 relations suspendues sur lesquelles reprendre les transferts.

Étapes

1. Dans la page Relations entre volumes, sélectionnez un ou plusieurs volumes avec des relations suspendues et, dans la barre d'outils, cliquez sur **Reprendre**.
2. Dans la boîte de dialogue **Reprendre**, cliquez sur **Continuer**.

Vous êtes renvoyé à la page Relations de volume.

3. Pour afficher les tâches associées et suivre leur progression, cliquez sur le lien de tâche affiché en haut de la page **Relations de volume**.
4. Effectuez l'une des opérations suivantes :
 - Si un seul travail est affiché, dans la page Détails du travail, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection et pour déterminer quand le travail est terminé.
 - Si plusieurs tâches sont affichées,
 - i. Sur la page Emplois, cliquez sur l'emploi dont vous souhaitez afficher les détails.
 - ii. Dans la page Détails du travail, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection et pour déterminer quand le travail est terminé. Une fois les tâches terminées, les transferts de données reprennent à l'intervalle de transfert planifié suivant.

Reprendre les transferts programmés sur une relation suspendue à partir de la page Détails du volume/de la santé

Une fois que vous avez suspendu une relation pour empêcher les transferts planifiés de se produire, vous pouvez utiliser **Reprendre** sur la page Détails du volume/de l'état de santé pour réactiver les transferts planifiés afin que les données sur le volume source ou principal soient protégées. Les transferts reprennent à partir d'un point de contrôle, s'il existe, au prochain intervalle de transfert planifié.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, cliquez avec le bouton droit dans la vue topologique sur une relation suspendue que vous souhaitez reprendre.

Vous pouvez également sélectionner **Reprendre** dans le menu **Actions > Relation**.

2. Dans la boîte de dialogue **Reprendre**, cliquez sur **Continuer**.

Vous êtes renvoyé à la page des détails Volume / Santé.

3. Pour afficher les tâches associées et suivre leur progression, cliquez sur le lien de la tâche affiché en haut de la page de détails **Volume / Santé**.
4. Dans la page des détails du **Tâche**, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et pour déterminer quand la tâche est terminée.

Une fois les tâches terminées, les transferts de données reprennent à l'intervalle de transfert planifié suivant.

Initialiser ou mettre à jour les relations de protection à partir de la page Relations de volume

À partir de la page Relations de volume, vous pouvez effectuer un premier transfert de référence sur une nouvelle relation de protection ou mettre à jour une relation si elle est déjà initialisée et que vous souhaitez effectuer une mise à jour incrémentielle manuelle non planifiée pour effectuer un transfert immédiat.



Vous ne pouvez pas initialiser ou mettre à jour les volumes protégés par des groupes de cohérence.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans la page **Relations de volume**, cliquez avec le bouton droit sur un volume et sélectionnez un ou plusieurs volumes avec les relations que vous souhaitez mettre à jour ou initialiser, puis, dans la barre d'outils, cliquez sur **Initialiser/Mettre à jour**.

La boîte de dialogue **Initialiser/Mettre à jour** s'affiche.

2. Dans l'onglet **Options de transfert**, sélectionnez une priorité de transfert et le taux de transfert maximal.
3. Cliquez sur **Copies d'instantanés source** ; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

La boîte de dialogue Sélectionner la copie d'instantané source s'affiche.

4. Si vous souhaitez spécifier une copie d'instantané existante plutôt que de transférer la copie d'instantané par défaut, cliquez sur **Copie d'instantané existante** et sélectionnez une copie d'instantané dans la liste.

5. Cliquez sur **Soumettre**.

Vous êtes renvoyé à la boîte de dialogue **Initialiser/Mettre à jour**.

6. Si vous avez sélectionné plusieurs sources à initialiser ou à mettre à jour, cliquez sur **Par défaut** pour la source suivante pour laquelle vous souhaitez spécifier une copie instantanée existante.

7. Cliquez sur **Soumettre** pour commencer le travail d'initialisation ou de mise à jour.

La tâche d'initialisation ou de mise à jour est démarrée, vous revenez à la page Relations de volume et un lien de tâches s'affiche en haut de la page.

8. **Facultatif** : cliquez sur **Afficher les tâches** dans la vue **Santé : tous les volumes** pour suivre l'état de chaque tâche d'initialisation ou de mise à jour.

Une liste filtrée de tâches s'affiche.

9. **Facultatif** : cliquez sur chaque tâche pour voir ses détails.

10. **Facultatif** : cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

L'opération d'initialisation ou de mise à jour est terminée lorsque toutes les tâches se terminent avec succès.

Initialiser ou mettre à jour les relations de protection à partir de la page Détails du volume/de la santé

Vous pouvez effectuer un premier transfert de référence sur une nouvelle relation de protection ou mettre à jour une relation si elle est déjà initialisée et que vous souhaitez effectuer une mise à jour incrémentielle manuelle non planifiée pour transférer les données immédiatement.

REMARQUE : vous ne pouvez pas initialiser ou mettre à jour les volumes protégés par des groupes de cohérence.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, recherchez dans la topologie la relation de protection que vous souhaitez initialiser ou mettre à jour, puis cliquez dessus avec le bouton droit de la souris.
2. Sélectionnez **Initialiser/Mettre à jour** dans le menu.

Alternativement, à partir du menu **Actions**, sélectionnez **Relation > Initialiser/Mettre à jour** pour initialiser ou mettre à jour la relation dont vous consultez actuellement les détails.

La boîte de dialogue Initialiser/Mettre à jour s'affiche.

3. Dans l'onglet **Options de transfert**, sélectionnez une priorité de transfert et le taux de transfert maximal.
4. Cliquez sur **Copies d'instantanés source** ; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

La boîte de dialogue Sélectionner la copie d'instantané source s'affiche.

5. Si vous souhaitez spécifier une copie d'instantané existante plutôt que de transférer la copie d'instantané par défaut, cliquez sur **Copie d'instantané existante** et sélectionnez une copie d'instantané dans la liste.
6. Cliquez sur **Soumettre**.

Vous revenez à la boîte de dialogue Initialiser/Mettre à jour.

7. Si vous avez sélectionné plusieurs sources à initialiser ou à mettre à jour, cliquez sur **Par défaut** pour la prochaine source de lecture/écriture pour laquelle vous souhaitez spécifier une copie Snapshot existante.

Vous ne pouvez pas sélectionner une copie Snapshot différente pour les volumes de protection des données.

8. Cliquez sur **Soumettre** pour commencer le travail d'initialisation ou de mise à jour.

La tâche d'initialisation ou de mise à jour est démarrée, vous revenez à la page des détails Volume / Santé et un lien vers les tâches s'affiche en haut de la page.

9. **Facultatif** : cliquez sur **Afficher les tâches** sur la page de détails **Volume/Santé** pour suivre l'état de chaque tâche d'initialisation ou de mise à jour.

Une liste filtrée de tâches s'affiche.

10. **Facultatif** : cliquez sur chaque tâche pour voir ses détails.

11. **Facultatif** : cliquez sur la flèche Retour de votre navigateur pour revenir à la page de détails **Volume / Santé**.

L'opération d'initialisation ou de mise à jour est terminée lorsque toutes les tâches sont terminées avec succès.

Resynchroniser les relations de protection à partir de la page Relations de volume

À partir de la page Relations de volume, vous pouvez resynchroniser une relation soit pour récupérer après un événement qui a désactivé votre volume source, soit lorsque vous souhaitez modifier la source actuelle vers un volume différent.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.

Étapes

1. Dans la page **Relations de volume**, sélectionnez un ou plusieurs volumes avec des relations suspendues et, dans la barre d'outils, cliquez sur **Resynchroniser**.

La boîte de dialogue Resynchroniser s'affiche.

2. Dans l'onglet **Options de resynchronisation**, sélectionnez une priorité de transfert et le débit de transfert maximal.
3. Cliquez sur **Copies d'instantanés source** ; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

La boîte de dialogue Sélectionner la copie d'instantané source s'affiche.

4. Si vous souhaitez spécifier une copie d'instantané existante plutôt que de transférer la copie d'instantané par défaut, cliquez sur **Copie d'instantané existante** et sélectionnez une copie d'instantané dans la liste.
5. Cliquez sur **Soumettre**.

Vous revenez à la boîte de dialogue Resynchroniser.

6. Si vous avez sélectionné plusieurs sources à resynchroniser, cliquez sur **Par défaut** pour la source suivante pour laquelle vous souhaitez spécifier une copie instantanée existante.
7. Cliquez sur **Soumettre** pour commencer le travail de resynchronisation.

La tâche de resynchronisation est démarrée, vous revenez à la page Relations de volume et un lien de tâches s'affiche en haut de la page.

8. **Facultatif** : cliquez sur **Afficher les tâches** sur la page **Relations de volume** pour suivre l'état de chaque tâche de resynchronisation.

Une liste filtrée de tâches s'affiche.

9. **Facultatif** : cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

L'opération de resynchronisation est terminée lorsque toutes les tâches sont terminées avec succès.

Relations de protection inverse à partir de la page Relations de volume

Lorsqu'un sinistre désactive le volume source dans votre relation de protection, vous pouvez utiliser le volume de destination pour diffuser des données en le convertissant en volume de lecture/écriture pendant que vous réparez ou remplacez la source. Lorsque la source est à nouveau disponible pour recevoir des données, vous pouvez utiliser l'opération de resynchronisation inverse pour établir la relation dans le sens inverse, en synchronisant les données sur la source avec les données sur la destination de lecture/écriture.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré l'automatisation du flux de travail.
- La relation ne doit pas être une relation SnapVault .
- Une relation de protection doit déjà exister.
- La relation de protection doit être rompue.
- La source et la destination doivent être en ligne.
- La source ne doit pas être la destination d'un autre volume de protection des données.
- Lorsque vous effectuez cette tâche, les données de la source qui sont plus récentes que les données de la

copie Snapshot commune sont supprimées.

- Les politiques et les planifications créées sur les relations de resynchronisation inverse sont les mêmes que celles de la relation de protection d'origine.

Si les politiques et les calendriers n'existent pas, ils sont créés.

Étapes

1. Dans la page **Relations de volume**, sélectionnez un ou plusieurs volumes avec des relations que vous souhaitez inverser et, dans la barre d'outils, cliquez sur **Resynchronisation inverse**.

La boîte de dialogue Resynchronisation inversée s'affiche.

2. Vérifiez que les relations affichées dans la boîte de dialogue **Resynchronisation inverse** sont celles pour lesquelles vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Soumettre**.

L'opération de resynchronisation inverse est lancée, vous revenez à la page Relations de volume et un lien de tâches s'affiche en haut de la page.

3. **Facultatif** : cliquez sur **Afficher les tâches** sur la page **Relations de volume** pour suivre l'état de chaque tâche de resynchronisation inverse.

Une liste filtrée des tâches liées à cette opération s'affiche.

4. **Facultatif** : cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

L'opération de resynchronisation inverse est terminée lorsque toutes les tâches sont terminées avec succès.

Restaurer les données à l'aide des pages de détails Volume et Volume/Santé

Vous pouvez restaurer des fichiers, des répertoires ou un volume entier écrasés ou supprimés à partir d'une copie instantanée en utilisant la fonction de restauration sur les pages de détails Volume et Volume/Santé.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.



Notez les points suivants :

- Vous ne pouvez pas restaurer les flux de fichiers NTFS.
- L'option de restauration n'est pas disponible lorsque :
 - L'ID de volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert.
 - Le volume est configuré pour la réplication synchrone SnapMirror .

Étapes

1. Dans le volet de navigation de gauche, accédez à **Stockage > Volumes**.
2. Sélectionnez le volume et cliquez sur le bouton **Restaurer**. Vous pouvez également cliquer sur le volume pour accéder à **Volume / Détails de santé > Actions > Restaurer**. La boîte de dialogue Restaurer s'affiche. Pour plus d'informations sur cette page, voir "[Restaurer la boîte de dialogue](#)".

3. Sélectionnez le volume et la copie instantanée à partir desquels vous souhaitez restaurer les données, si différents de la valeur par défaut.
4. Sélectionnez les éléments que vous souhaitez restaurer, par exemple le LUN source.

Vous pouvez restaurer l'intégralité du volume ou spécifier les dossiers et les fichiers que vous souhaitez restaurer.

5. Sélectionnez l'emplacement vers lequel vous souhaitez restaurer les éléments sélectionnés : soit **Emplacement d'origine**, soit **Autre emplacement existant**.
6. Si vous sélectionnez un autre emplacement existant, effectuez l'une des opérations suivantes :
 - Dans le champ de texte Chemin de restauration, saisissez le chemin de l'emplacement vers lequel vous souhaitez restaurer les données, puis cliquez sur **Sélectionner le répertoire**.
 - Cliquez sur **Parcourir** pour lancer la boîte de dialogue Parcourir les répertoires et effectuez les étapes suivantes :
 - i. Sélectionnez le cluster de destination, la machine virtuelle de stockage (SVM) et le volume vers lesquels vous souhaitez effectuer la restauration.
 - ii. Dans le tableau Nom, sélectionnez un nom de répertoire à restaurer.
 - iii. Cliquez sur **Sélectionner le répertoire**.
7. Cliquez sur **Restaurer**.

Le processus de restauration commence. Une tâche est créée au niveau du backend pour terminer le processus de restauration.

8. Si vous souhaitez afficher la progression du travail, à partir du volet de navigation de gauche, accédez à **Protection > Travaux** pour afficher l'état du travail de restauration à partir de la liste des travaux.



Si une opération de restauration échoue entre les clusters Cloud Volumes ONTAP HA avec une erreur NDMP, vous devrez peut-être ajouter une route AWS explicite dans le cluster de destination afin que la destination puisse communiquer avec le LIF de gestion de cluster du système source. Vous effectuez cette étape de configuration à l'aide de la NetApp Console.

Que sont les pools de ressources

Les pools de ressources sont des groupes d'agrégats créés par un administrateur de stockage à l'aide d'Unified Manager pour fournir un provisionnement aux applications partenaires pour la gestion des sauvegardes.

Vous pouvez regrouper vos ressources en fonction d'attributs tels que les performances, le coût, l'emplacement physique ou la disponibilité. En regroupant les ressources associées dans un pool, vous pouvez traiter le pool comme une unité unique pour la surveillance et le provisionnement. Cela simplifie la gestion de ces ressources et permet une utilisation plus flexible et efficace du stockage.

Lors de la mise en service du stockage secondaire, Unified Manager détermine l'agrégat le plus approprié dans le pool de ressources pour la protection à l'aide des critères suivants :

- L'agrégat est un agrégat de données (pas un agrégat racine) et il est EN LIGNE.
- L'agrégat se trouve sur un nœud de cluster de destination dont la version ONTAP est identique ou supérieure à la version principale du cluster source.

- L'agrégat dispose du plus grand espace disponible de tous les agrégats du pool de ressources.
- Après avoir provisionné le volume de destination, l'espace agrégé se situe dans le seuil presque plein et presque surchargé défini pour l'agrégat (seuil global ou local, selon le cas).
- Le nombre de volumes FlexVol sur le nœud de destination ne doit pas dépasser la limite de la plate-forme.

Créer des pools de ressources

Vous pouvez utiliser la boîte de dialogue Créer un pool de ressources pour regrouper des agrégats à des fins de provisionnement.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

Les pools de ressources peuvent contenir des agrégats provenant de différents clusters, mais le même agrégat ne peut pas appartenir à différents pools de ressources.

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Pools de ressources**.
2. Dans la page **Pools de ressources**, cliquez sur **Créer**.
3. Suivez les instructions de la boîte de dialogue **Créer un pool de ressources** pour fournir un nom et une description et pour ajouter des agrégats en tant que membres au pool de ressources que vous souhaitez créer.

Modifier les pools de ressources

Vous pouvez modifier un pool de ressources existant lorsque vous souhaitez modifier le nom du pool de ressources et la description.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Le bouton **Modifier** est activé uniquement lorsqu'un pool de ressources est sélectionné. Si plusieurs pools de ressources sont sélectionnés, le bouton **Modifier** est désactivé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Pools de ressources**.
2. Sélectionnez un pool de ressources dans la liste.
3. Cliquez sur **Modifier**.

La fenêtre Modifier le pool de ressources s'affiche.

4. Modifiez le nom et la description du pool de ressources selon vos besoins.
5. Cliquez sur **Enregistrer**.

Le nouveau nom et la nouvelle description s'affichent dans la liste du pool de ressources.

Afficher l'inventaire des pools de ressources

Vous pouvez utiliser la page Pools de ressources pour afficher l'inventaire des pools de ressources et surveiller la capacité restante pour chaque pool de ressources.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Pools de ressources**.

L'inventaire du pool de ressources est affiché.

Ajouter des membres au pool de ressources

Un pool de ressources est constitué d'un certain nombre d'agrégats de membres. Vous pouvez ajouter des agrégats aux pools de ressources existants pour augmenter la quantité d'espace disponible pour le provisionnement de volumes secondaires.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous ne pouvez pas ajouter plus de 200 agrégats à un pool de ressources à la fois. Les agrégats affichés dans la boîte de dialogue Agrégats n'appartiennent à aucun autre pool de ressources.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Pools de ressources**.
2. Sélectionnez un pool de ressources dans la liste **Pools de ressources**.

Les membres du pool de ressources sont affichés dans la zone située sous la liste du pool de ressources.

3. Dans la zone des membres du pool de ressources, cliquez sur **Ajouter**.

La boîte de dialogue Agrégats s'affiche.

4. Sélectionnez un ou plusieurs agrégats.
5. Cliquez sur **Ajouter**.

La boîte de dialogue est fermée et les agrégats sont affichés dans la liste des membres du pool de ressources sélectionné.

Supprimer les agrégats des pools de ressources

Vous pouvez supprimer des agrégats d'un pool de ressources existant : par exemple, lorsque vous souhaitez utiliser un agrégat à d'autres fins.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Les membres du pool de ressources s'affichent uniquement lorsqu'un pool de ressources est sélectionné.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Pools de ressources**.
2. Sélectionnez le pool de ressources à partir duquel vous souhaitez supprimer les agrégats de membres.

La liste des agrégats de membres s'affiche dans le volet Membres.

3. Sélectionnez un ou plusieurs agrégats.

Le bouton **Supprimer** est activé.

4. Cliquez sur **Supprimer**.

Une boîte de dialogue d'avertissement s'affiche.

5. Cliquez sur **Oui** pour continuer.

Les agrégats sélectionnés sont supprimés du volet Membres.

Supprimer les pools de ressources

Vous pouvez supprimer les pools de ressources lorsqu'ils ne sont plus nécessaires. Par exemple, vous souhaitez peut-être redistribuer les agrégats de membres d'un pool de ressources vers plusieurs autres pools de ressources, rendant ainsi le pool de ressources d'origine obsolète.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Le bouton **Supprimer** est activé uniquement lorsqu'au moins un pool de ressources est sélectionné.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Pools de ressources**.
2. Sélectionnez le pool de ressources que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

Le pool de ressources est supprimé de la liste des pools de ressources et ses agrégats sont supprimés de la liste des membres.

Surveiller les relations de protection de reprise après sinistre des machines virtuelles de stockage

Active IQ Unified Manager prend en charge la surveillance des relations de reprise après sinistre des machines virtuelles de stockage, ce qui permet une reprise après sinistre au niveau de la granularité d'une machine virtuelle de stockage. La reprise après sinistre de la machine virtuelle de stockage permet la récupération des données présentes dans les volumes constitutifs de la machine virtuelle de stockage et la récupération de la configuration de la machine virtuelle de stockage.

Une relation DR de machine virtuelle de stockage est créée à partir de la machine virtuelle de stockage source

vers la machine virtuelle de stockage de destination pour fournir une reprise après sinistre asynchrone. Vous pouvez choisir de répliquer la totalité ou un sous-ensemble de la configuration de la machine virtuelle de stockage (à l'exclusion de la configuration du réseau et du protocole) ainsi que les volumes de données en fonction de la configuration du cluster.

Une fois la relation de reprise après sinistre de la machine virtuelle de stockage configurée, lorsque la machine virtuelle de stockage source devient indisponible en raison d'une panne matérielle ou d'une catastrophe environnementale, la machine virtuelle de stockage de destination est démarrée, ce qui permet d'accéder aux données avec le moins de perturbations possible. De même, lorsque la machine virtuelle de stockage source devient disponible, elle est resynchronisée avec la machine virtuelle de stockage de destination, puis la source redémarre pour fournir des données. Vous pouvez utiliser les commandes SnapMirror pour configurer et gérer la relation de reprise après sinistre de la machine virtuelle de stockage.

Surveiller les machines virtuelles de stockage à l'aide de la page Relations

Vous pouvez surveiller les relations de reprise après sinistre de votre machine virtuelle de stockage à partir de la page Relations de la section PROTECTION de l'INVENTAIRE. Par défaut, la page Relations répertorie uniquement les relations de niveau supérieur lorsque le filtre des relations constitutives est appliqué.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous utilisez des filtres pour afficher les relations de reprise après sinistre des machines virtuelles de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **PROTECTION > Relations**.

La page affiche tous les types de relations : volume, groupe de cohérence et relations de stockage de machines virtuelles.

2. Cliquez sur **Filtre**, puis sélectionnez **Type d'objet de relation** et **VM de stockage** pour afficher uniquement les relations de reprise après sinistre de la machine virtuelle de stockage.
3. Cliquez sur **Appliquer le filtre**.



Vous devez effacer le filtre des relations constitutives pour afficher toutes les relations de protection.

La page affiche uniquement les relations de reprise après sinistre des machines virtuelles de stockage.

Afficher les relations de protection à partir de la page Machines virtuelles de stockage

À l'aide de la page Machines virtuelles de stockage, vous pouvez afficher l'état des relations de reprise après sinistre des machines virtuelles de stockage existantes.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous pouvez également examiner les détails des relations de protection, notamment l'état du transfert et du décalage, la source et les détails de destination. Vous pouvez planifier des rapports ou télécharger des rapports existants dans le format dont vous avez besoin. Le bouton **Afficher/Masquer** vous permet d'ajouter

les colonnes requises aux rapports car elles ne sont pas affichées par défaut.

Étapes

- 1. Dans le volet de navigation de gauche, cliquez sur **STOCKAGE > VM de stockage**.
- 2. Dans le menu **AFFICHAGE**, sélectionnez **Relation > Toutes les relations**.

La vue Relation : Toutes les relations s’affiche avec toutes les machines virtuelles de stockage configurées.

Afficher les machines virtuelles de stockage en fonction de l’état de protection

Vous pouvez utiliser la page Machines virtuelles de stockage de l’inventaire pour afficher toutes les machines virtuelles de stockage dans Active IQ Unified Manager et filtrer les machines virtuelles de stockage en fonction de leur état de protection.

Avant de commencer

Vous devez disposer du rôle d’administrateur d’application ou d’administrateur de stockage.

Une nouvelle colonne Rôle de protection est ajoutée à la vue des machines virtuelles de stockage qui fournit des informations indiquant si la machine virtuelle de stockage est protégée ou non protégée.



Si un cluster source n’est pas ajouté à Active IQ Unified Manager, toutes les informations liées à ce cluster ne sont pas disponibles dans les grilles.

Étapes

- 1. Dans le volet de navigation de gauche, cliquez sur **STOCKAGE > VM de stockage**.
- 2. Dans le menu **AFFICHAGE**, sélectionnez **Santé > Toutes les machines virtuelles de stockage**.

L’état de santé : toutes les machines virtuelles de stockage s’affichent.

- 3. Cliquez sur **Filtre** pour afficher l’une des machines virtuelles de stockage suivantes.

Pour voir	Valeur du filtre
VM de stockage protégées	Le rôle de protection est Protégé
VM de stockage non protégées	Le rôle de protection est non protégé



Vous ne pouvez pas afficher simultanément les machines virtuelles de stockage protégées et non protégées. Vous devrez effacer le filtre existant pour réappliquer une nouvelle option de filtre.

- 4. Cliquez sur **Appliquer le filtre**.

La vue Non enregistrée affiche toutes les machines virtuelles de stockage qui sont protégées ou non protégées par la récupération après sinistre des machines virtuelles de stockage en fonction de vos sélections de filtre.

Comprendre les associations de machines virtuelles de stockage

Les associations de machines virtuelles de stockage (VM de stockage) sont des mappages d'une VM de stockage source vers une VM de stockage de destination qui sont utilisées par les applications partenaires pour la sélection des ressources et le provisionnement des volumes secondaires.

Des associations sont créées entre une machine virtuelle de stockage source et une machine virtuelle de stockage de destination, que la machine virtuelle de stockage de destination soit une destination secondaire ou tertiaire. Vous ne pouvez pas utiliser une machine virtuelle de stockage de destination secondaire comme source pour créer une association avec une machine virtuelle de stockage de destination tertiaire.

En tant qu'administrateur d'application ou administrateur de stockage, vous pouvez afficher les associations de machines virtuelles de stockage dans votre environnement sur la page **Protection > Associations de machines virtuelles de stockage**.

Vous pouvez associer des SVM de trois manières :

- **Associer n'importe quelle machine virtuelle de stockage** : vous pouvez créer une association entre n'importe quelle machine virtuelle de stockage source principale et une ou plusieurs SVM de destination. Cela signifie que toutes les SVM existantes qui nécessitent actuellement une protection, ainsi que toutes les SVM créées à l'avenir, sont associées aux SVM de destination spécifiées. Par exemple, vous souhaitez peut-être que des applications provenant de plusieurs sources différentes situées à différents emplacements soient sauvegardées sur une ou plusieurs SVM de destination dans un seul emplacement.
- **Associer une machine virtuelle de stockage particulière** : vous pouvez créer une association entre une machine virtuelle de stockage source spécifique et une ou plusieurs SVM de destination spécifiques. Par exemple, si vous fournissez des services de stockage à de nombreux clients dont les données doivent être séparées les unes des autres, vous pouvez choisir cette option pour associer une machine virtuelle de stockage source spécifique à une machine virtuelle de stockage de destination spécifique attribuée uniquement à ce client.
- **Associer à une machine virtuelle de stockage externe** : vous pouvez créer une association entre une machine virtuelle de stockage source et un volume flexible externe d'une machine virtuelle de stockage de destination.

Créer des associations de machines virtuelles de stockage

L'assistant Créer des associations de machines virtuelles de stockage permet aux applications de protection des partenaires d'associer une machine virtuelle de stockage source à une machine virtuelle de stockage de destination à utiliser avec les relations SnapMirror et SnapVault . Les applications partenaires utilisent ces associations au moment du provisionnement initial des volumes de destination pour déterminer les ressources à sélectionner.dd

Avant de commencer

- La machine virtuelle de stockage que vous associez doit déjà exister.
- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Pour toute machine virtuelle de stockage source et tout type de relation, vous ne pouvez choisir qu'une seule machine virtuelle de stockage de destination sur chaque cluster de destination.

La modification des associations à l'aide des fonctions de suppression et de création affecte uniquement les opérations de provisionnement futures. Il ne déplace pas les volumes de destination existants.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Associations de machines virtuelles de stockage**.
2. Sur la page **Associations de machines virtuelles de stockage**, cliquez sur **Créer**.

L'assistant **Créer des associations de machines virtuelles de stockage** est lancé.

3. Sélectionnez l'une des sources suivantes :

- **N'importe lequel**

Choisissez cette option lorsque vous souhaitez créer une association entre une source de machine virtuelle de stockage principale et une ou plusieurs machines virtuelles de stockage de destination. Cela signifie que toutes les machines virtuelles de stockage existantes qui nécessitent actuellement une protection, ainsi que toutes les machines virtuelles de stockage créées à l'avenir, sont associées à la machine virtuelle de stockage de destination spécifiée. Par exemple, vous souhaitez peut-être que des applications provenant de plusieurs sources différentes situées à différents emplacements soient sauvegardées sur une ou plusieurs machines virtuelles de stockage de destination dans un seul emplacement.

- **Célibataire**

Choisissez cette option lorsque vous souhaitez sélectionner une machine virtuelle de stockage source spécifique associée à une ou plusieurs machines virtuelles de stockage de destination. Par exemple, si vous fournissez des services de stockage à de nombreux clients dont les données doivent être séparées les unes des autres, choisissez cette option pour associer une source de machine virtuelle de stockage spécifique à une destination de machine virtuelle de stockage spécifique attribuée uniquement à ce client.

- **Aucun (externe)**

Choisissez cette option lorsque vous souhaitez créer une association entre une machine virtuelle de stockage source et un volume flexible externe d'une machine virtuelle de stockage de destination.

4. Sélectionnez l'un ou les deux types de relations de protection que vous souhaitez créer :

- * SnapMirror*
- * SnapVault*

5. Cliquez sur **Suivant**.

6. Sélectionnez une ou plusieurs destinations de protection de machine virtuelle de stockage.

7. Cliquez sur **Terminer**.

Supprimer les associations de machines virtuelles de stockage

Vous pouvez supprimer les associations de machines virtuelles de stockage pour les applications partenaires afin de supprimer la relation de provisionnement secondaire entre les machines virtuelles de stockage source et de destination ; par exemple, vous pouvez le faire lorsque la machine virtuelle de stockage de destination est pleine et que vous souhaitez créer de nouvelles associations de protection de machine virtuelle de stockage.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Le bouton **Supprimer** est désactivé jusqu'à ce qu'au moins une association de machine virtuelle de stockage soit sélectionnée. La modification des associations à l'aide des fonctions de suppression et de création affecte uniquement les opérations de provisionnement futures ; elle ne déplace pas les volumes de destination existants.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Associations de machines virtuelles de stockage**.

2. Sélectionnez au moins une association de machine virtuelle de stockage.

Le bouton **Supprimer** est activé.

3. Cliquez sur **Supprimer**.

Une boîte de dialogue d'avertissement s'affiche.

4. Cliquez sur **Oui** pour continuer.

L'association de machine virtuelle de stockage sélectionnée est supprimée de la liste.

Exigences relatives aux SVM et aux pools de ressources pour prendre en charge les services de stockage

Vous pouvez mieux garantir la conformité dans les applications partenaires si vous respectez certaines exigences d'association SVM et de pool de ressources spécifiques aux services de stockage : par exemple, lorsque vous associez SVM et créez des pools de ressources dans Unified Manager pour prendre en charge une topologie de protection dans un service de stockage fourni par une application partenaire.

Certaines applications s'associent au serveur Unified Manager pour fournir des services qui configurent et exécutent automatiquement la protection de sauvegarde SnapMirror ou SnapVault entre les volumes sources et les volumes de protection dans des emplacements secondaires ou tertiaires. Pour prendre en charge ces services de stockage de protection, vous devez utiliser Unified Manager pour configurer les associations SVM et les pools de ressources nécessaires.

Pour prendre en charge la protection en cascade ou à saut unique du service de stockage, y compris la réplication à partir d'une source SnapMirror ou d'un volume principal SnapVault vers un SnapMirror de destination ou vers des volumes de sauvegarde SnapVault résidant dans des emplacements secondaires ou tertiaires, respectez les exigences suivantes :

- Les associations SVM doivent être configurées entre la SVM contenant la source SnapMirror ou le volume principal SnapVault et toute SVM sur laquelle réside un volume secondaire ou un volume tertiaire.
 - Par exemple, pour prendre en charge une topologie de protection dans laquelle le volume source Vol_A réside sur SVM_1, le volume de destination secondaire SnapMirror Vol_B réside sur SVM_2 et le volume de sauvegarde tertiaire SnapVault Vol_C réside sur SVM_3, vous devez utiliser l'interface utilisateur Web d'Unified Manager pour configurer une association SnapMirror entre SVM_1 et SVM_2 et une association de sauvegarde SnapVault entre SVM_1 et SVM_3.

Dans cet exemple, toute association SnapMirror ou association de sauvegarde SnapVault entre SVM_2 et SVM_3 n'est pas nécessaire et n'est pas utilisée.

- Pour prendre en charge une topologie de protection dans laquelle le volume source Vol_A et le volume

de destination SnapMirror Vol_B résident sur SVM_1, vous devez configurer une association SnapMirror entre SVM_1 et SVM_1.

- Les pools de ressources doivent inclure des ressources agrégées de cluster disponibles pour les SVM associées.

Vous configurez les pools de ressources via l'interface utilisateur Web d'Unified Manager, puis attribuez via l'application partenaire les nœuds cibles secondaires et tertiaires du service de stockage.

Quels sont les emplois

Un travail est une série de tâches que vous pouvez surveiller à l'aide d'Unified Manager. L'affichage des tâches et des tâches associées vous permet de déterminer si elles ont été exécutées avec succès.

Les tâches sont lancées lorsque vous créez des relations SnapMirror et SnapVault, lorsque vous effectuez une opération de relation (interrompre, modifier, suspendre, supprimer, reprendre, resynchroniser et inverser la resynchronisation), lorsque vous effectuez des tâches de restauration de données, lorsque vous vous connectez à un cluster, etc.

Lorsque vous lancez une tâche, vous pouvez utiliser la page Tâches et la page Détails de la tâche pour surveiller la tâche et la progression des tâches associées.

Surveiller les emplois

Vous pouvez utiliser la page Tâches pour surveiller l'état des tâches et afficher les propriétés des tâches telles que le type de service de stockage, l'état, l'heure de soumission et l'heure de fin pour déterminer si une tâche s'est terminée avec succès ou non.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Tâches**.

La page Emplois s'affiche.

2. Consultez la colonne **État** pour déterminer l'état des tâches en cours d'exécution.
3. Cliquez sur le nom d'un travail pour afficher les détails de ce travail particulier.

La page Détails du travail s'affiche.

Voir les détails du poste

Après avoir démarré une tâche, vous pouvez suivre sa progression à partir de la page Détails de la tâche et surveiller les tâches associées pour détecter d'éventuelles erreurs.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Tâches**.
2. Dans la page Tâches, cliquez sur le nom d'une tâche dans la colonne **Nom** pour afficher la liste des tâches associées à la tâche.
3. Cliquez sur une tâche pour afficher des informations supplémentaires dans le volet **Détails de la tâche** et le volet **Messages de la tâche** à droite de la liste des tâches.

Abandonner les tâches

Vous pouvez utiliser la page Tâches pour interrompre une tâche si elle prend trop de temps à se terminer, rencontre trop d'erreurs ou n'est plus nécessaire. Vous ne pouvez interrompre une tâche que si son statut et son type le permettent. Vous pouvez interrompre n'importe quelle tâche en cours d'exécution.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Tâches**.
2. Dans la liste des tâches, sélectionnez-en une, puis cliquez sur **Annuler**.
3. À l'invite de confirmation, cliquez sur **Oui** pour abandonner la tâche sélectionnée.

Réessayer une tâche de protection ayant échoué

Après avoir pris des mesures pour corriger une tâche de protection ayant échoué, vous pouvez utiliser **Réessayer** pour exécuter à nouveau la tâche. La nouvelle tentative d'exécution d'une tâche crée une nouvelle tâche en utilisant l'ID de tâche d'origine.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Vous ne pouvez réessayer qu'une seule tâche échouée à la fois. La sélection de plusieurs tâches désactive le bouton **Réessayer**. Seuls les travaux de type Configuration de protection et Opération de relation de protection peuvent être retentés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection > Tâches**.
2. Dans la liste des tâches, sélectionnez une seule tâche de type Configuration de protection ou Opération de relation de protection ayant échoué.

Le bouton **Réessayer** est activé.

3. Cliquez sur **Réessayer**.

Le travail est redémarré.

Description des fenêtres et boîtes de dialogue des relations de protection

Vous pouvez afficher et gérer les détails liés à la protection, tels que les pools de ressources, les associations SVM et les tâches de protection. Vous pouvez utiliser la page Seuils de santé appropriée pour configurer les valeurs de seuil de santé globales pour les agrégats, les volumes et les relations.

Page des pools de ressources

La page Pools de ressources affiche les pools de ressources existants et leurs membres, et vous permet de créer, surveiller et gérer des pools de ressources à des fins de provisionnement.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Créer**

Lance la boîte de dialogue Créer un pool de ressources, que vous pouvez utiliser pour créer des pools de ressources.

- **Modifier**

Vous permet de modifier le nom et la description des pools de ressources que vous créez.

- **Supprimer**

Vous permet de supprimer un ou plusieurs pools de ressources.

Liste des pools de ressources

La liste des pools de ressources affiche (sous forme de tableau) les propriétés des pools de ressources existants.

- **Réserve de ressources**

Affiche le nom du pool de ressources.

- **Description**

Décrit le pool de ressources.

- *** Type de SnapLock ***

Affiche le type SnapLock utilisé par les agrégats du pool de ressources. Les valeurs valides pour le type SnapLock sont Conformité, Entreprise et Non- SnapLock. Un pool de ressources ne peut contenir que des agrégats d'un seul type SnapLock .

- **Capacité totale**

Affiche la capacité totale (en Mo, Go, etc.) du pool de ressources.

- **Capacité utilisée**

Affiche la quantité d'espace (en Mo, Go, etc.) utilisée dans le pool de ressources.

- **Capacité disponible**

Affiche la quantité d'espace (en Mo, Go, etc.) disponible dans le pool de ressources.

- **Utilisé %**

Affiche le pourcentage d'espace utilisé dans le pool de ressources.

Boutons de commande de la liste des membres

Les boutons de commande de la liste des membres vous permettent d'effectuer les tâches suivantes :

- **Ajouter**

Vous permet d'ajouter des membres au pool de ressources.

- **Supprimer**

Vous permet de supprimer un ou plusieurs membres du pool de ressources.

Liste des membres

La liste des membres affiche (sous forme de tableau) les membres du pool de ressources et leurs propriétés lorsqu'un pool de ressources est sélectionné.

- **Statut**

Affiche l'état actuel de l'agrégat de membres. Le statut peut être Critique (❌), Erreur (!), Avertissement (⚠️), ou Normal (✅).

- **Nom global**

Affiche le nom de l'agrégat de membres.

- **État**

Affiche l'état actuel de l'agrégat, qui peut être l'un des suivants :

- Hors ligne

L'accès en lecture ou en écriture n'est pas autorisé.

- En ligne

L'accès en lecture et en écriture aux volumes hébergés sur cet agrégat est autorisé.

- Limité

Des opérations limitées (telles que la reconstruction de parité) sont autorisées, mais l'accès aux données n'est pas autorisé.

- Créer

L'agrégat est en cours de création.

- Détruire

L'agrégat est en train d'être détruit.

- Échec

L'agrégat ne peut pas être mis en ligne.

- Congelé

L'agrégat ne répond pas (temporairement) aux demandes.

- Incompatible

L'agrégat a été marqué comme corrompu ; vous devez contacter le support technique.

- Fer restreint

Les outils de diagnostic ne peuvent pas être exécutés sur l'agrégat.

- Montage

L'agrégat est en cours de montage.

- Partiel

Au moins un disque a été trouvé pour l'agrégat, mais deux disques ou plus sont manquants.

- Mise au repos

L'agrégat est en cours de mise au repos.

- Au repos

L'agrégat est mis au repos.

- Renversé

La conversion d'un agrégat est terminée.

- Non monté

L'agrégat a été démonté.

- Démontage

L'agrégat est en cours de mise hors ligne.

- Inconnu

L'agrégat est découvert, mais les informations agrégées ne sont pas encore récupérées par le serveur Unified Manager.

Par défaut, cette colonne est masquée.

- **Grappe**

Affiche le nom du cluster auquel appartient l'agrégat.

- **Nœud**

Affiche le nom du nœud sur lequel réside l'agrégat.

- **Capacité totale**

Affiche la capacité totale (en Mo, Go, etc.) de l'agrégat.

- **Capacité utilisée**

Affiche la quantité d'espace (en Mo, Go, etc.) utilisée dans l'ensemble.

- **Capacité disponible**

Affiche la quantité d'espace (en Mo, Go, etc.) disponible dans l'ensemble.

- **Utilisé %**

Affiche le pourcentage d'espace utilisé dans l'ensemble.

- **Type de disque**

Affiche le type de configuration RAID, qui peut être l'un des suivants :

- RAID0 : Tous les groupes RAID sont de type RAID0.
- RAID4 : Tous les groupes RAID sont de type RAID4.
- RAID-DP : Tous les groupes RAID sont de type RAID-DP.
- RAID-TEC: Tous les groupes RAID sont de type RAID-TEC.
- RAID mixte : l'agrégat contient des groupes RAID de différents types RAID (RAID0, RAID4, RAID-DP et RAID-TEC). Par défaut, cette colonne est masquée.

Boîte de dialogue Créer un pool de ressources

Vous pouvez utiliser la boîte de dialogue Créer un pool de ressources pour nommer et décrire un nouveau pool de ressources et pour ajouter et supprimer des agrégats de ce pool de ressources.

Nom du pool de ressources

Les zones de texte vous permettent d'ajouter les informations suivantes pour créer un pool de ressources :

Vous permet de spécifier un nom de pool de ressources.

Description

Vous permet de décrire un pool de ressources.

Membres

Affiche les membres du pool de ressources. Vous pouvez également ajouter et supprimer des membres.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Ajouter**

Ouvre la boîte de dialogue Agrégats afin que vous puissiez ajouter des agrégats d'un cluster spécifique au pool de ressources. Vous pouvez ajouter des agrégats provenant de différents clusters, mais les mêmes agrégats ne peuvent pas être ajoutés à plusieurs pools de ressources.

- **Retirer**

Vous permet de supprimer les agrégats sélectionnés du pool de ressources.

- **Créer**

Crée le pool de ressources. Ce bouton n'est pas activé tant que les informations n'ont pas été saisies dans les champs Nom du pool de ressources ou Description.

- **Annuler**

Annule les modifications et ferme la boîte de dialogue Créer un pool de ressources.

Boîte de dialogue Modifier le pool de ressources

Vous pouvez utiliser la boîte de dialogue Modifier le pool de ressources pour modifier le nom et la description d'un pool de ressources existant. Par exemple, si le nom et la description d'origine sont inexacts ou incorrects, vous pouvez les modifier pour qu'ils soient plus précis.

Zones de texte

Les zones de texte vous permettent de modifier les informations suivantes pour le pool de ressources sélectionné :

- **Nom du pool de ressources**

Vous permet de saisir un nouveau nom.

- **Description**

Vous permet de saisir une nouvelle description.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Sauvegarder**

Enregistre les modifications apportées au nom et à la description du pool de ressources.

- **Annuler**

Annule les modifications et ferme la boîte de dialogue Modifier le pool de ressources.

Boîte de dialogue Agrégats

Vous pouvez utiliser la boîte de dialogue Agrégats pour sélectionner les agrégats que vous souhaitez ajouter à votre pool de ressources.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Ajouter**

Ajoute les agrégats sélectionnés au pool de ressources. Le bouton Ajouter n'est pas activé tant qu'au moins un agrégat n'est pas sélectionné.

- **Annuler**

Annule les modifications et ferme la boîte de dialogue Agrégats.

Liste des agrégats

La liste des agrégats affiche (sous forme de tableau) les noms et les propriétés des agrégats surveillés.

