Documentation Active IQ Unified Manager

Active IQ Unified Manager 9.14

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-914/index.html on October 16, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation Active IQ Unified Manager . . . 1
Notes de mise à jour . . . 2
Commencez . . . 3
Instructions de démarrage rapide pour les installations VMware . . . 3
Configuration minimale requise . . . 3
Installation de Active IQ Unified Manager . . . 3
Instructions de démarrage rapide pour les installations Linux . . . 4
Configuration minimale requise . . . 4
Installation de Active IQ Unified Manager . . . 4
Instructions de démarrage rapide pour les installations Windows . . . 5
Configuration minimale requise . . . 5
Installation de Active IQ Unified Manager . . . 6
Installation de Unified Manager sur les systèmes VMware vSphere . . . 7
Introduction à Active IQ Unified Manager . . . 7
Rôle du serveur Unified Manager . . . 7
Présentation de la séquence d'installation . . . 7
Conditions requises pour l'installation de Unified Manager . . . 8
Configuration minimale requise pour l'infrastructure virtuelle et le système matériel . . . 8
Conditions requises pour le logiciel VMware et son installation . . . 10
Navigateurs pris en charge . . . 10
Exigences en matière de protocoles et de ports . . . 11
Remplir la fiche . . . 14
Installation, mise à niveau et suppression du logiciel Unified Manager . . . 16
Présentation du processus de déploiement . . . 16
Déployer Unified Manager . . . 17
Mise à niveau d'Unified Manager . . . 21
Redémarrage de la machine virtuelle Unified Manager . . . 24
Suppression de Unified Manager . . . 24
Installez Unified Manager sur les systèmes Linux . . . 26
Introduction à Active IQ Unified Manager . . . 26
Rôle du serveur Unified Manager . . . 26
Présentation de la séquence d'installation . . . 26
Conditions requises pour l'installation de Unified Manager . . . 27
Configuration minimale requise pour l'infrastructure virtuelle et le système matériel . . . 27
Conditions requises pour l'installation et le logiciel Linux . . . 29
Navigateurs pris en charge . . . 32
Exigences en matière de protocoles et de ports . . . 32
Remplir la fiche . . . 35
Installation, mise à niveau et suppression du logiciel Unified Manager . . . 36
Présentation du processus d'installation . . . 37
Configuration des référentiels logiciels requis . . . 37
Exigences SELinux sur les partages NFS et CIFS . . . 39
Installation de Unified Manager sur des systèmes Linux . . . 42

Mise à niveau de Unified Manager sur Red Hat Enterprise Linux ou CentOS . . . 49
Mise à niveau de produits tiers après l'installation de Unified Manager . . . 54
Redémarrage de Unified Manager . . . 55
Suppression de Unified Manager . . . 55
Suppression de l'utilisateur umadmin personnalisé et du groupe de maintenance . . . 56
Installation de Unified Manager sur les systèmes Windows . . . 57
Introduction à Active IQ Unified Manager . . . 57
Rôle du serveur Unified Manager . . . 57
Présentation de la séquence d'installation . . . 57
Conditions requises pour l'installation de Unified Manager . . . 58
Configuration minimale requise pour l'infrastructure virtuelle et le système matériel . . . 58
Conditions requises pour l'installation et le logiciel Windows . . . 60
Navigateurs pris en charge . . . 61
Exigences en matière de protocoles et de ports . . . 62
Remplir la fiche . . . 65
Installation, mise à niveau et suppression du logiciel Unified Manager . . . 67
Présentation du processus d'installation . . . 67
Installation de Unified Manager sous Windows . . . 68
Modification du mot de passe JBoss . . . 71
Chemin de mise à niveau pris en charge pour les versions de Unified Manager . . . 72
Mise à niveau d'Unified Manager . . . 73
Mise à niveau de produits tiers . . . 74
Redémarrage de Unified Manager . . . 75
Désinstallation d'Unified Manager . . . 76
Réaliser les tâches de configuration et d'administration . . . 78
Configuration d'Active IQ Unified Manager en cours . . . 78
Présentation de la séquence de configuration . . . 78
Accès à l'interface utilisateur Web de Unified Manager . . . 78
Configuration initiale de l'interface utilisateur Web de Unified Manager . . . 79
Ajout de clusters . . . 81
Configuration de Unified Manager pour envoyer des notifications d'alerte . . . 83
Modification du mot de passe de l'utilisateur local . . . 92
Définition du délai d'inactivité de la session . . . 93
Modification du nom d'hôte Unified Manager . . . 93
Activation et désactivation de la gestion du stockage basée sur des règles . . . 98
Configuration de la sauvegarde Unified Manager . . . 99
Gestion des paramètres des fonctions . . . 99
Permettre la gestion du stockage basée sur des règles . . . 100
Activation de la passerelle API . . . 100
Spécification du délai d'inactivité . . . 101
Activation des événements du portail Active IQ . . . 101
Activation et désactivation des paramètres de sécurité à des fins de conformité . . . 102
Activation et désactivation du téléchargement des scripts . . . 103
Ajout d'une bannière de connexion . . . 103
Utilisation de la console de maintenance . . . 103

Fonctionnalités offertes par la console de maintenance . . . 103
Rôle de l'utilisateur de maintenance . . . 104
Diagnostique des capacités utilisateur . . . 104
Accès à la console de maintenance . . . 104
Accès à la console de maintenance à l'aide de la console de machine virtuelle vSphere . . . 105
Menus de la console de maintenance . . . 106
Modification du mot de passe utilisateur de maintenance sous Windows . . . 111
Modification du mot de passe umadmin sur les systèmes Linux . . . 111
Changement des ports que Unified Manager utilise pour les protocoles HTTP et HTTPS . . . 112
Ajout d'interfaces réseau . . . 113
Ajout d'espace disque au répertoire de base de données Unified Manager . . . 113
Gestion de l'accès des utilisateurs . . . 117
Ajout d'utilisateurs . . . 117
Modification des paramètres utilisateur . . . 119
Affichage des utilisateurs . . . 119
Suppression d'utilisateurs ou de groupes . . . 119
En quoi consiste le RBAC . . . 120
Rôle du contrôle d'accès basé sur des rôles . . . 120
Définitions des types d'utilisateur . . . 120
Définitions des rôles utilisateur . . . 121
Fonctionnalités et rôles utilisateur de Unified Manager . . . 122
Gestion des paramètres d'authentification SAML . . . 124
Exigences du fournisseur d'identités . . . 124
Activation de l'authentification SAML . . . 126
Modification du fournisseur d'identités utilisé pour l'authentification SAML . . . 127
Mise à jour des paramètres d'authentification SAML après une modification du certificat de sécurité Unified Manager . . . 128
Désactivation de l'authentification SAML . . . 129
Désactivation de l'authentification SAML à partir de la console de maintenance . . . 130
Page authentification SAML . . . 130
Gestion de l'authentification . . . 131
Modification des serveurs d'authentification . . . 131
Suppression des serveurs d'authentification . . . 132
Authentification avec Active Directory ou OpenLDAP . . . 132
Consignation d'audits . . . 133
Page authentification à distance . . . 135
Gestion des certificats de sécurité . . . 139
Affichage du certificat de sécurité HTTPS . . . 139
Téléchargement d'une demande de signature de certificat HTTPS . . . 139
L'installation d'une autorité de certification a signé et renvoyé un certificat HTTPS . . . 140
Installation d'un certificat HTTPS généré à l'aide d'outils externes . . . 141
Descriptions des pages pour la gestion des certificats . . . 143
Surveillance et gestion du stockage . . . 146
Introduction à Active IQ Unified Manager . . . 146
Présentation de la surveillance de l'état de santé Active IQ Unified Manager . . . 146

Présentation de la surveillance des performances Active IQ Unified Manager . . . 147
Grâce aux API REST de Unified Manager . . . 148
Rôle du serveur Unified Manager . . . 148
Présentation de l'interface utilisateur . . . 149
Dispositions de fenêtre types . . . 149
Personnalisation de la disposition des fenêtres . . . 150
Utilisation de l'aide de Unified Manager . . . 151
Création de signets pour vos rubriques d'aide préférées . . . 152
Recherche d'objets de stockage . . . 152
Exportation des données de stockage sous forme de rapports . . . 153
Filtrage du contenu de la page d'inventaire . . . 155
Affichage des événements actifs à partir du signal sonore de notification . . . 156
Contrôle et gestion des clusters depuis le tableau de bord . . . 156
Page de tableau de bord . . . 157
Gestion des problèmes ou des fonctionnalités d'ONTAP directement à partir d'Unified Manager . . . 160
Gestion des clusters . . . 168
Fonctionnement du processus de détection du cluster . . . 168
Afficher la liste des clusters surveillés . . . 169
Ajout de clusters . . . 170
Modification des clusters . . . 172
Supprimer les clusters . . . 173
Détection des clusters à nouveau . . . 173
Surveillance de l'infrastructure virtuelle VMware . . . 174
Ce qui n'est pas pris en charge . . . 176
Affichage et ajout de vCenter Server . . . 177
Suppression de vCenter Server . . . 179
Surveillance des machines virtuelles . . . 179
Visualisation d'une infrastructure virtuelle dans une configuration de reprise après incident . . . 181
Provisionner et gérer les workloads . . . 183
Présentation des charges de travail . . . 184
Niveaux de services de performances . . . 191
Gestion des règles d'efficacité du stockage . . . 198
Gestion et contrôle des configurations MetroCluster . . . 200
Comportement des volumes lors du basculement et du rétablissement . . . 201
Définitions d'état de la connectivité des clusters pour la configuration MetroCluster over FC . . . 203
Définitions de l'état de la mise en miroir des données pour MetroCluster sur FC . . . 204
Contrôle des configurations MetroCluster . . . 204
Contrôle de la réplication MetroCluster . . . 207
Gestion des quotas . . . 208
Quelles sont les limites des quotas . . . 208
Affichage des quotas d'utilisateurs et de groupes d'utilisateurs . . . 208
Création de règles pour générer des adresses e-mail . . . 209
Création d'un format de notification par e-mail pour les quotas d'utilisateurs et de groupes d'utilisateurs . . . 210
Modification des adresses e-mail des quotas d'utilisateur et de groupe . . . 210