- **Statut**

Affiche l'état actuel d'un volume. Le statut peut être Critique (❌), Erreur (⚠️), Avertissement (⚠️), ou Normal (✅).

Vous pouvez déplacer le pointeur sur l'état pour afficher plus d'informations sur l'événement ou les événements générés pour le volume.

- **Nom global**

Affiche le nom de l'agrégat.

- **État**

Affiche l'état actuel de l'agrégat, qui peut être l'un des suivants :

- Hors ligne

L'accès en lecture ou en écriture n'est pas autorisé.

- Limité

Des opérations limitées (telles que la reconstruction de parité) sont autorisées, mais l'accès aux données n'est pas autorisé.

- En ligne

L'accès en lecture et en écriture aux volumes hébergés sur cet agrégat est autorisé.

- Créer

L'agrégat est en cours de création.

- Détruire

L'agrégat est en train d'être détruit.

- Échec

L'agrégat ne peut pas être mis en ligne.

- Congelé

L'agrégat ne répond pas (temporairement) aux demandes.

- Incompatible

L'agrégat a été marqué comme corrompu ; vous devez contacter le support technique.

- Fer restreint

Les outils de diagnostic ne peuvent pas être exécutés sur l'agrégat.

- Montage

L'agrégat est en cours de montage.

- Partiel

Au moins un disque a été trouvé pour l'agrégat, mais deux disques ou plus sont manquants.

- Mise au repos

L'agrégat est en cours de mise au repos.

- Au repos

L'agrégat est mis au repos.

- Renversé

La conversion d'un agrégat est terminée.

- Non monté

L'agrégat est hors ligne.

- Démontage

L'agrégat est en cours de mise hors ligne.

- Inconnu

L'agrégat est découvert, mais les informations agrégées ne sont pas encore récupérées par le serveur Unified Manager.

- **Grappe**

Affiche le nom du cluster sur lequel réside l'agrégat.

- **Nœud**

Affiche le nom du contrôleur de stockage qui contient l'agrégat.

- **Capacité totale**

Affiche la taille totale des données (en Mo, Go, etc.) de l'agrégat. Par défaut, cette colonne est masquée.

- **Capacité engagée**

Affiche l'espace total (en Mo, Go, etc.) engagé pour tous les volumes de l'agrégat. Par défaut, cette colonne est masquée.

- **Capacité utilisée**

Affiche la quantité d'espace (en Mo, Go, etc.) utilisée dans l'ensemble.

- **Capacité disponible**

Affiche la quantité d'espace (en Mo, Go, etc.) disponible pour les données dans l'ensemble. Par défaut, cette colonne est masquée.

- **Disponible %**

Affiche le pourcentage d'espace disponible pour les données dans l'agrégat. Par défaut, cette colonne est masquée.

- **Utilisé %**

Affiche le pourcentage d'espace utilisé par les données dans l'agrégat.

- **Type de RAID**

Affiche le type RAID du volume sélectionné. Le type RAID peut être RAID0, RAID4, RAID-DP, RAID-TEC ou RAID mixte.

Page d'emplois

La page Tâches vous permet d'afficher l'état actuel et d'autres informations sur toutes les tâches de protection des applications partenaires en cours d'exécution, ainsi que sur les tâches terminées. Vous pouvez utiliser ces informations pour voir quelles tâches sont toujours en cours d'exécution et si une tâche a réussi ou échoué.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Avorter**

Annule le travail sélectionné. Cette option n'est disponible que si le travail sélectionné est en cours

d'exécution.

- **Réessayer**

Redémarre une tâche ayant échoué de type Configuration de protection ou Opération de relation de protection. Vous ne pouvez réessayer qu'une seule tâche échouée à la fois. Si plusieurs tâches ayant échoué sont sélectionnées, le bouton **Réessayer** est désactivé. Vous ne pouvez pas réessayer les tâches de service de stockage ayant échoué.

- **Rafraîchir**

Actualise la liste des tâches et les informations qui leur sont associées.

Liste des emplois

La liste des tâches affiche, sous forme de tableau, une liste des tâches en cours. Par défaut, la liste affiche uniquement les tâches générées au cours de la semaine écoulée. Vous pouvez utiliser le tri et le filtrage des colonnes pour personnaliser les tâches affichées.

- **Statut**

Affiche l'état actuel d'un travail. Le statut peut être Erreur () ou Normal () .

- **Identifiant du travail**

Affiche le numéro d'identification du travail. Par défaut, cette colonne est masquée.

Le numéro d'identification du travail est unique et est attribué par le serveur lorsqu'il démarre le travail. Vous pouvez rechercher un emploi particulier en saisissant le numéro d'identification de l'emploi dans la zone de texte fournie par le filtre de colonne.

- **Nom**

Affiche le nom du travail.

- **Taper**

Affiche le type de travail. Les types d'emplois sont les suivants :

- **Acquisition de clusters**

Un travail d'automatisation du flux de travail redécouvre un cluster.

- **Configuration de protection**

Une tâche de protection lance des flux de travail d'automatisation des flux de travail, tels que les planifications cron, la création de politiques SnapMirror , etc.

- **Opération de relation de protection**

Une tâche de protection exécute des opérations SnapMirror .

- **Chaîne de flux de travail de protection**

Un travail d'automatisation de flux de travail exécute plusieurs flux de travail.

- **Restaurer**

Une tâche de restauration est en cours d'exécution.

- **Nettoyage**

La tâche consiste à nettoyer les artefacts des membres du service de stockage qui ne sont plus nécessaires à des fins de restauration.

- **Se conformer**

La tâche consiste à vérifier la configuration des membres du service de stockage pour s'assurer qu'ils sont conformes.

- **Détruire**

Le travail consiste à détruire un service de stockage.

- **Importer**

Le travail consiste à importer des objets de stockage non gérés dans un service de stockage existant.

- **Modifier**

Le travail consiste à modifier les attributs d'un service de stockage existant.

- **S'abonner**

Le travail consiste à abonner des membres à un service de stockage.

- **Se désabonner**

La tâche consiste à désabonner les membres d'un service de stockage.

- **Mise à jour**

Une tâche de mise à jour de protection est en cours d'exécution.

- **Configuration WFA**

Un travail d'automatisation du flux de travail consiste à envoyer les informations d'identification du cluster et à synchroniser les caches de base de données.

- **État**

Affiche l'état d'exécution du travail. Les options d'état sont les suivantes :

- **Avorté**

Le travail a été abandonné.

- **Abandon**

Le travail est en train d'être abandonné.

- **Complété**

Le travail est terminé.

- **En cours d'exécution**

Le travail est en cours d'exécution.

- **Heure de soumission**

Affiche l'heure à laquelle le travail a été soumis.

- **Durée**

Affiche le temps nécessaire à l'exécution du travail. Cette colonne est affichée par défaut.

- **Heure terminée**

Affiche l'heure à laquelle le travail est terminé. Par défaut, cette colonne est masquée.

Page de détails du travail

La page Détails du travail vous permet d'afficher l'état et d'autres informations sur les tâches de protection spécifiques en cours d'exécution, en file d'attente ou terminées. Vous pouvez utiliser ces informations pour surveiller la progression des tâches de protection et pour résoudre les échecs de tâches.

Résumé du poste

Le résumé du travail affiche les informations suivantes :

- ID de travail
- Type
- État
- Heure de soumission
- Heure d'achèvement
- Durée

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Rafraîchir**

Actualise la liste des tâches et les propriétés associées à chaque tâche.

- **Voir les offres d'emploi**

Vous ramène à la page Emplois.

Liste des tâches du poste

La liste des tâches du travail affiche dans un tableau toutes les tâches associées à un travail spécifique et les

propriétés liées à chaque tâche.

- **Heure de début**

Affiche le jour et l'heure de début de la tâche. Par défaut, les tâches les plus récentes sont affichées en haut de la colonne et les tâches plus anciennes sont affichées en bas.

- **Taper**

Affiche le type de tâche.

- **État**

L'état d'une tâche particulière :

- **Complété**

La tâche est terminée.

- **En file d'attente**

La tâche est sur le point d'être exécutée.

- **En cours d'exécution**

La tâche est en cours d'exécution.

- **En attendant**

Un travail a été soumis et certaines tâches associées attendent d'être mises en file d'attente et exécutées.

- **Statut**

Affiche l'état de la tâche :

- **Erreur (🚫)**

La tâche a échoué.

- **Normale (✅)**

La tâche a réussi.

- **Sauté (🔄)**

Une tâche a échoué, ce qui a entraîné l'ignorance des tâches suivantes.

- **Durée**

Affiche le temps écoulé depuis le début de la tâche.

- **Heure terminée**

Affiche l'heure à laquelle la tâche est terminée. Par défaut, cette colonne est masquée.

- **ID de tâche**

Affiche le GUID qui identifie une tâche individuelle pour un travail. La colonne peut être triée et filtrée. Par défaut, cette colonne est masquée.

- **Ordre de dépendance**

Affiche un entier représentant la séquence de tâches dans un graphique, zéro étant attribué à la première tâche. Par défaut, cette colonne est masquée.

- **Volet Détails de la tâche**

Affiche des informations supplémentaires sur chaque tâche, notamment le nom de la tâche, la description de la tâche et, si la tâche a échoué, la raison de l'échec.

- **Volet Messages de tâche**

Affiche les messages spécifiques à la tâche sélectionnée. Les messages peuvent inclure une raison de l'erreur et des suggestions pour la résoudre. Toutes les tâches n'affichent pas de messages de tâche.

Boîte de dialogue Paramètres secondaires avancés

Vous pouvez utiliser la boîte de dialogue Paramètres secondaires avancés pour activer la réplication flexible en termes de version, la sauvegarde de plusieurs copies et les paramètres liés à l'espace sur un volume secondaire. Vous pouvez utiliser la boîte de dialogue Paramètres secondaires avancés lorsque vous souhaitez modifier, activer ou désactiver les paramètres actuels.

Les paramètres liés à l'espace maximisent la quantité de données stockées, notamment les suivants : déduplication, compression des données, croissance automatique et garantie d'espace.

La boîte de dialogue comprend les champs suivants :

- **Activer la réplication flexible des versions**

Active SnapMirror avec une réplication flexible en fonction des versions. La réplication flexible en fonction des versions permet la protection SnapMirror d'un volume source même si le volume de destination s'exécute sous une version d' ONTAP antérieure à celle du volume source.

- Activer la sauvegarde

Si la réplication flexible en fonction des versions est activée, elle permet également de transférer et de conserver plusieurs copies Snapshot des données sources SnapMirror vers la destination SnapMirror .

- **Activer la déduplication**

Active la déduplication sur le volume secondaire dans une relation SnapVault afin que les blocs de données en double soient éliminés pour réaliser des économies d'espace. Vous pouvez utiliser la déduplication lorsque les économies d'espace sont d'au moins 10 % et lorsque le taux d'écrasement des données n'est pas rapide. La déduplication est souvent utilisée pour les environnements virtualisés, les partages de fichiers et les données de sauvegarde. Ce paramètre est désactivé par défaut. Lorsque cette option est activée, cette opération est lancée après chaque transfert.

- Activer la compression

Permet une compression transparente des données. Vous pouvez utiliser la compression lorsque les économies d'espace sont d'au moins 10 %, lorsque la surcharge potentielle est acceptable et lorsqu'il y a suffisamment de ressources système pour que la compression soit terminée en dehors des heures de pointe. Dans une relation SnapVault, ce paramètre est désactivé par défaut. La compression n'est disponible que lorsque la déduplication est sélectionnée.

- Compresser en ligne

Permet des économies d'espace immédiates en compressant les données avant de les écrire sur le disque. Vous pouvez utiliser la compression en ligne lorsque votre système n'a pas plus de 50 % d'utilisation pendant les heures de pointe et lorsque le système peut prendre en charge de nouvelles écritures et du CPU supplémentaire pendant les heures de pointe. Ce paramètre est disponible uniquement lorsque « Activer la compression » est sélectionné.

- **Activer la croissance automatique**

Vous permet d'augmenter automatiquement le volume de destination lorsque le pourcentage d'espace libre est inférieur au seuil spécifié, à condition que de l'espace soit disponible sur l'agrégat associé.

- **Taille maximale**

Définit le pourcentage maximal auquel un volume peut croître. La valeur par défaut est 20 % supérieure à la taille du volume source. Un volume ne se développe pas automatiquement si la taille actuelle est supérieure ou égale au pourcentage de croissance automatique maximal. Ce champ est activé uniquement lorsque le paramètre de croissance automatique est activé.

- **Augmenter la taille**

Spécifie l'incrément de pourcentage par lequel le volume augmente automatiquement avant d'atteindre le pourcentage maximal du volume source.

- **Garantie d'espace**

Garantit que suffisamment d'espace est alloué sur le volume secondaire afin que les transferts de données réussissent toujours. Le paramètre de garantie d'espace peut être l'un des suivants :

- Déposer
- Volume
- Aucun + Par exemple, vous pouvez avoir un volume de 200 Go contenant des fichiers totalisant 50 Go ; cependant, ces fichiers ne contiennent que 10 Go de données. La garantie de volume alloue 200 Go au volume de destination, quel que soit le contenu de la source. La garantie de fichier alloue 50 Go pour garantir que suffisamment d'espace est réservé aux fichiers sur la source ; sélectionner Aucun dans ce scénario signifie que seulement 10 Go sont alloués sur la destination pour l'espace réel utilisé par les données de fichier sur la source.

La garantie d'espace est définie sur Volume par défaut.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Appliquer**

Enregistre les paramètres d'efficacité sélectionnés et les applique lorsque vous cliquez sur **Appliquer** dans la boîte de dialogue Configurer la protection.

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Paramètres de destination avancés.

Boîte de dialogue Paramètres de destination avancés

Vous pouvez utiliser la boîte de dialogue Paramètres de destination avancés pour activer les paramètres de garantie d'espace sur un volume de destination. Vous pouvez sélectionner des paramètres avancés lorsque la garantie d'espace est désactivée sur la source, mais vous souhaitez qu'elle soit activée sur la destination. Les paramètres de déduplication, de compression et de croissance automatique dans une relation SnapMirror sont hérités du volume source et ne peuvent pas être modifiés.

Garantie d'espace

Garantit que suffisamment d'espace est alloué sur le volume de destination afin que les transferts de données réussissent toujours. Le paramètre de garantie d'espace peut être l'un des suivants :

- Déposer
- Volume
- Aucune

Par exemple, vous pouvez avoir un volume de 200 Go contenant des fichiers totalisant 50 Go ; cependant, ces fichiers ne contiennent que 10 Go de données. La garantie de volume alloue 200 Go au volume de destination, quel que soit le contenu de la source. La garantie de fichier alloue 50 Go pour garantir que suffisamment d'espace est réservé aux fichiers sources sur la destination ; la sélection de **Aucun** dans ce scénario signifie que seulement 10 Go sont alloués sur la destination pour l'espace réel utilisé par les données de fichier sur la source.

La garantie d'espace est définie sur Volume par défaut.

Restaurer la boîte de dialogue

Vous pouvez utiliser la boîte de dialogue Restaurer pour restaurer des données sur un volume à partir d'une copie instantanée spécifique.

Restaurer à partir de

La zone Restaurer à partir de vous permet de spécifier à partir de quel endroit vous souhaitez restaurer les données.

- **Volume**

Spécifie le volume à partir duquel vous souhaitez restaurer les données. Par défaut, le volume sur lequel vous avez lancé l'action de restauration est sélectionné. Vous pouvez sélectionner un volume différent dans la liste déroulante qui contient tous les volumes avec des relations de protection avec le volume sur lequel vous avez lancé l'action de restauration.

- **Copie instantanée**

Spécifie la copie instantanée que vous souhaitez utiliser pour restaurer les données. Par défaut, la copie instantanée la plus récente est sélectionnée. Vous pouvez également sélectionner une copie d'instantané

différente dans la liste déroulante. La liste des copies instantanées change en fonction du volume sélectionné.

- **Liste maximale de 995 fichiers et répertoires**

Par défaut, un maximum de 995 objets sont affichés dans la liste. Vous pouvez décocher cette case si vous souhaitez afficher tous les objets dans le volume sélectionné. Cette opération peut prendre un certain temps si le nombre d'éléments est très important.

Sélectionnez les éléments à restaurer

La zone Sélectionner les éléments à restaurer vous permet de sélectionner soit le volume entier, soit des fichiers et des dossiers spécifiques que vous souhaitez restaurer. Vous pouvez sélectionner un maximum de 10 fichiers, dossiers ou une combinaison des deux. Lorsque le nombre maximal d'éléments est sélectionné, les cases à cocher de sélection d'éléments sont désactivées.

- **Champ de chemin**

Affiche le chemin d'accès aux données que vous souhaitez restaurer. Vous pouvez soit accéder au dossier et aux fichiers que vous souhaitez restaurer, soit saisir le chemin. Ce champ est vide jusqu'à ce que vous sélectionniez ou saisissiez un chemin. En cliquant  après avoir choisi un chemin, vous remontez d'un niveau dans la structure du répertoire.

- **Liste des dossiers et fichiers**

Affiche le contenu du chemin que vous avez entré. Par défaut, le dossier racine est initialement affiché. Cliquer sur le nom d'un dossier affiche le contenu du dossier.

Vous pouvez sélectionner les éléments à restaurer comme suit :

- Lorsque vous entrez le chemin avec un nom de fichier particulier spécifié dans le champ chemin, le fichier spécifié s'affiche dans les dossiers et fichiers.
- Lorsque vous entrez un chemin sans spécifier de fichier particulier, le contenu du dossier s'affiche dans la liste Dossiers et fichiers, et vous pouvez sélectionner jusqu'à 10 fichiers, dossiers ou une combinaison des deux à restaurer.

Si un dossier contient plus de 995 éléments, un message s'affiche pour indiquer qu'il y a trop d'éléments à afficher, et si vous poursuivez l'opération, tous les éléments du dossier spécifié sont restaurés. Vous pouvez décocher la case « Répertorier un maximum de 995 fichiers et répertoires » si vous souhaitez afficher tous les objets dans le volume sélectionné.



Vous ne pouvez pas restaurer les flux de fichiers NTFS.

Restaurer à

La zone Restaurer vers vous permet de spécifier où vous souhaitez restaurer les données.

- **Emplacement d'origine dans Volume_Name**

Restaure les données sélectionnées dans le répertoire de la source à partir de laquelle les données ont été initialement sauvegardées.

- **Autre emplacement**

Restaure les données sélectionnées vers un nouvel emplacement :

- Restaurer le chemin

Spécifie un chemin alternatif pour restaurer les données sélectionnées. Le chemin doit déjà exister. Vous pouvez utiliser le bouton **Parcourir** pour accéder à l'emplacement où vous souhaitez restaurer les données, ou vous pouvez saisir le chemin manuellement en utilisant le format `cluster://svm/volume/path`.

- Préserver la hiérarchie des répertoires

Lorsque cette option est cochée, elle préserve la structure du fichier ou du répertoire d'origine. Par exemple, si la source est `/A/B/C/myFile.txt` et la destination est `/X/Y/Z`, Unified Manager restaure les données à l'aide de la structure de répertoire suivante sur la destination : `/X/Y/Z/A/B/C/myFile.txt`.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Restaurer.

- **Restaurer**

Applique vos sélections et commence le processus de restauration.

Boîte de dialogue Parcourir les répertoires

Vous pouvez utiliser la boîte de dialogue Parcourir les répertoires lorsque vous souhaitez restaurer des données dans un répertoire d'un cluster et d'un SVM différent de la source d'origine. Le cluster source et le volume d'origine sont sélectionnés par défaut.

La boîte de dialogue Parcourir les répertoires vous permet de sélectionner le cluster, le SVM, le volume et le chemin d'accès au répertoire vers lesquels vous souhaitez restaurer les données.

- **Grappe**

Répertorie les destinations de cluster disponibles vers lesquelles vous pouvez effectuer une restauration. Par défaut, le cluster du volume source d'origine est sélectionné.

- **Liste déroulante SVM**

Répertorie les SVM disponibles pour le cluster sélectionné. Par défaut, le SVM du volume source d'origine est sélectionné.

- **Volume**

Répertorie tous les volumes de lecture/écriture dans un SVM sélectionné. Vous pouvez filtrer les volumes par nom et par espace disponible. Le volume avec le plus d'espace est répertorié en premier, et ainsi de suite, par ordre décroissant. Par défaut, le volume source d'origine est sélectionné.

- **Zone de texte du chemin du fichier**

Vous permet de saisir le chemin du fichier vers lequel vous souhaitez restaurer les données. Le chemin que vous entrez doit déjà exister.

- **Nom**

Affiche les noms des dossiers disponibles pour le volume sélectionné. Cliquer sur un dossier dans la liste Nom affiche les sous-dossiers, s'il en existe. Les fichiers contenus dans les dossiers ne sont pas affichés.

En cliquant  après avoir sélectionné un dossier, vous remontez d'un niveau dans la structure du répertoire.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Sélectionner un répertoire**

Applique vos sélections et ferme la boîte de dialogue Parcourir les répertoires. Si aucun répertoire n'est sélectionné, ce bouton est désactivé.

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Parcourir les répertoires.

Boîte de dialogue Configurer la protection

Vous pouvez utiliser la boîte de dialogue Configurer la protection pour créer des relations SnapMirror et SnapVault pour tous les volumes de lecture, d'écriture et de protection des données sur les clusters afin de garantir que les données sur un volume source ou un volume principal sont répliquées.

Onglet Source

- **Vue topologique**

Affiche une représentation visuelle de la relation que vous créez. La source dans la topologie est mise en surbrillance par défaut.

- **Source d'information**

Affiche les détails sur les volumes sources sélectionnés, y compris les informations suivantes :

- Nom du cluster source
- Nom de la SVM source
- Volume cumulé taille totale

Affiche la taille totale de tous les volumes sources sélectionnés.

- Taille du volume cumulé utilisé

Affiche la taille cumulée du volume utilisé pour tous les volumes sources sélectionnés.

- Volume source

Affiche les informations suivantes dans un tableau :

- Volume source

Affiche les noms des volumes sources sélectionnés.

- Type

Affiche le type de volume.

- Type de SnapLock

Affiche le type SnapLock du volume. Les options sont Conformité, Entreprise et Non- SnapLock.

- Copie instantanée

Affiche la copie instantanée utilisée pour le transfert de base. Si le volume source est en lecture/écriture, la valeur Par défaut dans la colonne Copie d'instantané indique qu'une nouvelle copie d'instantané est créée par défaut et est utilisée pour le transfert de base. Si le volume source est un volume de protection des données, la valeur Par défaut dans la colonne Copie d'instantané indique qu'aucune nouvelle copie d'instantané n'est créée et que toutes les copies d'instantané existantes sont transférées vers la destination. Cliquer sur la valeur Copie d'instantané affiche une liste de copies d'instantané à partir de laquelle vous pouvez sélectionner une copie d'instantané existante à utiliser pour le transfert de base. Vous ne pouvez pas sélectionner une copie Snapshot par défaut différente si le type de source est la protection des données.

Onglet SnapMirror

Vous permet de spécifier un cluster de destination, une machine virtuelle de stockage (SVM) et un agrégat pour une relation de protection, ainsi qu'une convention de dénomination pour les destinations lors de la création d'une relation SnapMirror . Vous pouvez également spécifier une politique et une planification SnapMirror .

• Vue topologique

Affiche une représentation visuelle de la relation que vous créez. La ressource de destination SnapMirror dans la topologie est mise en surbrillance par défaut.

• Informations sur la destination

Vous permet de sélectionner les ressources de destination pour une relation de protection :

- Lien avancé

Lance la boîte de dialogue Paramètres de destination avancés lorsque vous créez une relation SnapMirror .

- Cluster

Répertorie les clusters disponibles en tant qu'hôtes de destination de protection. Ce champ est obligatoire.

- machine virtuelle de stockage (SVM)

Répertorie les SVM disponibles sur le cluster sélectionné. Un cluster doit être sélectionné avant que la liste SVM ne soit remplie. Ce champ est obligatoire.

- Agrégat

Répertorie les agrégats disponibles sur le SVM sélectionné. Un cluster doit être sélectionné avant que la liste agrégée ne soit remplie. Ce champ est obligatoire. La liste agrégée affiche les informations suivantes :

- Rang

Lorsque plusieurs agrégats satisfont à toutes les exigences d'une destination, le rang indique la priorité dans laquelle l'agrégat est répertorié, selon les conditions suivantes :

- A. Un agrégat situé sur un nœud différent du nœud de volume source est préféré pour permettre la séparation du domaine de panne.
- B. Un agrégat sur un nœud avec moins de volumes est préférable pour permettre l'équilibrage de charge entre les nœuds d'un cluster.
- C. Un agrégat disposant de plus d'espace libre que les autres agrégats est préféré pour permettre l'équilibrage des capacités. Un rang de 1 signifie que l'agrégat est le plus préféré selon les trois critères.

- Nom agrégé

Nom de l'agrégat

- Capacité disponible
 - Quantité d'espace disponible sur l'agrégat pour les données
 - Réserve de ressources

Nom du pool de ressources auquel appartient l'agrégat

- Convention de dénomination

Spécifie la convention de dénomination par défaut appliquée au volume de destination. Vous pouvez accepter la convention de dénomination fournie ou en créer une personnalisée. La convention de dénomination peut avoir les attributs suivants : %C, %M, %V et %N, où %C est le nom du cluster, %M est le nom du SVM, %V est le volume source et %N est le nom du nœud de destination de la topologie.

Le champ de convention de dénomination est surligné en rouge si votre entrée n'est pas valide. Cliquer sur le lien « Aperçu du nom » affiche un aperçu de la convention de nommage que vous avez saisie, et le texte d'aperçu se met à jour de manière dynamique lorsque vous saisissez une convention de nommage dans le champ de texte. Un suffixe compris entre 001 et 999 est ajouté au nom de destination lors de la création de la relation, remplaçant le nnn qui s'affiche dans le texte d'aperçu, 001 étant attribué en premier, 002 en second, et ainsi de suite.

- Paramètres de relation

Vous permet de spécifier le taux de transfert maximal, la politique SnapMirror et la planification utilisés par la relation de protection :

- Taux de transfert maximal

Spécifie le débit maximal auquel les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser de taux de transfert maximal, le transfert de base entre les relations est illimité.

- Politique SnapMirror

Spécifie la politique ONTAP SnapMirror pour la relation. La valeur par défaut est DPDefault.

- Créer une politique

Lance la boîte de dialogue Créer une stratégie SnapMirror , qui vous permet de créer et d'utiliser une nouvelle stratégie SnapMirror .

- Programme SnapMirror

Spécifie la politique ONTAP SnapMirror pour la relation. Les horaires disponibles incluent Aucun, 5 minutes, 8 heures, quotidien, horaire et hebdomadaire. La valeur par défaut est Aucun, ce qui indique qu'aucune planification n'est associée à la relation. Les relations sans planification n'ont pas de valeurs d'état de décalage, sauf si elles appartiennent à un service de stockage.

- Créer un calendrier

Lance la boîte de dialogue Créer une planification, qui vous permet de créer une nouvelle planification SnapMirror .

Onglet SnapVault

Vous permet de spécifier un cluster secondaire, un SVM et un agrégat pour une relation de protection, ainsi qu'une convention de dénomination pour les volumes secondaires lors de la création d'une relation SnapVault . Vous pouvez également spécifier une politique et une planification SnapVault .

- **Vue topologique**

Affiche une représentation visuelle de la relation que vous créez. La ressource secondaire SnapVault dans la topologie est mise en surbrillance par défaut.

- **Informations secondaires**

Vous permet de sélectionner les ressources secondaires pour une relation de protection :

- Lien avancé

Lance la boîte de dialogue Paramètres secondaires avancés.

- Cluster

Répertorie les clusters disponibles en tant qu'hôtes de protection secondaires. Ce champ est obligatoire.

- machine virtuelle de stockage (SVM)

Répertorie les SVM disponibles sur le cluster sélectionné. Un cluster doit être sélectionné avant que la liste SVM ne soit remplie. Ce champ est obligatoire.

- Agrégat

Répertorie les agrégats disponibles sur le SVM sélectionné. Un cluster doit être sélectionné avant que la liste agrégée ne soit remplie. Ce champ est obligatoire. La liste agrégée affiche les informations suivantes :

- Rang

Lorsque plusieurs agrégats satisfont à toutes les exigences d'une destination, le rang indique la priorité dans laquelle l'agrégat est répertorié, selon les conditions suivantes :

- A. Un agrégat situé sur un nœud différent du nœud de volume principal est préféré pour permettre la séparation des domaines de pannes.
- B. Un agrégat sur un nœud avec moins de volumes est préférable pour permettre l'équilibrage de charge entre les nœuds d'un cluster.
- C. Un agrégat disposant de plus d'espace libre que les autres agrégats est préféré pour permettre l'équilibrage des capacités. Un rang de 1 signifie que l'agrégat est le plus préféré selon les trois critères.

- Nom agrégé

Nom de l'agrégat

- Capacité disponible
- Quantité d'espace disponible sur l'agrégat pour les données
- Réserve de ressources

Nom du pool de ressources auquel appartient l'agrégat

- Convention de dénomination

Spécifie la convention de dénomination par défaut appliquée au volume secondaire. Vous pouvez accepter la convention de dénomination fournie ou en créer une personnalisée. La convention de dénomination peut avoir les attributs suivants : %C, %M, %V et %N, où %C est le nom du cluster, %M est le nom de la SVM, %V est le volume source et %N est le nom du nœud secondaire de topologie.

Le champ de convention de dénomination est surligné en rouge si votre entrée n'est pas valide. Cliquer sur le lien « Aperçu du nom » affiche un aperçu de la convention de nommage que vous avez saisie, et le texte d'aperçu se met à jour de manière dynamique lorsque vous saisissez une convention de nommage dans le champ de texte. Si vous saisissez une valeur non valide, les informations non valides s'affichent sous forme de points d'interrogation rouges dans la zone d'aperçu. Un suffixe compris entre 001 et 999 est ajouté au nom secondaire lors de la création de la relation, remplaçant le nnn qui s'affiche dans le texte d'aperçu, 001 étant attribué en premier, 002 en deuxième, et ainsi de suite.

- Paramètres de relation

Vous permet de spécifier le taux de transfert maximal, la politique SnapVault et la planification SnapVault utilisés par la relation de protection :

- Taux de transfert maximal

Spécifie le débit maximal auquel les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser de taux de transfert maximal, le transfert de base entre les relations est illimité.

- Politique SnapVault

Spécifie la stratégie ONTAP SnapVault pour la relation. La valeur par défaut est XDPDefault.

- **Créer une politique**

Lance la boîte de dialogue Créer une stratégie SnapVault , qui vous permet de créer et d'utiliser une nouvelle stratégie SnapVault .

- **Calendrier SnapVault**

Spécifie la planification ONTAP SnapVault pour la relation. Les horaires disponibles incluent Aucun, 5 minutes, 8 heures, quotidien, horaire et hebdomadaire. La valeur par défaut est Aucun, ce qui indique qu'aucune planification n'est associée à la relation. Les relations sans planification n'ont pas de valeurs d'état de décalage, sauf si elles appartiennent à un service de stockage.

- **Créer un calendrier**

Lance la boîte de dialogue Créer une planification, qui vous permet de créer une planification SnapVault .

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Configurer la protection.

- **Appliquer**

Applique vos sélections et commence le processus de protection.

Boîte de dialogue Créer un planning

La boîte de dialogue Créer une planification vous permet de créer une planification de protection de base ou avancée pour les transferts de relations SnapMirror et SnapVault . Vous pouvez créer une nouvelle planification pour augmenter la fréquence des transferts de données en raison de mises à jour fréquentes des données, ou vous pouvez créer une planification moins fréquente lorsque les données changent rarement.

Les planifications ne peuvent pas être configurées pour les relations synchrones SnapMirror .

- **Groupe de destinations**

Le nom du cluster que vous avez sélectionné dans l'onglet SnapVault ou SnapMirror de la boîte de dialogue Configurer la protection.

- **Nom de l'horaire**

Le nom que vous fournissez pour le calendrier. Les noms de planification peuvent être composés des caractères A à Z, a à z, 0 à 9, ainsi que de l'un des caractères spéciaux suivants : ! @ # \$ % ^ & * () _ - . Les noms de planification ne peuvent pas inclure les caractères suivants : < > .

- **Basique ou avancé**

Le mode de planification que vous souhaitez utiliser.

Le mode de base comprend les éléments suivants :

- Répéter

À quelle fréquence un transfert programmé a lieu. Les choix incluent des tarifs horaires, quotidiens et hebdomadaires.

- Jour

Lorsqu'une répétition hebdomadaire est sélectionnée, le jour de la semaine où un transfert a lieu.

- Durée

Lorsque Quotidien ou Hebdomadaire est sélectionné, l'heure de la journée à laquelle un transfert a lieu.

Le mode avancé comprend les éléments suivants :

- Mois

Une liste numérique séparée par des virgules représentant les mois de l'année. Les valeurs valides sont comprises entre 0 et 11, zéro représentant janvier, et ainsi de suite. Cet élément est facultatif. Laisser le champ vide implique que les transferts ont lieu tous les mois.

- Jours

Une liste numérique séparée par des virgules représentant le jour du mois. Les valeurs valides sont comprises entre 1 et 31. Cet élément est facultatif. Laisser le champ vide implique qu'un transfert a lieu chaque jour du mois.

- Jours de la semaine

Une liste numérique séparée par des virgules représentant les jours de la semaine. Les valeurs valides sont comprises entre 0 et 6, 0 représentant le dimanche, et ainsi de suite. Cet élément est facultatif. Laisser le champ vide implique qu'un transfert a lieu tous les jours de la semaine. Si un jour de la semaine est spécifié mais qu'un jour du mois n'est pas spécifié, un transfert se produit uniquement le jour de la semaine spécifié et non tous les jours.

- Heures

Une liste numérique séparée par des virgules représentant le nombre d'heures dans une journée. Les valeurs valides sont comprises entre 0 et 23, 0 représentant minuit. Cet élément est facultatif.

- Minutes

Une liste numérique séparée par des virgules représentant les minutes d'une heure. Les valeurs valides sont comprises entre 0 et 59. Cet élément est obligatoire.

Boîte de dialogue Créer une stratégie SnapMirror

La boîte de dialogue Créer une stratégie SnapMirror vous permet de créer une stratégie pour définir la priorité des transferts SnapMirror . Vous utilisez des politiques pour

maximiser l'efficacité des transferts de la source vers la destination.

- **Groupe de destinations**

Le nom du cluster que vous avez sélectionné dans l'onglet SnapMirror de la boîte de dialogue Configurer la protection.

- **Destination SVM**

Le nom du SVM que vous avez sélectionné dans l'onglet SnapMirror de la boîte de dialogue Configurer la protection.

- **Nom de la politique**

Le nom que vous fournissez pour la nouvelle politique. Les noms de politique peuvent être composés des caractères A à Z, a à z, 0 à 9, d'un point (.), d'un trait d'union (-) et d'un trait de soulignement (_).

- **Priorité de transfert**

La priorité à laquelle un transfert s'exécute pour les opérations asynchrones. Vous pouvez sélectionner Normal ou Faible. Les relations de transfert avec des stratégies qui spécifient une priorité de transfert normale s'exécutent avant celles avec des stratégies qui spécifient une priorité de transfert faible.

- **Commentaire**

Un champ facultatif dans lequel vous pouvez ajouter des commentaires sur la politique.

- **Redémarrage du transfert**

Indique l'action de redémarrage à entreprendre lorsqu'un transfert est interrompu par une opération d'abandon ou tout type de panne, comme une panne de réseau. Vous pouvez sélectionner l'une des options suivantes :

- Toujours

Spécifie qu'une nouvelle copie Snapshot est créée avant de redémarrer un transfert, puis, s'il en existe une, le transfert est redémarré à partir d'un point de contrôle, suivi d'un transfert incrémentiel à partir de la copie Snapshot nouvellement créée.

- Jamais

Spécifie que les transferts interrompus ne sont jamais redémarrés.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

Annule les sélections et ferme la boîte de dialogue Configurer la protection.

- **Appliquer**

Applique vos sélections et démarre le processus de protection.

Boîte de dialogue Créer une stratégie SnapVault

La boîte de dialogue Créer une stratégie SnapVault vous permet de créer une stratégie pour définir la priorité des transferts SnapVault . Vous utilisez des stratégies pour maximiser l'efficacité des transferts du volume principal vers le volume secondaire.

- **Groupe de destinations**

Le nom du cluster que vous avez sélectionné dans l'onglet SnapVault de la boîte de dialogue Configurer la protection.

- **Destination SVM**

Le nom du SVM que vous avez sélectionné dans l'onglet SnapVault de la boîte de dialogue Configurer la protection.

- **Nom de la politique**

Le nom que vous fournissez pour la nouvelle politique. Les noms de politique peuvent être composés des caractères A à Z, a à z, 0 à 9, d'un point (.), d'un trait d'union (-) et d'un trait de soulignement (_).

- **Priorité de transfert**

La priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner Normal ou Faible. Les relations de transfert avec des stratégies qui spécifient une priorité de transfert normale s'exécutent avant celles avec des stratégies qui spécifient une priorité de transfert faible. Le paramètre par défaut est Normal.

- **Commentaire**

Un champ facultatif dans lequel vous pouvez ajouter un commentaire contenant jusqu'à 255 caractères sur la politique SnapVault .

- **Ignorer le temps d'accès**

Spécifie si les transferts incrémentiels sont ignorés pour les fichiers dont seul le temps d'accès a été modifié.

- **Étiquette de réplication**

Répertorie dans un tableau les règles associées aux copies Snapshot sélectionnées par ONTAP qui ont une étiquette de réplication spécifique dans une politique. Les informations et actions suivantes sont également disponibles :

- Boutons de commande

Les boutons de commande vous permettent d'effectuer les actions suivantes :

- Ajouter

Vous permet de créer une étiquette de copie d'instantané et un nombre de rétentions.

- Modifier le nombre de rétentions

Vous permet de modifier le nombre de rétentions pour une étiquette de copie d'instantané existante. Le nombre de rétention doit être un nombre compris entre 1 et 251. La somme de tous

les nombres de rétention pour toutes les règles ne peut pas dépasser 251.

- **Supprimer**

Vous permet de supprimer une étiquette de copie d'instantané existante.

- **Étiquette de copie d'instantané**

Affiche l'étiquette de copie de l'instantané. Si vous sélectionnez un ou plusieurs volumes avec la même stratégie de copie Snapshot locale, une entrée pour chaque étiquette de la stratégie s'affiche. Si vous sélectionnez plusieurs volumes dotés de deux ou plusieurs stratégies de copie Snapshot locales, le tableau affiche toutes les étiquettes de toutes les stratégies.

- **Calendrier**

Affiche la planification associée à chaque étiquette de copie d'instantané. Si une étiquette est associée à plusieurs planifications, les planifications de cette étiquette sont affichées dans une liste séparée par des virgules. Si vous sélectionnez plusieurs volumes avec la même étiquette mais avec des planifications différentes, la planification affiche « Divers » pour indiquer que plusieurs planifications sont associées aux volumes sélectionnés.

- **Nombre de rétentions de destination**

Affiche le nombre de copies Snapshot avec l'étiquette spécifiée qui sont conservées sur le SnapVault secondaire. Les nombres de rétention pour les étiquettes avec plusieurs planifications affichent la somme des nombres de rétention de chaque paire d'étiquettes et de planifications. Si vous sélectionnez plusieurs volumes avec deux ou plusieurs stratégies de copie d'instantanés locaux, le nombre de rétentions est vide.

Boîte de dialogue Modifier la relation

Vous pouvez modifier une relation de protection existante pour modifier le taux de transfert maximal, la politique de protection ou la planification de protection.

Informations sur la destination

- **Groupe de destinations**

Le nom du cluster de destination sélectionné.

- **Destination SVM**

Le nom du SVM sélectionné

- **Paramètres de relation**

Vous permet de spécifier le taux de transfert maximal, la politique SnapMirror et la planification utilisés par la relation de protection :

- **Taux de transfert maximal**

Spécifie le débit maximal auquel les données de base sont transférées entre les clusters sur le réseau. Lorsque cette option est sélectionnée, la bande passante du réseau est limitée à la valeur que vous spécifiez. Vous pouvez saisir une valeur numérique, puis sélectionner kilo-octets par seconde (Ko/s), mégaoctets par seconde (Mo/s), gigaoctets par seconde (Go/s) ou téraoctets par seconde (To/s). Le

débit de transfert maximal que vous spécifiez doit être supérieur à 1 Ko/s et inférieur à 4 To/s. Si vous choisissez de ne pas utiliser de taux de transfert maximal, le transfert de base entre les relations est illimité. Si le cluster principal et le cluster secondaire sont identiques, ce paramètre est désactivé.

- **Politique SnapMirror**

Spécifie la politique ONTAP SnapMirror pour la relation. La valeur par défaut est DPDefault.

- **Créer une politique**

Lance la boîte de dialogue Créer une stratégie SnapMirror , qui vous permet de créer et d'utiliser une nouvelle stratégie SnapMirror .

- **Programme SnapMirror**

Spécifie la politique ONTAP SnapMirror pour la relation. Les horaires disponibles incluent Aucun, 5 minutes, 8 heures, quotidien, horaire et hebdomadaire. La valeur par défaut est Aucun, ce qui indique qu'aucune planification n'est associée à la relation. Les relations sans planification n'ont pas de valeurs d'état de décalage, sauf si elles appartiennent à un service de stockage.

- **Créer un calendrier**

Lance la boîte de dialogue Créer une planification, qui vous permet de créer une nouvelle planification SnapMirror .

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

Annule les sélections et ferme la boîte de dialogue Configurer la protection.

- **Soumettre**

Applique vos sélections et ferme la boîte de dialogue Modifier la relation.

Boîte de dialogue Initialiser/Mettre à jour

La boîte de dialogue Initialiser/Mettre à jour vous permet d'effectuer un premier transfert de ligne de base sur une nouvelle relation de protection ou de mettre à jour une relation si elle est déjà initialisée et que vous souhaitez effectuer une mise à jour manuelle, non planifiée et incrémentielle.

Onglet Options de transfert

L'onglet Options de transfert vous permet de modifier la priorité d'initialisation d'un transfert et de modifier la bande passante utilisée pendant les transferts.

- **Priorité de transfert**

La priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner Normal ou Faible. Les relations avec les politiques qui spécifient une priorité de transfert normale s'exécutent avant celles qui spécifient une priorité de transfert faible. Normal est sélectionné par défaut.

- **Taux de transfert maximal**

Spécifie le débit maximal auquel les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser de taux de transfert maximal, le transfert de base entre les relations est illimité. Si vous sélectionnez plusieurs relations avec des taux de transfert maximum différents, vous pouvez spécifier l'un des paramètres de taux de transfert maximum suivants :

- Utiliser les valeurs spécifiées lors de la configuration ou de la modification d'une relation individuelle

Lorsque cette option est sélectionnée, les opérations d'initialisation et de mise à jour utilisent le taux de transfert maximal spécifié au moment de la création ou de la modification de chaque relation. Ce champ est disponible uniquement lorsque plusieurs relations avec des taux de transfert différents sont initialisées ou mises à jour.