En savoir plus sur les quotas . . . 211
Description des boîtes de dialogue quotas . . . 212
Dépannage . . . 215
Ajout d'espace disque au répertoire de base de données Unified Manager . . . 215
Modification de l'intervalle de collecte des statistiques de performances . . . 219
Modification de la durée pendant laquelle Unified Manager conserve les données relatives aux événements et aux performances . . . 220
Erreur d'authentification inconnue . . . 221
Utilisateur introuvable . . . 221
Problème d'ajout de LDAP à l'aide d'autres services d'authentification . . . 221
Gestion des événements et des alertes . . . 223
Gestion des événements . . . 223
Sont les événements sur la plateforme Active IQ . . . 223
Quels sont les événements Event Management System . . . 223
Que se passe-t-il lorsqu'un événement est reçu . . . 229
Affichage des événements et des détails des événements . . . 231
Affichage des événements non assignés . . . 231
Confirmation et résolution des événements . . . 231
Attribution d'événements à des utilisateurs spécifiques . . . 232
Désactivation des événements indésirables . . . 233
Résolution des problèmes à l'aide de la correction automatique de Unified Manager . . . 234
Activation et désactivation du reporting des événements Active IQ . . . 235
Téléchargement d'un nouveau fichier de règles Active IQ . . . 236
Génération des événements de la plateforme Active IQ . . . 237
Résoudre les événements relatifs à la plateforme Active IQ . . . 237
Configuration des paramètres de conservation des événements . . . 238
Qu'est-ce qu'une fenêtre de maintenance Unified Manager . . . 238
Gestion des événements de ressources du système hôte . . . 241
Présentation des événements . . . 241
Liste des événements et types de gravité . . . 247
Description des fenêtres d'événement et des boîtes de dialogue . . . 309
Gestion des alertes . . . 322
Quelles sont les alertes . . . 322
Les informations contenues dans un e-mail d'alerte . . . 322
Ajout d'alertes . . . 323
Ajout d'alertes en cas d'événements de performances . . . 326
Test des alertes . . . 327
Activation et désactivation des alertes pour les événements résolus et Obsolète . . . 327
Exclusion de volumes de destination de reprise après incident de la génération des alertes . . . 328
Affichage des alertes . . . 329
Modification des alertes . . . 329
Suppression des alertes . . . 330
Description des fenêtres d'alerte et des boîtes de dialogue . . . 330
Gestion des scripts . . . 336
Fonctionnement des scripts avec les alertes . . . 336

Ajout de scripts . . . 337
Suppression de scripts . . . 338
Exécution du script de test . . . 339
Commandes CLI Unified Manager prises en charge . . . 339
Description des fenêtres de script et des boîtes de dialogue . . . 345
Contrôle et gestion des performances du cluster . . . 347
Présentation de la surveillance des performances Active IQ Unified Manager . . . 347
Fonctionnalités de contrôle des performances de Unified Manager . . . 347
Interfaces Unified Manager utilisées pour gérer les performances du système de stockage . . . 348
Activité de collecte des données sur la configuration et les performances du cluster . . . 348
Qu'est-ce qu'un cycle de collecte de continuité des données . . . 350
Signification de l'horodatage dans les données et les événements collectées . . . 351
Navigation dans les workflows de performances dans l'interface graphique d'Unified Manager . . . 351
Connexion à l'interface utilisateur . . . 352
Interface graphique et chemins de navigation . . . 352
Recherche d'objets de stockage . . . 358
Filtrage du contenu de la page d'inventaire . . . 359
Contrôle des performances du cluster depuis le tableau de bord . . . 361
Comprendre les panneaux de performances du tableau de bord . . . 361
Messages de bannière et descriptions de performances . . . 362
Modification de l'intervalle de collecte des statistiques de performances . . . 362
Dépannage des charges de travail à l'aide de l'analyseur de workloads . . . 363
Données affichées par l'analyseur de flux de travail . . . 364
Quand utiliser l'analyseur de charge de travail . . . 366
Utilisation de l'analyseur de flux de production . . . 366
Contrôle des performances des clusters à partir de la page d'accueil Performance Cluster . . . 366
Comprendre la page d'accueil de Performance Cluster . . . 367
Page d'accueil Performance Cluster . . . 367
Surveillance des performances à l'aide des pages d'inventaire des performances . . . 372
Affichage des pages d'inventaire des performances pour tous les objets de stockage . . . 373
Raffinage du contenu de la page d'inventaire des performances . . . 379
Comprendre les recommandations d'Unified Manager concernant le Tiering des données dans le cloud . . . 381
Contrôle des performances à l'aide des pages de l'explorateur de performances . . . 383
Présentation de l'objet racine . . . 383
Appliquer le filtrage pour réduire la liste des objets corrélés dans la grille . . . 383
Spécification d'une plage de temps pour les objets corrélés . . . 383
Définition de la liste des objets corrélés pour le graphique de comparaison . . . 385
Présentation des graphiques des compteurs . . . 386
Types de graphiques de compteur de performances . . . 387
Sélectionnez les graphiques de performances à afficher . . . 391
Développement du volet compteurs . . . 391
Modification de la mise au point des compteurs sur une période de temps plus courte . . . 392
Affichage des détails d'un événement dans la chronologie des événements . . . 392
Vue Zoom des diagrammes de compteur . . . 393

Affichage de la latence de volume par composant du cluster . . . 395
Affichage du trafic des IOPS du SVM par protocole . . . 396
Affichage des graphiques de latence des volumes et des LUN pour vérifier la performance garantie . . . 397
Affichage des performances de tous les clusters de baies SAN . . . 397
Affichage des IOPS du nœud en fonction des workloads qui ne résident que sur le nœud local . . . 398
Composants des pages d'arrivée d'objet . . . 399
Gestion des performances à l'aide des informations de groupe de règles de QoS . . . 405
Comment la QoS du stockage peut contrôler le débit des workloads . . . 405
Affichage de tous les groupes de règles de QoS disponibles sur tous les clusters . . . 406
Affichage des volumes ou des LUN qui appartiennent au même groupe de règles de QoS . . . 406
Affichage des paramètres de « policy group » QoS appliqués à des volumes ou LUN spécifiques . . . 407
Affichage des graphiques de performances pour comparer les volumes ou les LUN qui se trouvent dans le même groupe de règles de QoS . . . 408
Affichage des différents types de règles de QoS dans les graphiques de débit . . . 408
Affichage des paramètres minimal et maximal de QoS des charges de travail dans l'explorateur de performances . . . 410
Gestion des performances grâce à la capacité en termes de performances et aux informations d'IOPS disponibles . . . 411
Quelle est la capacité des performances utilisée . . . 412
Signification de la capacité en termes de performances utilisée . . . 413
Les IOPS disponibles . . . 414
Affichage des valeurs de capacité des nœuds et des performances des agrégats utilisées . . . 415
Affichage des valeurs d'IOPS disponibles du nœud et de l'agrégat . . . 416
Affichage des graphiques des compteurs de capacité de performances pour identifier les problèmes . . . 416
Conditions du seuil de performance utilisé par la capacité de performance . . . 418
Utilisation du compteur de performances utilisé pour gérer les performances . . . 419
Présentation et utilisation de la page planification du basculement de nœud . . . 419
Utilisation de la page planification de basculement de nœud pour déterminer les actions correctives . . . 420
Composants de la page planification de basculement de nœud . . . 420
Utilisation d'une stratégie de seuil avec la page planification du basculement de nœud . . . 422
Utilisation du tableau d'analyse de la capacité sur les performances utilisée pour la planification du basculement . . . 422
Collecte des données et contrôle des performances des workloads . . . 424
Types de charges de travail surveillés par Unified Manager . . . 424
Valeurs de mesure des performances des charges de travail . . . 425
Parmi les performances attendues . . . 427
Mode d'utilisation de la prévision de latence dans l'analyse des performances . . . 428
Comment Unified Manager utilise une latence de charge de travail pour identifier les problèmes de performance . . . 429
Comment les opérations d'un cluster peuvent affecter la latence des charges de travail . . . 430
Contrôle des performances des configurations MetroCluster . . . 431
Présentation des événements de performances et des alertes . . . 432
Sources des événements de performance . . . 432
Types de sévérité des événements de performance . . . 433
Modifications de configuration détectées par Unified Manager . . . 434