- Illimité

Indique qu'il n'y a pas de limitation de bande passante sur les transferts entre les relations. Ce champ est disponible uniquement lorsque plusieurs relations avec des taux de transfert différents sont initialisées ou mises à jour.

- Limiter la bande passante à

Lorsque cette option est sélectionnée, la bande passante du réseau est limitée à la valeur que vous spécifiez. Vous pouvez saisir une valeur numérique, puis sélectionner kilo-octets par seconde (Ko/s), méga-octets par seconde (Mo/s), giga-octets par seconde (Go/s) ou téra-octets par seconde (To/s). Le débit de transfert maximal que vous spécifiez doit être supérieur à 1 Ko/s et inférieur à 4 To/s.

Onglet Copies d'instantanés source

L'onglet Copies d'instantanés source affiche les informations suivantes sur la copie d'instantané source utilisée pour le transfert de base :

- **Volume source**

Affiche les noms des volumes sources correspondants.

- **Volume de destination**

Affiche les noms des volumes de destination sélectionnés.

- **Type de source**

Affiche le type de volume. Le type peut être Lecture/écriture ou Protection des données.

- *** Copie instantanée ***

Affiche la copie instantanée utilisée pour le transfert de données. Cliquer sur la valeur Copie d'instantané affiche la boîte de dialogue Sélectionner la copie d'instantané source, dans laquelle vous pouvez sélectionner une copie d'instantané spécifique pour votre transfert, en fonction du type de relation de protection dont vous disposez et de l'opération que vous effectuez. L'option permettant de spécifier une copie Snapshot différente n'est pas disponible pour les sources de type de protection des données.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Initialiser/Mettre à jour.

- **Soumettre**

Enregistre vos sélections et démarre le travail d'initialisation ou de mise à jour.

Boîte de dialogue de resynchronisation

La boîte de dialogue Resynchroniser vous permet de resynchroniser les données sur une relation SnapMirror ou SnapVault qui a été précédemment rompue et dont la destination est devenue un volume en lecture/écriture. Vous pouvez également resynchroniser lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, ce qui entraîne l'échec des mises à jour de SnapMirror ou de SnapVault .

Onglet Options de resynchronisation

L'onglet Options de resynchronisation vous permet de définir la priorité de transfert et le débit de transfert maximal pour la relation de protection que vous resynchronisez.

- **Priorité de transfert**

La priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner Normal ou Faible. Les relations avec des politiques qui spécifient une priorité de transfert normale s'exécutent avant celles avec des politiques qui spécifient une priorité de transfert faible.

- **Taux de transfert maximal**

Spécifie le débit maximal auquel les données sont transférées entre les clusters sur le réseau. Lorsque cette option est sélectionnée, la bande passante du réseau est limitée à la valeur que vous spécifiez. Vous pouvez saisir une valeur numérique, puis sélectionner kilo-octets par seconde (Ko/s), mégaoctets par seconde (Mo/s), gigaoctets par seconde (Go/s) ou To/s. Si vous choisissez de ne pas utiliser de taux de transfert maximal, le transfert de base entre les relations est illimité.

Onglet Copies d'instantanés source

L'onglet Copies d'instantanés source affiche les informations suivantes sur la copie d'instantané source utilisée pour le transfert de base :

- **Volume source**

Affiche les noms des volumes sources correspondants.

- **Volume de destination**

Affiche les noms des volumes de destination sélectionnés.

- **Type de source**

Affiche le type de volume : lecture/écriture ou protection des données.

- * Copie instantanée *

Affiche la copie instantanée utilisée pour le transfert de données. Cliquer sur la valeur Copie d'instantané affiche la boîte de dialogue Sélectionner la copie d'instantané source, dans laquelle vous pouvez sélectionner une copie d'instantané spécifique pour votre transfert, en fonction du type de relation de protection dont vous disposez et de l'opération que vous effectuez.

Boutons de commande

- **Soumettre**

Démarre le processus de resynchronisation et ferme la boîte de dialogue Resynchroniser.

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Resynchroniser.

Boîte de dialogue Sélectionner la copie de l'instantané source

Vous utilisez la boîte de dialogue Sélectionner une copie d'instantané source pour sélectionner une copie d'instantané spécifique pour transférer des données entre des relations de protection, ou vous sélectionnez le comportement par défaut, qui varie selon que vous initialisez, mettez à jour ou resynchronisez une relation, et si la relation est un SnapMirror ou un SnapVault.

Défaut

Vous permet de sélectionner le comportement par défaut pour déterminer quelle copie Snapshot est utilisée pour initialiser, mettre à jour et resynchroniser les transferts pour les relations SnapVault et SnapMirror .

Si vous effectuez un transfert SnapVault , le comportement par défaut de chaque opération est le suivant :

Opération	Comportement par défaut de SnapVault lorsque la source est en lecture/écriture	Comportement par défaut de SnapVault lorsque la source est la protection des données (DP)
Initialiser	Crée une nouvelle copie Snapshot et la transfère.	Transfère la dernière copie Snapshot exportée.
Mise à jour	Transfère uniquement les copies étiquetées Snapshot, comme spécifié dans la politique.	Transfère la dernière copie Snapshot exportée.
Resynchroniser	Transfère toutes les copies Snapshot étiquetées créées après la copie Snapshot commune la plus récente.	Transfère la copie Snapshot la plus récente étiquetée.

Si vous effectuez un transfert SnapMirror , le comportement par défaut de chaque opération est le suivant :

Opération	Comportement par défaut de SnapMirror	Comportement par défaut de SnapMirror lorsque la relation est le deuxième saut dans une cascade SnapMirror vers SnapMirror
Initialiser	Crée une nouvelle copie Snapshot et la transfère ainsi que toutes les copies Snapshot créées avant la nouvelle copie Snapshot.	Transfère toutes les copies Snapshot de la source.
Mise à jour	Crée une nouvelle copie Snapshot et la transfère ainsi que toutes les copies Snapshot créées avant la nouvelle copie Snapshot.	Transfère toutes les copies Snapshot.
Resynchroniser	Crée une nouvelle copie Snapshot, puis transfère toutes les copies Snapshot de la source.	Transfère toutes les copies Snapshot du volume secondaire vers le volume tertiaire et supprime toutes les données ajoutées après la création de la copie Snapshot commune la plus récente.

Copie d'instantané existante

Vous permet de sélectionner une copie d'instantané existante dans la liste si la sélection de copie d'instantané est autorisée pour cette opération.

- * Copie instantanée *

Affiche les copies Snapshot existantes parmi lesquelles vous pouvez sélectionner pour un transfert.

- Date de création

Affiche la date et l'heure de création de la copie instantanée. Les copies instantanées sont répertoriées du plus récent au moins récent, le plus récent se trouvant en haut de la liste.

Si vous effectuez un transfert SnapVault et que vous souhaitez sélectionner une copie Snapshot existante à transférer d'une source vers une destination, le comportement de chaque opération est le suivant :

Opération	Comportement de SnapVault lors de la spécification d'une copie Snapshot	Comportement de SnapVault lors de la spécification d'une copie Snapshot dans une cascade
Initialiser	Transfère la copie instantanée spécifiée.	La sélection de copie d'instantané source n'est pas prise en charge pour les volumes de protection des données.

Opération	Comportement de SnapVault lors de la spécification d'une copie Snapshot	Comportement de SnapVault lors de la spécification d'une copie Snapshot dans une cascade
Mise à jour	Transfère la copie instantanée spécifiée.	La sélection de copie d'instantané source n'est pas prise en charge pour les volumes de protection des données.
Resynchroniser	Transfère la copie instantanée sélectionnée.	La sélection de copie d'instantané source n'est pas prise en charge pour les volumes de protection des données.

Si vous effectuez un transfert SnapMirror et que vous souhaitez sélectionner une copie Snapshot existante à transférer d'une source vers une destination, le comportement de chaque opération est le suivant :

Opération	Comportement de SnapMirror lors de la spécification d'une copie Snapshot	Comportement de SnapMirror lors de la spécification d'une copie Snapshot dans une cascade
Initialiser	Transfère toutes les copies Snapshot sur la source, jusqu'à la copie Snapshot spécifiée.	La sélection de copie d'instantané source n'est pas prise en charge pour les volumes de protection des données.
Mise à jour	Transfère toutes les copies Snapshot sur la source, jusqu'à la copie Snapshot spécifiée.	La sélection de copie d'instantané source n'est pas prise en charge pour les volumes de protection des données.
Resynchroniser	Transfère toutes les copies Snapshot de la source jusqu'à la copie Snapshot sélectionnée, puis supprime toutes les données ajoutées après la création de la copie Snapshot commune la plus récente.	La sélection de copie d'instantané source n'est pas prise en charge pour les volumes de protection des données.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Soumettre**

Soumet vos sélections et ferme la boîte de dialogue Sélectionner la copie de l'instantané source.

- **Annuler**

Annule vos sélections et ferme la boîte de dialogue Sélectionner une copie d'instantané source.

Boîte de dialogue de resynchronisation inversée

Lorsque vous avez une relation de protection rompue parce que le volume source est désactivé et que la destination est transformée en volume de lecture/écriture, la resynchronisation inverse vous permet d'inverser le sens de la relation afin que la destination devienne la nouvelle source et que la source devienne la nouvelle destination.

Lorsqu'un sinistre désactive le volume source dans votre relation de protection, vous pouvez utiliser le volume de destination pour diffuser des données en le convertissant en lecture/écriture, pendant que vous réparez ou remplacez la source, mettez à jour la source et rétablissez la relation. Lorsque vous effectuez une opération de resynchronisation inverse, les données de la source qui sont plus récentes que les données de la copie Snapshot commune sont supprimées.

Avant la resynchronisation inverse

Affiche la source et la destination d'une relation avant une opération de resynchronisation inverse.

- **Volume source**

Le nom et l'emplacement du volume source avant une opération de resynchronisation inverse.

- **Volume de destination**

Le nom et l'emplacement du volume de destination avant une opération de resynchronisation inverse.

Après la resynchronisation inversée

Affiche la source et la destination d'une relation après une opération de resynchronisation de réserve.

- **Volume source**

Le nom et l'emplacement du volume source après une opération de resynchronisation inverse.

- **Volume de destination**

Le nom et l'emplacement du volume de destination après une opération de resynchronisation inverse.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les actions suivantes :

- **Soumettre**

Commence le processus de resynchronisation inverse.

- **Annuler**

Ferme la boîte de dialogue Resynchronisation inversée sans lancer une opération de resynchronisation inversée.

Relation : vue Toutes les relations

La vue Relation : Toutes les relations affiche des informations sur les relations de protection sur le système de stockage.

Par défaut, lorsque vous accédez à la page Relations, le rapport qui s'affiche inclut les relations de protection de niveau supérieur pour les volumes et les machines virtuelles de stockage. Les commandes situées en haut de la page vous permettent de sélectionner une vue particulière, d'effectuer des recherches pour localiser des objets spécifiques, de créer et d'appliquer des filtres pour affiner la liste des données affichées, d'ajouter/supprimer/réorganiser des colonnes sur la page et d'exporter les données de la page vers un fichier .csv, .pdf ou .xlsx. Après avoir personnalisé la page, vous pouvez enregistrer les résultats sous forme de vue personnalisée, puis planifier la génération et l'envoi régulier par courrier électronique d'un rapport de ces données. Par défaut, lorsque vous sélectionnez le menu **Relations**, le rapport affiché inclut les relations de protection pour les volumes et les machines virtuelles de stockage de votre centre de données. Vous pouvez utiliser l'option **Filtre** pour afficher uniquement les systèmes de stockage sélectionnés, comme uniquement les volumes ou uniquement les machines virtuelles de stockage. Le même rapport s'affiche dans la page Stockage et uniquement pour l'entité de stockage sélectionnée. Si vous souhaitez afficher les relations entre les volumes ou les machines virtuelles de stockage, vous pouvez accéder à la page **Stockage > Volumes > Relation : Toutes les relations** ou accéder à **Protection > Relations > Relation : Toutes les relations** et utiliser l'option **Type d'objet de relation** dans le **Filtre** pour filtrer uniquement les données des volumes ou des machines virtuelles de stockage.

La page Relations qui répertorie toutes les relations de protection comporte le lien **Afficher dans System Manager** pour le cluster de destination qui vous permet d'afficher les mêmes objets dans ONTAP System Manager.

- **Statut**

Affiche l'état actuel de la relation de protection.

Le statut peut être Erreur () , Avertissement () , ou OK () .

- **VM de stockage source**

Affiche le nom du SVM source. Vous pouvez afficher plus de détails sur le SVM source en cliquant sur le nom du SVM.

Lorsqu'un SVM existe sur le cluster mais n'a pas encore été ajouté à l'inventaire Unified Manager, ou que le SVM a été créé après la dernière actualisation du cluster, ce champ sera vide. Vous devez vous assurer que le SVM existe ou effectuer une redécouverte sur le cluster pour actualiser la liste des ressources.

- **Source**

Affiche soit le volume source, soit la machine virtuelle de stockage source protégée en fonction de votre sélection. Vous pouvez afficher plus de détails sur le volume source ou la machine virtuelle de stockage en cliquant sur le nom du volume ou de la machine virtuelle de stockage.

Si le message `Resource-key not discovered` s'affiche, cela peut indiquer que le volume existe sur le cluster mais n'a pas encore été ajouté à l'inventaire Unified Manager, ou que le volume a été créé après la dernière actualisation du cluster. Vous devez vous assurer que le volume existe ou effectuer une redécouverte sur le cluster pour actualiser la liste des ressources.

- **VM de stockage de destination**

Affiche le nom du SVM de destination. Vous pouvez afficher plus de détails sur le SVM de destination en

cliquant sur le nom du SVM.

- **Destination**

Affiche le nom du volume de destination ou de la machine virtuelle de stockage en fonction de votre sélection. Vous pouvez afficher plus de détails sur le volume de destination ou la machine virtuelle de stockage en cliquant sur le nom de l'objet correspondant.

- **Type d'objet de relation**

Affiche le type d'objet utilisé dans la relation, tel que la machine virtuelle de stockage, le volume et le groupe de cohérence. Pour les objets dans une relation de cohérence, la source et les destinations de la relation affichent le groupe de cohérence et, en cliquant dessus, vous accédez à la page LUN pour afficher la relation.

- **Politique**

Affiche le nom de la politique de protection pour la relation SnapMirror . Vous pouvez cliquer sur le nom de la politique pour afficher les détails associés à cette politique, y compris les informations suivantes :

- **Priorité de transfert**

Spécifie la priorité à laquelle un transfert s'exécute pour les opérations asynchrones. La priorité de transfert est Normale ou Faible. Les transferts prioritaires normaux sont planifiés avant les transferts de faible priorité. La valeur par défaut est Normal.

- **Ignorer le temps d'accès**

S'applique uniquement aux relations SnapVault . Cela spécifie si les transferts incrémentiels ignorent les fichiers dont seul le temps d'accès a été modifié. Les valeurs sont soit Vrai soit Faux. La valeur par défaut est Faux.

- **Quand la relation n'est pas synchronisée**

Spécifie l'action ONTAP exécute lorsqu'une relation synchrone ne peut pas être synchronisée. Les relations StrictSync restreindront l'accès au volume principal en cas d'échec de synchronisation avec le volume secondaire. Les relations de synchronisation ne restreignent pas l'accès au serveur principal en cas d'échec de synchronisation avec le serveur secondaire.

- **Limite d'essais**

Spécifie le nombre maximal de tentatives de transfert manuel ou planifié pour une relation SnapMirror . La valeur par défaut est 8.

- **Commentaires**

Fournit un champ de texte pour les commentaires spécifiques à la politique sélectionnée.

- **Étiquette SnapMirror**

Spécifie l'étiquette SnapMirror pour la première planification associée à la stratégie de copie Snapshot. L'étiquette SnapMirror est utilisée par le sous-système SnapVault lorsque vous sauvegardez des copies Snapshot vers une destination SnapVault .

- **Paramètre de rétention**

Spécifie la durée de conservation des sauvegardes, en fonction de l'heure ou du nombre de sauvegardes.

- Copies instantanées réelles

Spécifie le nombre de copies Snapshot sur ce volume qui correspondent à l'étiquette spécifiée.

- Conserver les copies instantanées

Spécifie le nombre de copies SnapVault Snapshot qui ne sont pas supprimées automatiquement même si la limite maximale de la stratégie est atteinte. Les valeurs sont soit Vrai soit Faux. La valeur par défaut est Faux.

- Seuil d'avertissement de rétention

Spécifie la limite de copie d'instantané à laquelle un avertissement est envoyé pour indiquer que la limite de rétention maximale est presque atteinte.

- **Durée du décalage**

Affiche la durée pendant laquelle les données sur le miroir sont en retard par rapport à la source.

La durée du décalage doit être proche ou égale à 0 seconde pour les relations StrictSync.

- **Statut de décalage**

Affiche l'état de décalage pour les relations gérées et pour les relations non gérées qui ont une planification associée à cette relation. L'état du décalage peut être :

- Erreur

La durée du décalage est supérieure ou égale au seuil d'erreur de décalage.

- Avertissement

La durée du décalage est supérieure ou égale au seuil d'avertissement de décalage.

- OK

La durée du décalage est dans les limites normales.

- Non applicable

L'état de décalage n'est pas applicable aux relations synchrones car une planification ne peut pas être configurée.

- **Dernière mise à jour réussie**

Affiche l'heure de la dernière opération SnapMirror ou SnapVault réussie.

La dernière mise à jour réussie n'est pas applicable aux relations synchrones.

- **Relations constitutives**

Affiche s'il y a des volumes dans l'objet sélectionné.

- **Type de relation**

Affiche le type de relation utilisé pour répliquer un volume. Les types de relations incluent :

- Miroir asynchrone
- Coffre-fort asynchrone
- MirrorVault asynchrone
- StrictSync
- Synchroniser

- **Statut du transfert**

Affiche l'état de transfert pour la relation de protection. Le statut du transfert peut être l'un des suivants :

- Avortement

Les transferts SnapMirror sont activés ; cependant, une opération d'abandon de transfert qui pourrait inclure la suppression du point de contrôle est en cours.

- Vérification

Le volume de destination subit une vérification de diagnostic et aucun transfert n'est en cours.

- Finalisation

Les transferts SnapMirror sont activés. Le volume est actuellement en phase de post-transfert pour les transferts SnapVault incrémentiels.

- Inactif

Les transferts sont activés et aucun transfert n'est en cours.

- Synchronisé

Les données des deux volumes dans la relation synchrone sont synchronisées.

- Désynchronisé

Les données du volume de destination ne sont pas synchronisées avec le volume source.

- Préparation

Les transferts SnapMirror sont activés. Le volume est actuellement en phase de pré-transfert pour les transferts SnapVault incrémentiels.

- En file d'attente

Les transferts SnapMirror sont activés. Aucun transfert n'est en cours.

- Au repos

Les transferts SnapMirror sont désactivés. Aucun transfert n'est en cours.

- Mise au repos

Un transfert SnapMirror est en cours. Les transferts supplémentaires sont désactivés.

- Transfert

Les transferts SnapMirror sont activés et un transfert est en cours.

- Transition

Le transfert asynchrone des données du volume source vers le volume de destination est terminé et la transition vers le fonctionnement synchrone a commencé.

- En attendant

Un transfert SnapMirror a été lancé, mais certaines tâches associées attendent d'être mises en file d'attente.

- **Durée du dernier transfert**

Affiche le temps nécessaire au dernier transfert de données.

La durée de transfert n'est pas applicable aux relations StrictSync car le transfert doit être simultané.

- **Taille du dernier transfert**

Affiche la taille, en octets, du dernier transfert de données.

La taille du transfert n'est pas applicable aux relations StrictSync.

- **Médiateurs**

Affiche le statut du médiateur.

- Non applicable

Si le cluster ne prend pas en charge la synchronisation active SnapMirror .

- Non configuré

S'il n'est pas configuré, ou s'il est configuré mais que seul le cluster de destination est ajouté et que le cluster source n'est pas ajouté dans Unified Manager.

- Adresse IP du médiateur

S'il est configuré, les clusters source et de destination sont ajoutés dans Unified Manager.

- **État**

Affiche l'état de la relation SnapMirror ou SnapVault . L'état peut être non initialisé, SnapMirrored ou cassé. Si un volume source est sélectionné, l'état de la relation n'est pas applicable et n'est pas affiché.

- **Santé relationnelle**

Affiche la santé relationnelle du cluster.

- **Raison malsaine**

La raison pour laquelle la relation est dans un état malsain.

- **Priorité de transfert**

Affiche la priorité à laquelle un transfert s'exécute. La priorité de transfert est Normale ou Faible. Les transferts prioritaires normaux sont planifiés avant les transferts de faible priorité.

La priorité de transfert n'est pas applicable aux relations synchrones car tous les transferts sont traités avec la même priorité.

- **Calendrier**

Affiche le nom du programme de protection attribué à la relation.

Le calendrier n'est pas applicable aux relations synchrones.

- **Version Réplication flexible**

Affiche soit Oui, Oui avec option de sauvegarde, soit Aucun.

- **Groupe source**

Affiche le nom de domaine complet, le nom court ou l'adresse IP du cluster source pour la relation SnapMirror .

- **FQDN du cluster source**

Affiche le nom du cluster source pour la relation SnapMirror .

- **Nœud source**

Affiche le nom du lien du nom du nœud source pour la relation SnapMirror d'un volume et affiche le lien du nombre de nœuds de relation SnapMirror lorsque l'objet est une machine virtuelle de stockage ou un groupe de cohérence.

Dans la vue personnalisée, lorsque vous cliquez sur le lien du nom du nœud, vous pouvez afficher et étendre la protection des objets de stockage sur lesquels les volumes de ces groupes de cohérence appartiennent à une relation de synchronisation active SnapMirror .

Lorsque vous cliquez sur le lien de comptage de nœuds, vous accédez à la page de nœuds contenant les nœuds respectifs associés à cette relation. Lorsque le nombre de nœuds est de 0, aucune valeur n'est affichée car aucun nœud n'est associé à la relation.

- **Nœud de destination**

Affiche le nom du lien du nom du nœud de destination pour la relation SnapMirror d'un volume et affiche le lien du nombre de nœuds de relation SnapMirror lorsque l'objet est une machine virtuelle de stockage ou un groupe de cohérence.

Lorsque vous cliquez sur le lien de comptage de nœuds, vous accédez à la page de nœuds contenant les nœuds respectifs associés à cette relation. Lorsque le nombre de nœuds est de 0, aucune valeur n'est affichée car aucun nœud n'est associé à la relation.

- **Groupe de destinations**

Affiche le nom du cluster de destination pour la relation SnapMirror .

- **FQDN du cluster de destination**

Affiche le nom de domaine complet, le nom court ou l'adresse IP du cluster de destination pour la relation SnapMirror .

- **Protégé par**

Affiche les différentes relations. Dans cette colonne, vous pouvez afficher les relations entre les volumes et les groupes de cohérence pour l'ordre des clusters et des machines virtuelles de stockage, notamment :

- SnapMirror
- Stockage VM DR
- SnapMirror, reprise après sinistre des machines virtuelles de stockage
- Groupe de cohérence
- SnapMirror, groupe de cohérence.

Informations connexes

- Pour plus d'informations sur la vue **Relationship: MetroCluster**, voir ["Surveillance des configurations MetroCluster"](#) .
- Pour plus d'informations sur la vue **Relation : Statut de transfert du dernier mois**, voir ["Relation : Affichage du statut de transfert du dernier mois"](#) .
- Pour plus d'informations sur la vue **Relation : Toutes les relations**, voir ["Relation : Taux de transfert du dernier mois"](#) .

Relation : Affichage du statut de transfert du dernier mois

La vue Relation : État du transfert du dernier mois vous permet d'analyser les tendances de transfert sur une période donnée pour les volumes et les machines virtuelles de stockage dans des relations asynchrones. Cette page indique également si le transfert a réussi ou échoué.

Les commandes situées en haut de la page vous permettent d'effectuer des recherches pour localiser des objets spécifiques, de créer et d'appliquer des filtres pour affiner la liste des données affichées, d'ajouter/supprimer/réorganiser des colonnes sur la page et d'exporter les données de la page vers un .csv , .pdf , ou .xlsx déposer. Après avoir personnalisé la page, vous pouvez enregistrer les résultats sous forme de vue personnalisée, puis planifier la génération et l'envoi régulier par courrier électronique d'un rapport de ces données. Vous pouvez utiliser l'option **Filtre** pour afficher uniquement les systèmes de stockage sélectionnés, comme uniquement les volumes ou uniquement les machines virtuelles de stockage. Le même rapport s'affiche dans la page Stockage et uniquement pour l'entité de stockage sélectionnée. Par exemple, si vous souhaitez afficher les relations entre les volumes, vous pouvez accéder au rapport Relation : État du transfert du dernier mois pour les machines virtuelles de stockage à partir du menu **Stockage > Machines virtuelles de stockage > Relation : État du transfert du dernier mois** ou à partir du menu **Protection > Relations > Relation : État du transfert du dernier mois**, et utiliser le menu **Filtre** pour afficher uniquement les données des volumes.

- **Volume source**

Affiche le nom du volume source.

- **Volume de destination**

Affiche le nom du volume de destination.

- **Type d'opération**

Affiche le type de transfert de volume.

- **Résultat de l'opération**

Affiche si le transfert de volume a réussi.

- **Heure de début du transfert**

Affiche l'heure de début du transfert de volume.

- **Heure de fin du transfert**

Affiche l'heure de fin du transfert de volume.

- **Durée du transfert**

Affiche le temps nécessaire (en heures) pour terminer le transfert de volume.

- **Taille du transfert**

Affiche la taille (en Mo) du volume transféré.

- **Source SVM**

Affiche le nom de la machine virtuelle de stockage (SVM).

- **Groupe source**

Affiche le nom du cluster source.

- **Destination SVM**

Affiche le nom du SVM de destination.

- **Groupe de destinations**

Affiche le nom du cluster de destination.

Informations connexes

- Pour plus d'informations sur la vue **Relation : Toutes les relations**, voir ["Relation : vue Toutes les relations"](#) .
- Pour plus d'informations sur la vue **Relationship: MetroCluster**, voir ["Surveillance des configurations MetroCluster"](#) .
- Pour plus d'informations sur la vue **Relation : Toutes les relations**, voir ["Relation : Taux de transfert du dernier mois"](#) .

Relation : Taux de transfert du dernier mois

La vue Relation : Taux de transfert du dernier mois vous permet d'analyser la quantité de

volume de données transférée au quotidien pour les volumes dans des relations asynchrones. Cette page fournit également des détails sur les transferts quotidiens et le temps nécessaire pour terminer l'opération de transfert pour les volumes et les machines virtuelles de stockage.

Les commandes situées en haut de la page vous permettent d'effectuer des recherches pour localiser des objets spécifiques, de créer et d'appliquer des filtres pour affiner la liste des données affichées, d'ajouter/supprimer/réorganiser des colonnes sur la page et d'exporter les données de la page vers un fichier .csv, .pdf ou .xlsx. Après avoir personnalisé la page, vous pouvez enregistrer les résultats sous forme de vue personnalisée, puis planifier la génération et l'envoi régulier par courrier électronique d'un rapport de ces données. Par exemple, si vous souhaitez afficher les relations entre les volumes, vous pouvez accéder au menu **Stockage > Volumes > Relation : Taux de transfert du dernier mois** ou accéder au menu **Protection > Relations > Relations : Taux de transfert du dernier mois** et utiliser le **Filtre** pour afficher uniquement les données des volumes.

- **Taille totale du transfert**

Affiche la taille totale du transfert de volume en gigaoctets.

- **Jour**

Affiche le jour où le transfert de volume a été initié.

- **Heure de fin**

Affiche l'heure de fin du transfert de volume avec la date.

Informations connexes

- Pour plus d'informations sur la vue **Relationship: MetroCluster**, voir "[Surveillance des configurations MetroCluster](#)".
- Pour plus d'informations sur la vue **Relation : Statut de transfert du dernier mois**, voir "[Relation : Affichage du statut de transfert du dernier mois](#)".
- Pour plus d'informations sur la vue **Relation : Toutes les relations**, voir "[Relation : Taux de transfert du dernier mois](#)".

Générer des rapports personnalisés

Rapports du gestionnaire unifié

Active IQ Unified Manager (anciennement OnCommand Unified Manager) offre la possibilité d'afficher, de personnaliser, de télécharger et de planifier des rapports pour vos systèmes de stockage ONTAP . Les rapports peuvent fournir des détails sur la capacité du système de stockage, la santé, les performances, la sécurité et les relations de protection.

La nouvelle fonctionnalité de création de rapports et de planification d'Unified Manager introduite dans Active IQ Unified Manager 9.6 remplace le moteur de création de rapports précédent qui a été retiré dans la version 9.5 d'Unified Manager.

Les rapports fournissent différentes vues de votre réseau, offrant des informations exploitables sur la capacité, la santé, les performances, la sécurité et les données de protection. Vous pouvez personnaliser vos vues en affichant, masquant et réorganisant les colonnes, en filtrant les données, en triant les données et en recherchant les résultats. Vous pouvez enregistrer des vues personnalisées pour les réutiliser, les télécharger sous forme de rapports et les planifier sous forme de rapports récurrents à distribuer par courrier électronique.

Vous pouvez télécharger des vues au format Microsoft® Excel et les personnaliser. Vous pouvez utiliser des fonctionnalités Excel avancées, telles que des tris complexes, des filtres en couches, des tableaux croisés dynamiques et des graphiques. Lorsque vous êtes satisfait du rapport Excel obtenu, vous pouvez télécharger le fichier Excel pour l'utiliser chaque fois que le rapport est planifié et partagé.

En plus de générer des rapports à partir de l'interface utilisateur, vous pouvez extraire des données de santé, de sécurité et de performances d'Unified Manager à l'aide de ces méthodes supplémentaires :

- Utilisation d'Open Database Connectivity (ODBC) et des outils ODBC pour accéder directement à la base de données pour obtenir des informations sur les clusters
- Exécution des API REST d'Unified Manager pour renvoyer les informations que vous souhaitez consulter

À partir de cette version d'Active IQ Unified Manager, les améliorations suivantes ont été apportées aux rapports :

- Un e-mail est envoyé pour un rapport selon le calendrier configuré. Même lorsque vous générez un rapport à la demande, vous recevrez un e-mail.
- Le nom de fichier du rapport et les métadonnées du rapport incluent le nom d'hôte à partir duquel le rapport a été généré. Même si quelqu'un modifie le nom du fichier, vous pouvez toujours identifier le nom d'hôte à partir duquel le rapport a été généré grâce à cette amélioration.

Points d'accès pour la génération de rapports

Vous pouvez collecter des informations dans Unified Manager sur vos clusters pour créer des rapports à partir de l'interface utilisateur, des requêtes de base de données MySQL et des API REST.

Ces sections décrivent les rapports et la planification d'Unified Manager via l'interface utilisateur.

Il existe trois manières d'accéder aux fonctionnalités de reporting fournies par Unified Manager :

- Extraction de données directement à partir des pages d'inventaire dans l'interface utilisateur.
- Utilisation d'Open Database Connectivity (ODBC) et des outils ODBC pour accéder à tous les objets disponibles.
- Exécution des API REST Unified Manager pour renvoyer les informations que vous souhaitez consulter.

Ces sections décrivent les rapports et la planification d'Unified Manager via l'interface utilisateur.

Bases de données Unified Manager accessibles pour des rapports personnalisés

Unified Manager utilise une base de données MySQL pour stocker les données des clusters qu'il surveille. Les données sont conservées dans différents schémas de la base de données MySQL.

Toutes les données des tables des bases de données suivantes sont disponibles :

Base de données	Description
modèle_netapp	Données sur les objets sur les contrôleurs ONTAP .
vue_modèle_netapp	Données sur les objets sur les contrôleurs ONTAP , adaptées à la consommation d'outils de rapport.
performances_netapp	Compteurs de performances spécifiques au cluster.
ocum	Données et informations de l'application Unified Manager pour prendre en charge le filtrage de l'interface utilisateur, le tri et le calcul de certains champs dérivés.
rapport_ocum	Données relatives à la configuration des stocks et aux informations relatives à la capacité.
ocum_report_birt	Vues pour la configuration des stocks et les données relatives à la capacité, adaptées à la consommation d'outils de rapport.
opm	Paramètres de configuration des performances et informations de seuil.
moniteur d'échelle	Données sur les problèmes de santé et de performances de l'application Unified Manager.
modèle_vmware	Données d'objet VMware pour les banques de données hébergées sur le stockage NetApp .
vue_modèle_vmware	Vues des données d'objet VMware pour les banques de données hébergées sur le stockage NetApp , adaptées à la consommation d'outils de rapport.

Base de données	Description
performances_vmware	Données de compteur de performances VMware pour les banques de données hébergées sur le stockage NetApp .

Un utilisateur de rapport (un utilisateur de base de données avec le rôle de schéma de rapport) peut accéder aux données de ces tables. Cet utilisateur dispose d'un accès en lecture seule aux rapports et aux autres vues de base de données directement à partir de la base de données Unified Manager. Notez que cet utilisateur n'a pas l'autorisation d'accéder aux tables contenant des données utilisateur ou des informations d'identification de cluster.

API REST d'Unified Manager pouvant être utilisées pour la création de rapports

Vous pouvez utiliser les API REST pour vous aider à gérer vos clusters en affichant les informations d'intégrité, de capacité, de performances et de sécurité capturées par Unified Manager.

Les API REST sont exposées via la page Web Swagger. Vous pouvez accéder à la page Web Swagger pour afficher la documentation de l'API REST d'Unified Manager, ainsi que pour émettre manuellement un appel d'API. Depuis l'interface Web d'Unified Manager, dans la barre de menus, cliquez sur le bouton **Aide**, puis sélectionnez **Documentation API**. Pour plus d'informations sur les API REST d'Unified Manager, consultez "[Prise en main des API REST Active IQ Unified Manager](#)".

Vous devez disposer du rôle d'opérateur, d'administrateur de stockage ou d'administrateur d'application pour accéder aux API REST.

Comprendre les rapports

Les rapports affichent des informations détaillées sur le stockage, le réseau, la qualité de service et les relations de protection, vous aidant à identifier et à résoudre les problèmes potentiels avant qu'ils ne surviennent.

Lorsque vous personnalisez une vue, vous pouvez l'enregistrer sous un nom unique pour une utilisation ultérieure. Vous pouvez planifier un rapport basé sur cette vue pour qu'il s'exécute régulièrement et le partager avec d'autres. Vous pouvez également télécharger la vue dans Excel pour la personnaliser à l'aide de fonctionnalités Excel avancées, puis télécharger à nouveau ce fichier dans Unified Manager. Si vous planifiez un rapport à l'aide de cette vue, il utilisera le fichier Excel que vous avez téléchargé pour créer des rapports robustes que vous pourrez partager.

Vous pouvez gérer tous les rapports qui ont été planifiés à partir de la page Planifications des rapports.



Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage pour gérer les rapports.

Vous pouvez télécharger des rapports sous forme de fichiers CSV, Excel ou PDF.

Comprendre la relation entre la vue et le rapport

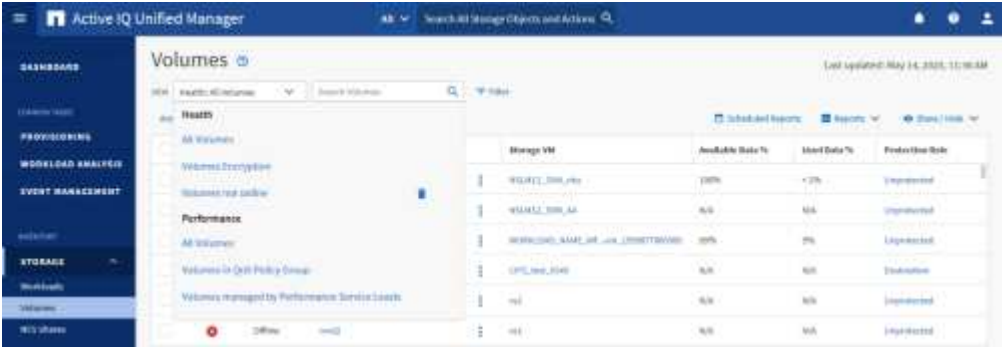
Les vues et les pages d'inventaire deviennent des rapports lorsque vous les téléchargez ou les planifiez.

Vous pouvez personnaliser et enregistrer des vues et des pages d’inventaire pour les réutiliser. Presque tout ce que vous pouvez afficher dans Unified Manager peut être enregistré, réutilisé, personnalisé, planifié et partagé sous forme de rapport.

Dans la liste déroulante de la vue, les éléments avec l’icône de suppression sont des vues personnalisées existantes que vous ou un autre utilisateur avez créées. Les éléments sans icône sont des vues par défaut fournies avec Unified Manager. Les vues par défaut ne peuvent pas être modifiées ou supprimées.



- Si vous supprimez une vue personnalisée de la liste, cela supprime également tous les fichiers Excel ou rapports planifiés qui utilisent cette vue.
- Si vous modifiez une vue personnalisée, les rapports qui utilisent cette vue refléteront la modification la prochaine fois que le rapport sera généré et envoyé par courrier électronique conformément au calendrier du rapport. Lorsque vous modifiez les vues, assurez-vous que vos modifications fonctionnent avec toutes les personnalisations Excel associées utilisées pour les rapports. Si nécessaire, vous pouvez mettre à jour le fichier Excel en le téléchargeant, en apportant les modifications requises et en le téléchargeant en tant que nouvelle personnalisation Excel pour la vue.



Seuls les utilisateurs disposant du rôle Administrateur d’application ou Administrateur de stockage peuvent voir l’icône de suppression, modifier ou supprimer une vue, ou modifier ou supprimer un rapport planifié.

Types de rapports

Ce tableau fournit une liste complète des vues et des pages d’inventaire disponibles sous forme de rapports que vous pouvez personnaliser, télécharger et planifier.

Rapports du Active IQ Unified Manager

Type	Objet de stockage ou de réseau
Capacité	Groupes
	Agrégats
	Volumes
	Qtrees

Type	Objet de stockage ou de réseau
Santé	Groupes Nœuds Agrégats Machines virtuelles de stockage Volumes Actions PME/CIFS Actions NFS
Performances	Groupes Nœuds Agrégats Machines virtuelles de stockage Volumes LUN Espaces de noms NVMe Interfaces réseau (LIF) Ports
Qualité de service	Groupes de politiques QoS traditionnels Groupes de politiques QoS adaptatifs Groupes de politiques de niveau de service de performance
Relations de protection des volumes (disponibles sur la page Volumes)	Toutes les relations Statut de transfert du dernier mois Taux de transfert du dernier mois
Sécurité	Machines virtuelles de stockage Groupes

Limitations des rapports

La nouvelle fonctionnalité de création de rapports Active IQ Unified Manager présente certaines limitations dont vous devez être conscient.

Rapports existants des versions précédentes d'Unified Manager

Vous ne pouvez modifier que la planification et les destinataires des rapports existants qui ont été créés et importés (sous forme de fichiers .rptdesign) dans Unified Manager 9.5 et les versions antérieures. Si vous avez personnalisé l'un des rapports standard fournis avec Unified Manager 9.5 ou une version antérieure, ces rapports personnalisés ne sont pas importés dans le nouvel outil de création de rapports.

Si vous devez modifier des rapports existants importés à partir de fichiers .rptdesign, effectuez l'une des opérations suivantes et supprimez le rapport importé :

- créer une nouvelle vue et planifier un rapport à partir de cette vue (préféré)
- passez la souris sur le rapport, copiez le SQL et extrayez les données à l'aide d'un outil externe

Les vues par défaut peuvent être générées sous forme de rapports sans nécessiter de personnalisation. Vous pouvez utiliser la nouvelle solution de reporting pour recréer n'importe quel rapport personnalisé.

Relation entre le calendrier et le rapport

Vous pouvez créer de nombreux calendriers différents avec n'importe quelle combinaison de destinataires pour chaque rapport enregistré. Cependant, vous ne pouvez pas réutiliser la planification pour plusieurs rapports.

Protection des rapports

Tout utilisateur disposant des autorisations appropriées peut modifier ou supprimer des rapports. Il n'existe aucun moyen d'empêcher les autres utilisateurs de supprimer ou d'apporter des modifications aux vues ou aux plannings enregistrés.

Rapports d'événements

Bien que vous puissiez personnaliser la vue des événements et télécharger le rapport résultant au format CSV, vous ne pouvez pas planifier la génération et la distribution de rapports d'événements récurrents.

Pièces jointes du rapport

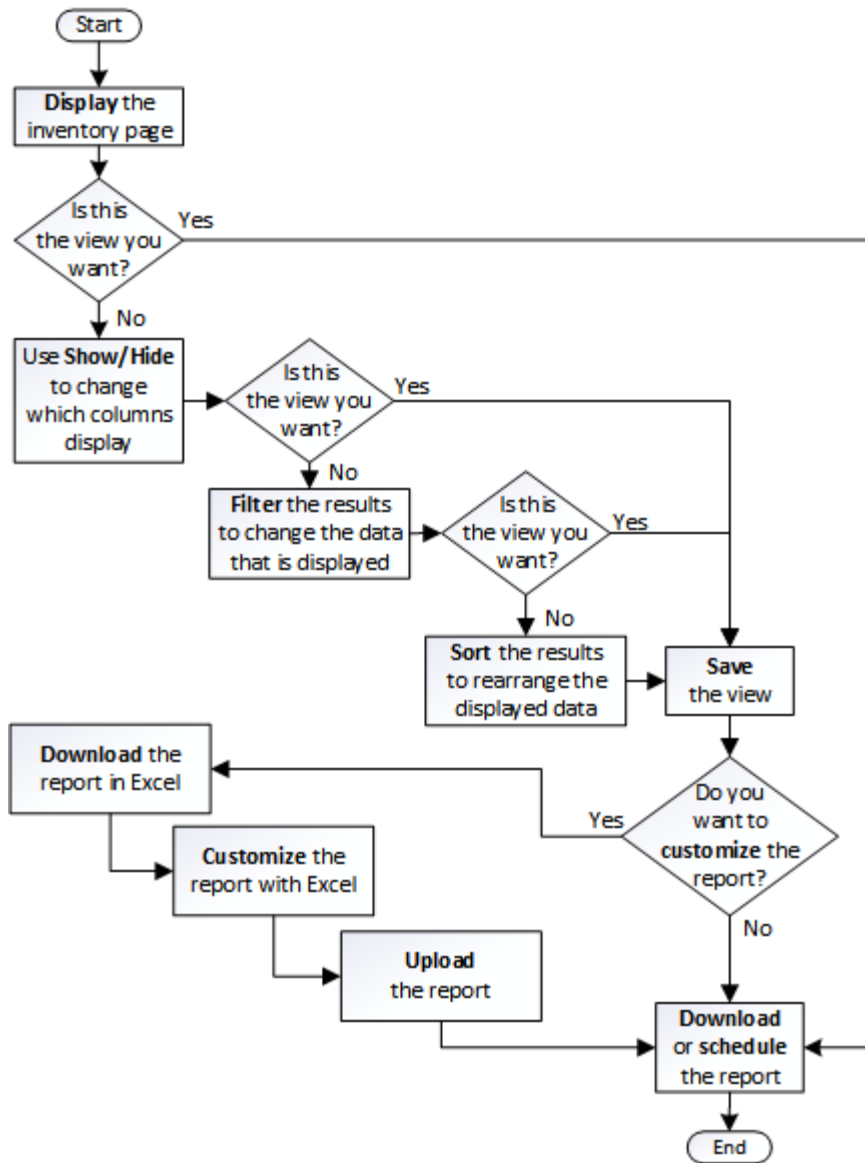
Les rapports ne peuvent pas être envoyés dans le corps d'un e-mail. Au lieu de cela, les rapports sont uniquement envoyés sous forme de pièces jointes PDF, Excel ou CSV.