Types de règles de seuils de performance définies par le système . . . 434
Analyse et notification des événements de performance . . . 437
Comment Unified Manager détermine l'impact sur les performances d'un événement . . . 439
Les composants du cluster et les conflits . . . 440
Rôles des charges de travail impliquées dans un événement de performance . . . 442
Gestion des seuils de performances . . . 443
Fonctionnement des règles de seuil de performances définies par l'utilisateur . . . 444
Que se passe-t-il lorsqu'une règle de seuil de performances est enfreinte . . . 446
Quels compteurs de performances peuvent être suivis à l'aide de seuils . . . 446
Quels objets et compteurs peuvent être utilisés dans les stratégies de seuils de combinaison . . . 449
Création de règles de seuils de performance définies par l'utilisateur . . . 449
Assignation de règles de seuil de performances aux objets de stockage . . . 451
Affichage des règles de seuils de performances . . . 452
Modification des règles de seuils de performances définies par l'utilisateur . . . 452
Suppression des règles de seuil de performances des objets de stockage . . . 453
Que se passe-t-il lorsqu'une règle de seuil de performances est modifiée . . . 454
Que se passe-t-il aux règles de seuils de performances lorsqu'un objet est déplacé . . . 454
Analyse des événements de performances . . . 455
Affichage des informations relatives aux événements de performances . . . 455
Analyse des événements à partir de seuils de performances définis par l'utilisateur . . . 456
Analyse des événements à partir de seuils de performances définis par le système . . . 457
Analyse des événements à partir de seuils de performances dynamiques . . . 463
Résoudre les événements de performances . . . 471
Confirmation que la latence se trouve dans la plage prévue . . . 471
Examinez l'impact des modifications de configuration sur les performances des charges de travail . . . 472
Possibilité d'améliorer les performances des charges de travail côté client . . . 472
Vérifiez si le client ou le réseau ne présentent pas de problème . . . 472
Vérifier si les autres volumes du groupe de règles de QoS ont une activité particulièrement élevée . . . 473
Déplacement des interfaces logiques . . . 473
Exécutez les opérations d'efficacité du stockage à un moment moins occupé . . . 474
Ajouter des disques et réaffecter des données . . . 475
Comment l'activation de Flash cache sur un nœud peut améliorer les performances des charges de travail . . . 475
Comment l'activation de Flash Pool sur un agrégat de stockage peut améliorer les performances des charges de travail . . . 476
Vérification de l'état de la configuration MetroCluster . . . 476
Vérification de la configuration MetroCluster . . . 477
Déplacement des charges de travail vers un autre agrégat . . . 477
Déplacement des workloads vers un nœud différent . . . 479
Déplacement des charges de travail vers un agrégat sur un autre nœud . . . 480
Déplacement des workloads vers un nœud dans une autre paire haute disponibilité . . . 482
Déplacement des workloads vers un autre nœud dans une paire haute disponibilité différente . . . 483
Utilisez les paramètres de règles de QoS pour hiérarchiser le travail sur ce nœud . . . 485
Supprimez les volumes et les LUN inactifs . . . 486
Ajout de disques et reconstruction des agrégats . . . 486

Configuration d'une connexion entre un serveur Unified Manager et un fournisseur de données externe . 487
Données de performances qui peuvent être envoyées à un serveur externe . . . 487
Configuration de Graphite pour recevoir les données de performances par Unified Manager . . . 488
Configuration d'une connexion à partir d'un serveur Unified Manager vers un fournisseur de données externe . . . 489
Contrôlez et gérez l'état du cluster . . . 492
Présentation de la surveillance de l'état de santé Active IQ Unified Manager . . . 492
Capacité physique et logique . . . 492
Unités de mesure de la capacité . . . 492
Fonctionnalités de contrôle de l'état de santé de Unified Manager . . . 493
Les interfaces Unified Manager utilisées pour gérer l'état du système de stockage . . . 494
Gestion et contrôle de l'état des clusters et des objets du cluster . . . 495
Présentation du contrôle des clusters . . . 495
Affichage de la liste et des détails des clusters . . . 497
Vérification de l'état de santé des clusters dans une configuration MetroCluster . . . 497
Affichage de l'état de santé et de capacité de tous les clusters de baies SAN . . . 499
Affichage de la liste des nœuds et des détails . . . 500
Génération d'un rapport d'inventaire du matériel pour le renouvellement du contrat . . . 501
Affichage de la liste des VM de stockage et des détails . . . 501
Affichage de la liste des agrégats et des détails . . . 502
Affichage des informations de capacité FabricPool . . . 503
Affichage des détails du pool de stockage . . . 504
Affichage de la liste des volumes et des détails . . . 504
Affichage des détails sur les partages NFS . . . 505
Affichage des détails sur les partages SMB/CIFS . . . 506
Affichage de la liste des copies Snapshot . . . 507
Suppression des copies Snapshot . . . 507
Calcul de l'espace récupérable pour les copies Snapshot . . . 508
Description des fenêtres et boîtes de dialogue d'objets de cluster . . . 509
Tâches et workflows d'état de Unified Manager communs . . . 509
Surveillance et résolution des problèmes de disponibilité des données . . . 510
Résoudre les problèmes de capacité . . . 517
Gestion des seuils de santé . . . 519
Gestion des objectifs de sécurité des clusters . . . 524
La gestion des opérations de sauvegarde et de restauration . . . 537
Gestion des scripts . . . 554
Gestion et suivi des groupes . . . 558
Hiérarchiser les événements d'objet de stockage à l'aide d'annotations . . . 567
Envoi d'un bundle via l'interface utilisateur Web et la console de maintenance . . . 576
Tâches et informations relatives à plusieurs flux de travail . . . 583
Protégez et restaurez les données . . . 642
Création, surveillance et résolution des problèmes de relations de protection . . . 642
Types de protection SnapMirror . . . 642
Configuration des relations de protection dans Unified Manager . . . 644
Effectuer un basculement et un retour arrière de la relation de protection . . . 646

Résolution de l'échec d'une tâche de protection . . . 650
Résolution des problèmes de décalage . . . 654
Gestion et surveillance des relations de protection . . . 655
Affichage de l'état de protection du volume . . . 656
Affichage des relations de protection des volumes . . . 658
Contrôle des LUN dans une relation de groupe de cohérence . . . 659
Création d'une relation de protection SnapVault depuis la vue Santé : tous les volumes . . . 659
Création d'une relation de protection SnapVault à partir de la page des détails du volume / intégrité . . . 661
Création d'une relation de protection SnapMirror depuis la vue Santé : tous les volumes . . . 661
Création d'une relation de protection SnapMirror à partir de la page des détails du volume / intégrité . . . 663
Création d'une relation SnapMirror avec la réplication flexible de la version . . . 664
Création de relations SnapMirror avec la réplication flexible de la version avec l'option de sauvegarde 665
Configuration des paramètres d'efficacité de la destination . . . 666
Création de planifications SnapMirror et SnapVault . . . 667
Création de relations en cascade ou en sortie pour étendre la protection à partir d'une relation de protection existante . . . 667
Modification des relations de protection à partir de la page relations de volume . . . 668
Modification des relations de protection à partir de la page Détails du volume/intégrité . . . 669
Création d'une règle SnapMirror pour optimiser l'efficacité du transfert . . . 669
Création d'une règle SnapVault pour optimiser l'efficacité du transfert . . . 670
Abandon d'un transfert actif de protection des données à partir de la page relations de volume . . . 671
Abandon d'un transfert actif de protection des données à partir de la page Détails du volume/intégrité 671
Mise en veille d'une relation de protection à partir de la page relations de volume . . . 672
Mise au repos d'une relation de protection à partir de la page Volume / informations d'intégrité . . . 673
Rompre une relation SnapMirror depuis la page Volume relations . . . 674
Suppression d'une relation de protection de la page relations de volume . . . 674
Reprise des transferts programmés sur une relation mise en veille à partir de la page de relations de volume . . . 675
Reprise des transferts programmés sur une relation mise en veille à partir de la page Volume / informations de santé . . . 676
Initialisation ou mise à jour des relations de protection à partir de la page relations de volume . . . 676
Initialisation ou mise à jour des relations de protection à partir de la page Détails du volume/intégrité . . . 677
Resynchronisation des relations de protection à partir de la page Volume relations . . . 678
Inversion des relations de protection à partir de la page relations de volume . . . 679
Restauration des données à l'aide des pages de détails Volume et Volume/intégrité . . . 680
En quoi sont les pools de ressources . . . 681
Création de pools de ressources . . . 682
Modification de pools de ressources . . . 682
Affichage de l'inventaire des pools de ressources . . . 683
Ajout de membres de pool de ressources . . . 683
Suppression d'agrégats des pools de ressources . . . 684
Suppression de pools de ressources . . . 684
Surveiller les relations de protection contre les reprises après incident des machines virtuelles de stockage . . . 685
Présentation des associations d'ordinateurs virtuels de stockage . . . 687

Les exigences en termes de SVM et de pool de ressources pour prendre en charge les services de stockage . . . 689
Quels sont les emplois . . . 690
Surveillance des tâches . . . 690
Affichage des détails du travail . . . 691
Abandon des travaux . . . 691
Nouvelle tentative d'échec d'une tâche de protection . . . 691
Description des fenêtres et boîtes de dialogue protection relations . . . 692
Générer des rapports personnalisés . . . 735
Création de rapports Unified Manager . . . 735
Points d'accès pour générer des rapports . . . 735
Présentation des rapports . . . 737
Comprendre la relation de vue et de rapport . . . 737
Types de rapports . . . 738
Limites de la création de rapports . . . 740
Utilisation des rapports . . . 740
Flux de travail des rapports . . . 740
Création rapide de rapports . . . 741
Recherche d'un rapport planifié . . . 744
Personnalisation des rapports . . . 744
Téléchargement de rapports . . . 748
Planification des rapports . . . 748
Planification d'un rapport . . . 749
Gestion des planifications de rapports . . . 751
Exemples de rapports personnalisés . . . 753
Personnalisation des rapports de stockage de cluster . . . 754
Personnalisation des rapports de capacité d'agrégats . . . 757
Personnalisation des rapports de capacité de volume . . . 759
Personnalisation des rapports de capacité qtree . . . 762
Personnalisation des rapports de partage NFS . . . 763
Personnalisation des rapports sur les machines virtuelles de stockage . . . 765
Personnalisation des rapports de relation de volume . . . 766
Personnalisation des rapports de performances des volumes . . . 770
Exemples de rapports Microsoft Excel . . . 771
Création d'un rapport pour afficher une table et un graphique de capacité d'agrégat . . . 772
Création d'un rapport pour afficher le total des agrégats par rapport aux graphiques de capacité disponible . . . 774
Création d'un rapport pour afficher les graphiques de capacité de volume disponibles . . . 778
Créez un rapport pour afficher les agrégats dont les IOPS sont les plus disponibles . . . 780
Gérer le stockage à l'aide des API REST . . . 783
Mise en route des API REST de Active IQ Unified Manager . . . 783
Public visé par ce contenu . . . 783
Accès et catégories à l'API Active IQ Unified Manager . . . 783
Services REST proposés en Active IQ Unified Manager . . . 785
Version de l'API dans Active IQ Unified Manager . . . 786