Travailler avec des rapports

Découvrez comment rechercher et personnaliser les pages vues d'inventaire dans des rapports planifiés partageables.

Flux de travail du rapport

Arbre de décision décrivant le flux de travail du rapport.



Démarrage rapide des rapports

Créez un exemple de rapport personnalisé pour découvrir l'exploration des vues et la planification des rapports. Ce rapport de démarrage rapide recherche une liste de volumes que vous souhaitez peut-être déplacer vers le niveau cloud, car il existe une quantité importante de données inactives (froides). Vous ouvrirez la vue Performances : tous les volumes, personnaliserez la vue à l'aide de filtres et de colonnes, enregistrerez la vue personnalisée en tant que rapport et planifierez le partage du rapport une fois par semaine.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré des agrégats FabricPool et disposer de volumes sur ces agrégats.

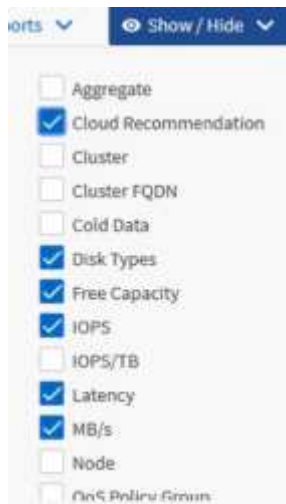
Suivez les étapes ci-dessous pour :

- Ouvrir la vue par défaut

- Personnalisez les colonnes en filtrant et en triant les données
- Enregistrer la vue
- Planifier la génération d'un rapport pour la vue personnalisée

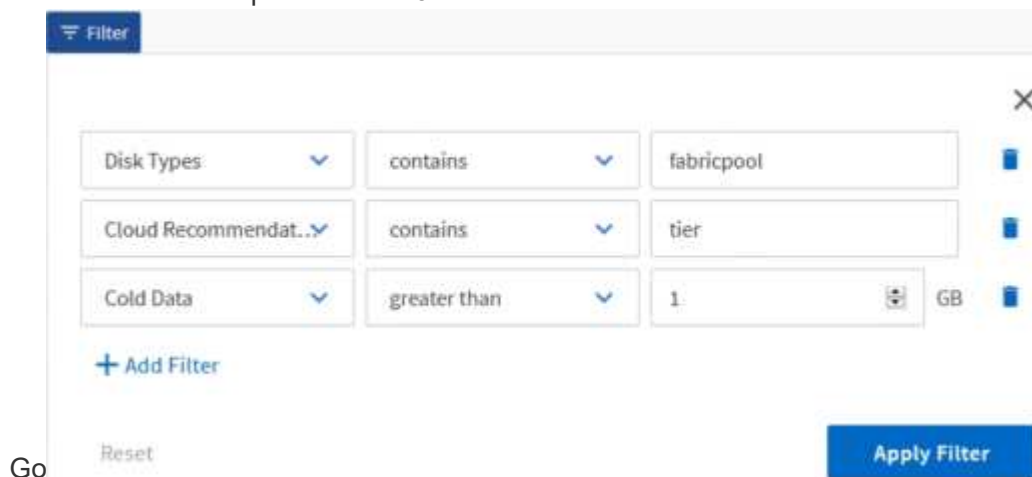
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Performances > Tous les volumes**.
3. Cliquez sur **Afficher/Masquer** pour vous assurer que la colonne « Types de disques » apparaît dans la vue.



Ajoutez ou supprimez d'autres colonnes pour créer une vue contenant les champs importants pour votre rapport.

4. Faites glisser la colonne « Types de disques » à côté de la colonne « Recommandation Cloud ».
5. Cliquez sur l'icône de filtre pour ajouter les trois filtres suivants, puis cliquez sur **Appliquer le filtre** :
 - Les types de disques contiennent FabricPool
 - La recommandation Cloud contient un niveau
 - Données froides supérieures à 10



Notez que chaque filtre est joint par un ET logique afin que tous les volumes renvoyés doivent répondre à tous les critères. Vous pouvez ajouter un maximum de cinq filtres.

6. Cliquez sur le haut de la colonne Données froides pour trier les résultats afin que les volumes contenant le plus de données froides apparaissent en haut de la vue.
7. Lorsque la vue est personnalisée, le nom de la vue est Vue non enregistrée. Nommez la vue pour refléter ce qu'elle montre, par exemple « Vols change tiering policy ». Une fois terminé, cliquez sur la coche ou appuyez sur **Entrée** pour enregistrer la vue avec le nouveau nom.

Volumes - Performance / Vols change tiering policy ⓘ Last updated: Feb 8, 2019, 12:26 PM ↻

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy 🔍 Search Volumes ⌵

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Reports ⌵ Show Hide ⌵

Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagntsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. Téléchargez le rapport au format **CSV**, **Excel** ou **PDF** pour voir le résultat avant de le planifier ou de le partager.

Ouvrez le fichier avec une application installée, telle que Microsoft Excel (CSV ou Excel) ou Adobe Acrobat (PDF), ou enregistrez le fichier.



Vous pouvez personnaliser davantage votre rapport à l'aide de filtres complexes, de tris, de tableaux croisés dynamiques ou de graphiques en téléchargeant la vue sous forme de fichier Excel. Après avoir ouvert le fichier dans Excel, utilisez les fonctionnalités avancées pour personnaliser votre rapport. Une fois satisfait, téléchargez le fichier Excel. Ce fichier, avec ses personnalisations, est appliqué à la vue lors de l'exécution du rapport.

Pour plus d'informations sur la personnalisation des rapports à l'aide d'Excel, consultez *Exemples de rapports Microsoft Excel*.

9. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire. Tous les rapports planifiés relatifs à l'objet, dans ce cas les volumes, apparaissent dans la liste.

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports

Volumes - Scheduled Reports View all Scheduled Reports

Add Schedule

Schedule Name	View	Recipients	Frequency	Format	
Weekly / Vols c... tiering policy	Performance / V... tiering policy	user@company.com	Weekly - Monday 1:00 PM	CSV	⋮

10. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
11. Saisissez un nom pour le rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

L'exemple de rapport suivant est au format CSV :

Status	Volume	Volume Id	Tiering Policy	Cold Data	Free Capacity	Total Capacity	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id
Ok	kjagnfsd1	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040
Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141

L'exemple de rapport suivant est au format PDF :

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	kjagnfsd1	Snapshot	28.01	121.32	150	ocum-mo	99018	aggr5_vs
Ok	nfs_vol4	Snapshot	379.64	2676.57	3072	ocum-mo	99113	aggr4

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP pour modifier la stratégie de hiérarchisation sur « auto » ou « all » pour certains volumes afin de décharger davantage de données froides vers le niveau cloud.

Rechercher un rapport planifié

Vous pouvez rechercher des rapports planifiés par nom, nom de vue, type d'objet ou destinataires.

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Planifications de rapport**.
2. Utilisez le champ de texte **Rechercher les rapports programmés**.

Pour rechercher des rapports par ...	Essayer ...
Nom de l'horaire	Tapez une partie du nom du calendrier du rapport.
Nom de la vue	Tapez une partie du nom de la vue du rapport. Les vues par défaut et les vues personnalisées apparaissent dans la liste des vues.
Destinataire	Tapez une partie de l'adresse e-mail.
Type de fichier	Tapez « PDF », « CSV » ou « XLSX ».

3. Vous pouvez cliquer sur un en-tête de colonne pour trier les rapports par ordre croissant ou décroissant selon cette colonne, par exemple en fonction du nom ou du format de la planification.

Personnaliser les rapports

Il existe de nombreuses façons de personnaliser les vues afin de créer un rapport contenant toutes les informations dont vous avez besoin pour gérer vos clusters ONTAP .

Commencez avec une page d'inventaire par défaut ou une vue personnalisée, puis personnalisez-la en ajoutant ou en supprimant des colonnes, en modifiant l'ordre des colonnes, en filtrant les données ou en triant une colonne spécifique par ordre croissant ou décroissant.

À partir de Unified Manager 9.8, vous pouvez également télécharger la vue dans Excel pour la personnaliser à l'aide de fonctionnalités avancées. Une fois terminé, téléchargez le fichier Excel personnalisé. Si vous planifiez un rapport à l'aide de cette vue, il utilise le fichier Excel personnalisé pour créer des rapports robustes que vous pouvez partager.

Pour plus d'informations sur la personnalisation des rapports à l'aide d'Excel, consultez *Exemples de rapports Microsoft Excel*.



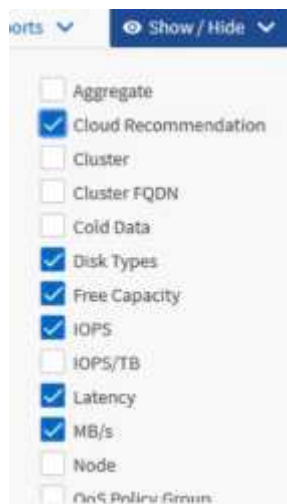
Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage pour gérer les rapports.

Personnaliser les colonnes

Utilisez **Afficher/Masquer** pour choisir les colonnes que vous souhaitez utiliser dans votre rapport. Faites glisser les colonnes sur la page d'inventaire pour les réorganiser.

Étapes

1. Cliquez sur **Afficher/Masquer** pour ajouter ou supprimer des colonnes.



2. Sur la page d'inventaire, faites glisser les colonnes pour les réorganiser dans l'ordre souhaité dans votre rapport.
3. Nommez la vue non enregistrée pour enregistrer vos modifications.

Filtrer les données

Filtrez les données pour vous assurer que les résultats correspondent aux exigences de votre rapport. Le filtrage vous permet d'afficher uniquement les données qui vous intéressent.

Étapes

1. Cliquez sur l'icône de filtre pour ajouter des filtres afin de concentrer les résultats que vous souhaitez afficher, puis cliquez sur **Appliquer le filtre**.

The screenshot shows a 'Filter' panel with a close button (X) in the top right. It contains three filter rules, each with a dropdown menu, a comparison operator, and a value field. The first rule is 'Disk Types' with 'contains' and 'fabricpool'. The second rule is 'Cloud Recommendation' with 'contains' and 'tier'. The third rule is 'Cold Data' with 'greater than' and '1' followed by a unit selector set to 'GB'. Below the rules is a '+ Add Filter' button. At the bottom are 'Reset' and 'Apply Filter' buttons.

2. Nommez la vue non enregistrée pour enregistrer vos modifications.

Trier les données

Pour trier les résultats, cliquez sur une colonne et indiquez l'ordre croissant ou décroissant. Le tri des données donne la priorité aux informations dont vous avez besoin pour le rapport.

Étapes

1. Cliquez en haut d'une colonne pour trier les résultats afin que les informations les plus importantes apparaissent en haut de la vue.
2. Nommez la vue non enregistrée pour enregistrer vos modifications.

Utiliser la recherche pour affiner votre vue

Une fois que vous avez obtenu la vue souhaitée, vous pouvez affiner davantage les résultats à l'aide du champ Rechercher pour vous concentrer sur les résultats que vous souhaitez inclure dans le rapport.

Étapes

1. Ouvrez la vue personnalisée ou par défaut que vous souhaitez utiliser comme base de votre rapport.
2. Tapez dans le champ Rechercher pour affiner les données répertoriées dans la vue. Vous pouvez saisir des données partielles dans l'une des colonnes affichées. Par exemple, si vous souhaitez rechercher des nœuds dont le nom inclut « US_East », vous pouvez affiner la liste complète des nœuds.

Les résultats de votre recherche sont enregistrés dans la vue personnalisée et utilisés dans le rapport planifié résultant.

3. Nommez la vue non enregistrée pour enregistrer vos modifications.

Utilisez Excel pour personnaliser votre rapport

Après avoir enregistré la vue, vous pouvez la télécharger au format Classeur Excel (.xlsx). Lorsque vous ouvrez le fichier Excel, vous pouvez utiliser les fonctionnalités avancées d'Excel pour personnaliser votre rapport.

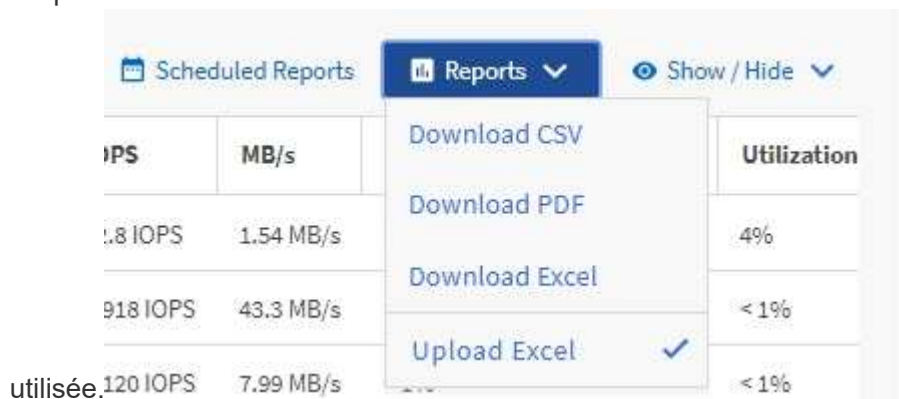
Avant de commencer

Vous ne pouvez télécharger qu'un fichier de classeur Excel avec l'extension .xlsx.

Par exemple, certaines fonctionnalités avancées d'Excel que vous pouvez utiliser dans votre rapport incluent :

- Tri multi-colonnes
- Filtrage complexe
- Tableaux croisés dynamiques
- Graphiques

- Le fichier Excel téléchargé utilise le nom de fichier par défaut pour la vue, et non votre nom enregistré.
 - Le format est <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
 - Par exemple, une vue personnalisée enregistrée nommée `Volumes-not online` a un nom de fichier de `health-volumes-05-May-2020-19-18-00.xlsx` si elle est sauvegardée à ce jour et à cette heure.
- Vous pouvez ajouter des feuilles au fichier Excel, mais ne pas modifier les feuilles existantes.
 - Ne modifiez pas les feuilles, données et informations existantes. Copiez plutôt les données sur une nouvelle page que vous créez.
 - Une exception à la règle ci-dessus est que vous pouvez créer des formules sur la page « données ». Utilisez les formules de page de données pour créer des graphiques sur de nouvelles pages.
 - Ne nommez pas une nouvelle feuille de données ou d'informations.
- Si un fichier Excel personnalisé existe, une coche est présente à côté de l'élément de menu **Rapports > Télécharger Excel**. Lorsque vous téléchargez le fichier Excel, la version avec les personnalisations est



Étapes

1. Ouvrez la vue par défaut, personnalisée ou enregistrée que vous souhaitez utiliser comme base de votre rapport.
2. Sélectionnez **Rapports > Télécharger Excel**.
3. Enregistrez le fichier. Le fichier est enregistré dans votre dossier de téléchargements.
4. Ouvrez le fichier enregistré dans Excel. Ne déplacez pas le fichier vers un nouvel emplacement ou, si vous travaillez dans un autre emplacement, enregistrez le fichier à l'emplacement d'origine en utilisant le nom

de fichier d'origine avant de télécharger le fichier.

5. Personnalisez le fichier à l'aide des fonctionnalités d'Excel, telles que les tris complexes, les filtres en couches, les tableaux croisés dynamiques ou les graphiques. Pour plus d'informations, consultez la documentation Microsoft® Excel.
6. Sélectionnez **Rapports > Télécharger Excel** et sélectionnez le fichier que vous avez modifié. Le fichier le plus récemment téléchargé est téléchargé à partir du même emplacement de fichier.
7. Envoyez-vous un rapport de test en utilisant la fonction **Rapports programmés**.

Télécharger les rapports

Vous pouvez télécharger des rapports et enregistrer les données sur un lecteur local ou réseau sous forme de fichier de valeurs séparées par des virgules (CSV), de fichier Microsoft Excel (.XLSX) ou de fichier PDF. Vous pouvez ouvrir les fichiers CSV et XLSX avec des applications de feuille de calcul, telles que Microsoft Excel, et les fichiers PDF avec des lecteurs tels qu'Adobe Acrobat.

Étapes

1. Cliquez sur le bouton **Rapports** pour télécharger le rapport sous l'un des formats suivants :

Choisir	À...
Télécharger CSV	Enregistrez le rapport sous forme de fichier de valeurs séparées par des virgules (CSV).
Télécharger le PDF	Enregistrez le rapport sous forme de fichier .pdf.
Télécharger Excel	Enregistrez le rapport sous forme de fichier Microsoft Excel (XLSX).

Rapports de planification

Une fois que vous avez une vue que vous souhaitez réutiliser et partager sous forme de rapport, vous pouvez la planifier à l'aide d'Active IQ Unified Manager. Vous pouvez gérer les rapports planifiés, en modifiant les destinataires et la fréquence de distribution pour chaque planification de rapport.

Vous pouvez planifier la plupart des vues ou des pages d'inventaire dans Unified Manager. Les exceptions sont les événements, qui sont des rapports que vous pouvez télécharger sous forme de fichiers CSV, mais vous ne pouvez pas planifier d'événements pour la régénération et le partage. Vous ne pouvez pas non plus télécharger ou planifier les tableaux de bord, les favoris ou les pages de configuration.

À partir d'Active IQ Unified Manager 9.8, vous pouvez télécharger des vues au format Microsoft® Excel et les personnaliser. Vous pouvez utiliser des fonctionnalités Excel avancées telles que des tris complexes, des filtres en couches, des tableaux croisés dynamiques et des graphiques. Lorsque vous êtes satisfait du rapport Excel obtenu, vous pouvez télécharger le fichier Excel pour l'utiliser chaque fois que le rapport est planifié et partagé.

Vous pouvez planifier les vues intégrées ou les vues que vous personnalisez. Vous pouvez choisir le type de

fichier à envoyer, CSV, PDF ou XSLX. Lorsque vous planifiez un rapport pour la première fois, vous pouvez le télécharger et vous désigner comme seul destinataire à voir le rapport, car vos destinataires le verront.

Planifier un rapport

Une fois que vous disposez d'une vue ou d'un fichier Excel que vous souhaitez planifier pour une génération et une distribution régulières, vous pouvez planifier le rapport.

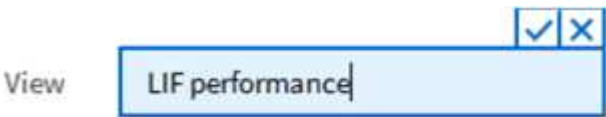
Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré les paramètres du serveur SMTP dans la page **Général > Notifications** afin que le moteur de création de rapports puisse envoyer des rapports sous forme de pièces jointes à la liste des destinataires à partir du serveur Unified Manager.
- Le serveur de messagerie doit être configuré pour permettre l'envoi de pièces jointes avec les e-mails générés.

Utilisez les étapes suivantes pour tester et planifier la génération d'un rapport pour une vue. Sélectionnez ou personnalisez la vue que vous souhaitez utiliser. La procédure suivante utilise une vue réseau qui affiche les performances de vos interfaces réseau, mais vous pouvez utiliser la vue de votre choix.

Étapes

1. Ouvrez votre vue. Cet exemple utilise la vue réseau par défaut qui affiche les performances LIF. Dans le volet de navigation de gauche, cliquez sur **Réseau > Interfaces réseau**.
2. Personnalisez la vue selon vos besoins à l'aide des fonctionnalités intégrées d'Unified Manager.
3. Après avoir personnalisé la vue, vous pouvez fournir un nom unique dans le champ **Vue** et cliquer sur la coche pour l'enregistrer.



4. Vous pouvez utiliser les fonctionnalités avancées de Microsoft® Excel pour personnaliser votre rapport. Pour plus de détails, voir "[Utiliser Excel pour personnaliser votre rapport](#)".
5. Pour voir le résultat avant de le planifier ou de le partager :

Option	Description
Si vous avez utilisé Excel pour personnaliser le rapport	Afficher le fichier Excel téléchargé existant.
Si vous n'avez pas utilisé Excel pour personnaliser le rapport	Téléchargez le rapport au format CSV , PDF ou XLSX .

Ouvrez le fichier avec une application installée, telle que Microsoft Excel (CSV/XSLX) ou Adobe Acrobat (PDF).

6. Si vous êtes satisfait du rapport, cliquez sur **Rapports programmés**.
7. Dans la page Calendriers de rapport, cliquez sur **Ajouter un calendrier**.
8. Acceptez le nom par défaut, qui est une combinaison du nom de la vue et de la fréquence, ou

personnalisez le **nom du programme**.

9. Pour tester le rapport planifié la première fois, ajoutez-vous uniquement en tant que **destinataire**. Une fois satisfait, ajoutez les adresses e-mail de tous les destinataires du rapport.
10. Spécifiez la fréquence à laquelle le rapport sera généré et envoyé aux destinataires. Vous pouvez choisir **Quotidien**, **Hebdomadaire** ou **Mensuel**.
11. Sélectionnez le format, soit **PDF**, **CSV** ou **XSLX**.



Pour les rapports dont vous avez utilisé Excel pour personnaliser le contenu, sélectionnez toujours **XSLX**.

12. Cliquez sur la coche (✓) pour enregistrer le calendrier du rapport.

LIFs - Scheduled Reports [View all Scheduled Reports](#)

[Add Schedule](#)

Schedule Name	View	Recipients	Frequency	Format
Weekly / LIF performar	Performance / LIF pe ▼	test@inetapp.com	Weekly ▼ Thursday ▼ 4:30 PM ▼	PDF ▼

✓ ✕

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence planifiée.

Planifier les rapports .rptdesign importés

Vous pouvez planifier des rapports existants qui ont été créés et importés dans une version antérieure de Unified Manager.

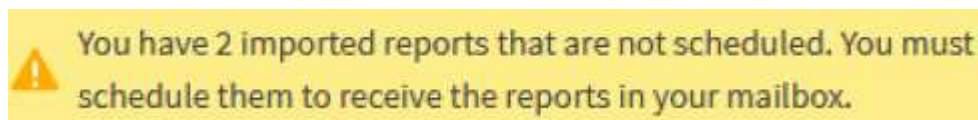
La planification des rapports importés nécessite les éléments suivants :

- rapports de fichiers .rptdesign conçus par BIRT importés dans une version antérieure d'Unified Manager
- applicable lors de la mise à niveau vers Unified Manager 9.6 GA ou version ultérieure

Après la mise à niveau vers Unified Manager 9.6 GA ou une version ultérieure, la page Planifications de rapport répertorie les rapports importés. Vous pouvez modifier la planification de ces rapports pour spécifier les adresses e-mail des destinataires, la fréquence et le format (PDF ou CSV). Sinon, ces rapports ne peuvent pas être modifiés ou affichés dans l'interface utilisateur d'Unified Manager.

Étapes

1. Ouvrez la page Calendriers de rapport. Si vous avez importé des rapports, un message apparaît.



2. Cliquez sur le nom **Vue** pour afficher la requête SQL utilisée pour générer le rapport.

**Imported Report**

This report is generated using following database query:

```
SELECT c.name AS 'Cluster', m.name AS 'SVM', v.name AS 'Volume', s.name AS 'Share',
s.path AS 'Path', q.name AS 'Qtree', s.shareProperties AS 'Properties', a.userOrGroup
AS 'User', a.permission AS 'Permission' FROM ocum_report.cifsshare s JOIN
ocum_report.cifsshareacl a ON s.id = a.cifsShareId JOIN ocum_report.cluster c ON
s.clusterId = c.id JOIN ocum_report.svm m ON s.svmId = m.id JOIN
ocum_report.volume v ON s.volumeId = v.id JOIN ocum_report.qtree q ON s.qtreeId =
q.id
```

3. Cliquez sur l'icône plus  , cliquez sur **Modifier**, définissez les détails du calendrier du rapport et enregistrez le rapport.



Vous pouvez également supprimer tous les rapports indésirables à partir de l'icône Plus  .

Gérer les calendriers de rapports

Vous pouvez gérer vos calendriers de rapport à partir de la page Calendriers de rapport. Vous pouvez afficher, modifier ou supprimer les plannings existants.



Avant de commencer

Vous ne pouvez pas planifier de nouveaux rapports à partir de la page Planifications de rapports. Vous ne pouvez ajouter des rapports planifiés qu'à partir des pages d'inventaire d'objets.

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Planifications de rapport**.
2. Sur la page Calendriers de rapport :

Si vous voulez...	Alors...
Afficher un planning existant	Faites défiler la liste des rapports existants à l'aide des barres de défilement et des commandes de page.

Si vous voulez...	Alors...
Modifier un planning existant	- Cliquez sur l'icône plus  pour le programme que vous souhaitez utiliser. - Cliquez sur Modifier. - Apportez les modifications nécessaires. - Cliquez sur la coche pour enregistrer vos modifications.
Supprimer un planning existant	- Cliquez sur l'icône plus  pour le programme que vous souhaitez utiliser. - Cliquez sur Supprimer. - Confirmez votre décision.

Modifier les rapports planifiés

Une fois les rapports planifiés, vous pouvez les modifier sur la page Planifications des rapports.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Planifications de rapport**.

Scheduled Reports

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Si vous disposez des autorisations appropriées, vous pouvez modifier n'importe quel rapport et sa planification dans le système.

2. Cliquez sur l'icône plus  pour l'horaire que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Vous pouvez modifier le **Nom du planning**, la liste des **Destinataires**, la **Fréquence** et le **Format** du planning du rapport.

5. Une fois terminé, cliquez sur la coche pour enregistrer vos modifications.

Supprimer les rapports planifiés

Une fois les rapports planifiés, vous pouvez les supprimer à partir de la page Planifications de rapports.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Planifications de rapport**.

Scheduled Reports ?

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

Search Scheduled Reports					
Schedule Name	View	Recipients	Frequency	Format	
Weekly /Node performance	Performance / Tom_test	test@netapp.com	Weekly - Monday 5:30 PM	PDF	
Weekly / my view	Health / my view	test@netapp.com	Weekly - Friday 5:30 PM	PDF	
Weekly / LIF performance	Performance / LIF performance	test@netapp.com	Weekly - Thursday 4:30 PM	PDF	



Si vous disposez des autorisations appropriées, vous pouvez supprimer n'importe quel rapport et sa planification dans le système.

2. Cliquez sur l'icône plus  pour le programme que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.
4. Confirmez votre décision.

Le rapport planifié est supprimé de la liste et ne sera plus généré ni distribué selon le calendrier défini.



Si vous supprimez une vue personnalisée de la page d'inventaire, tous les fichiers Excel personnalisés ou rapports planifiés qui utilisent cette vue sont également supprimés.

Exemples de rapports personnalisés

Ces exemples de rapports personnalisés sont couramment utilisés pour vous aider à identifier les problèmes potentiels et à y répondre avant qu'ils ne surviennent.

La liste des rapports de cette section n'est pas exhaustive et s'allongera au fil du temps. Vous pouvez suggérer des rapports personnalisés à ajouter à cette section en fournissant des commentaires sur la documentation.



Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage pour gérer les rapports.

Personnaliser les rapports de stockage en cluster

Les exemples de rapports de stockage de cluster de cette section ne sont que des exemples pour vous aider à comprendre comment créer des rapports sur la capacité du cluster pour vous aider à surveiller les ressources de votre système de stockage.

Créer un rapport pour afficher la capacité par modèle de cluster

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des clusters en fonction du modèle de système de stockage.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche la capacité par modèle de cluster, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer toutes les colonnes, telles que « Cluster FQDN » et « OS Version », que vous ne souhaitez pas dans le rapport.
4. Faites glisser la « Capacité brute totale », le « Modèle/Famille » et les trois colonnes agrégées près de la colonne « Cluster ».
5. Cliquez en haut de la colonne « Modèle/Famille » pour trier les résultats par type de cluster.
6. Enregistrez la vue sous un nom spécifique qui reflète ce que la vue montre, par exemple, « Capacité par modèle de cluster ».
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être ajouter davantage de capacité à certains clusters ou mettre à niveau des modèles de cluster plus anciens.

Créer un rapport pour identifier les clusters avec la plus grande capacité LUN non allouée

Vous pouvez créer un rapport pour rechercher les clusters avec la capacité LUN non allouée la plus importante, supérieure à 0,5 To, afin de vous aider à identifier où vous pouvez ajouter des charges de travail supplémentaires.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche les clusters avec la capacité LUN non allouée la plus importante, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne « Capacité LUN non allouée » près de la colonne « Paire HA ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - Capacité LUN non allouée supérieure à 0,5 To
6. Cliquez en haut de la colonne « Capacité LUN non allouée » pour trier les résultats en fonction de la plus grande quantité de capacité LUN non allouée.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Capacité LUN la plus non allouée » et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être utiliser la capacité LUN non allouée du cluster.

Créer un rapport pour afficher les paires HA avec la capacité la plus disponible

Vous pouvez créer un rapport pour trouver les paires haute disponibilité (HA) avec la plus grande capacité pour provisionner de nouveaux volumes et LUN.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche les paires HA triées par la capacité la plus disponible pour provisionner de nouveaux volumes et LUN, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne « Capacité globale inutilisée » près de la colonne « Paire HA ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - Capacité globale inutilisée supérieure à 0,5 To
6. Cliquez en haut de la colonne « Capacité globale inutilisée » pour trier les résultats en fonction de la plus

grande quantité de capacité globale inutilisée.

7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple, « Capacité globale la moins utilisée » et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être équilibrer les paires HA en fonction de la capacité globale.

Créer un rapport pour afficher les nœuds exécutant des versions plus anciennes d' ONTAP

Vous pouvez créer un rapport pour afficher la version du logiciel ONTAP installée sur tous les nœuds du cluster afin de voir quels nœuds vous devez mettre à niveau.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche les nœuds exécutant des versions plus anciennes d' ONTAP, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Nœuds**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
3. Faites glisser la colonne « Version du système d'exploitation » près de la colonne « Nœud ».
4. Cliquez en haut de la colonne « Version du système d'exploitation » pour trier les résultats par version la plus ancienne d' ONTAP.
5. Enregistrez la vue sous un nom spécifique qui reflète ce que la vue affiche, par exemple, « Nœuds par version ONTAP ».
6. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
7. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
8. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être mettre à niveau les nœuds exécutant des versions plus anciennes d' ONTAP.

Personnaliser les rapports de capacité globale

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier et à répondre aux problèmes potentiels liés à la capacité de stockage globale.

Les rapports de cette section ne sont que des exemples pour vous aider à comprendre comment créer des rapports sur la capacité globale pour vous aider à surveiller les ressources de votre système de stockage.

Créer un rapport pour afficher les agrégats atteignant leur pleine capacité

Vous pouvez créer un rapport pour rechercher les agrégats qui atteignent leur pleine capacité afin de pouvoir ajouter davantage de capacité ou déplacer des charges de travail vers d'autres agrégats.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour créer une vue personnalisée qui affiche les agrégats atteignant leur pleine capacité, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - Jours pour remplir moins de 45 jours
5. Cliquez en haut de la colonne « Jours avant la pleine capacité » pour trier les résultats en fonction du nombre minimum de jours restants pour atteindre la pleine capacité.
6. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple, « Jours avant la pleine capacité globale », et cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats présentés dans le rapport, vous souhaitez peut-être augmenter le stockage sur les agrégats atteignant leur pleine capacité. De plus, vous souhaitez peut-être augmenter le seuil de capacité en jours jusqu'à la pleine capacité à plus de 7 jours par défaut afin de recevoir des événements qui vous donnent plus de temps pour réagir lorsque l'espace disponible sur les agrégats diminue.

Créer un rapport pour afficher les agrégats remplis à 80 % ou plus

Vous pouvez créer un rapport pour mettre en évidence les agrégats qui sont remplis à 80 % ou plus.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour créer une vue personnalisée qui affiche les agrégats remplis à 80 % ou plus, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser les colonnes « Données disponibles % » et « Données utilisées % » près de la colonne « Agrégat ».
5. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **Appliquer le filtre** :
 - Le pourcentage de données utilisées est supérieur à 80 %
6. Cliquez en haut de la colonne « % de données utilisées » pour trier les résultats par pourcentage de capacité.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue montre, par exemple, « Agrégats presque pleins », et cliquez sur la coche (✓) .
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être déplacer certaines données de certains agrégats.

Créer un rapport pour afficher les agrégats surengagés

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des agrégats, et pour afficher les agrégats surchargés.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche les agrégats qui dépassent le seuil de surengagement, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne « Capacité surengagée % » près de la colonne « Agrégat ».

5. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **Appliquer le filtre** :
 - Le pourcentage de capacité surengagée est supérieur à 100 %
6. Cliquez en haut de la colonne « Capacité surengagée % » pour trier les résultats par pourcentage de capacité.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple, « Agrégats surengagés », et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être ajouter davantage de capacité aux agrégats ou déplacer certaines données de certains agrégats.

Personnaliser les rapports de capacité de volume

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier et à répondre aux problèmes potentiels liés à la capacité et aux performances du volume.

Créer un rapport pour identifier les volumes proches de leur pleine capacité pour lesquels la suppression automatique des instantanés est désactivée

Vous pouvez créer un rapport contenant la liste des volumes qui approchent de leur pleine capacité avec la fonction de suppression automatique des instantanés désactivée. Les résultats peuvent vous aider à identifier les volumes sur lesquels vous souhaitez peut-être configurer la suppression automatique des instantanés.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes ci-dessous pour créer une vue personnalisée qui affiche les colonnes requises dans le bon ordre, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser et déposez les colonnes « Suppression automatique des instantanés » et « Nombre de jours avant remplissage » près de la colonne « Capacité de données disponible ».
5. Cliquez sur l'icône de filtre, ajoutez les deux filtres suivants, puis cliquez sur **Appliquer le filtre** :
 - Jours avant épuisement moins de 30 jours
 - La suppression automatique des instantanés est désactivée

6. Cliquez sur le haut de la colonne **Jours restants** pour que les volumes avec le moins de jours restants apparaissent en haut de la liste.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Vols proches de la capacité ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être activer la suppression automatique des instantanés sur les volumes ou trouver un moyen d'augmenter l'espace disponible.

Créer un rapport pour identifier l'espace utilisé par les volumes avec le provisionnement léger désactivé

Lorsqu'un volume n'est pas provisionné de manière dynamique, il occupe la totalité de l'espace sur le disque tel que défini lors de la création du volume. L'identification des volumes pour lesquels le provisionnement dynamique est désactivé vous aide à décider si vous souhaitez activer le provisionnement dynamique sur certains volumes.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes ci-dessous pour créer une vue personnalisée qui affiche les colonnes requises dans le bon ordre, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Capacité > Tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser et déposez les colonnes « % de données utilisées » et « Provisionnement léger » près de la colonne « Capacité de données disponible ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, **Thin provisioned** est **Non**, puis cliquez sur **Appliquer le filtre**.
6. Cliquez en haut de la colonne « % de données utilisées » pour trier les résultats afin que les volumes avec le pourcentage le plus élevé apparaissent en haut de la liste.
7. Enregistrez la vue avec un nom reflétant ce qu'elle affiche, par exemple « Vols sans provisionnement léger ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par

courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être activer le provisionnement dynamique sur certains volumes.

Créer un rapport pour identifier les volumes sur les agrégats FabricPool qui doivent déplacer les données vers le niveau cloud

Vous pouvez créer un rapport contenant la liste des volumes qui résident actuellement sur des agrégats FabricPool , qui ont une recommandation cloud de niveau et qui ont une grande quantité de données froides. Ce rapport peut vous aider à décider si vous devez modifier la politique de hiérarchisation de certains volumes sur « auto » ou « all » pour décharger davantage de données froides (inactives) vers le niveau cloud.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.
- Vous devez avoir configuré des agrégats FabricPool et disposer de volumes sur ces agrégats.

Suivez les étapes ci-dessous pour créer une vue personnalisée qui affiche les colonnes requises dans le bon ordre, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Performances > Tous les volumes**.
3. Dans le sélecteur de colonnes, assurez-vous que la colonne « Type de disque » apparaît dans la vue.

Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Faites glisser et déposez la colonne « Type de disque » près de la colonne « Recommandation Cloud ».
5. Cliquez sur l'icône de filtre, ajoutez les trois filtres suivants, puis cliquez sur **Appliquer le filtre** :
 - Le type de disque contient FabricPool
 - La recommandation Cloud contient un niveau
 - Données froides supérieures à 10Go

6. Cliquez sur le haut de la colonne Données froides afin que les volumes contenant le plus de données froides apparaissent en haut de la vue.
7. Enregistrez la vue avec un nom reflétant ce qu'elle affiche, par exemple « Vols change tiering policy ».

Volumes - Performance / Vols change tiering policy

Last updated: Feb 8, 2019, 12:26 PM

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View Vols change tiering policy Search Volumes 3

Assign Performance Threshold Policy		Clear Performance Threshold Policy		Schedule Report		
Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être utiliser System Manager ou l'interface de ligne de commande ONTAP pour modifier la stratégie de hiérarchisation sur « auto » ou « all » pour certains volumes afin de décharger davantage de données froides vers le niveau cloud.

Personnaliser les rapports de capacité Qtree

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier et à répondre aux problèmes potentiels liés à la capacité de Qtree.

Créer un rapport pour afficher les qtrees presque pleins

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des qtrees, et pour afficher les qtrees presque pleins.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche les qtrees presque pleins, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Qtrees**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
3. Faites glisser la colonne « Disque utilisé % » près de la colonne « Qtrees ».
4. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **Appliquer le filtre** :
 - Le pourcentage d'utilisation du disque est supérieur à 75 %
5. Cliquez en haut de la colonne « % de disque utilisé » pour trier les résultats par pourcentage de capacité.
6. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue montre, par exemple, « Qtrees presque pleins », et cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être ajuster les limites matérielles et logicielles du disque (si définies) ou équilibrer les données entre les qtrees.

Personnaliser les rapports de partage NFS

Vous pouvez personnaliser les rapports de partage NFS pour analyser les informations sur les stratégies et règles d'exportation NFS pour les volumes sur vos systèmes de stockage. Par exemple, vous pouvez personnaliser les rapports pour afficher les volumes avec des chemins de montage inaccessibles et les volumes avec la stratégie d'exportation par défaut.

Créer un rapport pour afficher les volumes dont le chemin de montage est inaccessible

Vous pouvez créer un rapport pour rechercher les volumes dont le chemin de montage est inaccessible.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée pour les volumes dont le chemin de montage est inaccessible, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Partages NFS**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
3. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - Le chemin de montage actif est Non
4. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Volumes avec un chemin de montage inaccessible » et cliquez sur la coche (✓).
5. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
6. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
7. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être corriger les chemins de montage inaccessibles.

Créer un rapport pour afficher les volumes qui utilisent la politique d'exportation par défaut

Vous pouvez créer un rapport pour rechercher les volumes qui utilisent la politique d'exportation par défaut.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée pour les volumes qui utilisent la stratégie d'exportation par défaut, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Partages NFS**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
3. Faites glisser la colonne « Politique d'exportation » près de la colonne « Volume ».
4. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - La politique d'exportation contient les valeurs par défaut
5. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Volumes avec une politique d'exportation par défaut » et cliquez sur la coche (✓).
6. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
7. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
8. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être configurer une politique d'exportation personnalisée.

Personnaliser les rapports de VM de stockage

Vous pouvez créer des rapports de machine virtuelle de stockage pour analyser les informations de volume et afficher l'état général et la disponibilité du stockage. Par exemple, vous pouvez créer des rapports pour afficher les SVM atteignant le volume maximal et pour analyser les SVM arrêtées.

Créer un rapport pour afficher les machines virtuelles de stockage atteignant la limite de volume maximale

Vous pouvez créer un rapport pour rechercher les SVM qui atteignent la limite de volume maximale.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui affiche les machines virtuelles de stockage qui atteignent la limite de volume maximale, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
3. Faites glisser les colonnes « Nombre de volumes » et « Volumes maximum autorisés » près de la colonne « VM de stockage ».
4. Cliquez en haut de la colonne « Volumes maximum autorisés » pour trier les résultats en fonction du nombre de volumes le plus élevé.
5. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « SVM atteignant les volumes maximum » et cliquez sur la coche (✓).
6. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
7. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
8. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être équilibrer les volumes attribués aux machines virtuelles de stockage ou, si possible, utiliser ONTAP System Manager pour modifier les volumes maximum autorisés.

Créer un rapport pour afficher les machines virtuelles de stockage arrêtées

Vous pouvez créer un rapport pour afficher une liste de tous les SVM arrêtés.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour créer une vue personnalisée qui affiche les machines virtuelles de stockage arrêtées, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.
2. Dans le menu Affichage, sélectionnez **Santé > Toutes les machines virtuelles de stockage**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne « État » près de la colonne « VM de stockage ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - L'état est arrêté
6. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « SVM arrêtées » et cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être rechercher la raison pour laquelle le SVM est arrêté pour voir si vous devez redémarrer les SVM arrêtés.

Personnaliser les rapports de relation de volume

Le rapport Inventaire des relations de volume vous permet d'analyser les détails de l'inventaire de stockage dans un cluster, de comprendre le degré de protection requis pour les volumes et de filtrer les détails du volume en fonction de la source de défaillance, du modèle et des planifications.

Créer un rapport pour regrouper les relations de volume par source de défaillance

Vous pouvez créer un rapport qui regroupe les volumes en fonction de la raison pour laquelle la relation est dans un état non sain.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui regroupe les volumes par source de défaillance, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Toutes les relations**.
3. Sélectionnez **Afficher/Masquer** pour vous assurer que les colonnes « Santé de la relation » et « Raison malsaine » apparaissent dans la vue.

Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Faites glisser les colonnes « Santé de la relation » et « Raison malsaine » près de la colonne « État ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - La santé des relations est mauvaise
6. Cliquez en haut de la colonne « Raison de défaillance » pour regrouper les relations de volume par source de défaillance.
7. Enregistrez la vue sous un nom spécifique qui reflète ce que la vue affiche, par exemple, « Relations vol. par échec ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats affichés dans le rapport, vous pouvez étudier la source et l'impact de chaque type de défaillance.