Ressources de stockage dans ONTAP . . . 786
Accès à l'API REST et authentification dans Active IQ Unified Manager . . . 787
Authentification . . . 789
Codes d'état HTTP utilisés dans Active IQ Unified Manager . . . 790
Recommandations pour l'utilisation des API pour Active IQ Unified Manager . . . 791
Journaux pour le dépannage . . . 792
Processus asynchrones des objets de travail . . . 792
Bonjour serveur API . . . 793
API REST Unified Manager . . . 797
Gestion des objets de stockage dans un data Center à l'aide d'API . . . 798
Accès aux API ONTAP via un accès proxy . . . 805
Exécution des tâches administratives à l'aide d'API . . . 808
Gestion des utilisateurs à l'aide d'API . . . 810
Affichage des metrics de performances à l'aide d'API . . . 811
Affichage des travaux et des détails du système . . . 822
Gestion des événements et des alertes à l'aide d'API . . . 823
Gestion des workloads à l'aide d'API . . . 826
Workflows API communs pour la gestion du stockage . . . 835
Présentation des appels API utilisés dans les workflows . . . 835
Détermination des problèmes d'espace dans les agrégats à l'aide d'API . . . 836
Détermination des problèmes dans les objets de stockage à l'aide des API d'événements . . . 837
Dépannage des volumes ONTAP à l'aide d'API de passerelle . . . 838
Des workflows API pour la gestion des workloads . . . 843
Mentions légales . . . 870
Droits d'auteur . . . 870
Marques déposées . . . 870
Brevets . . . 870
Politique de confidentialité . . . 870
Source ouverte . . . 870

Documentation Active IQ Unified Manager

Notes de mise à jour

Le fournit un résumé des nouvelles fonctionnalités, des limites et des problèmes connus de Active IQ Unified Manager 9.14.

Pour plus d'informations, voir "Notes de version de Active IQ Unified Manager".

Commencez

Instructions de démarrage rapide pour les installations VMware

Vous pouvez télécharger le `.tar` fichier qui contient un certificat racine, un `README` fichier et un `OVA` fichier, puis déployer Unified Manager en tant qu'appliance virtuelle.

Configuration minimale requise

- Système d'exploitation : VMware ESXi 7.0 et 8.0
- RAM : 12 GO
- CPU : 9572 MHz au total
- Espace disque libre : 5 Go (provisionnement fin), 152 Go (provisionnement lourd)

Pour obtenir des informations détaillées sur la configuration système requise, reportez-vous aux sections "Conditions requises pour l'installation de Unified Manager"et "Matrice d'interopérabilité".

Installation de Active IQ Unified Manager

Téléchargez le programme d'installation

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

Vérification de l'intégrité

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

Installez Unified Manager

1. Dans vSphere client, 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. Dans la section Éditeur de la page Détails de révision, le message `Entrust Code Signing - OVCS2 (Trusted certificate)` confirme l'intégrité du fichier téléchargé `OVA`. 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, remplissez les champs requis pour le type d'installation que vous effectuez :
   - Pour la configuration statique, entrez les informations requises dans tous les champs. L'ajout d'informations pour le champ **DNS secondaire** n'est pas nécessaire.
   - 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 un autre champ.

5. Mise sous tension de la machine virtuelle
6. Cliquez sur l’onglet Console pour afficher le processus de démarrage initial.
7. Configurer le fuseau horaire.
8. Entrez un nom d’utilisateur et un mot de passe pour la maintenance Unified Manager.

À la fin de l’installation, les informations de connexion à l’interface utilisateur Web de Unified Manager sont affichées.

Instructions de démarrage rapide pour les installations Linux

Vous pouvez télécharger le pack d’installation et installer Unified Manager sur une plateforme Red Hat Enterprise Linux ou CentOS physique ou virtuelle.

Configuration minimale requise

- Système d’exploitation : Red Hat Enterprise Linux versions 7.x et 8.0 à 8.9, ou CentOS version 7.x basé sur l’architecture x86_64, installé à l’aide de l’environnement de base « serveur avec interface utilisateur graphique » de l’option **Software Selection** du programme d’installation du système d’exploitation
- RAM : 12 Go, CPU : 9572 MHz au total
- Espace disque disponible : 100 Go d’espace disque dans le `/opt/netapp/data` répertoire, 50 Go dans la partition racine. Pour les répertoires et `/var/log` montés séparément `/opt`, assurez-vous que `/opt` dispose de 15 Go, `/var/log` de 16 Go et `/tmp` de 10 Go d’espace libre.

Pour obtenir des informations détaillées sur la configuration système requise et sur l’installation du produit sur un site sécurisé, reportez-vous aux sections "Conditions requises pour l’installation de Unified Manager"et "Matrice d’interopérabilité".

Installation de Active IQ Unified Manager

Téléchargez le programme d’installation

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

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

Vérification de l’intégrité

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

- Exécutez `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` pour créer un fichier avec la clé publique à partir du certificat de signature de code.

- Exécutez `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` pour vérifier la signature sur le package d'installation.

Vérifiez la configuration du référentiel

Les procédures de configuration des référentiels Red Hat Enterprise Linux ou CentOS 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 les instructions de configuration des référentiels Red Hat Enterprise Linux ou CentOS.

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

Installez Unified Manager

Unified Manager utilise l' `yum`utilitaire pour installer le logiciel et les logiciels qui en dépendent. Étant donné qu'il existe différentes images de Red Hat Enterprise Linux ou CentOS, les packages installés dépendent du logiciel présent dans les images. `yum`L'utilitaire détermine les progiciels dépendants à installer. Si vous avez besoin de plus d'informations sur les progiciels dépendants, consultez le "Conditions requises pour l'installation et le logiciel Linux".

Pour installer Unified Manager, exécutez la commande suivante, en tant qu'utilisateur root ou en utilisant `sudo`, dans le 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 de connexion à l'interface utilisateur Web de Unified Manager sont affichées. Si vous ne parvenez pas à vous connecter à l'interface utilisateur Web, reportez-vous au `README` fichier fourni avec le logiciel pour plus d'informations sur les restrictions de port 443.

Instructions de démarrage rapide pour les installations Windows

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

Configuration minimale requise

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

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

  - Anglais

    - 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 obtenir des informations détaillées sur la configuration système requise, reportez-vous aux sections "Conditions requises pour l'installation de Unified Manager"et "Matrice d'interopérabilité".

Installation de Active IQ Unified Manager

Téléchargez le programme d'installation

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

Installez Unified Manager

Pour installer Unified Manager, assurez-vous que Microsoft .NET 4.5.2 ou une version ultérieure est installée. Dans le cadre du processus d'installation, Unified Manager installe d'autres modules tiers, le cas échéant. Pour plus d'informations sur les progiciels dépendants, reportez-vous au "Conditions requises pour l'installation et le logiciel Windows".

1. Connectez-vous à Windows à l'aide du compte d'administrateur local par défaut.
2. Dans le répertoire dans lequel 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, entrez le nom d'utilisateur et le mot de passe pour créer l'utilisateur de maintenance Unified Manager.
4. Dans l'Assistant connexion à la base de données, saisissez le mot de passe racine MySQL.
5. Suivez les autres invites pour terminer l'installation.
6. Cliquez sur **Finish** à la fin de l'installation et l'interface utilisateur Web Unified Manager s'affiche.

Installation de 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 seule interface. Unified Manager peut être déployé sur un serveur Linux, sur un serveur Windows ou en tant que dispositif virtuel sur un hôte VMware.

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

Informations connexes

"Matrice d'interopérabilité NetApp"

Rôle du serveur Unified Manager

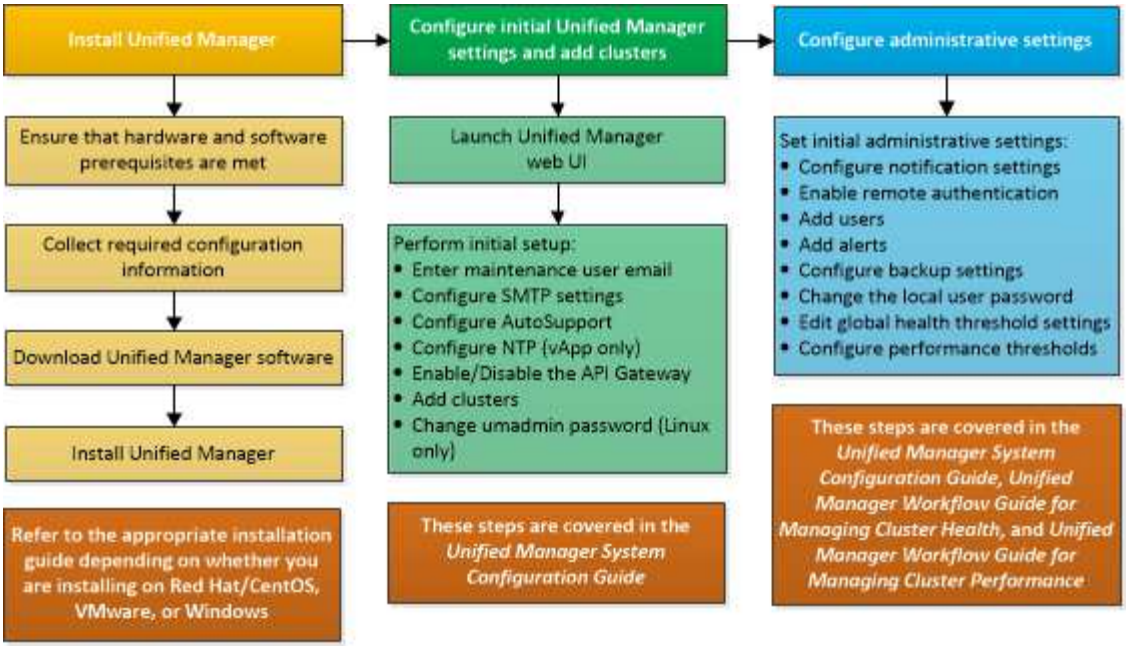
L'infrastructure de serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la détection, la surveillance, le contrôle d'accès basé sur des rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations sur le cluster, stocke les données dans la base de données et analyse ces données afin de voir en cas de problème au niveau du cluster.