Créer un rapport pour regrouper les relations de volume par problème

Vous pouvez créer un rapport qui regroupe les relations de volume par problème.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée qui regroupe les relations de volume par problème, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Toutes les relations**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne « Raison malsaine » près de la colonne « État ».
5. Cliquez en haut de la colonne « Raison insalubre » pour regrouper les volumes par problème.
6. Enregistrez la vue sous un nom spécifique qui reflète ce que la vue affiche, par exemple, « Relations vol. par problème ».
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats affichés dans le rapport, vous pouvez étudier la source et l'impact de chaque type de problème.

Créer un rapport pour afficher les tendances de transfert de volume à des intervalles de temps spécifiques

Vous pouvez créer un rapport qui affiche les tendances de transfert de volume à des intervalles de temps spécifiques.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée pour les volumes à des intervalles de temps spécifiques, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Statut du transfert du dernier mois**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne **Durée du transfert** près de la colonne « Résultat opérationnel ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - Heure de fin du transfert au cours des 7 derniers jours
6. Cliquez en haut de la colonne « **Durée de transfert** » pour trier les volumes par intervalle de temps.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Volumes par durée ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Saisissez un nom pour le calendrier du rapport, définissez la fréquence sur **Hebdomadaire** et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats affichés dans le rapport, vous pouvez étudier les intervalles de temps de transfert.

Créer un rapport pour afficher les transferts de volume échoués ou réussis

Vous pouvez créer un rapport qui affiche l'état des transferts de volume. Vous pouvez afficher les transferts de volumes ayant échoué et réussi dans ce rapport.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour créer une vue personnalisée afin d'afficher les transferts ayant échoué et ceux ayant réussi, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Statut du transfert du dernier mois**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas dans le rapport.
4. Faites glisser la colonne « Résultat de l'opération » près de la colonne « État ».
5. Cliquez en haut de la colonne « Résultat de l'opération » pour trier les volumes par statut.
6. Enregistrez la vue sous un nom spécifique qui reflète ce que la vue affiche, par exemple « Volumes par statut de transfert ».
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous pouvez examiner l'état du transfert.

Créer un rapport pour afficher les transferts de volume en fonction de la taille du transfert

Vous pouvez créer un rapport pour afficher les transferts de volume en fonction de la taille du transfert.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée pour les transferts de volume en fonction de la taille du transfert, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Taux de transfert du dernier mois**.
3. Cliquez en haut de la colonne « Taille totale du transfert » pour trier les transferts de volume par taille.
4. Enregistrez la vue sous un nom spécifique qui reflète ce que la vue affiche, par exemple « Volumes par taille de transfert ».
5. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
6. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats affichés dans le rapport, vous pouvez étudier les relations de volume par taille de transfert.

Créer un rapport pour afficher les transferts de volume regroupés par jour

Vous pouvez créer un rapport pour afficher les transferts de volume regroupés par jour.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour créer une vue personnalisée pour les transferts de volume regroupés par jour, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation > Taux de transfert du dernier mois**.
3. Cliquez en haut de la colonne « Jour » pour trier les transferts de volume par jour.
4. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Transferts de volume par jour ».
5. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
6. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats affichés dans le rapport, vous pouvez étudier les transferts de volume par jour.

Personnaliser les rapports de performances de volume

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier et à répondre aux problèmes potentiels liés aux performances du volume.

Créer un rapport pour afficher les volumes avec une grande quantité de données froides sur un agrégat qui n'est pas compatible avec FabricPool

Vous pouvez créer un rapport pour afficher les volumes avec une grande quantité de données froides sur un agrégat non FabricPool . Cela peut vous aider à identifier les volumes qui doivent être déplacés vers un agrégat FabricPool .

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Utilisez les étapes suivantes pour créer une vue personnalisée pour les volumes avec une grande quantité de données froides sur un agrégat non compatible FabricPool, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.
2. Dans le menu Affichage, sélectionnez **Performances > Tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour vous assurer que la colonne « Type de disque » apparaît dans la vue.

Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Faites glisser la colonne « Type de disque » près de la colonne « Données froides ».

5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre** :
 - Données froides supérieures à 100 Go
 - Le type de disque contient SSD
6. Cliquez en haut de la colonne « Type de disque » pour trier les volumes par type de disque afin que le type de disque SSD (FabricPool) soit en bas.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « Volumes de données froides non FabricPool ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

Sur la base des résultats affichés dans le rapport, vous pouvez trouver des volumes qui sont de bons candidats pour être déplacés vers des agrégats FabricPool .

Exemples de rapports Microsoft Excel

Ces exemples de rapports Microsoft Excel sont destinés à présenter les options de création de rapports disponibles à l'aide des fonctionnalités avancées d'Excel.

Les fonctionnalités avancées d'Excel permettent de créer une large gamme de rapports adaptés à vos besoins. Pour obtenir des informations complètes sur l'utilisation d'Excel, consultez la documentation du produit.



Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage pour gérer les rapports.

Créer un rapport pour afficher un tableau et un graphique de capacité globale

Vous pouvez créer un rapport pour analyser la capacité dans un fichier Excel en utilisant des totaux additionnés et le format de graphique à colonnes groupées.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour ouvrir une vue Santé : tous les agrégats, télécharger la vue dans Excel, créer un graphique de capacité disponible, télécharger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Sélectionnez **Rapports > Télécharger Excel**.



Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

3. Si nécessaire, cliquez sur **Activer la modification**.
4. Dans Excel, ouvrez le fichier téléchargé.
5. Créer une nouvelle feuille () après le data feuille et nommez-la **Capacité totale de données**.
6. Ajoutez les colonnes suivantes sur la nouvelle feuille Capacité totale des données :
 - a. Capacité totale de données (Go)
 - b. Capacité engagée (Go)
 - c. Capacité de données utilisée (Go)
 - d. Capacité de données disponible (Go)
7. Dans la première ligne de chaque colonne, saisissez la formule suivante, en vous assurant qu'elle fait référence à la feuille de données (données !) et qu'elle fait référence aux spécificateurs de colonne et de ligne corrects pour les données capturées (Total Data Capacity extrait les données de la colonne E, lignes 2 à 20).
 - a. =SOMME(données!E\$2:données!E\$20)
 - b. =SOMME(données!F\$2:données!F\$50)
 - c. =SOMME(données!G\$2:données!G\$50)
 - d. =SOMME(données!H\$2:données!H\$50)

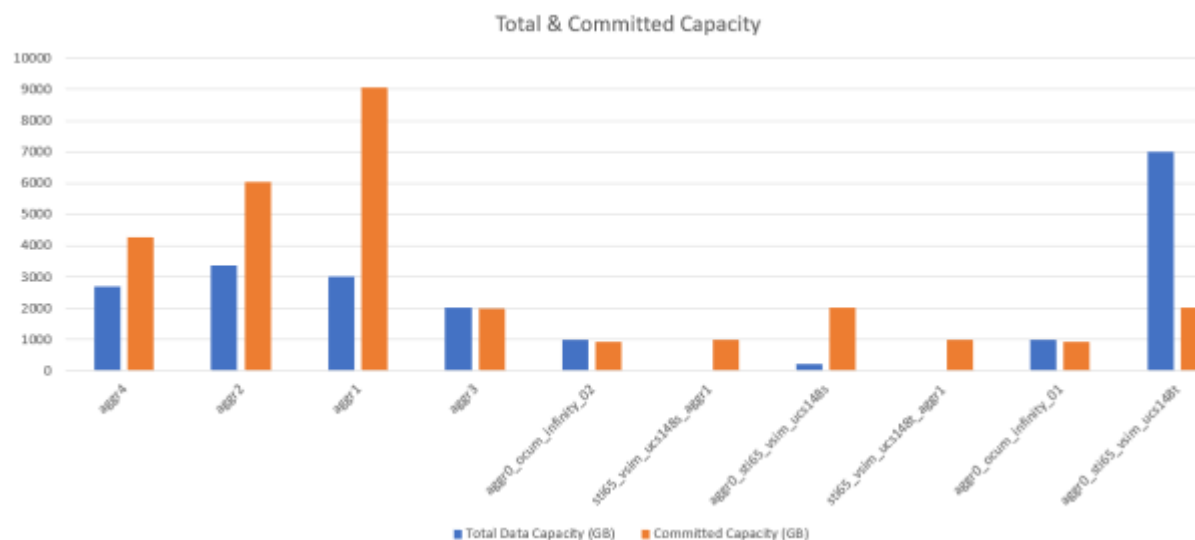
La formule totalise chaque colonne en fonction des données actuelles.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. Sur la feuille de données, sélectionnez les colonnes **Capacité totale des données (Go)** et **Capacité engagée (Go)**.
2. Sélectionnez **Graphiques recommandés** dans le menu **Insertion** et sélectionnez le graphique **Colonnes groupées**.
3. Cliquez avec le bouton droit sur le graphique et sélectionnez **Déplacer le graphique** pour déplacer le graphique vers le Total Data Capacity feuille.
4. À l'aide des menus **Conception** et **Format**, disponibles lorsque le graphique est sélectionné, vous pouvez

personnaliser l'apparence du graphique.

5. Lorsque vous êtes satisfait, enregistrez le fichier avec vos modifications. Ne modifiez pas le nom du fichier ni son emplacement.



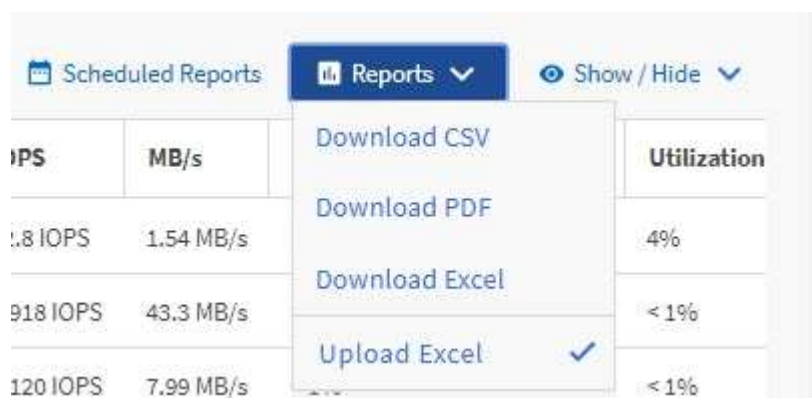
6. Dans Unified Manager, sélectionnez **Rapports > Télécharger Excel**.



Assurez-vous que vous êtes dans la même vue où vous avez téléchargé le fichier Excel.

7. Sélectionnez le fichier Excel que vous avez modifié.
8. Cliquez sur **Ouvrir**.
9. Cliquez sur **Soumettre**.

Une coche apparaît à côté de l'élément de menu **Rapports > Télécharger Excel**.



10. Cliquez sur **Rapports planifiés**.
11. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.



Sélectionnez le format **XLSX** pour le rapport.

12. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats présentés dans le rapport, vous souhaitez peut-être étudier la meilleure façon d'utiliser la capacité disponible sur votre réseau.

Créer un rapport pour afficher les graphiques de capacité totale agrégée par rapport à la capacité disponible

Vous pouvez créer un rapport pour analyser la capacité totale de stockage et la capacité engagée dans un format de graphique Excel.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour ouvrir une vue Santé : tous les agrégats, télécharger la vue dans Excel, créer un graphique de capacité totale et engagée, télécharger le fichier Excel personnalisé et planifier le rapport final.

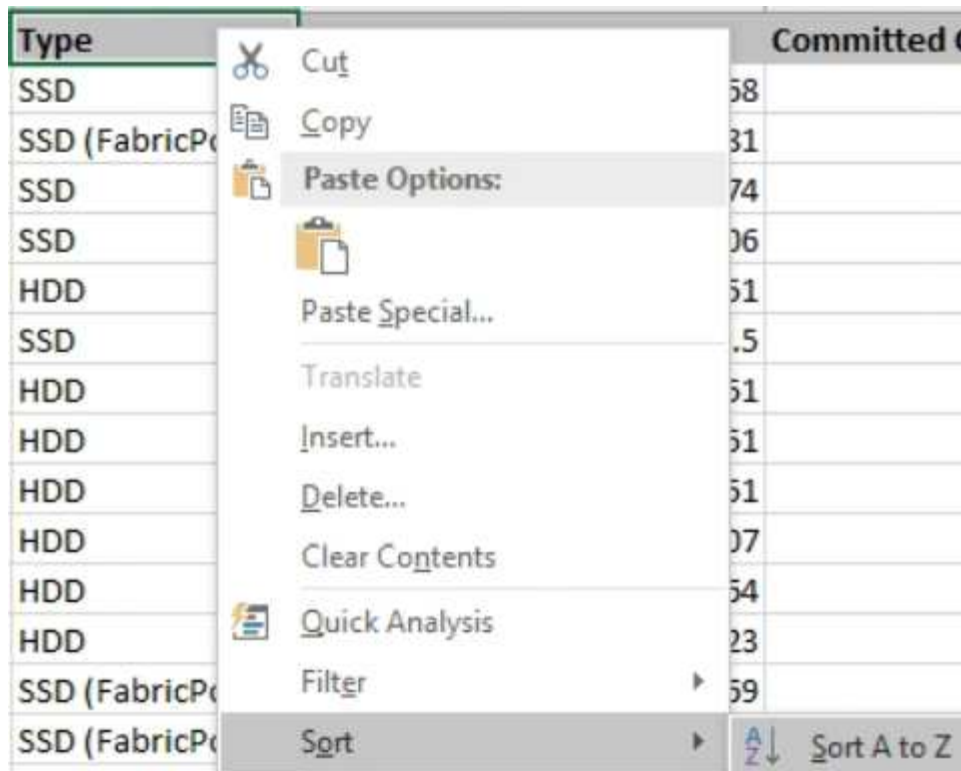
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Sélectionnez **Rapports > Télécharger Excel**.



Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

3. Dans Excel, ouvrez le fichier téléchargé.
4. Si nécessaire, cliquez sur **Activer la modification**.
5. Sur la feuille de données, cliquez avec le bouton droit sur la colonne Type et sélectionnez **Trier > Trier de A à Z**.

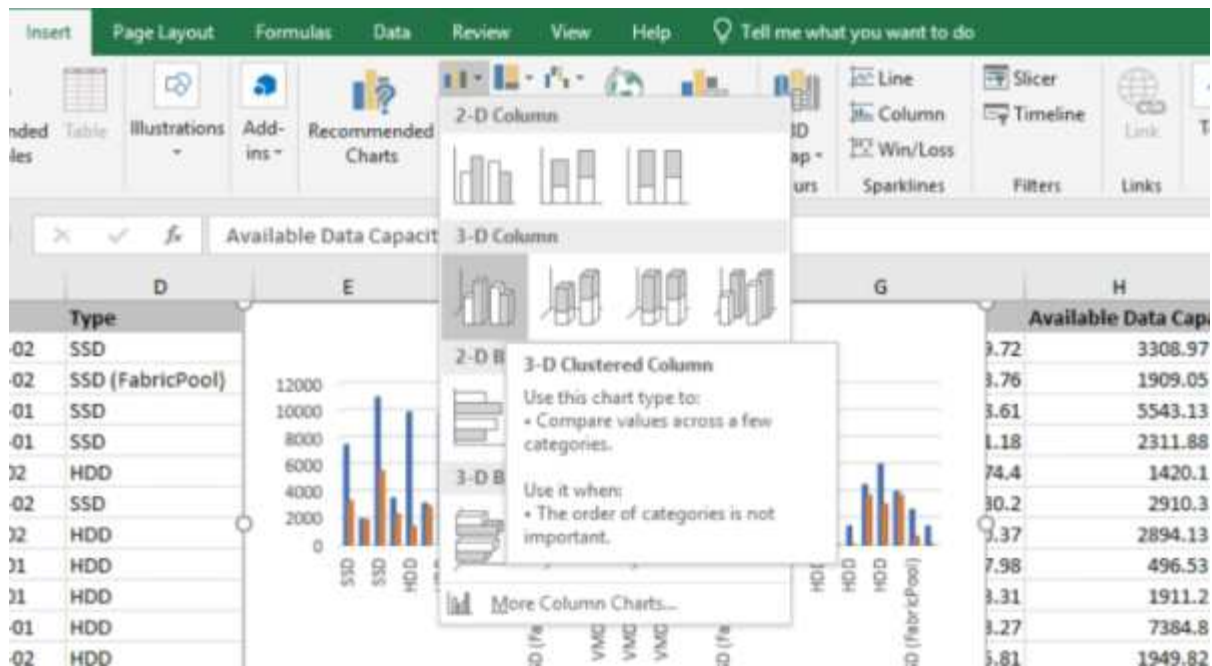


Cela organisera vos données par type de stockage, par exemple :

- Disque dur
- Hybride
- SSD
- SSD (FabricPool)

6. Sélectionnez le **Type**, **Total Data Capacity**, et **Available Data Capacity** colonnes.
7. Dans le menu **Insertion**, sélectionnez un 3-D column graphique.

Le graphique apparaît sur la fiche technique.



8. Cliquez avec le bouton droit sur le graphique et sélectionnez **Déplacer le graphique**.

9. Sélectionnez **Nouvelle feuille** et nommez la feuille **Graphiques de stockage total**.

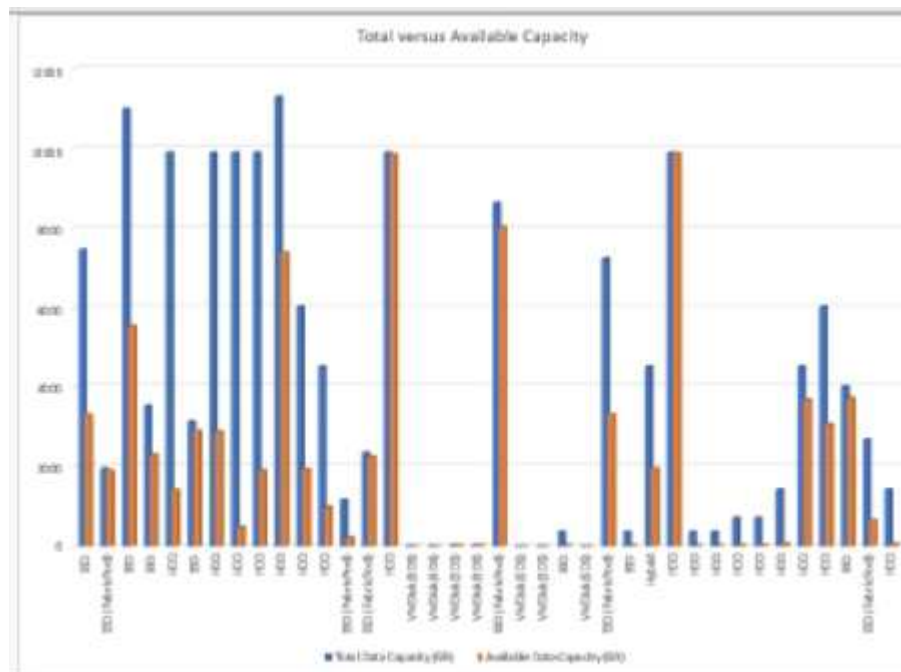


Assurez-vous que la nouvelle feuille apparaît après les feuilles d'informations et de données.

10. Nommez le titre du graphique **Capacité totale par rapport à la capacité disponible**.

11. À l'aide des menus **Conception** et **Format**, disponibles lorsque le graphique est sélectionné, vous pouvez personnaliser l'apparence du graphique.

12. Lorsque vous êtes satisfait, enregistrez le fichier avec vos modifications. Ne modifiez pas le nom du fichier ni son emplacement.



13. Dans Unified Manager, sélectionnez **Rapports > Télécharger Excel**.



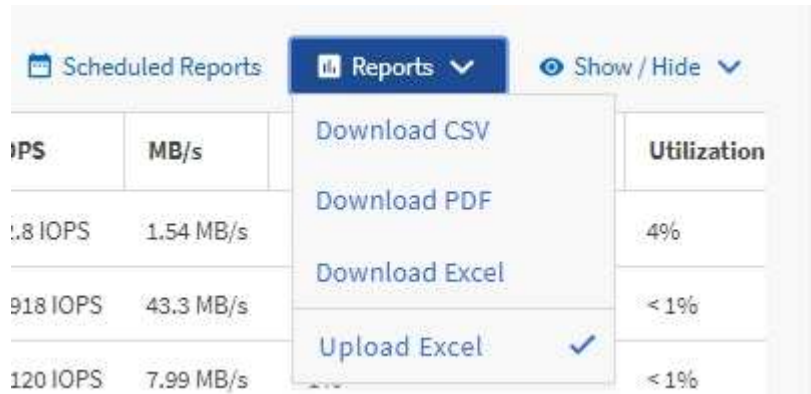
Assurez-vous que vous êtes dans la même vue où vous avez téléchargé le fichier Excel.

14. Sélectionnez le fichier Excel que vous avez modifié.

15. Cliquez sur **Ouvrir**.

16. Cliquez sur **Soumettre**.

Une coche apparaît à côté de l'élément de menu **Rapports > Télécharger Excel**.



17. Cliquez sur **Rapports planifiés**.

18. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.



Sélectionnez le format **XLSX** pour le rapport.

19. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être équilibrer la charge sur vos agrégats.

Créer un rapport pour afficher les graphiques de capacité de volume disponibles

Vous pouvez créer un rapport pour analyser la capacité de volume disponible dans un graphique Excel.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour ouvrir une vue Santé : tous les volumes, télécharger la vue dans Excel, créer un graphique de capacité disponible, télécharger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Volumes**.

2. Sélectionnez **Rapports > Télécharger Excel**.



Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

3. Si nécessaire, cliquez sur **Activer la modification**.
4. Dans Excel, ouvrez le fichier téléchargé.
5. Sur le data feuille, sélectionnez les données que vous souhaitez utiliser dans la Volume et Available Data % colonnes.
6. Dans le menu **Insertion**, sélectionnez un 3-D piechart.

Le graphique montre quels volumes ont le plus grand espace disponible. Le graphique apparaît sur la fiche technique.

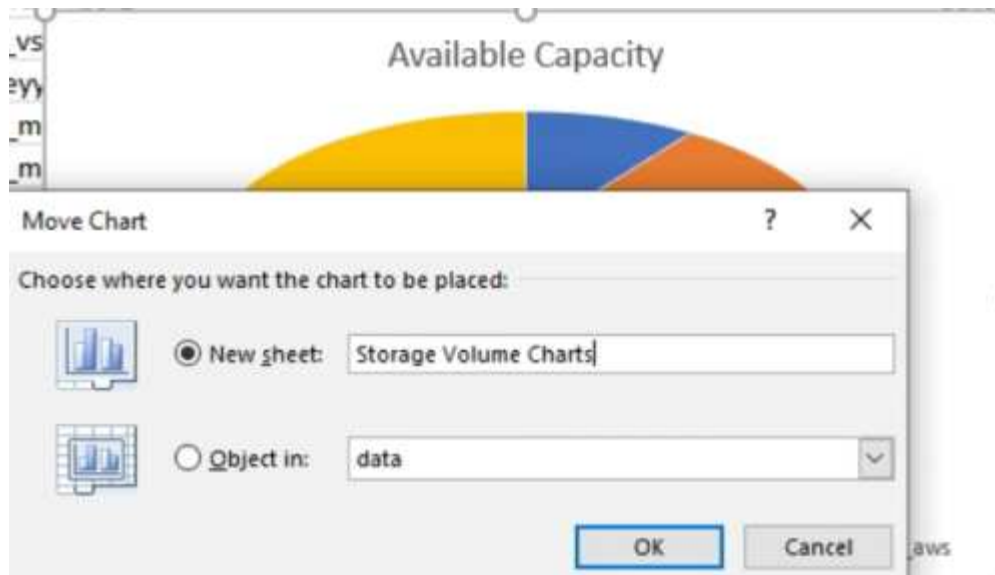


Selon la configuration de votre réseau, la sélection de colonnes entières ou d'un trop grand nombre de lignes de données peut rendre votre graphique à secteurs illisible. Cet exemple utilise le graphique à secteurs 3D, mais vous pouvez utiliser n'importe quel type de graphique. Utilisez le graphique qui affiche le mieux les données que vous souhaitez capturer.

7. Nommez le titre du graphique **Capacité disponible**.
8. Cliquez avec le bouton droit sur le graphique et sélectionnez **Déplacer le graphique**.
9. Sélectionnez **Nouvelle feuille** et nommez la feuille **Graphiques de volume de stockage**.



Assurez-vous que la nouvelle feuille apparaît après les feuilles d'informations et de données.



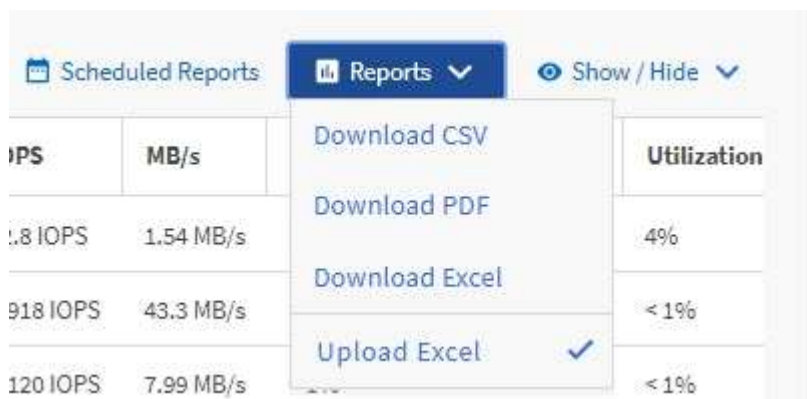
10. À l'aide des menus **Conception** et **Format**, disponibles lorsque le graphique est sélectionné, vous pouvez personnaliser l'apparence du graphique.
11. Lorsque vous êtes satisfait, enregistrez le fichier avec vos modifications.
12. Dans Unified Manager, sélectionnez **Rapports > Télécharger Excel**.



Assurez-vous que vous êtes dans la même vue où vous avez téléchargé le fichier Excel.

13. Sélectionnez le fichier Excel que vous avez modifié.
14. Cliquez sur **Ouvrir**.
15. Cliquez sur **Soumettre**.

Une coche apparaît à côté de l'élément de menu **Rapports > Télécharger Excel**.



16. Cliquez sur **Rapports planifiés**.
17. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications de rapport** afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
18. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.



Sélectionnez le format **XLSX** pour le rapport.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être équilibrer la charge sur vos volumes.

Créer un rapport pour afficher les agrégats qui ont le plus d'IOPS disponibles

Ce rapport indique quels agrégats ont le plus d'IOPS disponibles par type d'agrégat sur lequel vous pouvez provisionner de nouvelles charges de travail.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Suivez les étapes suivantes pour ouvrir une vue Santé : tous les volumes, télécharger la vue dans Excel, créer un graphique de capacité disponible, télécharger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Agrégats**.
2. Sélectionnez **Performance : tous les agrégats** dans la liste déroulante **Affichage**.
3. Sélectionnez **Afficher/Masquer** pour afficher le `Available IOPS` colonne et masquer la `Cluster FQDN`, `Inactive Data Reporting`, et `Threshold Policy` colonnes.
4. Faites glisser et déposez le `Available IOPS` et `Free Capacity` colonnes à côté de la `Type` colonne.
5. Nommez et enregistrez la vue personnalisée `Available IOPS Per Aggr`.
6. Sélectionnez **Rapports > Télécharger Excel**.



Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

7. Si nécessaire, cliquez sur **Activer la modification**.
8. Dans Excel, ouvrez le fichier téléchargé.
9. Sur la feuille de données, cliquez sur le petit triangle en haut à gauche de la feuille pour sélectionner la feuille entière.
10. Sur le ruban **Données**, sélectionnez **Trier** dans le `Sort & Filter` area.
11. Définissez les niveaux de tri suivants :

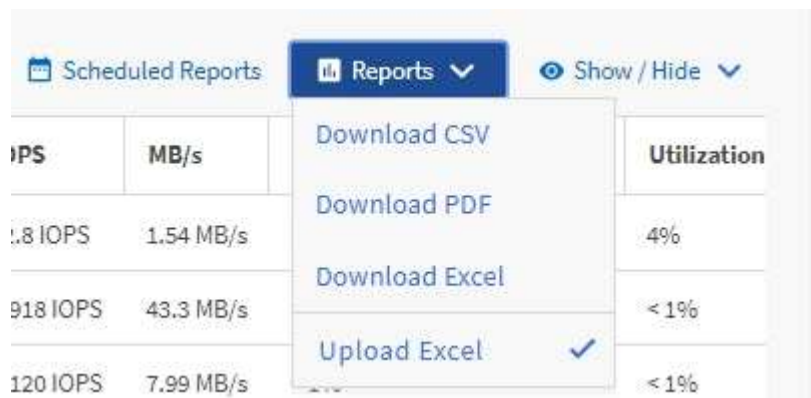
- a. Spécifiez le **Trier par** comme Available IOPS (IOPS), le **Trier sur** comme Cell Values, et l'**Ordre** comme Largest to Smallest.
 - b. Cliquez sur **Ajouter un niveau**.
 - c. Spécifiez le **Trier par** comme Type, le **Trier sur** comme Cell Values, et l'**Ordre** comme Z to A.
 - d. Cliquez sur **Ajouter un niveau**.
 - e. Spécifiez le **Trier par** comme Free Capacity (GB), le **Sort On** comme Cell Values, et l'**Ordre** comme Largest to Smallest.
 - f. Cliquez sur **OK**.
12. Enregistrez et fermez le fichier Excel.
 13. Dans Unified Manager, sélectionnez **Rapports > Télécharger Excel**.



Assurez-vous que vous êtes dans la même vue où vous avez téléchargé le fichier Excel.

14. Sélectionnez le fichier Excel que vous avez modifié, dans ce cas performance-aggregates-
<date>.xlsx.
15. Cliquez sur **Ouvrir**.
16. Cliquez sur **Soumettre**.

Une coche apparaît à côté de l'élément de menu **Rapports > Télécharger Excel**.



17. Cliquez sur **Rapports planifiés**.
18. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications de rapport afin de pouvoir définir les caractéristiques de planification du nouveau rapport.
19. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la rangée.



Sélectionnez le format **XLSX** pour le rapport.

Le rapport est envoyé immédiatement à titre de test. Après cela, le rapport est généré et envoyé par courrier électronique aux destinataires répertoriés en utilisant la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous souhaitez peut-être provisionner de nouvelles charges de travail sur les agrégats disposant des plus grandes IOPS disponibles.

Gérer le stockage à l'aide des API REST

Démarrer avec les API REST Active IQ Unified Manager

Active IQ Unified Manager fournit un ensemble d'API pour gérer vos ressources de stockage sur les systèmes de stockage pris en charge via une interface de service Web RESTful pour toute intégration tierce.

Dans ces rubriques, vous trouverez des informations sur les API Unified Manager, des exemples de workflows pour résoudre des problèmes spécifiques et des exemples de codes. À l'aide de ces informations, vous pouvez créer des clients RESTful de solutions logicielles NetApp Manageability pour la gestion des systèmes NetApp. Les API sont basées sur le style architectural Representational State Transfer (REST). Les quatre opérations REST Créer, Lire, Mettre à jour et Supprimer (également appelées CRUD) sont prises en charge.

Voir ["Active IQ Unified Manager"](#) pour des ressources supplémentaires et des détails sur les avantages de l'API REST Active IQ Unified Manager.

Audience pour ce contenu

Les sujets ici sont destinés aux développeurs créant des applications qui s'interfaçent avec le logiciel Active IQ Unified Manager via des API REST.

Les administrateurs et architectes de stockage peuvent se référer à ces informations pour acquérir une compréhension de base de la manière dont les API REST d'Unified Manager peuvent être utilisées pour créer des applications clientes permettant de gérer et de surveiller les systèmes de stockage NetApp.

Vous devez utiliser ces informations si vous souhaitez utiliser le fournisseur de stockage, le cluster ONTAP et les API d'administration de gestion pour gérer votre stockage.



Vous devez avoir l'un des rôles suivants : opérateur, administrateur de stockage ou administrateur d'application. Vous devez connaître l'adresse IP ou le nom de domaine complet du serveur Unified Manager sur lequel vous souhaitez exécuter les API REST.

Accès et catégories de l'API Active IQ Unified Manager

Les API Active IQ Unified Manager vous permettent de gérer et de provisionner des objets de stockage dans votre environnement. Vous pouvez également accéder à l'interface Web d'Unified Manager pour exécuter certaines de ces fonctions.

Construire une URL pour accéder directement aux API REST

Vous pouvez accéder aux API REST directement via un langage de programmation, tel que Python, C#, C++, JavaScript, etc. Saisissez le nom d'hôte ou l'adresse IP et l'URL pour accéder aux API REST au format

`https://<nom d'hôte>/api`



Le port par défaut est 443. Vous pouvez configurer le port selon les besoins de votre environnement.

Accéder à la page de documentation de l'API en ligne

Vous pouvez accéder à la page de contenu de référence *Documentation API* fournie avec le produit pour afficher la documentation API, ainsi que pour émettre manuellement un appel API (sur l'interface, par exemple, Swagger). Vous pouvez accéder à cette documentation en cliquant sur la **Barre de menu > Bouton Aide > Documentation API**

Vous pouvez également saisir le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page de l'API REST au format

`https://<nom d'hôte>/docs/api/`

Catégories

Les appels d'API sont organisés fonctionnellement en fonction des domaines ou des catégories. Pour localiser une API spécifique, cliquez sur la catégorie d'API applicable.

Les API REST fournies avec Unified Manager vous aident à exécuter des fonctions d'administration, de surveillance et de provisionnement. Les API sont regroupées sous les catégories suivantes.

- **centre de données**

Cette catégorie contient les API qui vous aident dans la gestion et l'analyse du stockage du centre de données à l'aide d'outils tels que Work Flow Automation et Ansible. Les API REST de cette catégorie fournissent des informations sur les clusters, les nœuds, les agrégats, les volumes, les LUN, les partages de fichiers, les espaces de noms et d'autres éléments de votre centre de données.

- **serveur de gestion**

Les API de la catégorie **management-server** contiennent les `jobs`, `system`, et `events` Apis. Les tâches sont des opérations planifiées pour une exécution asynchrone liée à la gestion des objets de stockage ou des charges de travail sur Unified Manager. Le `events` L'API renvoie des événements dans votre centre de données et le `system` L'API renvoie les détails de l'instance Unified Manager.

- **fournisseur de stockage**

Cette catégorie contient toutes les API de provisionnement requises pour la gestion et le provisionnement des partages de fichiers, des LUN, des niveaux de service de performances et des politiques d'efficacité du stockage. Les API vous permettent également de configurer des points de terminaison d'accès, des annuaires Active Directory, ainsi que d'attribuer des niveaux de service de performances et des politiques d'efficacité de stockage sur les charges de travail de stockage.

- **administration**

Cette catégorie contient les API utilisées pour exécuter des tâches administratives, telles que la maintenance des paramètres de sauvegarde, l'affichage des certificats du magasin de confiance pour les sources de données Unified Manager et la gestion des clusters ONTAP en tant que sources de données pour Unified Manager.

- **porte**

Unified Manager vous permet d'appeler les API REST ONTAP via les API sous la catégorie passerelle et de gérer les objets de stockage dans votre centre de données.

- **sécurité**

Cette catégorie contient des API pour la gestion des utilisateurs d'Unified Manager.

Services REST proposés dans Active IQ Unified Manager

Vous devez connaître les services et opérations REST proposés avant de commencer à utiliser les API Active IQ Unified Manager .

Les API de provisionnement et d'administration utilisées pour configurer le serveur API prennent en charge les opérations de lecture (GET) ou d'écriture (POST, PATCH, DELETE). Voici quelques exemples des opérations GET, PATCH, POST et DELETE prises en charge par les API :

- Exemple pour GET : `GET /datacenter/cluster/clusters` récupère les détails du cluster dans votre centre de données. Le nombre maximal d'enregistrements renvoyés par le GET l'opération est 1000.



Les API vous permettent de filtrer, trier et commander les enregistrements par attributs pris en charge.

- Exemple pour POST : `POST /datacenter/svm/svms` crée une machine virtuelle de stockage (SVM) personnalisée.
- Exemple pour PATCH : `PATCH /datacenter/svm/svms/{key}` modifie les propriétés d'un SVM, en utilisant sa clé unique.
- Exemple pour SUPPRIMER : `DELETE /storage-provider/access-endpoints/{key}` supprime un point de terminaison d'accès d'un LUN, d'un SVM ou d'un partage de fichiers à l'aide de sa clé unique.

Les opérations REST qui peuvent être effectuées à l'aide des API dépendent du rôle de l'opérateur, de l'administrateur de stockage ou de l'administrateur d'application.

Rôle de l'utilisateur	Méthode REST prise en charge
Opérateur	Accès en lecture seule aux données. Les utilisateurs disposant de ce rôle peuvent exécuter toutes les requêtes GET.
Administrateur de stockage	Accès en lecture à toutes les données. Les utilisateurs disposant de ce rôle peuvent exécuter toutes les requêtes GET. De plus, ils disposent d'un accès en écriture (pour exécuter des requêtes PATCH, POST et DELETE) afin d'effectuer des activités spécifiques, telles que la gestion des objets de service de stockage et les options de gestion du stockage.
Administrateur d'application	Accès en lecture et en écriture à toutes les données. Les utilisateurs disposant de ce rôle peuvent exécuter des requêtes GET, PATCH, POST et DELETE pour toutes les fonctions.

Pour plus d'informations sur toutes les opérations REST, consultez la *documentation de l'API en ligne*.

Version de l'API dans Active IQ Unified Manager

Les URI de l'API REST dans Active IQ Unified Manager spécifient un numéro de version. Par exemple, `/v2/datacenter/svm/svms`. Le numéro de version `v2` dans `/v2/datacenter/svm/svms` indique la version de l'API utilisée dans une version spécifique. Le numéro de version minimise l'impact des modifications de l'API sur le logiciel client en renvoyant une réponse que le client peut traiter.

La partie numérique de ce numéro de version est incrémentielle par rapport aux versions. Les URI avec un numéro de version fournissent une interface cohérente qui maintient la compatibilité descendante dans les versions futures. Vous trouverez également les mêmes API sans version, par exemple `/datacenter/svm/svms`, qui indiquent les API de base sans version. Les API de base sont toujours la dernière version des API.



Dans le coin supérieur droit de votre interface Swagger, vous pouvez sélectionner la version de l'API à utiliser. La version la plus élevée est sélectionnée par défaut. Il est recommandé d'utiliser la version la plus élevée d'une API particulière (par rapport à l'entier incrémentiel) disponible dans votre instance Unified Manager.

Pour toutes les demandes, vous devez explicitement demander la version d'API que vous souhaitez utiliser. Lorsque le numéro de version est spécifié, le service ne renvoie pas d'éléments de réponse que votre application n'est pas conçue pour gérer. Dans les requêtes REST, vous devez inclure le paramètre de version. Les versions antérieures des API sont finalement obsolètes après quelques versions. Dans cette version, le `v1` la version des API est obsolète.

Ressources de stockage dans ONTAP

Les ressources de stockage dans ONTAP peuvent être globalement classées en *ressources de stockage physiques* et *ressources de stockage logiques*. Pour gérer efficacement vos systèmes ONTAP à l'aide des API fournies dans Active IQ Unified Manager, vous devez comprendre le modèle de ressources de stockage et la relation entre les différentes ressources de stockage.

- **Ressources de stockage physique**

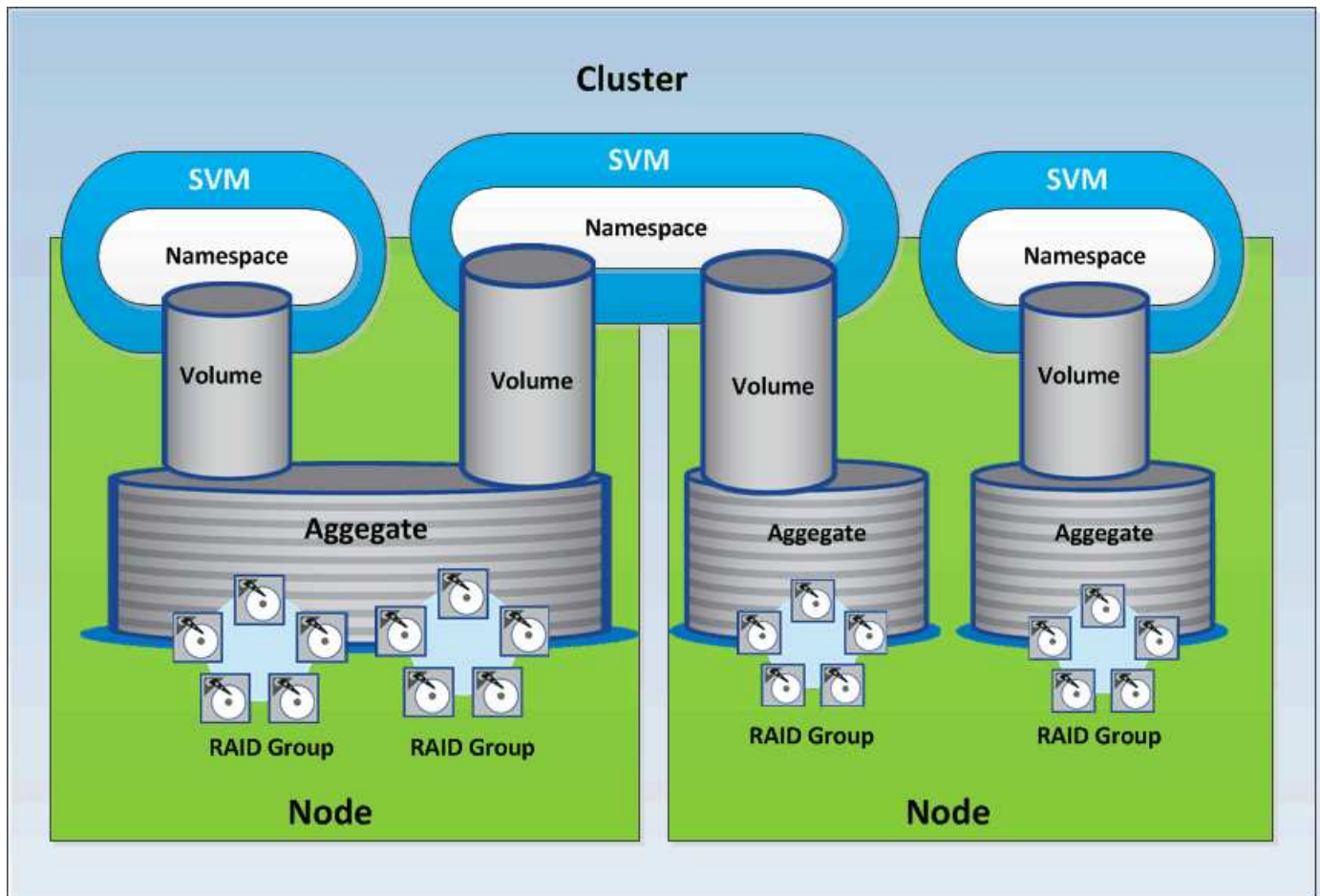
Fait référence aux objets de stockage physique fournis par ONTAP. Les ressources de stockage physique incluent les disques, les clusters, les contrôleurs de stockage, les nœuds et les agrégats.

- **Ressources de stockage logique**

Fait référence aux ressources de stockage fournies par ONTAP qui ne sont pas liées à une ressource physique. Ces ressources sont associées à une machine virtuelle de stockage (SVM, anciennement appelée Vserver) et existent indépendamment de toute ressource de stockage physique spécifique telle qu'un disque, un LUN de baie ou un agrégat.

Les ressources de stockage logique incluent des volumes de tous types et qtrees, ainsi que les capacités et configurations que vous pouvez utiliser avec ces ressources, telles que les copies instantanées, la déduplication, la compression et les quotas.

L'illustration suivante montre les ressources de stockage dans un cluster à 2 nœuds :



Accès et authentification de l'API REST dans Active IQ Unified Manager

L'API REST Active IQ Unified Manager est accessible à l'aide de n'importe quel client REST ou plate-forme de programmation capable d'émettre des requêtes HTTP avec un mécanisme d'authentification HTTP de base.

Un exemple de demande et de réponse :

- **Demande**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Réponse**

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
```

```

00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
  "name": "fas8040-206-21",
  "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
  "contact": null,
  "location": null,
  "version": {
    "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
    "generation": 9,
    "major": 5,
    "minor": 0
  },
  "isSanOptimized": false,
  "management_ip": "10.226.207.25",
  "nodes": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
      "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
      "name": "fas8040-206-21-01",
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
        }
      },
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "model": "FAS8040",
      "uptime": 13924095,
      "serial_number": "701424000157"
    },
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
      "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
      "name": "fas8040-206-21-02",

```

```

    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-00a0985bb9b7"
      }
    },
    "location": null,
    "version": {
      "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33 UTC 2019",
      "generation": 9,
      "major": 5,
      "minor": 0
    },
    "model": "FAS8040",
    "uptime": 14012386,
    "serial_number": "701424000564"
  }
],
"_links": {
  "self": {
    "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb"
  }
}
},

```

- ``IP address/hostname`` est l'adresse IP ou le nom de domaine complet (FQDN) du serveur API.
- Port 443

443 est le port HTTPS par défaut. Vous pouvez personnaliser le port HTTPS, si nécessaire.

Pour émettre des requêtes HTTP à partir d'un navigateur Web, vous devez utiliser les plugins de navigateur REST API. Vous pouvez également accéder à l'API REST en utilisant des plateformes de script telles que cURL et Perl.

Authentification

Unified Manager prend en charge le schéma d'authentification HTTP de base pour les API. Pour un flux d'informations sécurisé (requête et réponse), les API REST sont accessibles uniquement via HTTPS. Le serveur API fournit un certificat SSL auto-signé à tous les clients pour la vérification du serveur. Ce certificat peut être remplacé par un certificat personnalisé (ou certificat CA).

Vous devez configurer l'accès utilisateur au serveur API pour appeler les API REST. Les utilisateurs peuvent être des utilisateurs locaux (profils utilisateur stockés dans la base de données locale) ou des utilisateurs LDAP (si vous avez configuré le serveur API pour s'authentifier via LDAP). Vous pouvez gérer l'accès des

utilisateurs en vous connectant à l'interface utilisateur de la console d'administration d'Unified Manager.

Codes d'état HTTP utilisés dans Active IQ Unified Manager

Lors de l'exécution des API ou du dépannage des problèmes, vous devez connaître les différents codes d'état HTTP et codes d'erreur utilisés par les API Active IQ Unified Manager .

Le tableau suivant répertorie les codes d'erreur liés à l'authentification :

Code d'état HTTP	Titre du code d'état	Description
200	OK	Renvoyé lors de l'exécution réussie des appels API synchrones.
201	Créé	Création de nouvelles ressources par appels synchrones, comme la configuration d'Active Directory.
202	Accepté	Renvoyé lors de l'exécution réussie d'appels asynchrones pour les fonctions de provisionnement, telles que la création de LUN et de partages de fichiers.
400	Demande invalide	Indique un échec de validation d'entrée. L'utilisateur doit corriger les entrées, par exemple, les clés valides dans le corps d'une requête.
401	Demande non autorisée	Vous n'êtes pas autorisé à consulter la ressource/Non autorisé.
403	Demande interdite	L'accès à la ressource que vous tentiez d'atteindre est interdit.
404	Ressource non trouvée	La ressource que vous essayez d'atteindre n'est pas trouvée.
405	Méthode non autorisée	Méthode non autorisée.
429	Trop de demandes	Renvoyé lorsque l'utilisateur envoie trop de requêtes dans un délai spécifique.

Code d'état HTTP	Titre du code d'état	Description
500	Erreur interne du serveur	Erreur interne du serveur. Impossible d'obtenir la réponse du serveur. Cette erreur interne du serveur peut être permanente ou non. Par exemple, si vous exécutez un GET ou GET ALL opération et recevez cette erreur, il est recommandé de répéter cette opération pendant au moins cinq tentatives. S'il s'agit d'une erreur permanente, le code d'état renvoyé reste 500. Si l'opération réussit, le code d'état renvoyé est 200.

Recommandations d'utilisation des API pour Active IQ Unified Manager

Lorsque vous utilisez les API dans Active IQ Unified Manager, vous devez suivre certaines pratiques recommandées.

- Tous les types de contenu de réponse doivent être au format suivant pour une exécution valide :

```
application/json
```

- Le numéro de version de l'API n'est pas lié au numéro de version du produit. Vous devez utiliser la dernière version de l'API disponible pour votre instance Unified Manager. Pour plus d'informations sur les versions d'API Unified Manager, consultez la section « Versionnage de l'API REST dans Active IQ Unified Manager ».
- Lors de la mise à jour des valeurs de tableau à l'aide d'une API Unified Manager, vous devez mettre à jour la chaîne de valeurs entière. Vous ne pouvez pas ajouter de valeurs à un tableau. Vous ne pouvez remplacer qu'un tableau existant.
- Vous pouvez utiliser des opérateurs de filtre, tels que le pipe (|) et le caractère générique (*) pour tous les paramètres de requête, à l'exception des valeurs doubles, par exemple, les IOPS et les performances dans les API de métriques.
- Évitez d'interroger des objets en utilisant une combinaison des opérateurs de filtre caractère générique (*) et barre verticale (|). Il se peut qu'il récupère un nombre incorrect d'objets.
- Lorsque vous utilisez des valeurs pour le filtre, assurez-vous que la valeur ne contient aucun ? personnage. Ceci vise à atténuer les risques d'injection SQL.
- Notez que le GET (toutes) les demandes d'API renvoient un maximum de 1 000 enregistrements. Même si vous exécutez la requête en définissant le max_records paramètre à une valeur supérieure à 1000, seuls 1000 enregistrements sont renvoyés.
- Pour exécuter des fonctions administratives, il est recommandé d'utiliser l'interface utilisateur d'Unified Manager.

Journaux de dépannage

Les journaux système vous permettent d'analyser les causes d'échec et de résoudre les problèmes qui peuvent survenir lors de l'exécution des API.

Récupérez les journaux à partir de l'emplacement suivant pour résoudre les problèmes liés aux appels d'API.

Emplacement du journal	Utiliser
<code>/var/log/ocie/access_log.log</code>	Contient tous les détails de l'appel d'API, tels que le nom d'utilisateur de l'utilisateur qui appelle l'API, l'heure de début, l'heure d'exécution, l'état et l'URL. Vous pouvez utiliser ce fichier journal pour vérifier les API fréquemment utilisées ou dépanner n'importe quel flux de travail d'interface graphique. Vous pouvez également l'utiliser pour mettre à l'échelle l'analyse, en fonction du temps d'exécution.
<code>/var/log/ocum/ocumserver.log</code>	Contient tous les journaux d'exécution de l'API. Vous pouvez utiliser ce fichier journal pour dépanner et déboguer les appels d'API.
<code>/var/log/ocie/server.log</code>	Contient tous les déploiements de serveurs Wildfly et les journaux liés au service de démarrage/arrêt. Vous pouvez utiliser ce fichier journal pour trouver la cause première de tout problème survenant lors du démarrage, de l'arrêt ou du déploiement du serveur Wildfly.
<code>/var/log/ocie/au.log</code>	Contient les journaux liés à l'unité d'acquisition. Vous pouvez utiliser ce fichier journal lorsque vous avez créé, modifié ou supprimé des objets dans ONTAP , mais ils ne sont pas reflétés pour les API REST Active IQ Unified Manager .

Objets de travail processus asynchrones

Active IQ Unified Manager fournit le `jobs` API qui récupère des informations sur les tâches effectuées lors de l'exécution d'autres API. vous devez savoir comment fonctionne le traitement asynchrone à l'aide de l'objet Job.

Certains appels d'API, en particulier ceux utilisés pour ajouter ou modifier des ressources, peuvent prendre plus de temps que d'autres appels. Unified Manager traite ces demandes de longue durée de manière asynchrone.

Requêtes asynchrones décrites à l'aide de l'objet Job

Après un appel d'API exécuté de manière asynchrone, le code de réponse HTTP 202 indique que la requête a été validée et acceptée, mais pas encore terminée. La requête est traitée en tâche d'arrière-plan et continue de s'exécuter après la réponse HTTP initiale au client. La réponse inclut l'objet Job ancrant la requête, ainsi que son identifiant unique.

Interroger l'objet Job associé à une requête API

L'objet Job renvoyé dans la réponse HTTP contient plusieurs propriétés. Vous pouvez interroger la propriété « state » pour déterminer si la requête a abouti. Un objet Job peut être dans l'un des états suivants :

- NORMAL
- WARNING
- PARTIAL_FAILURES
- ERROR

Il existe deux techniques que vous pouvez utiliser lors de l'interrogation d'un objet Job pour détecter un état terminal pour la tâche, soit un succès, soit un échec :

- Demande d'interrogation standard : l'état actuel du travail est renvoyé immédiatement.
- Demande d'interrogation longue : lorsque l'état du travail passe à NORMAL, ERROR, ou PARTIAL_FAILURES.

Étapes d'une requête asynchrone

Vous pouvez utiliser la procédure de haut niveau suivante pour terminer un appel d'API asynchrone :

1. Émettez l'appel API asynchrone.
2. Recevez une réponse HTTP 202 indiquant l'acceptation réussie de la demande.
3. Extraire l'identifiant de l'objet Job du corps de la réponse.
4. Dans une boucle, attendez que l'objet Job atteigne l'état terminal NORMAL, ERROR, ou PARTIAL_FAILURES.
5. Vérifiez l'état terminal du travail et récupérez le résultat du travail.

Bonjour serveur API

Le *serveur API Hello* est un exemple de programme qui montre comment appeler une API REST dans Active IQ Unified Manager à l'aide d'un client REST simple. L'exemple de programme vous fournit des détails de base sur le serveur API au format JSON (le serveur ne prend en charge que application/json format).

L'URI utilisée est : <https://<hostname>/api/datacenter/svm/svms>. Cet exemple de code prend les paramètres d'entrée suivants :

- L'adresse IP ou FQDN du serveur API
- Facultatif : numéro de port (par défaut : 443)
- Nom d'utilisateur

- Mot de passe
- Format de réponse(application/json)

Pour appeler les API REST, vous pouvez également utiliser d'autres scripts tels que Jersey et RESTEasy pour écrire un client Java REST pour Active IQ Unified Manager. Vous devez tenir compte des considérations suivantes concernant l'exemple de code :

- Utilisez une connexion HTTPS à Active IQ Unified Manager pour appeler l'URI REST spécifié
- Ignore le certificat fourni par Active IQ Unified Manager
- Ignore la vérification du nom d'hôte pendant la négociation
- Utilisez `javax.net.ssl.HttpURLConnection` pour une connexion URI
- Utilisez une bibliothèque tierce(`org.apache.commons.codec.binary.Base64`) pour construire la chaîne codée en Base64 utilisée dans l'authentification de base HTTP

Pour compiler et exécuter l'exemple de code, vous devez utiliser le compilateur Java 1.8 ou une version ultérieure.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
        }
    }
}
```

```

        System.exit(1);
    }
    setUserArguments(args);
    String serverBaseUrl = "https://" + server;
    if (null != port) {
        serverBaseUrl = serverBaseUrl + ":" + port;
    }
    server_url = serverBaseUrl + "/api/datacenter/svm/svms";
    try {
        HttpURLConnection connection =
getAllTrustingHttpsURLConnection();
        if (connection == null) {
            System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
            System.exit(1);
        }
        System.out.println("Invoking API: " + server_url);
        connection.setRequestMethod("GET");
        connection.setRequestProperty("Accept", "application/" +
response_format);
        String authString = getAuthorizationString();
        connection.setRequestProperty("Authorization", "Basic " +
authString);
        if (connection.getResponseCode() != 200) {
            System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
+ connection.getResponseMessage());
            System.exit(1);
        }
        BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
        String response;
        System.out.println("Response:");
        while ((response = br.readLine()) != null) {
            System.out.println(response);
        }
        connection.disconnect();
    } catch (Exception e) {
        e.printStackTrace();
    }
}

/* Print the usage of this sample code */ private static void
printUsage() {
    System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
}

```

```

        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
        String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
    * * Create a trust manager which accepts all certificates and * use
this trust
    * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
    * SSL Context and skip * server hostname verification during SSL
handshake. * *
    * Note: Trusting all certificates or skipping hostname verification *
is not
    * required for API Services to work. These are done here to * keep
this sample
    * REST Client code as simple as possible.
    */ private static HttpURLConnection
getAllTrustingHttpsURLConnection() {
    null;
    try {
        /* Creating a trust manager that does not
validate certificate chains */
        TrustManager[]
trustAllCertificatesManager = new
TrustManager[]{new
X509TrustManager(){
    public X509Certificate[] getAcceptedIssuers(){return null;}
    public void checkClientTrusted(X509Certificate[]
certs, String authType){}

```

```

        public void checkServerTrusted(X509Certificate[]
certs, String authType){}                               };           /* Initialize the
SSLContext with the all-trusting trust manager */
        SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));           URL url = new URL(server_url);           conn =
(HttpsURLConnection) url.openConnection();           /* Do not perform an
actual hostname verification during SSL Handshake.           Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {           public
boolean verify(String host, SSLSession session) {
return true;           }           });           } catch (Exception e)
{           e.printStackTrace();           }           return conn;           }

/*
* * This forms the Base64 encoded string using the username and
password *
* provided by the user. This is required for HTTP Basic
Authentication.
*/ private static String getAuthorizationString() {
    String userPassword = user + ":" + password;
    byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
    String authString = new String(authEncodedBytes);
    return authString;
}

}

```

API REST d'Unified Manager

Les API REST pour Active IQ Unified Manager sont répertoriées dans cette section, en fonction de leurs catégories.

Vous pouvez consulter la page de documentation en ligne de votre instance Unified Manager qui inclut les détails de chaque appel d'API REST. Ce document ne reprend pas les détails de la documentation en ligne. Chaque appel d'API répertorié ou décrit dans ce document inclut uniquement les informations dont vous avez besoin pour localiser l'appel sur la page de documentation. Après avoir localisé un appel d'API spécifique, vous pouvez consulter les détails complets de cet appel, y compris les paramètres d'entrée, les formats de sortie, les codes d'état HTTP et le type de traitement de la demande.

Les informations suivantes sont incluses pour chaque appel d'API dans un workflow pour aider à localiser l'appel sur la page de documentation :

- Catégorie

Les appels d'API sont organisés sur la page de documentation en zones ou catégories fonctionnellement liées. Pour localiser un appel d'API spécifique, faites défiler la page jusqu'en bas, puis cliquez sur la catégorie d'API applicable.

- Verbe HTTP (appeler)

Le verbe HTTP identifie l'action effectuée sur une ressource. Chaque appel d'API est exécuté via un seul verbe HTTP.

- Chemin

Le chemin détermine la ressource spécifique que l'action utilise dans le cadre de l'exécution d'un appel. La chaîne de chemin est ajoutée à l'URL principale pour former l'URL complète identifiant la ressource.

Gérer les objets de stockage dans un centre de données à l'aide d'API

Les API REST sous le `datacenter` La catégorie vous permet de gérer les objets de stockage dans votre centre de données, tels que les clusters, les nœuds, les agrégats, les machines virtuelles de stockage, les volumes, les LUN, les partages de fichiers et les espaces de noms. Ces API sont disponibles pour interroger la configuration des objets, tandis que certaines d'entre elles vous permettent d'effectuer les opérations d'ajout, de suppression ou de modification de ces objets.

La plupart de ces API sont des appels GET qui fournissent une agrégation inter-clusters avec prise en charge du filtrage, du tri et de la pagination. Lors de l'exécution de ces API, elles renvoient des données de la base de données. Par conséquent, les objets nouvellement créés doivent être découverts lors du prochain cycle d'acquisition pour apparaître dans la réponse.

Si vous souhaitez interroger les détails d'un objet spécifique, vous devez saisir l'ID unique de cet objet pour afficher ses détails. Par exemple, pour les informations sur les métriques et les analyses des objets de stockage, voir ["Affichage des indicateurs de performance"](#) .

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```



Les commandes CURL, les exemples, les requêtes et les réponses aux API sont disponibles sur votre interface API Swagger. Vous pouvez filtrer et commander les résultats selon des paramètres spécifiques comme indiqué sur Swagger. Ces API vous permettent de filtrer les résultats pour des objets de stockage spécifiques, tels qu'un cluster, un volume ou une machine virtuelle de stockage.

API pour les objets de stockage dans votre centre de données

verbe HTTP	Chemin	Description
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des clusters ONTAP dans le centre de données. L'API renvoie des informations, telles que l'adresse IPv4 ou IPv6 du cluster, des informations sur le nœud, telles que l'intégrité du nœud, la capacité de performance et la paire haute disponibilité (HA), et indique si le cluster est une baie All SAN.
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Renvoie les détails des licences installées sur les clusters de votre centre de données. Vous pouvez filtrer vos résultats en fonction des critères requis. Des informations telles que la clé de licence, la clé de cluster, la date d'expiration et l'étendue de la licence sont renvoyées. Vous pouvez saisir une clé de licence pour récupérer les détails d'une licence spécifique.
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des nœuds du centre de données. Vous pouvez afficher des informations sur le cluster, l'état du nœud, la capacité de performance et la paire haute disponibilité (HA) du nœud.
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des partages CIFS dans le centre de données. Outre les détails du cluster, du SVM et du volume, des informations sur la liste de contrôle d'accès (ACL) sont également renvoyées.

verbe HTTP	Chemin	Description
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des politiques d'exportation pour les services NFS pris en charge. Vous pouvez interroger les stratégies d'exportation d'un cluster ou d'une machine virtuelle de stockage et réutiliser la clé de stratégie d'exportation pour provisionner les partages de fichiers NFS. Pour plus d'informations sur l'attribution et la réutilisation des stratégies d'exportation sur les charges de travail, consultez « Provisionnement des partages de fichiers CIFS et NFS ».
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Vous pouvez utiliser cette méthode pour afficher la collection d'agrégats dans le centre de données ou un agrégat spécifique pour provisionner des charges de travail sur ceux-ci ou les surveiller. Des informations telles que les détails du cluster et du nœud, la capacité de performance utilisée, l'espace disponible et utilisé et l'efficacité du stockage sont renvoyées.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Vous pouvez utiliser cette méthode pour afficher la collection de LUN dans l'ensemble du centre de données. Vous pouvez afficher des informations sur le LUN, telles que les détails du cluster et du SVM, les stratégies QoS et les igroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Vous pouvez utiliser cette méthode pour afficher les détails de toutes les politiques QoS applicables aux objets de stockage dans le centre de données. Des informations telles que les détails du cluster et du SVM, les détails de la politique fixe ou adaptative et le nombre d'objets applicables à cette politique sont renvoyées.

verbe HTTP	Chemin	Description
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Vous pouvez utiliser cette méthode pour afficher les détails de l'arbre Q sur l'ensemble du centre de données pour tous les volumes FlexVol ou FlexGroup . Des informations telles que les détails du cluster et du SVM, le FlexVol volume et la politique d'exportation sont renvoyées.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Vous pouvez utiliser cette méthode pour afficher la collection de volumes dans le centre de données. Des informations sur les volumes, telles que les détails du SVM et du cluster, la qualité de service et les politiques d'exportation, que le volume soit de type lecture-écriture, protection des données ou partage de charge, sont renvoyées. Pour les volumes FlexVol et FlexClone , vous pouvez afficher les informations sur les agrégats respectifs. Pour un volume FlexGroup , la requête renvoie la liste des agrégats constitutifs.

verbe HTTP	Chemin	Description
GET	/datacenter/protocols/san/igroups	Vous pouvez attribuer des groupes d'initiateurs (igroups) autorisés à accéder à des cibles LUN particulières. S'il existe un igroup, vous pouvez l'attribuer. Vous pouvez également créer des igroups et les attribuer aux LUN.
POST		
DELETE		
PATCH		
	/datacenter/protocols/san/igroups/{key}	Vous pouvez utiliser ces méthodes pour interroger, créer, supprimer et modifier respectivement des igroups. Points à noter : • `POST:` Lors de la création d'un igroup, vous pouvez désigner la machine virtuelle de stockage sur laquelle vous souhaitez attribuer l'accès. • `DELETE:` Vous devez fournir la clé igroup comme paramètre d'entrée pour supprimer un igroup particulier. Si vous avez déjà attribué un igroup à un LUN, vous ne pouvez pas supprimer cet igroup. • `PATCH:` Vous devez fournir la clé igroup comme paramètre d'entrée pour modifier un igroup particulier. Vous devez également saisir la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.

verbe HTTP	Chemin	Description
GET	/datacenter/svm/svms	Vous pouvez utiliser ces méthodes pour afficher, créer, supprimer et modifier des machines virtuelles de stockage (VM de stockage). • POST: Vous devez entrer l'objet VM de stockage que vous souhaitez créer comme paramètre d'entrée. Vous pouvez créer une machine virtuelle de stockage personnalisée, puis lui attribuer les propriétés requises. • DELETE: Vous devez fournir la clé de machine virtuelle de stockage pour supprimer une machine virtuelle de stockage particulière. • PATCH: Vous devez fournir la clé de la machine virtuelle de stockage pour modifier une machine virtuelle de stockage particulière. Vous devez également saisir les propriétés que vous souhaitez mettre à jour, ainsi que leurs valeurs.
POST	/datacenter/svm/svms/{key}	
DELETE		
PATCH		



Points à noter :

Si vous avez activé le provisionnement de charge de travail basé sur SLO sur votre environnement, lors de la création de la machine virtuelle de stockage, assurez-vous qu'elle prend en charge tous les protocoles requis pour provisionner les LUN et les partages de fichiers sur ceux-ci, par exemple, CIFS ou SMB, NFS, FCP et iSCSI. Les flux de travail de provisionnement peuvent échouer si la machine virtuelle de stockage ne prend pas en charge les services requis. Il est recommandé que les services pour les types de charges de travail respectifs soient également activés sur la machine virtuelle de stockage.

Si vous avez activé le provisionnement de charges de travail basé sur SLO sur votre environnement, vous ne pouvez pas supprimer la machine virtuelle de stockage sur laquelle les charges de travail de stockage ont été provisionnées. Lorsque vous supprimez une machine virtuelle de stockage sur laquelle un serveur CIFS ou SMB a été configuré, cette API supprime également le serveur CIFS ou SMB, ainsi que la configuration Active Directory locale. Cependant, le nom du serveur CIFS ou SMB continue de figurer dans la configuration Active Directory que vous devez supprimer manuellement du serveur Active Directory.

API pour les éléments réseau de votre centre de données

Les API suivantes de la catégorie centre de données récupèrent des informations sur les ports et les interfaces réseau de votre environnement, en particulier les ports FC, les interfaces FC, les ports Ethernet et les interfaces IP.

verbe HTTP	Chemin	Description
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Récupère des informations sur tous les ports Ethernet de votre environnement de centre de données. Avec une clé de port comme paramètre d'entrée, vous pouvez afficher les informations de ce port spécifique. Des informations telles que les détails du cluster, le domaine de diffusion, les détails du port, tels que l'état, la vitesse et le type, et si le port est activé, sont récupérées.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des interfaces FC dans votre environnement de centre de données. Avec une clé d'interface comme paramètre d'entrée, vous pouvez afficher les informations de cette interface spécifique. Des informations telles que les détails du cluster, les détails du nœud d'origine et les détails du port d'origine sont récupérées.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Récupère des informations sur tous les ports FC utilisés dans les nœuds de votre environnement de centre de données. Avec une clé de port comme paramètre d'entrée, vous pouvez afficher les informations de ce port spécifique. Des informations telles que les détails du cluster, la description du port, le protocole pris en charge et l'état du port sont récupérées.

verbe HTTP	Chemin	Description
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des interfaces IP dans votre environnement de centre de données. Avec une clé d'interface comme paramètre d'entrée, vous pouvez afficher les informations de cette interface spécifique. Des informations telles que les détails du cluster, les détails de l'espace IP, les détails du nœud domestique et si le basculement est activé sont récupérées.

Accéder aux API ONTAP via un accès proxy

Les API de passerelle vous offrent l'avantage d'utiliser les informations d'identification Active IQ Unified Manager pour exécuter les API REST ONTAP et gérer les objets de stockage. Ces API sont disponibles lorsque la fonctionnalité API Gateway est activée à partir de l'interface utilisateur Web d'Unified Manager.

Les API REST d'Unified Manager prennent en charge uniquement un ensemble sélectionné d'actions à effectuer sur les sources de données d'Unified Manager, c'est-à-dire les clusters ONTAP . Vous pouvez bénéficier des autres fonctionnalités via les API ONTAP . Les API de passerelle permettent à Unified Manager d'être une interface de transfert pour le tunneling de toutes les requêtes API à exécuter sur les clusters ONTAP qu'il gère, sans se connecter individuellement à chaque cluster de centre de données. Il fonctionne comme un point de gestion unique pour l'exécution des API sur les clusters ONTAP gérés par votre instance Unified Manager. La fonctionnalité API Gateway permet à Unified Manager d'être un plan de contrôle unique à partir duquel vous pouvez gérer plusieurs clusters ONTAP , sans vous connecter à eux individuellement. Les API de passerelle vous permettent de rester connecté à Unified Manager et de gérer les clusters ONTAP en exécutant des opérations d'API REST ONTAP .



Tous les utilisateurs peuvent exécuter une requête en utilisant l'opération GET. Les administrateurs d'applications peuvent exécuter toutes les opérations ONTAP REST.

La passerelle agit comme un proxy pour tunneliser les requêtes API en conservant l'en-tête et le corps des requêtes dans le même format que dans les API ONTAP . Vous pouvez utiliser vos informations d'identification Unified Manager et exécuter les opérations spécifiques pour accéder et gérer les clusters ONTAP sans transmettre les informations d'identification de cluster individuelles. Il continue de gérer l'authentification du cluster et la gestion du cluster, mais redirige les requêtes API pour qu'elles s'exécutent directement sur le cluster spécifique. La réponse renvoyée par les API est la même que la réponse renvoyée par les API REST ONTAP respectives exécutées directement depuis ONTAP.

verbe HTTP	Chemin (URL)	Description
GET	/gateways	Cette méthode GET récupère la liste de tous les clusters gérés par Unified Manager qui prennent en charge les appels ONTAP REST. Vous pouvez vérifier les détails du cluster et choisir d'exécuter d'autres méthodes en fonction de l'UUID du cluster ou de l'identifiant unique universel (UUID).  Les API de passerelle récupèrent uniquement les clusters pris en charge par ONTAP 9.5 ou version ultérieure et ajoutés à Unified Manager via HTTPS.

verbe HTTP	Chemin (URL)		Description
GET	/gateways/{uuid}/{path}		Il s'agit d'une API proxy à point unique, prenant en charge les opérations POST, DELETE, PATCH et GET pour toutes les API REST ONTAP . Aucune restriction ne s'applique à aucune API tant qu'elle est prise en charge par ONTAP. La fonctionnalité de tunneling ou de proxy ne peut pas être désactivée. Le OPTIONS la méthode renvoie toutes les opérations prises en charge par une API REST ONTAP . Par exemple, si une API ONTAP prend en charge uniquement le GET opération, exécution du OPTIONS la méthode utilisant cette API de passerelle renvoie GET comme réponse. Cette méthode n'est pas prise en charge sur Swagger, mais peut être exécutée sur d'autres outils API. Le OPTIONS la méthode détermine si une ressource est disponible. Cette opération peut être utilisée pour afficher les métadonnées sur une ressource dans les en-têtes de réponse HTTP. Cette méthode n'est pas prise en charge sur Swagger, mais peut être exécutée sur d'autres outils API.
POST	 La valeur de {uuid} doit être remplacée par l'UUID du cluster sur lequel l'opération REST doit être effectuée. Assurez-vous également que l'UUID provient du cluster pris en charge par ONTAP 9.5 ou version ultérieure et ajouté à Unified Manager via HTTPS. {path} doit être remplacé par l'URL REST ONTAP . Vous devez supprimer /api/ à partir de l'URL.		
DELETE			
PATCH			
OPTIONS(non disponible sur Swagger)			
HEAD(non disponible sur Swagger)			

Comprendre le tunneling de la passerelle API

Les API de passerelle vous permettent de gérer les objets ONTAP via Unified Manager. Unified Manager gère les clusters et les détails d'authentification et redirige les demandes vers le point de terminaison ONTAP REST. L'API de passerelle transforme l'URL et les liens Hypermedia as the Engine of Application State (HATEOAS) dans l'en-tête et le corps de la réponse avec l'URL de base de la passerelle API. L'API de passerelle agit comme l'URL de base du proxy à laquelle vous ajoutez l'URL ONTAP REST et exécutez le point de terminaison ONTAP REST requis.



Pour qu'une API ONTAP s'exécute correctement via la passerelle API, l'API doit être prise en charge par la version du cluster ONTAP sur lequel elle est exécutée. L'exécution d'une API qui n'est pas prise en charge sur le cluster ONTAP ne renvoie aucun résultat.

Dans cet exemple, l'API de passerelle (URL de base du proxy) est : /gateways/{uuid}/

L'API ONTAP utilisée est : /storage/volumes . Vous devez ajouter l'URL REST de l'API ONTAP comme valeur pour le paramètre de chemin.



Lors de l'ajout du chemin, assurez-vous d'avoir supprimé le "/" symbol at the beginning of the URL. For the API `/storage/volumes`, ajouter `storage/volumes`.

L'URL ajoutée est : `/gateways/{uuid}/storage/volumes`

En exécutant le GET opération, l'URL générée est la suivante :

`GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes`

Le `/api` la balise de l'URL REST ONTAP est supprimée dans l'URL ajoutée et celle de l'API de passerelle est conservée.

Exemple de commande cURL

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

L'API renvoie la liste des volumes de stockage dans ce cluster. Le format de réponse est le même que celui que vous recevez lorsque vous exécutez la même API depuis ONTAP. Les codes d'état renvoyés sont les codes d'état ONTAP REST.

Définir la portée de l'API

Toutes les API ont un contexte défini dans le cadre du cluster. Les API qui fonctionnent sur la base de machines virtuelles de stockage ont également le cluster comme portée, c'est-à-dire que les opérations API sont effectuées sur une machine virtuelle de stockage particulière au sein d'un cluster géré. Lorsque vous exécutez le `/gateways/{uuid}/{path}` API, assurez-vous de saisir l'UUID du cluster (UUID de la source de données Unified Manager) pour le cluster sur lequel vous exécutez l'opération. Pour définir le contexte d'une machine virtuelle de stockage particulière au sein de ce cluster, entrez la clé de la machine virtuelle de stockage comme paramètre `X-Dot-SVM-UUID` ou le nom de la machine virtuelle de stockage comme paramètre `X-Dot-SVM-Name`. Le paramètre est ajouté en tant que filtre dans l'en-tête de chaîne et l'opération est exécutée dans le cadre de cette machine virtuelle de stockage à l'intérieur de ce cluster.

Exemple de commande cURL

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f" -H "Authorization: Basic <Base64EncodedCredentials>"
```

Pour plus d'informations sur l'utilisation des API REST ONTAP , consultez<https://docs.netapp.com/us-en/ontap-automation/index.html>["Automatisation de l'API REST ONTAP"]

Effectuer des tâches administratives à l'aide d'API

Vous pouvez utiliser les API sous le `administration` catégorie permettant de modifier les paramètres de sauvegarde, de vérifier les informations du fichier de sauvegarde et les certificats de cluster, et également de gérer les clusters ONTAP en tant que sources de



Vous devez disposer du rôle d'administrateur d'application pour exécuter ces opérations. Vous pouvez également utiliser l'interface Web d'Unified Manager pour configurer ces paramètres.

verbe HTTP	Chemin	Description
GET PATCH	/admin/backup-settings /admin/backup-settings	Vous pouvez utiliser le <code>GET</code> méthode pour afficher les paramètres de la planification de sauvegarde configurés dans Unified Manager par défaut. Vous pouvez vérifier les éléments suivants : • Que la planification soit activée ou désactivée • Fréquence de la sauvegarde planifiée (quotidienne ou hebdomadaire) • Heure de la sauvegarde • Nombre maximal de fichiers de sauvegarde devant être conservés dans l'application L'heure de la sauvegarde est dans le fuseau horaire du serveur. Les paramètres de sauvegarde de la base de données sont disponibles sur Unified Manager par défaut et vous ne pouvez pas créer de planification de sauvegarde. Cependant, vous pouvez utiliser le <code>PATCH</code> méthode pour modifier les paramètres par défaut.
GET	/admin/backup-file-info	Un fichier de vidage de sauvegarde est généré chaque fois que la planification de sauvegarde est modifiée pour Unified Manager. Vous pouvez utiliser cette méthode pour vérifier si le fichier de sauvegarde est généré conformément aux paramètres de sauvegarde modifiés et si les informations du fichier correspondent aux paramètres modifiés.

verbe HTTP	Chemin	Description
GET	/admin/datasource-certificate	Vous pouvez utiliser cette méthode pour afficher le certificat de source de données (cluster) à partir du magasin de confiance. La validation du certificat est requise avant d'ajouter un cluster ONTAP en tant que source de données Unified Manager.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Vous pouvez utiliser le GET méthode pour récupérer les détails des sources de données (clusters ONTAP) gérées par Unified Manager. Vous pouvez également ajouter un nouveau cluster à Unified Manager en tant que source de données. Pour ajouter un cluster, vous devez connaître son nom d'hôte, son nom d'utilisateur et son mot de passe. Pour modifier et supprimer un cluster géré comme source de données par Unified Manager, utilisez la clé de cluster ONTAP .

Gérer les utilisateurs à l'aide des API

Vous pouvez utiliser les API dans le `security` catégorie pour contrôler l'accès des utilisateurs aux objets de cluster sélectionnés dans Active IQ Unified Manager. Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données. Vous pouvez également ajouter des utilisateurs ou des groupes distants appartenant à un serveur d'authentification. En fonction des privilèges des rôles que vous attribuez aux utilisateurs, ils peuvent gérer les objets de stockage ou afficher les données dans Unified Manager.



Vous devez disposer du rôle d'administrateur d'application pour exécuter ces opérations. Vous pouvez également utiliser l'interface Web d'Unified Manager pour configurer ces paramètres.

Les API sous le `security` la catégorie utilise le paramètre `utilisateurs`, c'est-à-dire le nom d'utilisateur, et non le paramètre `clé` comme identifiant unique pour l'entité utilisateur.

verbe HTTP	Chemin	Description
GET POST	 /security/users	Vous pouvez utiliser ces méthodes pour obtenir les détails des utilisateurs ou ajouter un nouvel utilisateur à Unified Manager. Vous pouvez ajouter des rôles spécifiques aux utilisateurs en fonction de leurs types d'utilisateurs. Lors de l'ajout d'utilisateurs, vous devez fournir des mots de passe pour l'utilisateur local, l'utilisateur de maintenance et l'utilisateur de la base de données.
GET PATCH DELETE	/security/users/{name}	La méthode GET vous permet de récupérer tous les détails d'un utilisateur, tels que le nom, l'adresse e-mail, le rôle, le type d'autorisation. La méthode PATCH vous permet de mettre à jour les détails. La méthode DELETE vous permet de supprimer l'utilisateur.

Afficher les indicateurs de performance à l'aide des API

Active IQ Unified Manager vous fournit un ensemble d'API sous le `/datacenter` catégorie qui vous permet d'afficher les données de performances de vos clusters et objets de stockage dans un centre de données. Ces API récupèrent les données de performances des différents objets de stockage tels que les clusters, les nœuds, les LUN, les volumes, les agrégats, les machines virtuelles de stockage, les interfaces FC, les ports FC, les ports Ethernet et les interfaces IP.

Le `/metrics` et `/analytics` Les API offrent différentes vues des mesures de performances, grâce auxquelles vous pouvez accéder à différents niveaux de détails pour les objets de stockage suivants dans votre centre de données :

- groupes
- nœuds
- machines virtuelles de stockage
- agrégats
- volumes
- LUN
- Interfaces FC
- Ports FC

- Ports Ethernet
- Interfaces IP

Le tableau suivant établit une comparaison entre les `/metrics` et `/analytics` API concernant les détails des données de performances récupérées.

Métrique	Analytique
Détails des performances pour un seul objet. Par exemple, le <code>/datacenter/cluster/clusters/{key}/metrics</code> L'API nécessite que la clé du cluster soit saisie comme paramètre de chemin pour récupérer les métriques de ce cluster spécifique.	Détails des performances de plusieurs objets du même type dans un centre de données. Par exemple, le <code>/datacenter/cluster/clusters/analytics</code> L'API récupère les métriques collectives de tous les clusters d'un centre de données.
Exemple de mesures de performances pour un objet de stockage basé sur le paramètre d'intervalle de temps pour la récupération.	La valeur agrégée de haut niveau des performances pour un certain type d'objet de stockage pendant une certaine période (supérieure à 72 heures).
Les détails de base de l'objet sont récupérés, tels que les détails d'un nœud ou d'un cluster.	Aucun détail spécifique n'est récupéré.
Les compteurs accumulés, tels que les valeurs de performances minimales, maximales, du 95e centile et moyennes sur une période donnée, sont récupérés pour un seul objet, tel que les compteurs de lecture, d'écriture, de total et autres.	Une seule valeur agrégée est affichée pour tous les objets du même type.

Métrique	Analytique
La plage horaire et les données d'échantillon sont basées sur le calendrier suivant : La plage horaire pour les données. Les exemples peuvent être 1h, 12h, 1j, 2j, 3j, 15j, 1s, 1m, 2m, 3m, 6m. Vous obtenez des échantillons d'une heure si la plage est supérieure à 3 jours (72 heures), sinon ce sont des échantillons de 5 minutes. La période pour chaque plage horaire est la suivante : • 1h : Mesures sur l'heure la plus récente échantillonnées sur 5 minutes. • 12h : Mesures sur les 12 heures les plus récentes échantillonnées sur 5 minutes. • 1d : Mesures sur la journée la plus récente échantillonnées sur 5 minutes. • 2d : Mesures sur les 2 derniers jours échantillonnés sur 5 minutes. • 3d : Mesures sur les 3 derniers jours échantillonnées sur 5 minutes. • 15j : métriques sur les 15 derniers jours échantillonnés sur 1 heure. • 1 semaine : métriques sur la semaine la plus récente échantillonnées sur 1 heure. • 1m : métriques sur le mois le plus récent échantillonnées sur 1 heure. • 2m : métriques sur les 2 derniers mois échantillonnés sur 1 heure. • 3m : métriques sur les 3 derniers mois échantillonnées sur 1 heure. • 6 m : métriques sur les 6 derniers mois échantillonnées sur 1 heure. Valeurs disponibles : 1h, 12h, 1j, 2j, 3j, 15j, 1s, 1m, 2m, 3m, 6m Valeur par défaut : 1h	Plus de 72 heures. La durée sur laquelle cet échantillon est calculé est représentée dans le format standard ISO-8601.

Exemple de sortie pour les API de métriques

Par exemple, le `/datacenter/cluster/nodes/{key}/metrics` L'API récupère les détails suivants (entre autres) pour un nœud :



Le 95e percentile dans la valeur récapitulative indique que 95 % des échantillons collectés pour la période ont une valeur de compteur inférieure à la valeur spécifiée comme 95e percentile.