Présentation de la séquence d'installation

Le workflow d'installation décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.

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



Conditions requises pour l'installation de 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 logiciels, de matériel, de processeur et de mémoire.

NetApp ne prend pas en charge les modifications du code de l'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 d'informations sur l'application de 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 "Matrice d'interopérabilité NetApp"

Configuration minimale requise pour l'infrastructure virtuelle et le système matériel

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

Le tableau suivant affiche les valeurs recommandées pour les ressources mémoire, processeur et espace disque. Ces valeurs ont été qualifiées pour permettre à Unified Manager de satisfaire à des niveaux de performances acceptables.

Configuration matérielle	Paramètres recommandés
RAM	12 Go (minimum requis : 8 Go)
Processeurs	4 processeurs
Capacité du cycle du processeur	9572 MHz au total (exigence minimale : 9572 MHz)
Espace disque disponible	• 5 Go (provisionnement fin) • 152 Go (provisionnement lourd)

Unified Manager peut être installé sur des systèmes disposant d'une petite quantité de mémoire, mais les 12 Go recommandés de RAM garantissent qu'un volume suffisant de mémoire est disponible pour des performances optimales de façon à ce que le système puisse prendre en charge des clusters et des objets de stockage supplémentaires à mesure que votre configuration évolue. Vous ne devez pas définir de limites de mémoire sur la machine virtuelle où Unified Manager est déployé, et ne devez pas activer de fonctions (par exemple, l'option de création de bulles) qui empêchent le logiciel d'utiliser la mémoire allouée au système.

De plus, le nombre de nœuds qu'une seule instance de Unified Manager peut contrôler avant d'installer une deuxième instance de Unified Manager est limité. Pour plus d'informations, voir "Guide des meilleures pratiques de Unified Manager".

Les échanges de pages mémoire ont un impact négatif sur les performances du système et de l'application de gestion. La concurrence pour les ressources de processeur indisponibles en raison de l'utilisation globale de l'hôte peut dégrader les performances.

Exigence pour une 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 de Unified Manager.

Besoins en espace pour les sauvegardes

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

Conditions requises pour la connectivité hôte

Le système physique ou virtuel sur lequel vous installez Unified Manager doit être configuré de manière à ce que le nom d'hôte puisse être correctement `ping` attribué à l'hôte lui-même. En cas de configuration IPv6, vérifiez que `ping6` le nom d'hôte a réussi pour vous assurer 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 pendant le déploiement, vous avez 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 du DNS.

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 sur un FQDN valide.

Conditions requises pour le logiciel VMware et son installation

Le système VMware vSphere sur lequel vous installez Unified Manager nécessite des versions spécifiques du système d'exploitation et des logiciels de prise en charge.

Logiciel de système d'exploitation

Les versions suivantes de VMware ESXi sont prises en charge :

- ESXi 7.0 et 8.0

> Unified Manager OVA sur les systèmes VMware vSphere exécute Debian OS 11 (bullseye) en interne. Pour plus d'informations sur les versions du matériel de la machine virtuelle prises en charge par les versions des serveurs VMware ESXi, 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"

Le temps du serveur VMware ESXi doit être identique au temps du serveur NTP pour que l'appliance virtuelle fonctionne correctement. La synchronisation de l'heure du serveur VMware ESXi avec celle du serveur NTP empêche une défaillance de temps.

Conditions requises pour l'installation

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

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

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

> Lors de l'installation ou de la mise à niveau d'Unified Manager, les correctifs de sécurité et les logiciels tiers 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 de Unified Manager contrôlent ces composants, il n'est pas recommandé d'effectuer une installation ou une mise à niveau autonome d'un composant tiers.

Navigateurs pris en charge

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

La matrice d'interopérabilité répertorie les versions de navigateur prises en charge.

"mysupport.netapp.com/matrix"

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit que les fonctions logicielles sont affichées correctement.

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

Exigences en matière de protocoles et de ports

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

Connexions au serveur Unified Manager

Dans les installations courantes, il n'est pas nécessaire de spécifier les 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, comme Unified Manager tente toujours de s'exécuter sur son port par défaut, vous pouvez entrer à `https://<host>` la place de `https://<host>:443` .

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

Interface	Protocole	Port	Description
Interface Web Unified Manager	HTTP	80	Permet d'accéder à l'interface utilisateur Web d'Unified Manager et de la rediriger automatiquement vers le port sécurisé 443.
L'interface utilisateur et les programmes Web Unified Manager utilisant des API	HTTPS	443	Permet d'accéder de façon sécurisée à l'interface utilisateur Web d'Unified Manager ou de passer des appels d'API. Les appels d'API ne peuvent être effectués qu'à l'aide de HTTPS.
Console de maintenance	SSH/SFTP	22	Permet d'accéder à la console de maintenance et de récupérer les packs de support.
Ligne de commande Linux	SSH/SFTP	22	Permet d'accéder à la ligne de commande Red Hat Enterprise Linux ou CentOS et de récupérer les packs de support.

Interface	Protocole	Port	Description
Syslog	UDP	514	Permet d'accéder aux messages EMS basés sur un abonnement à partir des systèmes ONTAP et de créer des événements en fonction des messages.
REPOS	HTTPS	9443	Permet d'accéder aux événements EMS REST basés sur API en temps réel à partir de systèmes ONTAP authentifiés.

Le port par défaut pour MySQL, 3306, est limité à localhost uniquement 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 mise à disposition d'autres hôtes à l'aide de l' `Control access to MySQL port 3306`option de la console de maintenance. Pour plus d'informations, voir "Options de menu supplémentaires". Les ports utilisés pour les communications 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 à partir du serveur Unified Manager

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

Selon l'environnement du client, il est possible 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, serveurs et autres composants :

Destination	Protocole	Port	Description
Adieu les migrations de données onéreuses	HTTPS	443/TCP	Permet de surveiller et de gérer les systèmes de stockage. Si vous utilisez ce port ou tout autre port pour vous connecter au serveur VMware vCenter Server ou ESXi, assurez-vous que le port est disponible et qu'il peut être connecté sur un site sécurisé.
Adieu les migrations de données onéreuses	NDMP	10000/TCP	Utilisée pour certaines opérations de restauration Snapshot.
Serveur AutoSupport	HTTPS	443	Permet d'envoyer des informations AutoSupport. Nécessite l'accès à 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 des communications LDAP sécurisées.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	Expéditeur du trap SNMP

Destination	Protocole	Port	Description
SNMPv1 ou SNMPv3	162/UDP	Permet d'envoyer des alertes de notification des interruptions SNMP.	Serveur de fournisseur de données externe
TCP	2003	Permet d'envoyer les données de performances à un fournisseur de données externe, comme Graphite.	Serveur NTP
NTP	123/UDP	Permet de synchroniser l'heure sur le serveur Unified Manager avec un serveur de temps NTP externe. (Systèmes VMware uniquement)	Syslog

Remplir la fiche

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

Informations sur l'installation de Unified Manager

Détails requis pour installer Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Adresse IP du serveur ESXi	
Nom de domaine complet de l'hôte	
Adresse IP de l'hôte	
Masque de réseau	
Adresse IP de la passerelle	
Adresse DNS principale	
Adresse DNS secondaire	
Domaines de recherche	
Nom d'utilisateur de maintenance	

Système sur lequel le logiciel est déployé	Votre valeur
Mot de passe utilisateur de maintenance	

Informations sur la configuration de Unified Manager

Détails de la configuration d'Unified Manager après l'installation. Certaines valeurs sont facultatives en fonction de votre configuration.

Réglage	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 d'administrateur Active Directory ou nom distinctif de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom distinctif de la base du serveur d'authentification	
URL du fournisseur d'identités	
Métadonnées du fournisseur d'identités	
Adresses IP de l'hôte de destination de l'interruption SNMP	
Port SNMP	

Informations sur le cluster

Détails des systèmes de stockage que vous gérez à l'aide de Unified Manager.