```

{
  "iops": {
    "local": {
      "other": 100.53,
      "read": 100.53,
      "total": 100.53,
      "write": 100.53
    },
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  },
  "latency": {
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  },
  "performance_capacity": {
    "available_iops_percent": 0,
    "free_percent": 0,
    "system_workload_percent": 0,
    "used_percent": 0,
    "user_workload_percent": 0
  },
  "throughput": {
    "other": 100.53,
    "read": 100.53,
    "total": 100.53,
    "write": 100.53
  },
  "timestamp": "2018-01-01T12:00:00-04:00",
  "utilization_percent": 0
}
],
"start_time": "2018-01-01T12:00:00-04:00",
"summary": {
  "iops": {
    "local_iops": {
      "other": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      }
    }
  },

```

```
"read": {
  "95th_percentile": 28,
  "avg": 28,
  "max": 28,
  "min": 5
},
"total": {
  "95th_percentile": 28,
  "avg": 28,
  "max": 28,
  "min": 5
},
"write": {
  "95th_percentile": 28,
  "avg": 28,
  "max": 28,
  "min": 5
}
},
```

Exemple de sortie pour les API d'analyse

Par exemple, le `/datacenter/cluster/nodes/analytics` L'API récupère les valeurs suivantes (entre autres) pour tous les nœuds :

```

{
  "iops": 1.7471,
  "latency": 60.0933,
  "throughput": 5548.4678,
  "utilization_percent": 4.8569,
  "period": 72,
  "performance_capacity": {
    "used_percent": 5.475,
    "available_iops_percent": 168350
  },
  "node": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
    "name": "ocum-infinity-01",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
      }
    }
  },
  "cluster": {
    "key": "37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
    "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
    "name": "ocum-infinity",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/datacenter/cluster/nodes/analytics"
    }
  }
},

```

Liste des API disponibles

Le tableau suivant décrit les `/metrics` et `/analytics` Les API en détail.



Les IOPS et les mesures de performances renvoyées par ces API sont des valeurs doubles, par exemple 100.53 . Le filtrage de ces valeurs flottantes par les caractères pipe (|) et générique (*) n'est pas pris en charge.

Verbe HTTP	Chemin	Description
GET	/datacenter/cluster/clusters/{key}/metrics	Récupère les données de performances (échantillon et résumé) pour un cluster spécifié par le paramètre d'entrée de la clé de cluster. Des informations telles que la clé du cluster et l'UUID, la plage horaire, les IOPS, le débit et le nombre d'échantillons sont renvoyées.
GET	/datacenter/cluster/clusters/analytics	Récupère les mesures de performances de haut niveau pour tous les clusters d'un centre de données. Vous pouvez filtrer vos résultats en fonction des critères requis. Des valeurs telles que les IOPS agrégées, le débit et la période de collecte (en heures) sont renvoyées.
GET	/datacenter/cluster/nodes/{key}/metrics	Récupère les données de performances (échantillon et résumé) pour un nœud spécifié par le paramètre d'entrée de la clé de nœud. Des informations telles que l'UUID du nœud, la plage horaire, le résumé des IOPS, le débit, la latence et les performances, le nombre d'échantillons collectés et le pourcentage utilisé sont renvoyés.
GET	/datacenter/cluster/nodes/analytics	Récupère les mesures de performances de haut niveau pour tous les nœuds d'un centre de données. Vous pouvez filtrer vos résultats en fonction des critères requis. Des informations, telles que les clés de nœud et de cluster, ainsi que des valeurs, telles que les IOPS agrégées, le débit et la période de collecte (en heures) sont renvoyées.

Verbe HTTP	Chemin	Description
GET	/datacenter/storage/aggregates/{key}/metrics	Récupère les données de performances (échantillon et résumé) pour un agrégat spécifié par le paramètre d'entrée de la clé d'agrégat. Des informations telles que la plage horaire, le résumé des IOPS, la latence, le débit et la capacité de performance, le nombre d'échantillons collectés pour chaque compteur et le pourcentage utilisé sont renvoyés.
GET	/datacenter/storage/aggregates/analytics	Récupère des mesures de performances de haut niveau pour tous les agrégats d'un centre de données. Vous pouvez filtrer vos résultats en fonction des critères requis. Des informations, telles que les clés agrégées et de cluster, ainsi que des valeurs, telles que les IOPS agrégées, le débit et la période de collecte (en heures) sont renvoyées.
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	Récupère les données de performances (échantillon et résumé) pour un LUN ou un partage de fichiers (volume) spécifié par le paramètre d'entrée de la clé LUN ou de volume. Des informations telles que le résumé du minimum, du maximum et de la moyenne des IOPS de lecture, d'écriture et totales, la latence et le débit, ainsi que le nombre d'échantillons collectés pour chaque compteur sont renvoyés.
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	Récupère les mesures de performances de haut niveau pour tous les LUN ou volumes d'un centre de données. Vous pouvez filtrer vos résultats en fonction des critères requis. Des informations, telles que les clés de cluster et de machine virtuelle de stockage, ainsi que des valeurs, telles que les IOPS agrégées, le débit et la période de collecte (en heures) sont renvoyées.

Verbe HTTP	Chemin	Description
GET	/datacenter/svm/svms/{key}/metrics	Récupère les données de performances (échantillon et résumé) pour une machine virtuelle de stockage spécifiée par le paramètre d'entrée de la clé de machine virtuelle de stockage. Résumé des IOPS en fonction de chaque protocole pris en charge, tel que <code>nvmf</code> , <code>fcp</code> , <code>iscsi</code> , et <code>nfs</code> , le débit, la latence et le nombre d'échantillons collectés sont renvoyés.
GET	/datacenter/svm/svms/analytics	Récupère les mesures de performances de haut niveau pour toutes les machines virtuelles de stockage d'un centre de données. Vous pouvez filtrer vos résultats en fonction des critères requis. Des informations telles que l'UUID de la machine virtuelle de stockage, les IOPS agrégées, la latence, le débit et la période de collecte (en heures) sont renvoyées.
GET	/datacenter/network/ethernet/ports/{key}/metrics	Récupère les mesures de performances pour un port Ethernet spécifique spécifié par le paramètre d'entrée de la clé de port. Lorsqu'un intervalle (plage de temps) est fourni à partir de la plage prise en charge, l'API renvoie les compteurs accumulés, tels que les valeurs de performances minimales, maximales et moyennes sur la période.

Verbe HTTP	Chemin	Description
GET	/datacenter/network/ethernet/ports/analytics	Récupère les mesures de performances de haut niveau pour tous les ports Ethernet de votre environnement de centre de données. Des informations telles que la clé du cluster et du nœud et l'UUID, le débit, la période de collecte et le pourcentage d'utilisation des ports sont renvoyées. Vous pouvez filtrer le résultat en fonction des paramètres disponibles, tels que la clé de port, le pourcentage d'utilisation, le nom du cluster et du nœud et l'UUID, etc.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Récupère les mesures de performances pour une interface FC réseau spécifique spécifiée par le paramètre d'entrée de la clé d'interface. Lorsqu'un intervalle (plage de temps) est fourni à partir de la plage prise en charge, l'API renvoie les compteurs accumulés, tels que les valeurs de performances minimales, maximales et moyennes sur la période.
GET	/datacenter/network/fc/interfaces/analytics	Récupère les mesures de performances de haut niveau pour tous les ports Ethernet de votre environnement de centre de données. Des informations telles que la clé et l'UUID de l'interface cluster et FC, le débit, les IOPS, la latence et la machine virtuelle de stockage sont renvoyées. Vous pouvez filtrer le résultat en fonction des paramètres disponibles, tels que le nom et l'UUID du cluster et de l'interface FC, la machine virtuelle de stockage, le débit, etc.

Verbe HTTP	Chemin	Description
GET	/datacenter/network/fc/ports/{key}/metrics	Récupère les mesures de performances pour un port FC spécifique spécifié par le paramètre d'entrée de la clé de port. Lorsqu'un intervalle (plage de temps) est fourni à partir de la plage prise en charge, l'API renvoie les compteurs accumulés, tels que les valeurs de performances minimales, maximales et moyennes sur la période.
GET	/datacenter/network/fc/ports/analytics	Récupère les mesures de performances de haut niveau pour tous les ports FC de votre environnement de centre de données. Des informations telles que la clé du cluster et du nœud et l'UUID, le débit, la période de collecte et le pourcentage d'utilisation des ports sont renvoyées. Vous pouvez filtrer le résultat en fonction des paramètres disponibles, tels que la clé de port, le pourcentage d'utilisation, le nom du cluster et du nœud et l'UUID, etc.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Récupère les mesures de performances d'une interface IP réseau telles que spécifiées par le paramètre d'entrée de la clé d'interface. Lorsqu'un intervalle (plage de temps) est fourni à partir de la plage prise en charge, l'API renvoie des informations, telles que le nombre d'échantillons, les compteurs accumulés, le débit et le nombre de paquets reçus et transmis.

Verbe HTTP	Chemin	Description
GET	/datacenter/network/ip/interfaces/analytics	Récupère les mesures de performances de haut niveau pour toutes les interfaces IP réseau de votre environnement de centre de données. Des informations telles que la clé et l'UUID du cluster et de l'interface IP, le débit, les IOPS et la latence sont renvoyées. Vous pouvez filtrer le résultat en fonction des paramètres disponibles, tels que le nom du cluster et de l'interface IP, l'UUID, les IOPS, la latence, le débit, etc.

Afficher les tâches et les détails du système

Vous pouvez utiliser le `jobs` API sous le `management-server` catégorie pour afficher les détails d'exécution des opérations asynchrones. Le `system` API sous le `management-server` La catégorie vous permet d'afficher les détails de l'instance dans votre environnement Active IQ Unified Manager .

Voir les offres d'emploi

Dans Active IQ Unified Manager, les opérations telles que l'ajout et la modification de ressources sont effectuées par des appels d'API synchrones et asynchrones. Les appels planifiés pour une exécution asynchrone peuvent être suivis par un objet Job créé pour cet appel. Chaque objet Job possède une clé unique pour l'identification. Chaque objet Job renvoie l'URI de l'objet Job pour vous permettre d'accéder et de suivre la progression du travail. Vous pouvez utiliser cette API pour récupérer les détails de chaque exécution.

En utilisant cette API, vous pouvez interroger tous les objets Job de votre centre de données, y compris les données historiques. L'interrogation de tous les travaux, par défaut, renvoie les détails des 20 derniers travaux déclenchés via l'interface utilisateur Web et l'interface API. Utilisez les filtres intégrés pour afficher des tâches spécifiques. Vous pouvez également utiliser la touche Job pour interroger les détails d'un travail spécifique et exécuter l'ensemble d'opérations suivant sur les ressources.

Catégorie	verbe HTTP	Chemin	Description
serveur de gestion	OBTENIR	/management-server/jobs	Renvoie les détails du travail de tous les travaux. Sans aucun ordre de tri, le dernier objet Job soumis est renvoyé en haut.

Catégorie	verbe HTTP	Chemin	Description
serveur de gestion	OBTENIR	/management-server/jobs/{key} Saisissez la clé de travail de l'objet Travail pour afficher les détails spécifiques de ce travail.	Renvoie les détails de l'objet Job spécifique.

Afficher les détails du système

En utilisant le `/management-server/system` API, vous pouvez interroger les détails spécifiques à l'instance de votre environnement Unified Manager. L'API renvoie des informations sur le produit et les services, telles que la version d'Unified Manager installée sur votre système, l'UUID, le nom du fournisseur, le système d'exploitation hôte, ainsi que le nom, la description et l'état des services exécutés sur l'instance d'Unified Manager.

Catégorie	verbe HTTP	Chemin	Description
serveur de gestion	OBTENIR	/management-server/system	Aucun paramètre d'entrée n'est requis pour exécuter cette API. Les détails système de l'instance actuelle d'Unified Manager sont renvoyés par défaut.

Gérer les événements et les alertes à l'aide d'API

Le `events`, `alerts`, et `scripts` API sous le `management-server` La catégorie vous permet de gérer les événements, les alertes et les scripts associés aux alertes dans votre environnement Active IQ Unified Manager .

Afficher et modifier les événements

Unified Manager reçoit les événements générés sur ONTAP pour les clusters surveillés et gérés par Unified Manager. En utilisant ces API, vous pouvez afficher les événements générés pour vos clusters, les résoudre et les mettre à jour.

En exécutant le `GET` méthode pour la `/management-server/events` API, vous pouvez interroger les événements de votre centre de données, y compris les données historiques. Utilisez les filtres intégrés, tels que le nom, le niveau d'impact, la zone d'impact, la gravité, l'état, le nom de la ressource et le type de ressource, pour afficher des événements spécifiques. Les paramètres de type de ressource et de zone renvoient des informations sur l'objet de stockage sur lequel l'événement s'est produit, et la zone d'impact renvoie les informations sur le problème pour lequel l'événement est déclenché, comme la disponibilité, la capacité, la configuration, la sécurité, la protection et les performances.

En exécutant l'opération `PATCH` pour cette API, vous pouvez activer le flux de travail de résolution pour l'événement. Vous pouvez attribuer un événement à vous-même ou à un autre utilisateur et accuser réception de l'événement. En exécutant les étapes sur les ressources pour résoudre le problème qui a déclenché

l'événement, vous pouvez utiliser cette API pour marquer l'événement comme résolu.

Pour plus d'informations sur les événements, voir ["Gérer les événements"](#) .

Catégorie	verbe HTTP	Chemin	Description
serveur de gestion	OBTENIR	/management-server/events /management-server/events/{key}	Lorsque vous exécutez la méthode Get ALL, le corps de la réponse se compose des détails de tous les événements de votre centre de données. Lorsque vous récupérez les détails de l'événement à l'aide d'une clé spécifique, vous pouvez afficher les détails d'un événement spécifique et exécuter l'ensemble d'opérations suivant sur les ressources. Le corps de la réponse contient les détails de cet événement.
serveur de gestion	CORRECTIF	management-server/events/{key}	Exécutez cette API pour attribuer un événement ou modifier l'état en reconnu ou résolu. Vous pouvez également utiliser cette méthode pour attribuer l'événement à vous-même ou à un autre utilisateur. C'est une opération synchrone.

Gérer les alertes

Les événements sont générés automatiquement et en continu. Unified Manager génère une alerte uniquement lorsqu'un événement répond à certains critères de filtre. Vous pouvez sélectionner les événements pour lesquels des alertes doivent être générées. En utilisant le /management-server/alerts API, vous pouvez configurer des alertes pour envoyer des notifications automatiquement lorsque des événements spécifiques ou des événements de certains types de gravité se produisent.

Pour plus d'informations sur les alertes, voir ["Gérer les alertes"](#) .

Catégorie	verbe HTTP	Chemin	Description
serveur de gestion	OBTENIR	/management-server/alerts /management-server/alerts/{key}	Interrogez toutes les alertes existantes dans votre environnement ou une alerte spécifique, en utilisant la clé d'alerte. Vous pouvez afficher les informations sur les alertes générées dans votre environnement, telles que la description de l'alerte, l'action, l'ID de messagerie auquel la notification est envoyée, l'événement et la gravité.
serveur de gestion	POSTE	/management-server/alerts	Cette méthode vous permet d'ajouter des alertes pour des événements spécifiques. Vous devez ajouter le nom de l'alerte, la ressource physique ou logique ou l'événement sur lequel l'alerte est applicable, si l'alerte est activée et si vous émettez des interruptions SNMP. Vous pouvez ajouter des détails supplémentaires pour lesquels vous souhaitez générer l'alerte, tels que l'action, l'ID de l'e-mail de notification, les détails du script, au cas où vous ajouteriez un script d'alerte, etc.
serveur de gestion	PATCH et SUPPRESSION	management-server/events/{key}	Vous pouvez utiliser ces méthodes pour modifier et supprimer des alertes spécifiques. Vous pouvez modifier différents attributs, tels que la description, le nom et l'activation et la désactivation de l'alerte. Vous pouvez supprimer une alerte lorsque celle-ci n'est plus nécessaire.



Lors de la sélection d'une ressource pour ajouter une alerte, notez que la sélection d'un cluster comme ressource ne sélectionne pas automatiquement les objets de stockage dans ce cluster. Par exemple, si vous créez une alerte pour tous les événements critiques de tous les clusters, vous recevrez des alertes uniquement pour les événements critiques du cluster. Vous ne recevrez pas d'alertes pour les événements critiques sur les nœuds, les agrégats, etc.

Gérer les scripts

En utilisant le `/management-server/scripts` API, vous pouvez également associer une alerte à un script qui est exécuté lorsqu'une alerte est déclenchée. Vous pouvez utiliser des scripts pour modifier ou mettre à jour automatiquement plusieurs objets de stockage dans Unified Manager. Le script est associé à une alerte. Lorsqu'un événement déclenche une alerte, le script est exécuté. Vous pouvez télécharger des scripts personnalisés et tester leur exécution lorsqu'une alerte est générée. Vous pouvez associer une alerte à votre script afin que le script soit exécuté lorsqu'une alerte est déclenchée pour un événement dans Unified Manager.

Pour plus d'informations sur les scripts, voir "[Gérer les scripts](#)".

Catégorie	verbe HTTP	Chemin	Description
serveur de gestion	OBTENIR	<code>/management-server/scripts</code>	Utilisez cette API pour interroger tous les scripts existants dans votre environnement. Utilisez le filtre standard et les opérations de tri par pour afficher uniquement des scripts spécifiques.
serveur de gestion	POSTER	<code>/management-server/scripts</code>	Utilisez cette API pour ajouter une description au script et télécharger le fichier de script associé à une alerte.

Gérer les charges de travail à l'aide d'API

Les API décrites ici couvrent diverses fonctions d'administration du stockage, telles que l'affichage des charges de travail de stockage, la création de LUN et de partages de fichiers, la gestion des niveaux de service de performances et des politiques d'efficacité du stockage, ainsi que l'attribution des politiques sur les charges de travail de stockage.

Afficher les charges de travail de stockage à l'aide des API

Les API répertoriées ici vous permettent d'afficher une liste consolidée des charges de travail de stockage pour tous les clusters ONTAP de votre centre de données. Les API fournissent également une vue récapitulative du nombre de charges de travail de stockage provisionnées dans votre environnement Active IQ Unified Manager, ainsi que leurs statistiques de capacité et de performances (IOPS).

Afficher les charges de travail de stockage

Vous pouvez utiliser la méthode suivante pour afficher toutes les charges de travail de stockage dans tous les clusters de votre centre de données. Pour plus d'informations sur le filtrage de la réponse en fonction de colonnes spécifiques, consultez la documentation de référence de l'API disponible dans votre instance Unified Manager.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/workloads

Afficher le résumé des charges de travail de stockage

Vous pouvez utiliser la méthode suivante pour évaluer la capacité utilisée, la capacité disponible, les IOPS utilisées, les IOPS disponibles et le nombre de charges de travail de stockage gérées par chaque niveau de service de performances. Les charges de travail de stockage affichées peuvent concerner n'importe quel LUN, partage de fichiers NFS ou partage CIFS. L'API fournit une vue d'ensemble des charges de travail de stockage, une vue d'ensemble des charges de travail de stockage provisionnées par Unified Manager, une vue d'ensemble du centre de données, une vue d'ensemble de l'espace total, utilisé et disponible et des IOPS dans le centre de données, en termes de niveaux de service de performances attribués. Les informations reçues en réponse à cette API sont utilisées pour remplir le tableau de bord dans l'interface utilisateur d'Unified Manager.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/workloads-summary

Gérer les points d'accès à l'aide d'API

Vous devez créer des points de terminaison d'accès ou des interfaces logiques (LIF), qui sont nécessaires au provisionnement des machines virtuelles de stockage (SVM), des LUN et des partages de fichiers. Vous pouvez afficher, créer, modifier et supprimer les points de terminaison d'accès pour les SVM, les LUN ou les partages de fichiers dans votre environnement Active IQ Unified Manager .

Afficher les points d'accès

Vous pouvez afficher une liste des points de terminaison d'accès dans votre environnement Unified Manager à l'aide de la méthode suivante. Pour interroger une liste de points de terminaison d'accès d'un SVM, d'un LUN ou d'un partage de fichiers particulier, vous devez saisir l'identifiant unique du SVM, du LUN ou du partage de fichiers. Vous pouvez également saisir la clé de point de terminaison d'accès unique pour récupérer les détails du point de terminaison d'accès particulier.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

Ajouter des points d'accès

Vous pouvez créer des points de terminaison d'accès personnalisés et leur attribuer les propriétés requises. Vous devez saisir les détails du point de terminaison d'accès que vous souhaitez créer comme paramètres d'entrée. Vous pouvez utiliser cette API, le gestionnaire système ou l'interface de ligne de commande ONTAP pour créer un point de terminaison d'accès sur chaque nœud. Les adresses IPv4 et IPv6 sont prises en charge pour la création de points de terminaison d'accès.



Vous devez configurer votre SVM avec un nombre minimum de points de terminaison d'accès par nœud pour un provisionnement réussi des LUN et des partages de fichiers. Vous devez configurer votre SVM avec au moins deux points de terminaison d'accès par nœud, l'un prenant en charge le protocole CIFS et/ou NFS, l'autre prenant en charge le protocole iSCSI ou FCP.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTER	/storage-provider/access-endpoints

Supprimer les points d'accès

Vous pouvez supprimer un point de terminaison d'accès spécifique à l'aide de la méthode suivante. Vous devez fournir la clé de point de terminaison d'accès comme paramètre d'entrée pour supprimer un point de terminaison d'accès particulier.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	/storage-provider/access-endpoints/{key}

Modifier les points d'accès

Vous pouvez modifier un point de terminaison d'accès et mettre à jour ses propriétés à l'aide de la méthode suivante. Vous devez fournir la clé de point de terminaison d'accès pour modifier un point de terminaison d'accès particulier. Vous devez également saisir la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/access-endpoints/{key}

Gérer le mappage Active Directory à l'aide d'API

Vous pouvez utiliser les API répertoriées ici pour gérer les mappages Active Directory sur le SVM qui sont requis pour le provisionnement des partages CIFS sur les SVM. Les mappages Active Directory doivent être configurés pour mapper les SVM avec ONTAP.

Afficher les mappages Active Directory

Vous pouvez afficher les détails de configuration des mappages Active Directory pour un SVM à l'aide de la méthode suivante. Pour afficher les mappages Active Directory sur un SVM, vous devez saisir la clé SVM. Pour interroger les détails d'un mappage particulier, vous devez saisir la clé de mappage.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/active-directories-mappings /storage-provider/active-directories-mappings/{key}

Ajouter un mappage Active Directory

Vous pouvez créer des mappages Active Directory sur une SVM en utilisant la méthode suivante. Vous devez saisir les détails de mappage comme paramètres d'entrée.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTER	/storage-provider/active-directories-mappings

Gérer les partages de fichiers à l'aide d'API

Vous pouvez utiliser le `/storage-provider/file-shares` API pour afficher, ajouter, modifier et supprimer les volumes de partage de fichiers CIFS et NFS dans votre environnement de centre de données.

Avant de provisionner les volumes de partage de fichiers, assurez-vous que le SVM a été créé et provisionné avec les protocoles pris en charge. Si vous attribuez des niveaux de service de performances (PSL) ou des politiques d'efficacité de stockage (SEP), lors du provisionnement, les PSL ou les SEP doivent être créés avant de créer les partages de fichiers.

Afficher les partages de fichiers

Vous pouvez utiliser la méthode suivante pour afficher les volumes de partage de fichiers disponibles dans votre environnement Unified Manager. Lorsque vous avez ajouté un cluster ONTAP en tant que source de données sur Active IQ Unified Manager, les charges de travail de stockage de ces clusters sont automatiquement ajoutées à votre instance Unified Manager. Cette API récupère automatiquement et manuellement les partages de fichiers ajoutés à votre instance Unified Manager. Vous pouvez afficher les détails d'un partage de fichiers spécifique en exécutant cette API avec la clé de partage de fichiers.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/file-shares /storage-provider/file-shares/{key}

Ajouter des partages de fichiers

Vous pouvez utiliser la méthode suivante pour ajouter des partages de fichiers CIFS et NFS dans votre SVM. Vous devez saisir les détails du partage de fichiers que vous souhaitez créer, comme paramètres d'entrée. Vous ne pouvez pas utiliser cette API pour ajouter des volumes FlexGroup .

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTE	/storage-provider/file-shares



Selon que les paramètres de la liste de contrôle d'accès (ACL) ou les paramètres de la stratégie d'exportation sont fournis, des partages CIFS ou des partages de fichiers NFS sont créés. Si vous ne fournissez pas les valeurs des paramètres ACL, les partages CIFS ne sont pas créés et les partages NFS sont créés par défaut, offrant un accès à tous.

Création de volumes de protection des données : Lorsque vous ajoutez des partages de fichiers à votre SVM, le type de volume monté, par défaut, est `rw` (lecture-écriture). Pour créer des volumes de protection des données (DP), spécifiez `dp` comme valeur pour le `type` paramètre.

Supprimer les partages de fichiers

Vous pouvez utiliser la méthode suivante pour supprimer un partage de fichiers spécifique. Vous devez saisir la clé de partage de fichiers comme paramètre d'entrée pour supprimer un partage de fichiers particulier.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	/storage-provider/file-shares/{key}

Modifier les partages de fichiers

Vous pouvez utiliser la méthode suivante pour modifier un partage de fichiers et mettre à jour ses propriétés.

Vous devez fournir la clé de partage de fichiers pour modifier un partage de fichiers particulier. De plus, vous devez saisir la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.



Notez que vous ne pouvez mettre à jour qu'une seule propriété lors d'une seule invocation de cette API. Pour plusieurs mises à jour, vous devez exécuter cette API autant de fois que nécessaire.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/file-shares/{key}

Gérer les LUN à l'aide d'API

Vous pouvez utiliser le `/storage-provider/luns` API pour afficher, ajouter, modifier et supprimer les LUN dans votre environnement de centre de données.

Avant de provisionner les LUN, assurez-vous que le SVM a été créé et provisionné avec les protocoles pris en charge. Si vous attribuez des niveaux de service de performances (PSL) ou des politiques d'efficacité de stockage (SEP), lors du provisionnement, les PSL ou les SEP doivent être créés avant de créer le LUN.

Afficher les LUN

Vous pouvez utiliser la méthode suivante pour afficher les LUN dans votre environnement Unified Manager. Lorsque vous avez ajouté un cluster ONTAP en tant que source de données sur Active IQ Unified Manager, les charges de travail de stockage de ces clusters sont automatiquement ajoutées à votre instance Unified Manager. Cette API récupère automatiquement et manuellement tous les LUN ajoutés à votre instance Unified Manager. Vous pouvez afficher les détails d'un LUN spécifique en exécutant cette API avec la clé LUN.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/luns /storage-provider/luns/{key}

Ajouter des LUN

Vous pouvez utiliser la méthode suivante pour ajouter des LUN à vos SVM.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTER	/storage-provider/luns



Dans votre requête cURL, si vous fournissez une valeur pour le paramètre facultatif `volume_name_tag` dans l'entrée, cette valeur est utilisée lors de la dénomination du volume lors de la création du LUN. Cette balise permet de rechercher facilement le volume. Si vous fournissez la clé de volume dans la demande, le balisage est ignoré.

Supprimer les LUN

Vous pouvez utiliser la méthode suivante pour supprimer un LUN spécifique. Vous devez fournir la clé LUN pour supprimer un LUN particulier.



Si vous avez créé un volume dans ONTAP, puis provisionné des LUN via Unified Manager sur ce volume, lorsque vous supprimez tous les LUN à l'aide de cette API, le volume est également supprimé du cluster ONTAP.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	/storage-provider/luns/{key}

Modifier les LUN

Vous pouvez utiliser la méthode suivante pour modifier un LUN et mettre à jour ses propriétés. Vous devez fournir la clé LUN pour modifier un LUN particulier. Vous devez également saisir la propriété LUN que vous souhaitez mettre à jour, ainsi que sa valeur. Pour mettre à jour les baies LUN à l'aide de cette API, vous devez consulter les recommandations dans « Recommandations pour l'utilisation des API ».



Vous ne pouvez mettre à jour qu'une seule propriété lors d'une seule invocation de cette API. Pour plusieurs mises à jour, vous devez exécuter cette API autant de fois que nécessaire.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/luns/{key}

Gérer les niveaux de service de performance à l'aide d'API

Vous pouvez afficher, créer, modifier et supprimer les niveaux de service de performances à l'aide des API du fournisseur de stockage sur votre Active IQ Unified Manager.

Afficher les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour afficher les niveaux de service de performances afin de les attribuer aux charges de travail de stockage. L'API répertorie tous les niveaux de service de performances définis par le système et créés par l'utilisateur et récupère les attributs de tous les niveaux de service de performances. Si vous souhaitez interroger un niveau de service de performance spécifique, vous devez saisir l'ID unique du niveau de service de performance pour récupérer ses détails.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/performance-service-levels /storage-provider/performance-service-levels/{key}

Ajouter des niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour créer des niveaux de service de performances personnalisés et les attribuer à vos charges de travail de stockage si les niveaux de service de performances définis par le système ne répondent pas aux objectifs de niveau de service (SLO) requis pour les charges de travail de stockage. Saisissez les détails du niveau de service de performance que vous souhaitez créer. Pour les

propriétés IOPS, assurez-vous de saisir une plage de valeurs valide.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTE	/storage-provider/performance-service-levels

Supprimer les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour supprimer un niveau de service de performances spécifique. Vous ne pouvez pas supprimer un niveau de service de performances s'il est attribué à une charge de travail ou s'il s'agit du seul niveau de service de performances disponible. Vous devez fournir l'ID unique du niveau de service de performances comme paramètre d'entrée pour supprimer un niveau de service de performances particulier.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	/storage-provider/performance-service-levels/{key}

Modifier les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour modifier un niveau de service de performances et mettre à jour ses propriétés. Vous ne pouvez pas modifier un niveau de service de performances défini par le système ou attribué à une charge de travail. Vous devez fournir l'ID unique pour modifier un niveau de service de performance particulier. Vous devez également saisir la propriété IOPS que vous souhaitez mettre à jour, ainsi qu'une valeur valide.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/performance-service-levels/{key}

Afficher les capacités globales en fonction des niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour interroger les capacités agrégées en fonction des niveaux de service de performances. Cette API renvoie la liste des agrégats disponibles dans votre centre de données et indique les capacités en termes de niveaux de service de performances qui peuvent être prises en charge dans ces agrégats. Lors du provisionnement des charges de travail sur un volume, vous pouvez afficher la capacité d'un agrégat à prendre en charge un niveau de service de performances particulier et provisionner les charges de travail en fonction de cette capacité. Votre capacité à spécifier l'agrégat n'est disponible que lorsque vous provisionnez une charge de travail à l'aide d'API. Cette fonctionnalité n'est pas disponible sur l'interface Web d'Unified Manager.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/aggregate-capabilities /storage-provider/aggregate-capabilities/{key}

Gérer les politiques d'efficacité du stockage à l'aide d'API

Vous pouvez afficher, créer, modifier et supprimer des stratégies d'efficacité de stockage à l'aide des API du fournisseur de stockage.

Notez les points suivants :



- Il n'est pas obligatoire d'attribuer une politique d'efficacité de stockage lors de la création d'une charge de travail sur Unified Manager.
- Vous ne pouvez pas annuler l'attribution d'une stratégie d'efficacité de stockage à une charge de travail une fois qu'une stratégie lui a été attribuée.
- Si une charge de travail comporte des paramètres de stockage spécifiés sur les volumes ONTAP, tels que la déduplication et la compression, ces paramètres peuvent être remplacés par les paramètres spécifiés dans la stratégie d'efficacité du stockage que vous appliquez lorsque vous ajoutez les charges de travail de stockage sur Unified Manager.

Afficher les politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour afficher les stratégies d'efficacité du stockage avant de les attribuer aux charges de travail de stockage. Cette API répertorie toutes les politiques d'efficacité du stockage définies par le système et créées par l'utilisateur et récupère les attributs de toutes les politiques d'efficacité du stockage. Si vous souhaitez interroger une politique d'efficacité de stockage spécifique, vous devez saisir l'ID unique de la politique pour récupérer ses détails.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/storage-efficiency-policies /storage-provider/storage-efficiency-policies/{key}

Ajouter des politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour créer des stratégies d'efficacité de stockage personnalisées et les attribuer à vos charges de travail de stockage si les stratégies définies par le système ne répondent pas aux exigences de provisionnement de vos charges de travail de stockage. Saisissez les détails de la politique d'efficacité de stockage que vous souhaitez créer, en tant que paramètres d'entrée.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTE	/storage-provider/storage-efficiency-policies

Supprimer les politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour supprimer une stratégie d'efficacité de stockage spécifique. Vous ne pouvez pas supprimer une stratégie d'efficacité du stockage si elle est attribuée à une charge de travail ou s'il s'agit de la seule stratégie d'efficacité du stockage disponible. Vous devez fournir l'ID unique de la politique d'efficacité de stockage comme paramètre d'entrée pour supprimer une politique d'efficacité de stockage particulière.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	/storage-provider/storage-efficiency-policies/{key}

Modifier les politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour modifier une stratégie d'efficacité de stockage et mettre à jour ses propriétés. Vous ne pouvez pas modifier une stratégie d'efficacité de stockage définie par le système ou attribuée à une charge de travail. Vous devez fournir l'ID unique de la politique d'efficacité de stockage pour modifier une politique d'efficacité de stockage particulière. De plus, vous devez fournir la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/storage-efficiency-policies/{key}

Flux de travail API courants pour la gestion du stockage

Les flux de travail communs fournissent aux développeurs d'applications clientes des exemples de la manière dont les API Active IQ Unified Manager peuvent être appelées par une application cliente pour exécuter des fonctions de gestion de stockage courantes. Cette section contient certains de ces exemples de flux de travail.

Les flux de travail décrivent certains des cas d'utilisation de gestion du stockage couramment utilisés ainsi que des exemples de codes que vous pouvez utiliser. Chacune des tâches est décrite à l'aide d'un processus de workflow composé d'un ou plusieurs appels d'API.

Comprendre les appels API utilisés dans les workflows

Vous pouvez consulter la page de documentation en ligne de votre instance Unified Manager qui inclut les détails de chaque appel d'API REST. Ce document ne reprend pas les détails de la documentation en ligne. Chaque appel d'API utilisé dans les exemples de workflow de ce document inclut uniquement les informations dont vous avez besoin pour localiser l'appel sur la page de documentation. Après avoir localisé un appel d'API spécifique, vous pouvez consulter ses détails complets, notamment les paramètres d'entrée, les formats de

sortie, les codes d'état HTTP et le type de traitement de la requête.

Les informations suivantes sont incluses pour chaque appel d'API dans un workflow pour aider à localiser l'appel sur la page de documentation :

- **Catégorie** : Les appels d'API sont organisés sur la page de documentation en domaines ou catégories fonctionnellement liés. Pour localiser un appel d'API spécifique, faites défiler la page jusqu'en bas et cliquez sur la catégorie d'API correspondante.
- **Verbe HTTP (appel)** : Le verbe HTTP identifie l'action effectuée sur une ressource. Chaque appel d'API est exécuté via un seul verbe HTTP.
- **Chemin** : le chemin détermine la ressource spécifique à laquelle l'action s'applique dans le cadre de l'exécution d'un appel. La chaîne de chemin est ajoutée à l'URL principale pour former l'URL complète identifiant la ressource.

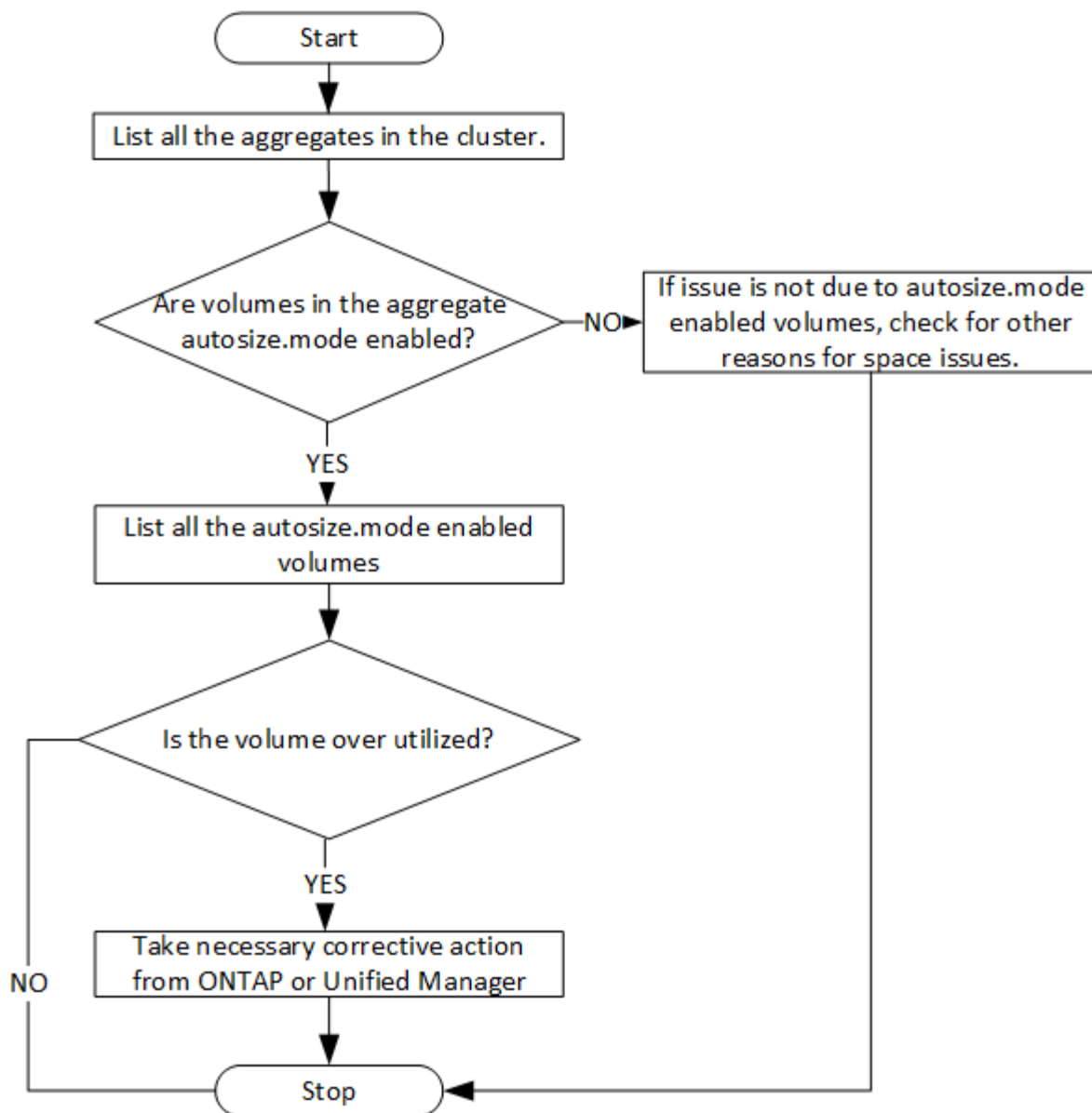
Déterminer les problèmes d'espace dans les agrégats à l'aide d'API

Vous pouvez utiliser les API du centre de données dans Active IQ Unified Manager pour surveiller la disponibilité et l'utilisation de l'espace dans vos volumes. Vous pouvez déterminer les problèmes d'espace dans votre volume et identifier les ressources de stockage surutilisées ou sous-utilisées.

Les API du centre de données pour les agrégats récupèrent les informations pertinentes sur l'espace disponible et utilisé, ainsi que sur les paramètres d'efficacité d'économie d'espace. Vous pouvez également filtrer les informations récupérées en fonction d'attributs spécifiés.

Une méthode pour déterminer tout manque d'espace dans vos agrégats consiste à vérifier s'il existe des volumes dans votre environnement avec le mode de taille automatique activé. Vous devez ensuite identifier les volumes surutilisés et effectuer les actions correctives nécessaires.

Le diagramme suivant illustre le processus de récupération d'informations sur les volumes avec le mode de taille automatique activé :



Ce flux suppose que les clusters ont déjà été créés dans ONTAP et ajoutés à Unified Manager.

1. Obtenez la clé du cluster, sauf si vous connaissez la valeur :

Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/cluster/clusters

2. En utilisant la clé de cluster comme paramètre de filtre, interrogez les agrégats sur ce cluster.

Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/storage/aggregates

- À partir de la réponse, analysez l'utilisation de l'espace des agrégats et déterminez quels agrégats présentent des problèmes d'espace. Pour chaque agrégat avec problème d'espace, obtenez la clé d'agrégat à partir de la même sortie JSON.
- À l'aide de chaque clé agrégée, filtrez tous les volumes qui ont la valeur du paramètre `autosize.mode` comme `grow`.

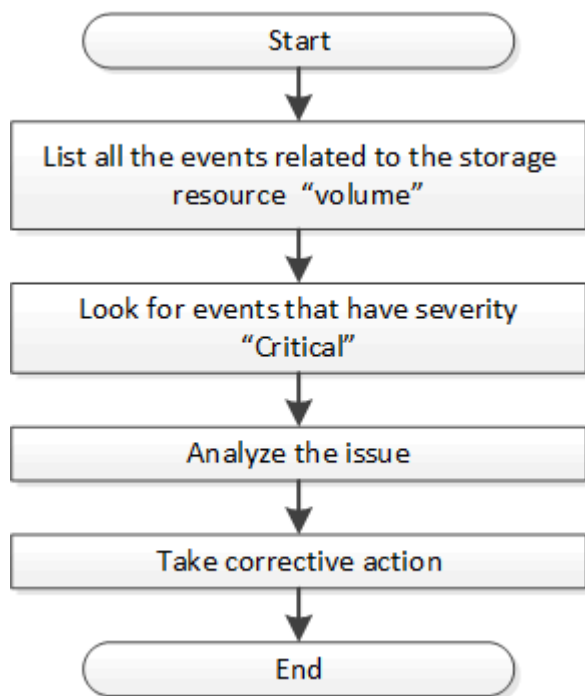
Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/storage/volumes

- Analyser les volumes qui sont surutilisés.
- Effectuez toute action corrective nécessaire, telle que le déplacement du volume entre les agrégats, pour résoudre les problèmes d'espace dans votre volume. Vous pouvez effectuer ces actions à partir de l'interface Web ONTAP ou Unified Manager.

Déterminer les problèmes dans les objets de stockage à l'aide des API d'événements

Lorsqu'un objet de stockage dans votre centre de données dépasse un seuil, vous recevez une notification concernant cet événement. À l'aide de cette notification, vous pouvez analyser le problème et prendre des mesures correctives en utilisant le `events` Apis.

Ce flux de travail prend l'exemple d'un volume comme objet ressource. Vous pouvez utiliser le `events` API permettant de récupérer la liste des événements liés à un volume, d'analyser les problèmes critiques de ce volume, puis de prendre des mesures correctives pour rectifier le problème.



Suivez ces étapes pour déterminer les problèmes de votre volume avant de prendre des mesures correctives.

Étapes

1. Analysez les notifications d'événements critiques Active IQ Unified Manager pour les volumes de votre centre de données.
2. Interrogez tous les événements des volumes en utilisant les paramètres suivants dans l'API /management-server/events :

"resource_type": "volume"

"severity": "critical"

Catégorie	verbe HTTP	Chemin
serveur de gestion	OBTENIR	/serveur-de-gestion/événements

3. Visualisez la sortie et analysez les problèmes dans les volumes spécifiques.
4. Effectuez les actions nécessaires en utilisant les API REST ou l'interface utilisateur Web d'Unified Manager pour résoudre les problèmes.

Dépanner les volumes ONTAP à l'aide des API de passerelle

Les API de passerelle agissent comme une passerelle pour appeler les API ONTAP afin d'interroger des informations sur vos objets de stockage ONTAP et de prendre des mesures correctives pour résoudre les problèmes signalés.

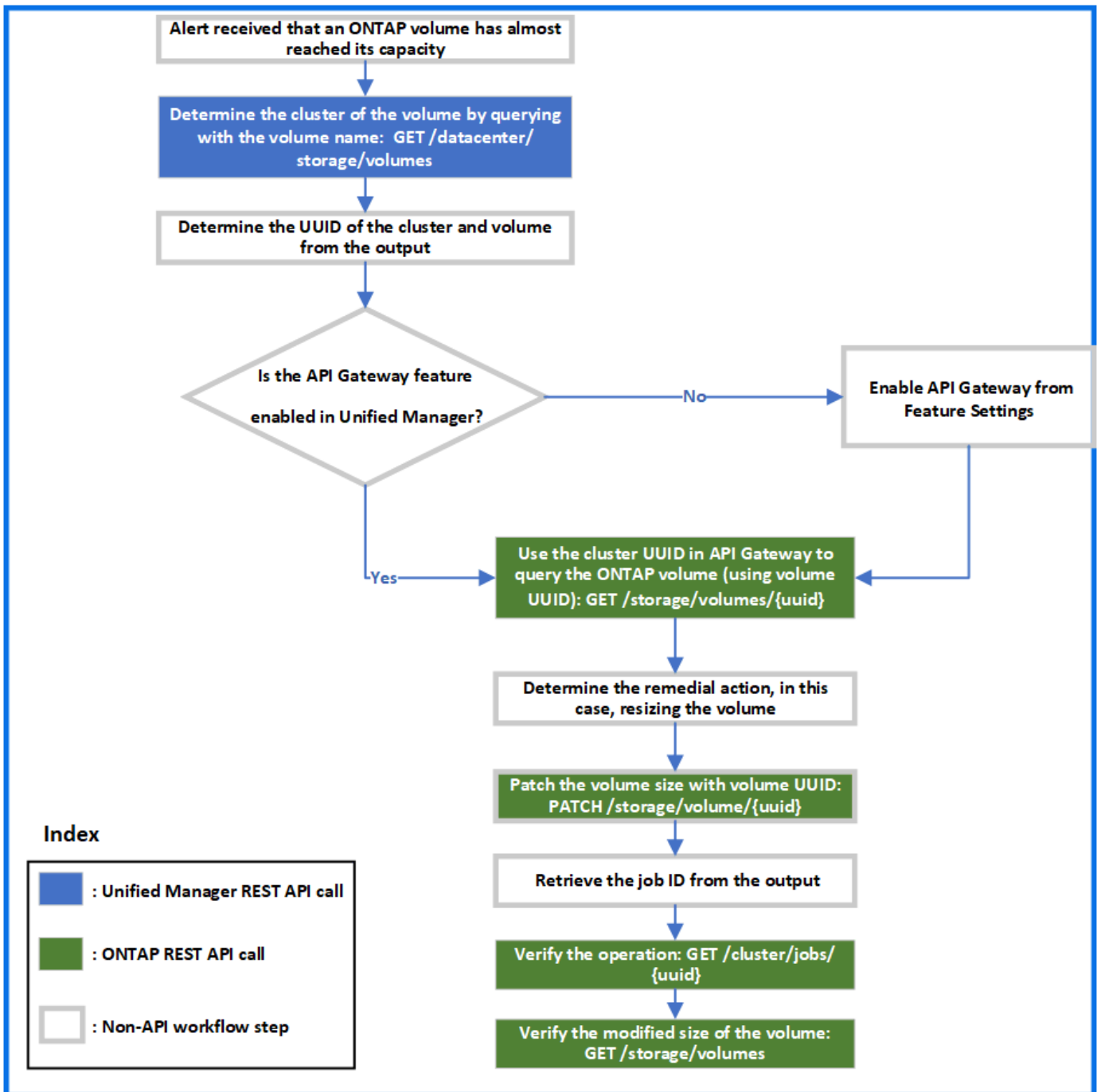
Ce workflow reprend un exemple de cas d'utilisation dans lequel un événement est déclenché lorsqu'un volume ONTAP atteint presque sa capacité. Le flux de travail montre également comment résoudre ce problème en invoquant une combinaison d'API REST Active IQ Unified Manager et ONTAP .

Avant d'exécuter les étapes du workflow, assurez-vous des points suivants :



- Vous connaissez les API de passerelle et la manière dont elles sont utilisées. Pour plus d'informations, voir [Accéder aux API ONTAP via un accès proxy](#) .
- Vous connaissez l'utilisation des API REST ONTAP . Pour plus d'informations sur l'utilisation des API REST ONTAP , consultez <https://docs.netapp.com/us-en/ontap-automation/index.html> ["Documentation sur l'automatisation ONTAP"] .
- Vous êtes un administrateur d'application.
- Le cluster sur lequel vous souhaitez exécuter les opérations de l'API REST est pris en charge par ONTAP 9.5 ou version ultérieure, et le cluster est ajouté à Unified Manager via HTTPS.

Le diagramme suivant illustre chaque étape du flux de travail de résolution du problème d'utilisation de la capacité du volume ONTAP .



Le workflow couvre les points d'invocation des API REST Unified Manager et ONTAP .

1. Notez le nom du volume à partir de l'événement notifiant l'utilisation de la capacité du volume.
2. En utilisant le nom du volume comme valeur dans le paramètre de nom, interrogez le volume en exécutant l'API Unified Manager suivante.

Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/storage/volumes

3. Récupérez l'UUID du cluster et l'UUID du volume à partir de la sortie.

- Sur l'interface Web d'Unified Manager, accédez à **Général > Paramètres des fonctionnalités > Passerelle API** pour vérifier si la fonctionnalité Passerelle API est activée. À moins qu'elle ne soit activée, les API sous la catégorie passerelle ne sont pas disponibles pour que vous puissiez les appeler. Activez la fonctionnalité si elle est désactivée.
- Utiliser l'UUID du cluster pour exécuter l'API `ONTAP/storage/volumes/{uuid}` via la passerelle API. La requête renvoie les détails du volume lorsque l'UUID du volume est transmis en tant que paramètre API.

Pour exécuter les API ONTAP via la passerelle API, les informations d'identification d'Unified Manager sont transmises en interne pour l'authentification et vous n'avez pas besoin d'exécuter une étape d'authentification supplémentaire pour l'accès individuel au cluster.

Catégorie	verbe HTTP	Chemin
Gestionnaire unifié : passerelle	OBTENIR	API de passerelle : <code>/gateways/{uuid}/{path}</code>
ONTAP: stockage		API ONTAP : <code>/storage/volumes/{uuid}</code>



Dans `/gateways/{uuid}/{path}`, la valeur de `{uuid}` doit être remplacée par l'UUID du cluster sur lequel l'opération REST doit être effectuée. `{path}` doit être remplacé par l'URL ONTAP REST `/storage/volumes/{uuid}`.

L'URL ajoutée est : `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

Lors de l'exécution de l'opération GET, l'URL générée est :

```
GEThttps://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}
```

Exemple de commande cURL

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

- À partir des résultats, déterminez la taille, l'utilisation et les mesures correctives à prendre. Dans ce flux de travail, la mesure corrective prise consiste à redimensionner le volume.
- Utilisez l'UUID du cluster et exécutez l'API ONTAP suivante via la passerelle API pour redimensionner le volume. Pour plus d'informations sur les paramètres d'entrée pour la passerelle et les API ONTAP, consultez l'étape 5.

Catégorie	verbe HTTP	Chemin
Gestionnaire unifié : passerelle ONTAP: stockage	CORRECTIF	API de passerelle : /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}



Outre l'UUID du cluster et l'UUID du volume, vous devez saisir une valeur pour le paramètre de taille pour redimensionner le volume. Assurez-vous de saisir la valeur *en octets*. Par exemple, si vous souhaitez augmenter la taille d'un volume de 100 Go à 120 Go, saisissez la valeur du paramètre size à la fin de la requête : `-d {"size": 128849018880}`

Exemple de commande cURL

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size": 128849018880}"
```

La sortie JSON renvoie un UUID de tâche.