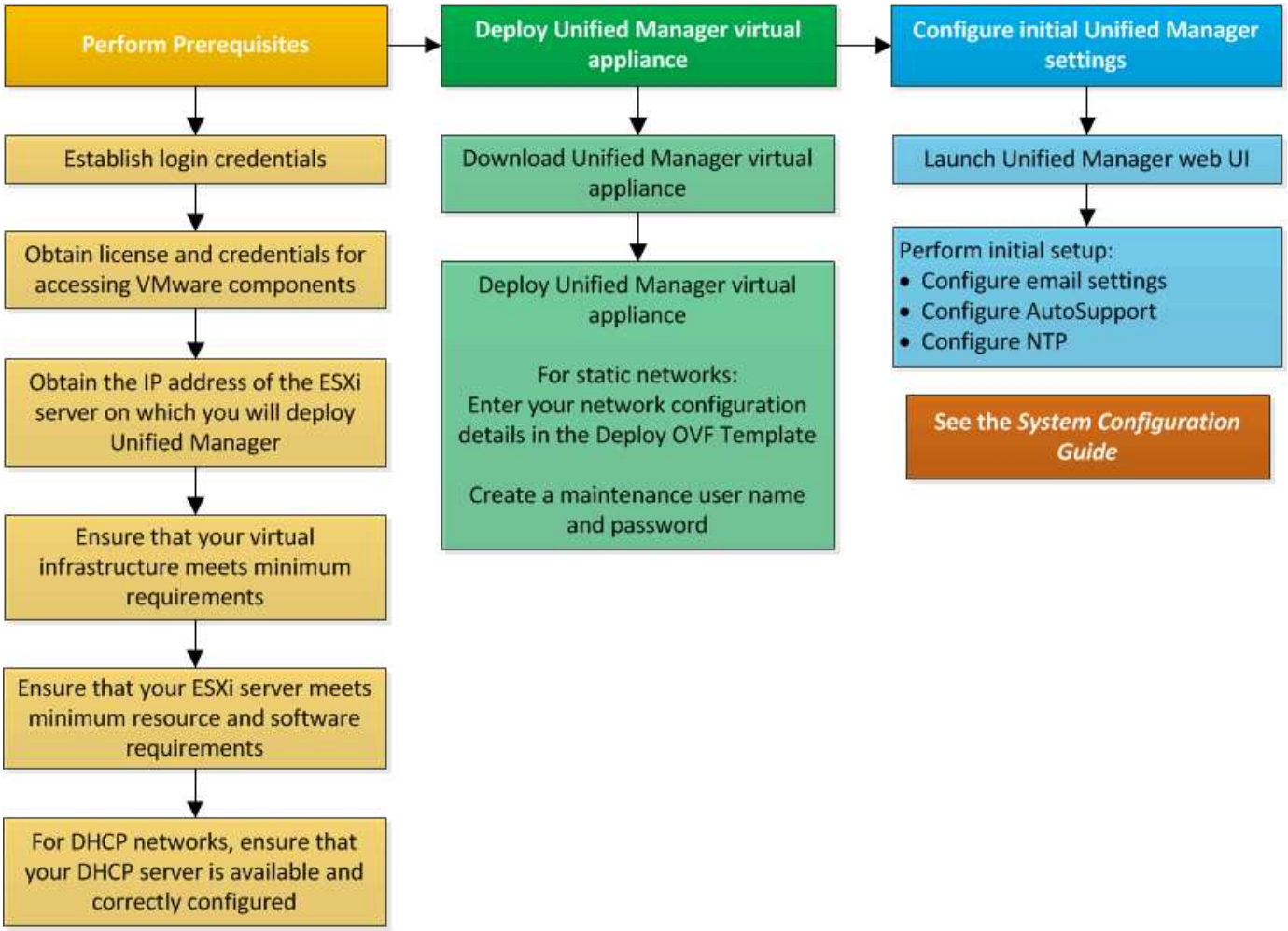
Cluster 1 de N	Votre valeur
Nom d'hôte ou adresse IP de gestion du cluster	
Nom d'utilisateur de l'administrateur ONTAP L'administrateur doit avoir reçu le rôle « admin ».	
Mot de passe administrateur ONTAP	
Protocole	HTTPS

Installation, mise à niveau et suppression du 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).

Présentation du processus de déploiement

Le workflow de déploiement décrit les tâches à effectuer avant d'utiliser Unified Manager.



Déployer Unified Manager

Le déploiement de Unified Manager inclut le téléchargement de logiciels, le déploiement de l'appliance virtuelle, la création d'un nom d'utilisateur et d'un mot de passe pour la maintenance, ainsi que la configuration initiale dans l'interface utilisateur Web.

Ce dont vous aurez besoin

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

  Voir "Configuration minimale requise".

- Vérifiez que vous disposez des informations suivantes :
  - Identifiants de connexion pour le site du support NetApp
  - Informations d'identification pour l'accès à VMware vCenter Server et au client Web vSphere
  - 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 le datastore 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.

> Depuis 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` il est inclus dans le package d'installation d'Unified Manager.

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

Étapes

1. Suivez les étapes de la section "Télécharger Unified Manager".
2. En outre, suivez les étapes de la section "Déployez l'appliance virtuelle Unified Manager".

Téléchargement du fichier d'installation de Unified Manager

Téléchargez le fichier d'installation Unified Manager depuis le site de support NetApp pour déployer Unified Manager en tant que dispositif virtuel.

Ce dont vous aurez besoin

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

Le fichier d'installation est un `.tar` fichier qui contient 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 de Unified Manager :

   "Site de support NetApp"

2. Sélectionnez la version requise de 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 correctement téléchargé.
5. Accédez au répertoire dans lequel vous avez téléchargé le `.tar` fichier et entrez la commande suivante dans la fenêtre de terminal pour développer le bundle Unified Manager :

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

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

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

Déploiement de l'appliance virtuelle Unified Manager

Après avoir téléchargé le fichier d'installation, vous déployez Unified Manager en tant

qu'appliance virtuelle. Utilisez le client Web vSphere pour déployer l'appliance virtuelle sur un serveur ESXi. Lorsque vous déployez l'appliance virtuelle, une machine virtuelle est créée.

Ce dont vous aurez besoin

Il est recommandé de passer en revue la configuration système requise. Apportez les modifications nécessaires avant de déployer l'appliance virtuelle Unified Manager.

Voir "Besoins de l'infrastructure virtuelle".

Voir "Conditions requises pour le logiciel VMware et son installation".

Si vous utilisez le protocole DHCP (Dynamic Host Configuration Protocol), assurez-vous que le serveur DHCP est disponible et que les configurations de l'adaptateur 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.

Avant de déployer l'appliance virtuelle, procurez-vous les informations suivantes :

- Informations d'identification pour l'accès à VMware vCenter Server et au client Web vSphere
- Adresse IP du serveur ESXi sur lequel vous déployez l'appliance virtuelle Unified Manager
- Détails sur le data Center, tels que la disponibilité de l'espace de stockage
- Si vous n'utilisez pas DHCP, procurez-vous les adresses IPv4 ou IPv6 pour les périphériques réseau auxquels vous prévoyez de vous connecter :
  - Nom de domaine complet (FQDN) de l'hôte
  - Adresse IP de l'hôte
  - Masque de réseau
  - Adresse IP de la passerelle par défaut
  - Adresses DNS principale et secondaire
  - Domaines de recherche

Depuis 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` il est inclus dans le package d'installation d'Unified Manager.

Lors du déploiement de l'appliance virtuelle, un certificat unique auto-signé pour l'accès HTTPS est généré. Lors de l'accès à l'interface utilisateur Web Unified Manager, un avertissement s'affiche dans le navigateur concernant les certificats non fiables.

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

Étapes

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

   Sur la page Détails de la révision :

- Vérifiez les détails de la section Éditeur. Le message **Entrust Code Signing - OVCS2 (Trusted Certificate)** confirme l'intégrité du fichier téléchargé `OVA`. + si le message **Entrust Code Signing - OVCS2 (certificat non valide)** s'affiche, mettez à niveau VMware vCenter Server vers 7.0U3E ou une version ultérieure.

  Sur la page Personnaliser le modèle :

- Laissez tous les champs vides lors de l'utilisation de l'adressage DHCP et IPv4.
- Cochez la case « Activer l'adressage IPv6 automatique » et laissez tous les autres champs vides lors de l'utilisation de l'adressage DHCP et IPv6.
- Si vous souhaitez utiliser une configuration de réseau statique, vous pouvez remplir les champs de cette page et ces paramètres sont appliqués pendant le 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 possède une entrée DNS valide.

3. Une fois l'appliance virtuelle Unified Manager déployée sur le serveur ESXi, mettez la machine virtuelle sous tension en cliquant avec le bouton droit de la souris sur la machine virtuelle, puis en sélectionnant **Power On**.

   Si l'opération de mise sous tension échoue en raison de ressources insuffisantes, ajoutez des ressources, puis recommencez 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 indiqué 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 de vos périphériques 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 Snapshot à l'aide d'un périphérique configuré à l'aide d'un fuseau horaire différent de celui du serveur de gestion, l'horodatage correspond au temps 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, procédez comme ça…
DHCP	Sélectionnez **Réessayer DHCP**. Si vous envisagez d'utiliser DHCP, assurez-vous qu'il est correctement configuré. Si vous utilisez un réseau compatible DHCP, les entrées de FQDN et de serveur DNS sont automatiquement données au serveur virtuel. 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.
Une configuration de réseau statique	a. Sélectionnez **Entrez les détails de la configuration du réseau statique**. La 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 d'utilisateur de maintenance doit commencer par une lettre de a à z, suivie de toute combinaison de -, a à z ou 0 à 9.

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

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

Vous pouvez accéder à l'interface utilisateur Web pour effectuer la configuration initiale d'Unified Manager, comme décrit dans le "Configuration d'Active IQ Unified Manager en cours".

Mise à niveau d'Unified Manager

Vous pouvez mettre à niveau Active IQ Unified Manager vers la version 9.14 à partir de la version 9.12 ou 9.13 uniquement.

Unified Manager n'est pas disponible lors du processus de mise à niveau. Pour effectuer toute opération en cours d'exécution, vous devez effectuer la mise à niveau de Unified Manager.

Si Unified Manager est associé à une instance de OnCommand Workflow Automation et que de nouvelles versions du logiciel sont disponibles pour les deux produits, vous devez déconnecter les deux produits et 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, puis vérifier que les données sont toujours acquises depuis Unified Manager.

Étapes

1. Suivez les étapes de la section "Téléchargez l'image ISO Unified Manager".

2. En outre, suivez les étapes décrites "Mettez à niveau Unified Manager"à la section .

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

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

Toutes les versions de Unified Manager ne peuvent pas effectuer de mise à niveau sans déplacement des données vers les versions ultérieures. Les mises à niveau de Unified Manager sont limitées à un modèle N-2. Ainsi, la mise à niveau ne peut être effectuée que dans les 2 versions suivantes, sur toutes les plateformes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.14 à partir d'Unified Manager 9.12 et 9.13 uniquement.

Si vous exécutez une version antérieure aux versions prises en charge, votre instance Unified Manager doit 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 la version installée est Unified Manager 9.9 et que vous souhaitez effectuer une mise à niveau vers Unified Manager 9.14, vous suivez une séquence de mises à niveau.

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.9 → 9.11
2. Mise à niveau 9.11 → 9.13
3. Mise à niveau 9.13 → 9.14

Pour plus d'informations sur la matrice de chemin de mise à niveau, reportez-vous à la section "Article de la base de connaissances (KB)" .

Téléchargement du fichier de mise à niveau Unified Manager

Avant de mettre à niveau Unified Manager, téléchargez le fichier de mise à niveau Unified Manager depuis le site de support NetApp.

Ce dont vous aurez besoin

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

Étapes

1. Connectez-vous au site de support NetApp :

   "Site de support NetApp"

2. Accédez à la page Download pour la mise à niveau d'Unified Manager sur VMware vSphere.
3. Téléchargez l' `.iso`image pour la mise 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.

Mise à niveau de l'appliance virtuelle Unified Manager

Vous pouvez mettre à niveau l'appliance virtuelle Active IQ Unified Manager des versions 9.12 ou 9.13 vers la version 9.14.

Ce dont vous aurez besoin

Vérifiez les points suivants :

- Vous avez téléchargé le fichier de mise à niveau, l'image ISO, depuis le site de support NetApp.
- Le système sur lequel vous mettez à niveau Unified Manager répond à la configuration système et logicielle requise.

  Voir "Besoins de l'infrastructure virtuelle".

  Voir "Conditions requises pour le logiciel VMware et son installation".

- Pour les utilisateurs de vSphere 6.5 et des versions ultérieures, vous avez installé VMware Remote Console (VMRC).
- Lors d'une mise à niveau, vous pouvez être invité à confirmer si vous souhaitez conserver les paramètres par défaut précédents pour conserver les données de performances pendant 13 mois ou à les modifier à 6 mois. A la confirmation, les données historiques de performance sont supprimées au bout de 6 mois.
- Vous disposez des informations suivantes :
  - Identifiants de connexion pour le site du support NetApp
  - Informations d'identification pour l'accès à VMware vCenter Server et au client Web vSphere
  - Informations d'identification pour l'utilisateur responsable de la maintenance Unified Manager

Unified Manager n'est pas disponible lors du processus de mise à niveau. Pour effectuer toute opération en cours d'exécution, vous devez effectuer la mise à niveau de 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 vSphere client, cliquez sur **Accueil** > **Inventaire** > **VM et modèles**.
2. Sélectionnez la machine virtuelle (VM) sur laquelle l'appliance virtuelle Unified Manager est installée.
3. Si la machine virtuelle Unified Manager est en cours d'exécution, accédez à **Résumé** > **commandes** > **Arrêter invité**.
4. Créer une copie de sauvegarde, par exemple une copie Snapshot ou un clone, de la machine virtuelle Unified Manager pour créer une sauvegarde cohérente avec les applications.
5. À partir du client vSphere, mettez la machine virtuelle sous tension.
6. Lancez la console à distance VMware.
7. Cliquez sur l'icône **CDROM** et sélectionnez **connexion 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 de Unified Manager.
11. Dans le menu principal, sélectionnez **Upgrade**.

    Un message s'affiche indiquant que Unified Manager doit être indisponible durant la mise à niveau, et qu'il reprend après la fin du processus.

12. Tapez `y` pour continuer.

    Un avertissement s'affiche, vous rappelant de sauvegarder la machine virtuelle sur laquelle réside l'appliance virtuelle.

13. Tapez `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 détection avant d'effectuer une tâche dans l'interface utilisateur.

Redémarrage de 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 en cas de problème avec la machine virtuelle.

Ce dont vous aurez besoin

- L'appliance virtuelle 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 à partir de vSphere en utilisant l'option VMware **Restart Guest**.

Étapes

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

Informations connexes

"Références des applets de commande VMware vSphere PowerCLI : restart-VMGuest"

Suppression de Unified Manager

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

Ce dont vous aurez besoin

- Vous devez disposer d'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 vSphere client, cliquez sur **Accueil** > **Inventaire** > **VM et modèles**.
3. Sélectionnez la VM que vous souhaitez supprimer, puis cliquez sur l'onglet **Résumé**.
4. Si la machine virtuelle est en cours d'exécution, cliquez sur **Power** > **Shut Guest**.
5. Cliquez avec le bouton droit de la souris sur la machine virtuelle que vous souhaitez supprimer, puis cliquez sur **Supprimer du disque**.

Installez 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 seule interface. Il est possible de 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 à gérer ajoutés, Unified Manager offre une interface graphique qui affiche la capacité, la disponibilité, la protection et les performances des systèmes de stockage surveillés.

Informations connexes

"Matrice d'interopérabilité NetApp"

Rôle du serveur Unified Manager

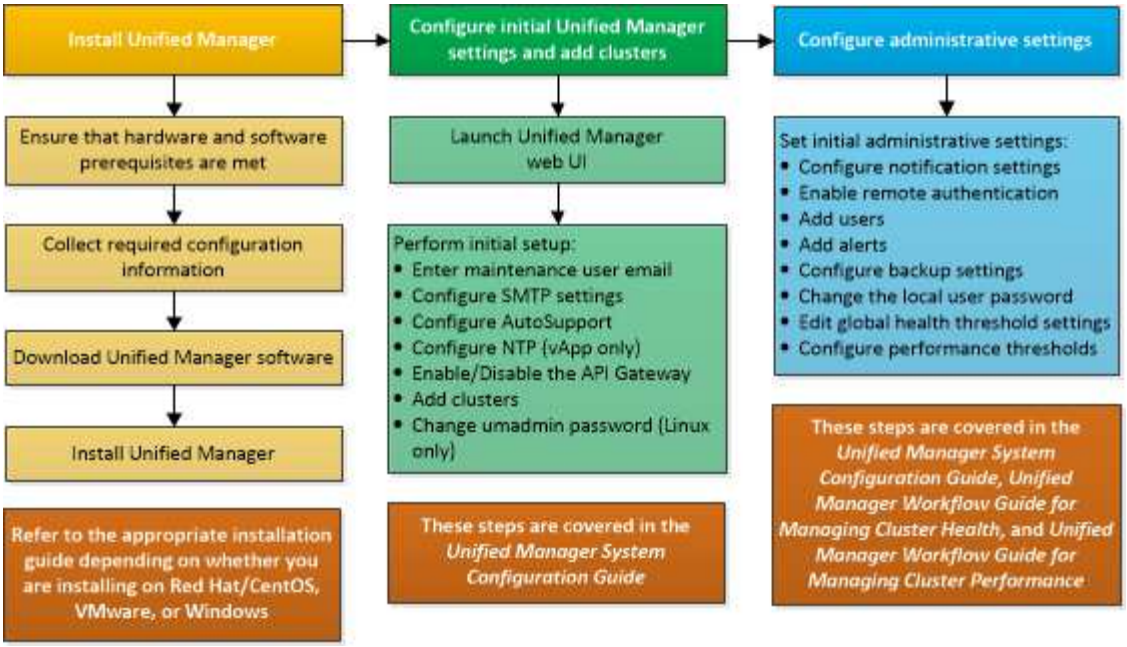
L'infrastructure de serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la détection, la surveillance, le contrôle d'accès basé sur des rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations sur le cluster, stocke les données dans la base de données et analyse ces données afin de voir en cas de problème au niveau du cluster.

Présentation de la séquence d'installation

Le workflow d'installation décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.

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



Conditions requises pour l'installation de 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 logiciels, de matériel, de processeur et de mémoire.

NetApp ne prend pas en charge les modifications du code de l'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 d'informations sur l'application de 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

"Matrice d'interopérabilité NetApp"

Configuration minimale requise pour l'infrastructure virtuelle et le système matériel

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

Le tableau suivant affiche les valeurs recommandées pour les ressources mémoire, processeur et espace disque. Ces valeurs ont été qualifiées pour permettre à Unified Manager de satisfaire à des niveaux de performances acceptables.

Configuration matérielle	Paramètres recommandés
RAM	12 Go (minimum requis : 8 Go)
Processeurs	4 processeurs
Capacité du cycle du processeur	9572 MHz au total (exigence minimale : 9572 MHz)
Espace disque disponible	150 Go, où la capacité est allouée comme suit : • 50 Go alloués à la partition racine • 100 Go d'espace disque disponible alloué au `/opt/netapp/data` répertoire, qui est monté sur un lecteur LVM ou sur un disque local distinct connecté au système cible Pour les répertoires et `/var/log` montés séparément `/opt`, assurez-vous que `/opt` dispose de 15 Go et `/var/log` dispose de 16 Go d'espace libre. Le `/tmp` répertoire doit disposer d'au moins 10 Go d'espace libre.

Unified Manager peut être installé sur des systèmes disposant d'une petite quantité de mémoire, mais les 12 Go recommandés de RAM garantissent qu'un volume suffisant de mémoire est disponible pour des performances optimales de façon à ce que le système puisse prendre en charge des clusters et des objets de stockage supplémentaires à mesure que votre configuration évolue. Vous ne devez pas définir de limites de mémoire sur la machine virtuelle où Unified Manager est déployé, et ne devez pas activer de fonctions (par exemple, l'option de création de bulles) qui empêchent le logiciel d'utiliser la mémoire allouée au système.

De plus, le nombre de nœuds qu'une seule instance de Unified Manager peut contrôler avant d'installer une deuxième instance de Unified Manager est limité. Pour plus d'informations, consultez le *Guide des meilleures pratiques*.