- Vérifiez si le travail s'est exécuté avec succès en utilisant l'UUID du travail. Utilisez l'UUID du cluster et l'UUID du travail pour exécuter l'API ONTAP suivante via la passerelle API. Pour plus d'informations sur les paramètres d'entrée pour la passerelle et les API ONTAP , consultez l'étape 5.

Catégorie	verbe HTTP	Chemin
Gestionnaire unifié : passerelle ONTAP: cluster	OBTENIR	API de passerelle : /gateways/{uuid}/{path} API ONTAP : /cluster/jobs/{uuid}

Les codes HTTP renvoyés sont les mêmes que les codes d'état HTTP de l'API REST ONTAP .

- Exécutez l'API ONTAP suivante pour interroger les détails du volume redimensionné. Pour plus d'informations sur les paramètres d'entrée pour la passerelle et les API ONTAP , consultez l'étape 5.

Catégorie	verbe HTTP	Chemin
Gestionnaire unifié : passerelle ONTAP: stockage	OBTENIR	API de passerelle : /gateways/{uuid}/{path} API ONTAP : /storage/volumes/{uuid}

La sortie affiche une taille de volume augmentée de 120 Go.

Workflows API pour la gestion de la charge de travail

À l'aide d'Active IQ Unified Manager, vous pouvez provisionner et modifier les charges de travail de stockage (LUN, partages de fichiers NFS et partages CIFS). Le provisionnement comprend plusieurs étapes, depuis la création de la machine virtuelle de stockage (SVM) jusqu'à l'application des politiques de niveau de service de performances et d'efficacité du stockage sur les charges de travail de stockage. La modification des charges de travail comprend les étapes de modification de paramètres spécifiques et d'activation de fonctionnalités supplémentaires sur celles-ci.

Les flux de travail suivants sont décrits :

- Workflow pour le provisionnement des machines virtuelles de stockage (SVM) sur Unified Manager.



ce flux de travail doit être exécuté avant le provisionnement des LUN ou des partages de fichiers sur Unified Manager.

- Provisionnement des partages de fichiers.
- Provisionnement des LUN.
- Modification des LUN et des partages de fichiers (en utilisant l'exemple de mise à jour du paramètre Niveau de service de performance pour les charges de travail de stockage).
- Modification d'un partage de fichiers NFS pour prendre en charge le protocole CIFS
- Modification des charges de travail pour mettre à niveau la qualité de service vers l'AQoS



Pour chaque workflow de provisionnement (LUN et partages de fichiers), assurez-vous d'avoir terminé le workflow de vérification des SVM sur les clusters.

Vous devez également lire les recommandations et les limitations avant d'utiliser chaque API dans les workflows. Les détails pertinents des API sont disponibles dans leurs sections individuelles répertoriées dans les concepts et références associés.

Vérifier les SVM sur les clusters à l'aide d'API

Avant de provisionner des partages de fichiers ou des LUN, vous devez vérifier si des machines virtuelles de stockage (SVM) ont été créées sur les clusters.



Le flux de travail suppose que les clusters ONTAP ont été ajoutés à Unified Manager et que la clé de cluster a été obtenue. Les clusters doivent disposer des licences requises pour provisionner des LUN et des partages de fichiers sur eux.

1. Vérifiez si le cluster a une SVM créée.

Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/svm/svms /datacenter/svm/svms/{key} }

Exemple de cURL

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

- Si la clé SVM n'est pas renvoyée, créez la SVM. Pour créer les SVM, vous avez besoin de la clé de cluster sur laquelle vous provisionnez le SVM. Vous devez également spécifier le nom du SVM. Suivez ces étapes.

Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

Obtenez la clé du cluster.

Exemple de cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

- À partir de la sortie, récupérez la clé de cluster, puis utilisez-la comme entrée pour créer le SVM.



Lors de la création du SVM, assurez-vous qu'il prend en charge tous les protocoles requis pour provisionner les LUN et les partages de fichiers sur ceux-ci, par exemple, CIFS, NFS, FCP et iSCSI. Les flux de travail de provisionnement peuvent échouer si le SVM ne prend pas en charge les services requis. Il est recommandé que les services pour les types de charges de travail respectifs soient également activés sur la SVM.

Catégorie	verbe HTTP	Chemin
centre de données	POSTE	/datacenter/svm/svms

Exemple de cURL

Saisissez les détails de l'objet SVM comme paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcg\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" } },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" } }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le SVM que vous avez créé.

4. Vérifiez la création de SVM en utilisant la clé d'objet de travail pour la requête. Si le SVM est créé avec succès, la clé SVM est renvoyée dans la réponse.

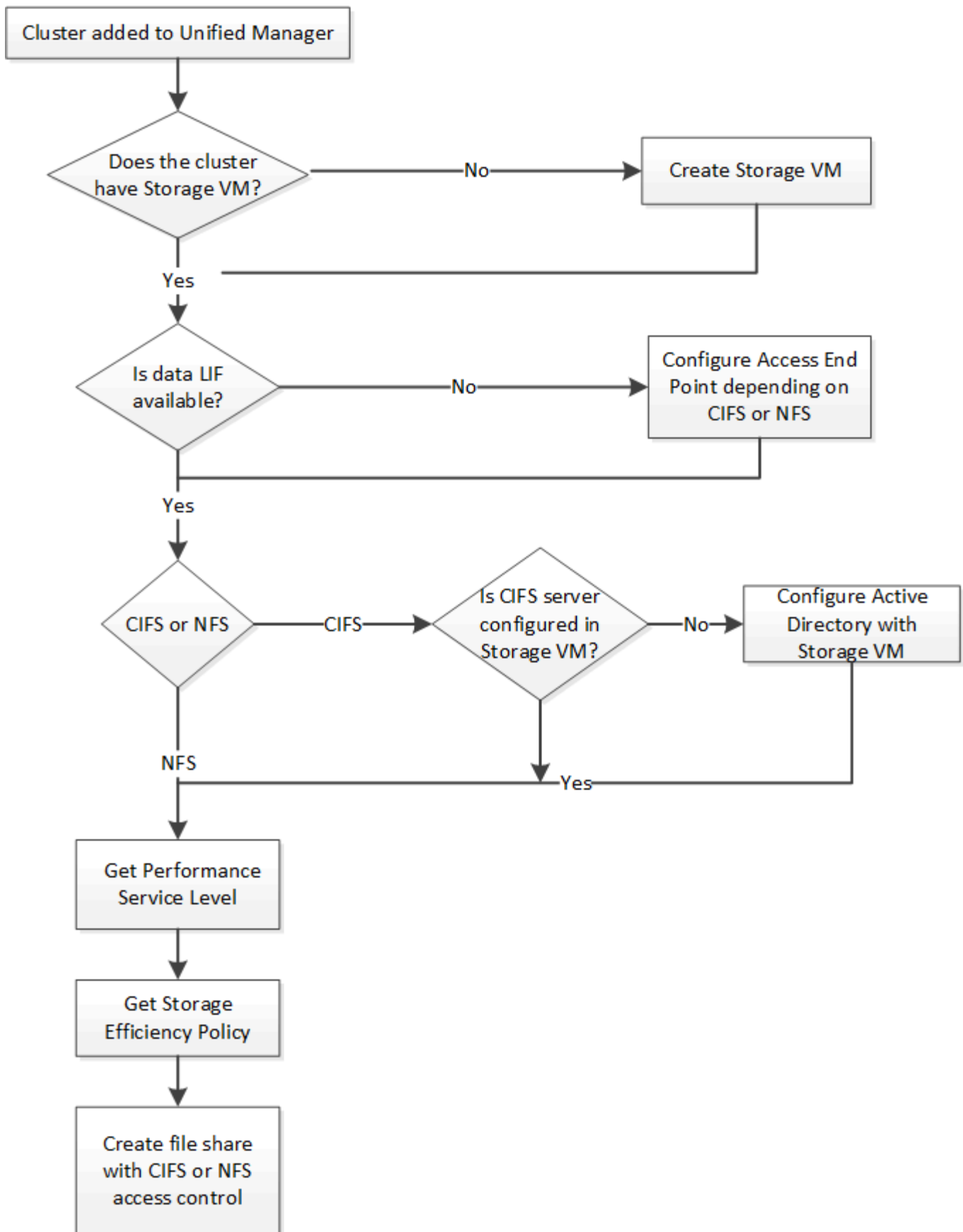
Catégorie	verbe HTTP	Chemin
serveur de gestion	OBTENIR	/management-server/jobs/{key}

Provisionnez les partages de fichiers CIFS et NFS à l'aide d'API

Vous pouvez provisionner des partages CIFS et des partages de fichiers NFS sur vos

machines virtuelles de stockage (SVM) à l'aide des API de provisionnement fournies dans le cadre d' Active IQ Unified Manager. Ce flux de travail de provisionnement détaille les étapes de récupération des clés des SVM, des niveaux de service de performances et des politiques d'efficacité de stockage avant de créer les partages de fichiers.

Le diagramme suivant illustre chaque étape d'un flux de travail de provisionnement de partage de fichiers. Il inclut le provisionnement des partages CIFS et des partages de fichiers NFS.



Assurez-vous de ce qui suit :



- Les clusters ONTAP ont été ajoutés à Unified Manager et la clé de cluster a été obtenue.
- Des SVM ont été créés sur les clusters.
- Les SVM prennent en charge les services CIFS et NFS. Le provisionnement des partages de fichiers peut échouer si les SVM ne prennent pas en charge les services requis.
- Le port FCP est en ligne pour le provisionnement des ports.

1. Déterminez si les LIF de données ou les points de terminaison d'accès sont disponibles sur la SVM sur laquelle vous souhaitez créer le partage CIFS. Obtenez la liste des points de terminaison d'accès disponibles sur la SVM :

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

Exemple de cURL

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si votre point de terminaison d'accès est disponible dans la liste, obtenez la clé du point de terminaison d'accès, sinon créez le point de terminaison d'accès.



Assurez-vous de créer des points de terminaison d'accès sur lesquels le protocole CIFS est activé. Le provisionnement des partages CIFS échoue sauf si vous avez créé un point de terminaison d'accès avec le protocole CIFS activé.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTER	/storage-provider/access-endpoints

Exemple de cURL

Vous devez saisir les détails du point de terminaison d'accès que vous souhaitez créer, en tant que paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
  \"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
  \"gateway\": \"10.132.72.12\",
  \"ip\": { \"address\": \"10.162.83.26\",
  \"ha_address\": \"10.142.83.26\",
  \"netmask\": \"255.255.0.0\" },
  \"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
  \"mtu\": 15000, \"name\": \"aep1\",
  \"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
  \"vlan\": 10}
```

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le point de terminaison d'accès que vous avez créé.

3. Vérifiez le point de terminaison d'accès :

Catégorie	verbe HTTP	Chemin
serveur de gestion	OBTENIR	/management-server/jobs/{key}

4. Déterminez si vous devez créer un partage CIFS ou un partage de fichiers NFS. Pour créer des partages CIFS, suivez ces sous-étapes :

- Déterminez si le serveur CIFS est configuré sur votre SVM, c'est-à-dire si un mappage Active Directory est créé sur le SVM.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/active-directories-mappings

- Si le mappage Active Directory est créé, prenez la clé, sinon créez le mappage Active Directory sur le SVM.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTE	/storage-provider/active-directories-mappings

Exemple de cURL

Vous devez saisir les détails pour la création du mappage Active Directory, en tant que paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/storage-provider/active-  
directories-mappings" -H "accept: application/json" -H "Content-Type:  
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"  
{ \"_links\": {},  
  \"dns\": \"10.000.000.000\",  
  \"domain\": \"example.com\",  
  \"password\": \"string\",  
  \"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-  
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },  
  \"username\": \"string\"}
```

+

Il s'agit d'un appel synchrone et vous pouvez vérifier la création du mappage Active Directory dans la sortie. En cas d'erreur, le message d'erreur s'affiche pour vous permettre de résoudre le problème et de réexécuter la demande.

5. Obtenez la clé SVM pour la SVM sur laquelle vous souhaitez créer le partage CIFS ou le partage de fichiers NFS, comme décrit dans la rubrique de workflow *Vérification des SVM sur les clusters*.
6. Obtenez la clé du niveau de service de performance en exécutant l'API suivante et en récupérant la clé à partir de la réponse.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/performance-service-levels



Vous pouvez récupérer les détails des niveaux de service de performance définis par le système en définissant le `system_defined` paramètre d'entrée à `true`. À partir de la sortie, obtenez la clé du niveau de service de performances que vous souhaitez appliquer sur le partage de fichiers.

7. Vous pouvez également obtenir la clé de stratégie d'efficacité de stockage pour la stratégie d'efficacité de stockage que vous souhaitez appliquer sur le partage de fichiers en exécutant l'API suivante et en récupérant la clé à partir de la réponse.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/storage-efficiency-policies

8. Créez le partage de fichiers. Vous pouvez créer un partage de fichiers prenant en charge CIFS et NFS en

spécifiant la liste de contrôle d'accès et la politique d'exportation. Les sous-étapes suivantes fournissent des informations si vous souhaitez créer un partage de fichiers pour prendre en charge un seul des protocoles sur le volume. Vous pouvez également mettre à jour un partage de fichiers NFS pour inclure la liste de contrôle d'accès après avoir créé le partage NFS. Pour plus d'informations, consultez la rubrique *Modification des charges de travail de stockage*.

- a. Pour créer uniquement un partage CIFS, collectez les informations sur la liste de contrôle d'accès (ACL). Pour créer le partage CIFS, fournissez des valeurs valides pour les paramètres d'entrée suivants. Pour chaque groupe d'utilisateurs que vous attribuez, une ACL est créée lorsqu'un partage CIFS/SMB est provisionné. En fonction des valeurs que vous entrez pour le mappage ACL et Active Directory, le contrôle d'accès et le mappage sont déterminés pour le partage CIFS lors de sa création.

Une commande cURL avec des exemples de valeurs

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
  },
}
```

- b. Pour créer uniquement un partage de fichiers NFS, collectez les informations sur la politique d'exportation. Pour créer le partage de fichiers NFS, fournissez des valeurs valides pour les paramètres d'entrée suivants. En fonction de vos valeurs, la politique d'exportation est associée au partage de fichiers NFS lors de sa création.



Lors de l'approvisionnement du partage NFS, vous pouvez soit créer une politique d'exportation en fournissant toutes les valeurs requises, soit fournir la clé de politique d'exportation et réutiliser une politique d'exportation existante. Si vous souhaitez réutiliser une politique d'exportation pour la machine virtuelle de stockage, vous devez ajouter la clé de politique d'exportation. À moins que vous ne connaissiez la clé, vous pouvez récupérer la clé de la politique d'exportation en utilisant le `/datacenter/protocols/nfs/export-policies` API. Pour créer une nouvelle politique, vous devez saisir les règles telles qu'elles sont affichées dans l'exemple suivant. Pour les règles saisies, l'API tente de rechercher une politique d'exportation existante en faisant correspondre l'hôte, la machine virtuelle de stockage et les règles. S'il existe une politique d'exportation, elle est utilisée. Sinon, une nouvelle politique d'exportation est créée.

Une commande cURL avec des exemples de valeurs

```
"export_policy": {
  "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
  "name_tag": "ExportPolicyNameTag",
  "rules": [
    {
      "clients": [
        {
          "match": "0.0.0.0/0"
        }
      ]
    }
  ]
}
```

Après avoir configuré la liste de contrôle d'accès et la politique d'exportation, fournissez les valeurs valides pour les paramètres d'entrée obligatoires pour les partages de fichiers CIFS et NFS :



La politique d'efficacité du stockage est un paramètre facultatif pour la création de partages de fichiers.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTER	/storage-provider/file-shares

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le partage de fichiers que vous avez créé. . Vérifiez la création du partage de fichiers à l'aide de la clé d'objet Job renvoyée lors de l'interrogation du travail :

Catégorie	verbe HTTP	Chemin
serveur de gestion	OBTENIR	/management-server/jobs/{key}

À la fin de la réponse, vous voyez la clé du partage de fichiers créé.

```

],
"job_results": [
  {
    "name": "fileshareKey",
    "value": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
  }
],
"_links": {
  "self": {
    "href": "/api/management-server/jobs/06a6148bf9e862df:-2611856e:16e8d47e722:-7f87"
  }
}
}

```

1. Vérifiez la création du partage de fichiers en exécutant l'API suivante avec la clé renvoyée :

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/file-shares/{key}

Exemple de sortie JSON

Vous pouvez voir que la méthode POST de /storage-provider/file-shares appelle en interne toutes les API requises pour chacune des fonctions et crée l'objet. Par exemple, il invoque le /storage-provider/performance-service-levels/ API pour attribuer le niveau de service de performance sur le partage de fichiers.

```

{
  "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
  "name": "FileShare_377",
  "cluster": {
    "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
    "name": "AFFA300-206-68-70-72-74",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959"
      }
    }
  }
}

```



```

    },
    "svm": {
      "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
      "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
      "name": "RRT_ritu_vs1",
      "_links": {
        "self": {
          "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959"
        }
      }
    },
    "assigned_performance_service_level": {
      "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
      "name": "Value",
      "peak_iops": 75,
      "expected_iops": 75,
      "_links": {
        "self": {
          "href": "/api/storage-provider/performance-service-levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
        }
      }
    },
    "recommended_performance_service_level": {
      "key": null,
      "name": "Idle",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
    "space": {
      "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
      "key": null,
      "name": "Unassigned",
      "_links": {}
    },
    "access_control": {
      "acl": [
        {
          "user_or_group": "everyone",

```

```

        "permission": "read"
    }
],
"export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 1,
            "protocols": [
                "nfs3",
                "nfs4"
            ],
            "ro_rule": [
                "sys"
            ],
            "rw_rule": [
                "sys"
            ],
            "superuser": [
                "none"
            ]
        },
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 2,
            "protocols": [
                "cifs"
            ],
            "ro_rule": [
                "ntlm"
            ],
            "rw_rule": [

```

```

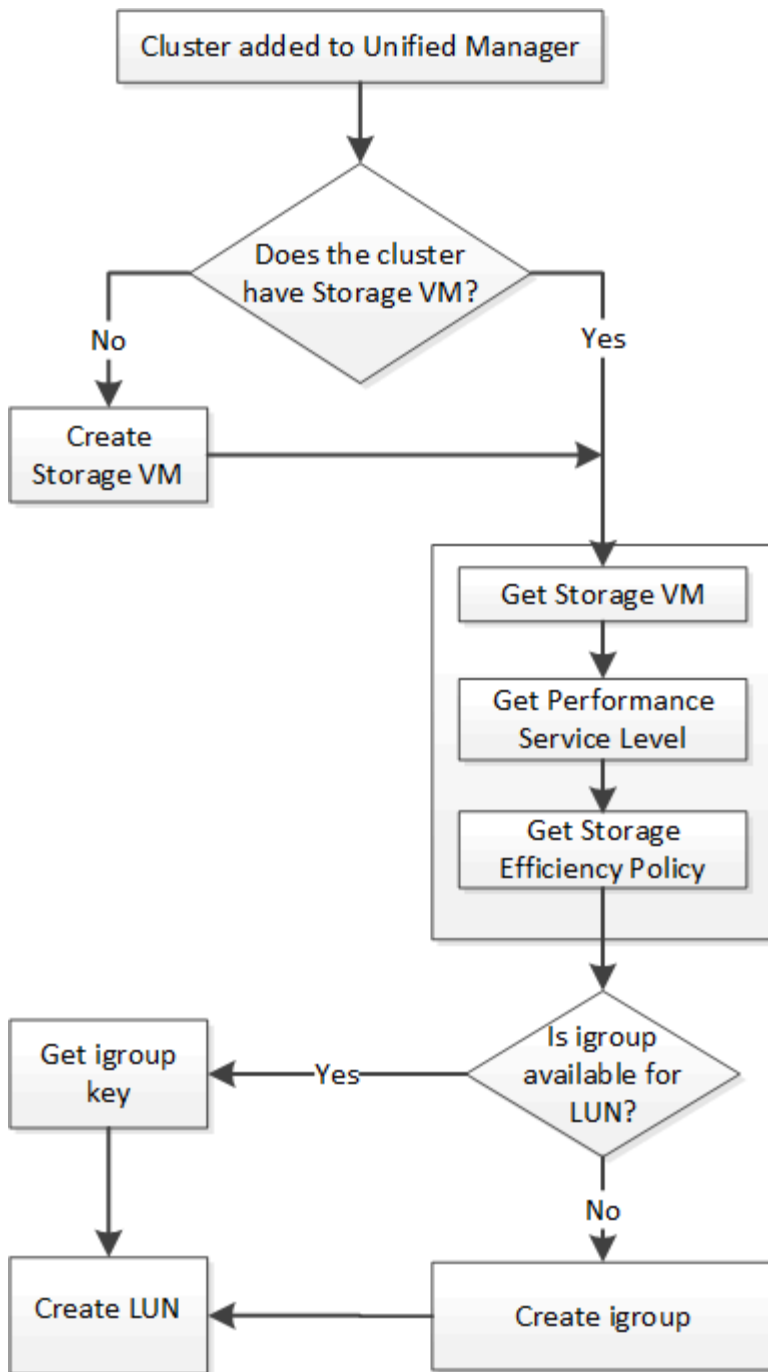
        "ntlm"
    ],
    "superuser": [
        "none"
    ]
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
}

```

Provisionner des LUN à l'aide d'API

Vous pouvez provisionner des LUN sur vos machines virtuelles de stockage (SVM) à l'aide des API de provisionnement fournies dans le cadre d'Active IQ Unified Manager. Ce flux de travail de provisionnement détaille les étapes de récupération des clés des SVM, des niveaux de service de performances et des politiques d'efficacité de stockage avant de créer le LUN.

Le diagramme suivant illustre les étapes d'un flux de travail de provisionnement de LUN.



Ce workflow suppose que les clusters ONTAP ont été ajoutés à Unified Manager et que la clé de cluster a été obtenue. Le workflow suppose également que les SVM ont déjà été créés sur les clusters.

1. Obtenez la clé SVM pour la SVM sur laquelle vous souhaitez créer le LUN, comme décrit dans la rubrique de workflow *Vérification des SVM sur les clusters*.
2. Obtenez la clé du niveau de service de performance en exécutant l'API suivante et en récupérant la clé à partir de la réponse.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/performance-service-levels



Vous pouvez récupérer les détails des niveaux de service de performance définis par le système en définissant le `system_defined` paramètre d'entrée à `true`. À partir de la sortie, obtenez la clé du niveau de service de performances que vous souhaitez appliquer sur le LUN.

- Vous pouvez également obtenir la clé de stratégie d'efficacité de stockage pour la stratégie d'efficacité de stockage que vous souhaitez appliquer sur le LUN en exécutant l'API suivante et en récupérant la clé à partir de la réponse.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/storage-efficiency-policies

- Déterminez si des groupes initiateurs (igroups) ont été créés pour accorder l'accès à la cible LUN que vous souhaitez créer.

Catégorie	verbe HTTP	Chemin
centre de données	OBTENIR	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

Vous devez saisir la valeur du paramètre pour indiquer le SVM pour lequel le groupe *i* a autorisé l'accès. De plus, si vous souhaitez interroger un igroup particulier, entrez le nom de l'igroup (clé) comme paramètre d'entrée.

- Dans la sortie, si vous pouvez trouver le groupe auquel vous souhaitez accorder l'accès, obtenez la clé. Sinon créez le igroup.

Catégorie	verbe HTTP	Chemin
centre de données	POSTE	/datacenter/protocols/san/igroups

Vous devez saisir les détails du groupe *i* que vous souhaitez créer, comme paramètres d'entrée. Il s'agit d'un appel synchrone et vous pouvez vérifier la création du groupe *i* dans la sortie. En cas d'erreur, un message s'affiche pour vous permettre de résoudre le problème et de réexécuter l'API.

- Créez le LUN.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTE	/storage-provider/luns

Pour créer le LUN, assurez-vous d'avoir ajouté les valeurs récupérées comme paramètres d'entrée obligatoires.



La politique d'efficacité du stockage est un paramètre facultatif pour la création de LUN.

Exemple de cURL

Vous devez saisir tous les détails du LUN que vous souhaitez créer, comme paramètres d'entrée.

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le LUN que vous avez créé.

- Vérifiez la création du LUN en utilisant la clé d'objet Job renvoyée lors de l'interrogation du Job :

Catégorie	verbe HTTP	Chemin
serveur de gestion	OBTENIR	/management-server/jobs/{key}

À la fin de la réponse, vous voyez la clé du LUN créé.

- Vérifiez la création du LUN en exécutant l'API suivante avec la clé renvoyée :

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/luns/{key}

Exemple de sortie JSON

Vous pouvez voir que la méthode POST de `/storage-provider/luns` appelle en interne toutes les API requises pour chacune des fonctions et crée l'objet. Par exemple, il invoque le `/storage-provider/performance-service-levels/` API pour l'attribution du niveau de service de performance sur le LUN.

== Étapes de dépannage en cas d'échec de création ou de mappage de LUN

Une fois ce workflow terminé, vous constaterez peut-être encore un échec dans la création de votre LUN. Même si le LUN est créé avec succès, le mappage du LUN avec l'igroup peut échouer en raison de l'indisponibilité d'un SAN LIF ou d'un point de terminaison d'accès sur le nœud sur lequel vous créez le LUN. En cas d'échec, vous pouvez voir le message suivant :

The nodes <node_name> and <partner_node_name> have no LIFs configured with the iSCSI or FCP protocol for Vserver <server_name>. Use the access-endpoints API to create a LIF for the LUN.

Suivez ces étapes de dépannage pour contourner cette panne.

1. Créez un point de terminaison d'accès prenant en charge le protocole iSCSI/FCP sur la SVM sur laquelle vous avez essayé de créer le LUN.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	POSTER	/storage-provider/access-endpoints

Exemple de cURL

Vous devez saisir les détails du point de terminaison d'accès que vous souhaitez créer, comme paramètres d'entrée.



Assurez-vous que dans le paramètre d'entrée, vous avez ajouté l'adresse pour indiquer le nœud d'origine du LUN et l'adresse ha pour indiquer le nœud partenaire du nœud d'origine. Lorsque vous exécutez cette opération, elle crée des points de terminaison d'accès sur le nœud d'origine et sur le nœud partenaire.

2. Interrogez le travail avec la clé d'objet Job renvoyée dans la sortie JSON pour vérifier qu'il a été exécuté avec succès pour ajouter les points de terminaison d'accès sur le SVM et que les services iSCSI/FCP ont été activés sur le SVM.

Catégorie	verbe HTTP	Chemin
serveur de gestion	OBTENIR	/management-server/jobs/{key}

Exemple de sortie JSON

À la fin de la sortie, vous pouvez voir la clé des points d'accès créés. Dans la sortie suivante, la valeur « name » : « accessEndpointKey » indique le point de terminaison d'accès créé sur le nœud d'origine du LUN, pour lequel la clé est 9c964258-14ef-11ea-95e2-00a098e32c28. La valeur « name » : « accessEndpointHAKey » indique le point de terminaison d'accès créé sur le nœud partenaire du nœud domestique, pour lequel la clé est 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modifiez le LUN pour mettre à jour le mappage igroup. Pour plus d'informations sur la modification du flux de travail, consultez « Modification des charges de travail de stockage ».

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/lun/{key}

Dans l'entrée, spécifiez la clé igroup avec laquelle vous souhaitez mettre à jour le mappage LUN, ainsi que la clé LUN.

Exemple de cURL

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier si le mappage est réussi.

4. Vérifiez le mappage LUN en interrogeant la clé LUN.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/luns/{key}

Exemple de sortie JSON

Dans la sortie, vous pouvez voir que le LUN a été correctement mappé avec l'igroup (clé d19ec2fa-fec7-11e8-b23d-00a098e32c28) avec lequel il a été initialement provisionné.

Modifier les charges de travail de stockage à l'aide d'API

La modification des charges de travail de stockage consiste à mettre à jour les LUN ou les partages de fichiers avec des paramètres manquants, ou à modifier les paramètres existants.

Ce flux de travail prend l'exemple de la mise à jour des niveaux de service de performances pour les LUN et les partages de fichiers.



Le flux de travail suppose que le LUN ou le partage de fichiers a été provisionné avec des niveaux de service de performances.

Modifier les partages de fichiers

Lors de la modification d'un partage de fichiers, vous pouvez mettre à jour les paramètres suivants :

- Capacité ou taille.
- Paramètre en ligne ou hors ligne.
- Politique d'efficacité du stockage.
- Niveau de service de performance.
- Paramètres de la liste de contrôle d'accès (ACL).
- Exporter les paramètres de politique. Vous pouvez également supprimer les paramètres de stratégie d'exportation et rétablir les règles de stratégie d'exportation par défaut (vides) sur le partage de fichiers.



Au cours d'une seule exécution d'API, vous ne pouvez mettre à jour qu'un seul paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performances à un partage de fichiers. Vous pouvez utiliser la même procédure pour mettre à jour toute autre propriété de partage de fichiers.

1. Obtenez la clé de partage CIFS ou de partage de fichiers NFS du partage de fichiers que vous souhaitez mettre à jour. Cette API interroge tous les partages de fichiers de votre centre de données. Ignorez cette

étape si vous connaissez déjà la clé de partage de fichiers.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/file-shares

- Affichez les détails du partage de fichiers en exécutant l'API suivante avec la clé de partage de fichiers que vous avez obtenue.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/file-shares/{key}

Affichez les détails du partage de fichiers dans la sortie.

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

- Obtenez la clé pour le niveau de service de performances que vous souhaitez attribuer sur ce partage de fichiers. Actuellement, aucune politique ne lui est attribuée.

Catégorie	verbe HTTP	Chemin
Niveaux de service de performance	OBTENIR	/storage-provider/performance-service-levels



Vous pouvez récupérer les détails des niveaux de service de performance définis par le système en définissant le `system_defined` paramètre d'entrée à `true`. À partir de la sortie, obtenez la clé du niveau de service de performances que vous souhaitez appliquer au partage de fichiers.

- Appliquez le niveau de service de performance sur le partage de fichiers.

Catégorie	verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	/storage-provider/file-shares/{key}

Dans l'entrée, vous devez spécifier uniquement le paramètre que vous souhaitez mettre à jour, ainsi que la

clé de partage de fichiers. Dans ce cas, il s'agit de la clé du Niveau de Service de Performance.

Exemple de cURL

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

La sortie JSON affiche un objet Job que vous pouvez utiliser pour vérifier si les points de terminaison d'accès sur les nœuds domestiques et partenaires ont été créés avec succès.

5. Vérifiez si le niveau de service de performances a été ajouté au partage de fichiers à l'aide de la clé d'objet Job affichée dans votre sortie.

Catégorie	verbe HTTP	Chemin
Serveur de gestion	OBTENIR	/management-server/jobs/{key}

Si vous interrogez par l'ID de l'objet Job, vous voyez si le partage de fichiers est mis à jour avec succès. En cas d'échec, résolvez le problème et exécutez à nouveau l'API. Une fois la création réussie, interrogez le partage de fichiers pour voir l'objet modifié :

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/file-shares/{key}

Affichez les détails du partage de fichiers dans la sortie.

```
"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}
```

Mettre à jour les LUN

Lors de la mise à jour d'un LUN, vous pouvez modifier les paramètres suivants :

- Capacité ou taille
- Paramètre en ligne ou hors ligne
- Politique d'efficacité du stockage
- Niveau de service de performance
- Carte LUN



Au cours d'une seule exécution d'API, vous ne pouvez mettre à jour qu'un seul paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performances à un LUN. Vous pouvez utiliser la même procédure pour mettre à jour n'importe quelle autre propriété LUN.

1. Obtenez la clé LUN du LUN que vous souhaitez mettre à jour. Cette API renvoie les détails de tous les LUN de votre centre de données. Ignorez cette étape si vous connaissez déjà la clé LUN.

Catégorie	verbe HTTP	Chemin
Fournisseur de stockage	OBTENIR	/storage-provider/luns

2. Affichez les détails du LUN en exécutant l'API suivante avec la clé LUN que vous avez obtenue.

Catégorie	verbe HTTP	Chemin
Fournisseur de stockage	OBTENIR	/storage-provider/luns/{key}

Afficher les détails du LUN dans la sortie. Vous pouvez voir qu'aucun niveau de service de performance n'est attribué à ce LUN.

Exemple de sortie JSON

```
"assigned_performance_service_level": {
  "key": null,
  "name": "Unassigned",
  "peak_iops": null,
  "expected_iops": null,
  "_links": {}
},
```

3. Obtenez la clé pour le niveau de service de performances que vous souhaitez attribuer au LUN.

Catégorie	verbe HTTP	Chemin
Niveaux de service de performance	OBTENIR	/storage-provider/performance-service-levels



Vous pouvez récupérer les détails des niveaux de service de performance définis par le système en définissant le `system_defined` paramètre d'entrée à `true`. À partir de la sortie, obtenez la clé du niveau de service de performances que vous souhaitez appliquer sur le LUN.

4. Appliquer le niveau de service de performance sur le LUN.

Catégorie	verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	/storage-provider/lun/{key}

Dans l'entrée, vous devez spécifier uniquement le paramètre que vous souhaitez mettre à jour, ainsi que la clé LUN. Dans ce cas, il s'agit de la clé du niveau de service de performance.

Exemple de cURL

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" } }"
```

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le LUN que vous avez mis à jour.

5. Affichez les détails du LUN en exécutant l'API suivante avec la clé LUN que vous avez obtenue.

Catégorie	verbe HTTP	Chemin
Fournisseur de stockage	OBTENIR	/storage-provider/luns/{key}

Afficher les détails du LUN dans la sortie. Vous pouvez voir que le niveau de service de performance est attribué à ce LUN.

Exemple de sortie JSON

```

"assigned_performance_service_level": {
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
  "name": "Value",
  "peak_iops": 75,
  "expected_iops": 75,
  "_links": {
    "self": {
      "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
    }
  }
}

```

Modifier un partage de fichiers NFS à l'aide d'API pour prendre en charge CIFS

Vous pouvez modifier un partage de fichiers NFS pour prendre en charge le protocole CIFS. Lors de la création d'un partage de fichiers, il est possible de spécifier à la fois les paramètres de la liste de contrôle d'accès (ACL) et les règles de politique d'exportation pour le même partage de fichiers. Toutefois, si vous souhaitez activer CIFS sur le même volume sur lequel vous avez créé un partage de fichiers NFS, vous pouvez mettre à jour les paramètres ACL sur ce partage de fichiers pour prendre en charge CIFS.

Avant de commencer

1. Un partage de fichiers NFS doit avoir été créé avec uniquement les détails de la politique d'exportation. Pour plus d'informations, voir *Gestion des partages de fichiers et Modification des charges de travail de stockage*.
2. Vous devez disposer de la clé de partage de fichiers pour exécuter cette opération. Pour plus d'informations sur l'affichage des détails du partage de fichiers et la récupération de la clé de partage de fichiers à l'aide de l'ID de tâche, voir *Provisionnement des partages de fichiers CIFS et NFS*.

Ceci s'applique à un partage de fichiers NFS que vous avez créé en ajoutant uniquement des règles de stratégie d'exportation et non des paramètres ACL. Vous modifiez le partage de fichiers NFS pour inclure les paramètres ACL.

Étapes

1. Sur le partage de fichiers NFS, effectuez une `PATCH` opération avec les détails ACL pour autoriser l'accès CIFS.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	/storage-provider/file-shares

Exemple de cURL

En fonction des privilèges d'accès que vous attribuez au groupe d'utilisateurs, comme indiqué dans l'exemple suivant, une ACL est créée et attribuée au partage de fichiers.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}
```

Exemple de sortie JSON

L'opération renvoie l'ID de tâche du travail qui exécute la mise à jour.

2. Vérifiez si les paramètres ont été ajoutés correctement en interrogeant les détails du partage de fichiers pour le même partage de fichiers.

Catégorie	verbe HTTP	Chemin
fournisseur de stockage	OBTENIR	/storage-provider/file-shares/{key}

Exemple de sortie JSON

```
"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ]
      }
    ]
  }
},
```

```

        "index": 1,
        "protocols": [
            "nfs3",
            "nfs4"
        ],
        "ro_rule": [
            "sys"
        ],
        "rw_rule": [
            "sys"
        ],
        "superuser": [
            "none"
        ]
    },
    {
        "anonymous_user": "65534",
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
},

```

```
    "_links": {  
      "self": {  
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-  
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-  
00a098dcc6b6"  
      }  
    }  
  }
```

Vous pouvez voir l'ACL attribuée avec la politique d'exportation au même partage de fichiers.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d’auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques 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

Une liste actuelle des brevets détenus par NetApp est disponible 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/)

Open source

Informations sur les droits d’auteur et les licences de tiers utilisés dans ce produit.

["Avis concernant Active IQ Unified Manager 9.16"](#)

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 DÉLICTELLE (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.