"Rapport technique 4621 : Guide des meilleures pratiques de Unified Manager"

Les échanges de pages mémoire ont un impact négatif sur les performances du système et de l'application de gestion. La concurrence pour les ressources de processeur indisponibles en raison de l'utilisation globale de l'hôte peut dégrader les performances.

Exigence pour une 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 de Unified Manager.

Besoins en espace pour les sauvegardes

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

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

Conditions requises pour la connectivité hôte

Le système physique ou virtuel sur lequel vous installez Unified Manager doit être configuré de manière à ce que le nom d'hôte puisse être correctement `ping` attribué à l'hôte lui-même. En cas de configuration IPv6, vérifiez que `ping6` le nom d'hôte a réussi pour vous assurer 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 pendant le déploiement, vous avez 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 du DNS.

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 sur un FQDN valide.

Conditions requises pour l'installation et le logiciel Linux

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

Logiciel de système d'exploitation

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

- Red Hat Enterprise Linux versions 7.x et 8.0 à 8.9, basée sur l'architecture x86_64.
- CentOS version 7.x basé sur l'architecture x86_64. CentOS Stream n'est pas pris en charge.

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

"mysupport.netapp.com/matrix"

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

> Les scanneurs de vulnérabilité (tels que Qualys) peuvent entraîner une utilisation élevée du CPU lors de l'analyse de la machine virtuelle en interne (où Unified Manager et l'analyse de vulnérabilité sont installés sur la même machine virtuelle) ou en externe (où Unified Manager et l'analyse des vulnérabilités sont installés sur deux serveurs différents et que l'analyse des vulnérabilités analyse la machine virtuelle sur laquelle Unified Manager est installé). Ce problème entraîne souvent une non-réponse de la machine virtuelle et affecte les services Unified Manager. Par conséquent, NetApp recommande de désactiver l'analyse des vulnérabilités sur la machine virtuelle sur laquelle Unified Manager est installé. Si la désactivation du scanner n'est pas une option, scanner la machine virtuelle pendant les heures non ouvrables et redémarrer 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 ils ne sont pas inclus avec Unified Manager. Ces packages sont automatiquement installés par le `yum` programme d'installation lors de l'installation, à condition que vous ayez configuré les référentiels comme indiqué dans les sections suivantes.

- MySQL Community Edition version 8.0.34 (à partir du référentiel MySQL).
- OpenJDK version 11.0.21 (à partir du référentiel Red Hat Extra Enterprise Linux Server)
- Python 3.6.x
- P7zip version 16.02 ou ultérieure (à partir du référentiel Red Hat Extra Packages for Enterprise Linux)

> Vous devez arrêter une instance en cours d'exécution de 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 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 la `sudo` commande.

En outre, l'installation par défaut de 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/` répertoire. Si vous supprimez ce contenu de votre environnement en raison de stratégies de sécurité ou en raison d'un outil de surveillance de la sécurité, vous devez le réintégrer. Vous devez conserver la configuration des sudoers car certaines opérations Unified Manager nécessitent ces privilèges de sudo.

Conditions requises pour l'installation

Les meilleures pratiques d'installation de Red Hat Enterprise Linux ou CentOS ainsi que les 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 s'exécuter correctement dans de tels déploiements.

- Vous devez installer Red Hat Enterprise Linux ou CentOS conformément aux meilleures pratiques de Red Hat, et vous devez sélectionner les options par défaut suivantes, qui nécessitent de sélectionner l'environnement de base "serveur avec interface utilisateur graphique".
- Lors de l'installation de Unified Manager sur Red Hat Enterprise Linux ou CentOS, le système doit avoir accès au référentiel approprié afin que le programme d'installation puisse accéder à toutes les dépendances logicielles requises et les installer.
- Pour que le `yum` programme d'installation puisse trouver des 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 par la suite en utilisant un abonnement Red Hat valide.

  Pour plus d'informations sur le Gestionnaire d'abonnement Red Hat, reportez-vous à la documentation Red Hat.

- Vous devez activer le référentiel des progiciels supplémentaires pour Enterprise Linux (EPEL) pour installer correctement 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 correctement 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 devez installer une seule version de Java sur votre hôte Unified Manager ; sinon, le système peut 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 à partir 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 les `.rpm` fichiers sur le système sur lequel vous prévoyez d'installer Unified Manager. Pour télécharger les artéfacts et les packages, vous devez utiliser `yum install` la commande. Vous devez vous assurer que les deux systèmes exécutent la même version de système d'exploitation et que la licence d'abonnement est pour la version appropriée de Red Hat Enterprise Linux ou CentOS.

> Vous ne devez pas installer les logiciels tiers requis à partir d'autres référentiels que ceux répertoriés ici. Les logiciels installés à partir des référentiels Red Hat sont conçus explicitement pour Red Hat Enterprise Linux et respectent les meilleures pratiques Red Hat (mises en page des répertoires, autorisations, etc.). Il est possible que les logiciels provenant d'autres emplacements ne respectent pas ces directives, ce qui peut entraîner l'échec de l'installation de Unified Manager ou risque de provoquer des problèmes lors des mises à niveau futures.

Orifice 443 requis

Des images génériques de Red Hat Enterprise Linux et CentOS peuvent bloquer l'accès externe au port 443. En raison de cette restriction, il se peut que vous ne puissiez pas vous connecter à l'interface utilisateur Web de l'administrateur après avoir installé Unified Manager. L'exécution de la commande suivante permet d'accéder au port 443 pour tous les utilisateurs et applications externes sur un système Red Hat Enterprise Linux ou CentOS générique.

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

Vous devez installer Red Hat Enterprise Linux et CentOS avec l'environnement de base "serveur avec interface utilisateur 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 stratégies de sécurité nécessitent une procédure différente.

THP (transparent énorme pages) doit être désactivé sur les systèmes CentOS et Red Hat. Lorsqu'il est activé, dans certains cas, Unified Manager peut être arrêté lorsque certains processus consomment trop de mémoire et sont arrêtés.

Navigateurs pris en charge

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

La matrice d'interopérabilité répertorie les versions de navigateur prises en charge.

"mysupport.netapp.com/matrix"

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit que les fonctions logicielles sont affichées correctement.

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

Exigences en matière de protocoles et de ports

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

Connexions au serveur Unified Manager

Dans les installations courantes, il n'est pas nécessaire de spécifier les 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, comme Unified Manager tente toujours de s'exécuter sur son port par défaut, vous pouvez entrer à `https://<host>` la place de `https://<host>:443` .

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

Interface	Protocole	Port	Description
Interface Web Unified Manager	HTTP	80	Permet d'accéder à l'interface utilisateur Web d'Unified Manager et de la rediriger automatiquement vers le port sécurisé 443.
L'interface utilisateur et les programmes Web Unified Manager utilisant des API	HTTPS	443	Permet d'accéder de façon sécurisée à l'interface utilisateur Web d'Unified Manager ou de passer des appels d'API. Les appels d'API ne peuvent être effectués qu'à l'aide de HTTPS.

Interface	Protocole	Port	Description
Console de maintenance	SSH/SFTP	22	Permet d'accéder à la console de maintenance et de récupérer les packs de support.
Ligne de commande Linux	SSH/SFTP	22	Permet d'accéder à la ligne de commande Red Hat Enterprise Linux ou CentOS et de récupérer les packs de support.
Base de données MySQL	MySQL	3306	Permet d'activer l'accès aux services d'API OnCommand Workflow Automation et OnCommand à Unified Manager.
Syslog	UDP	514	Permet d'accéder aux messages EMS basés sur un abonnement à partir des systèmes ONTAP et de créer des événements en fonction des messages.
REPOS	HTTPS	9443	Permet d'accéder aux événements EMS REST basés sur API en temps réel à partir de systèmes ONTAP authentifiés.

Le port par défaut pour MySQL, 3306, est limité à localhost uniquement 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 mise à disposition d'autres hôtes à l'aide de l' `Control access to MySQL port 3306`option de la console de maintenance. Pour plus d'informations, voir "Options de menu supplémentaires". Les ports utilisés pour les communications 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 à partir du serveur Unified Manager

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

Selon l'environnement du client, il est possible 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, serveurs et autres composants :

Destination	Protocole	Port	Description
Adieu les migrations de données onéreuses	HTTPS	443/TCP	Permet de surveiller et de gérer les systèmes de stockage.
Adieu les migrations de données onéreuses	NDMP	10000/TCP	Utilisée pour certaines opérations de restauration Snapshot.
Serveur AutoSupport	HTTPS	443	Permet d'envoyer des informations AutoSupport. Nécessite l'accès à 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 des communications LDAP sécurisées.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	Expéditeur du trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Permet d'envoyer des alertes de notification des interruptions SNMP.	Serveur de fournisseur de données externe
TCP	2003	Permet d'envoyer les données de performances à un fournisseur de données externe, comme Graphite.	Serveur NTP
NTP	123/UDP	Permet de synchroniser l'heure sur le serveur Unified Manager avec un serveur de temps NTP externe. (Systèmes VMware uniquement)	Syslog

Remplir la fiche

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

Informations sur l'installation de Unified Manager

Détails requis pour installer Unified Manager.

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

Informations sur la configuration de Unified Manager

Détails de la configuration d'Unified Manager après l'installation. Certaines valeurs sont facultatives en fonction de votre configuration.

Réglage	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)

Réglage	Votre valeur
E-mail à partir duquel les notifications d'alerte sont envoyées	
Nom d'hôte ou adresse IP du serveur d'authentification	
Nom d'administrateur Active Directory ou nom distinctif de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom distinctif de la base du serveur d'authentification	
URL du fournisseur d'identités	
Métadonnées du fournisseur d'identités	
Adresses IP de l'hôte de destination de l'interruption SNMP	
Port SNMP	

Informations sur le cluster

Détails des systèmes de stockage que vous gérez à l'aide de Unified Manager.

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

Installation, mise à niveau et suppression du logiciel Unified Manager

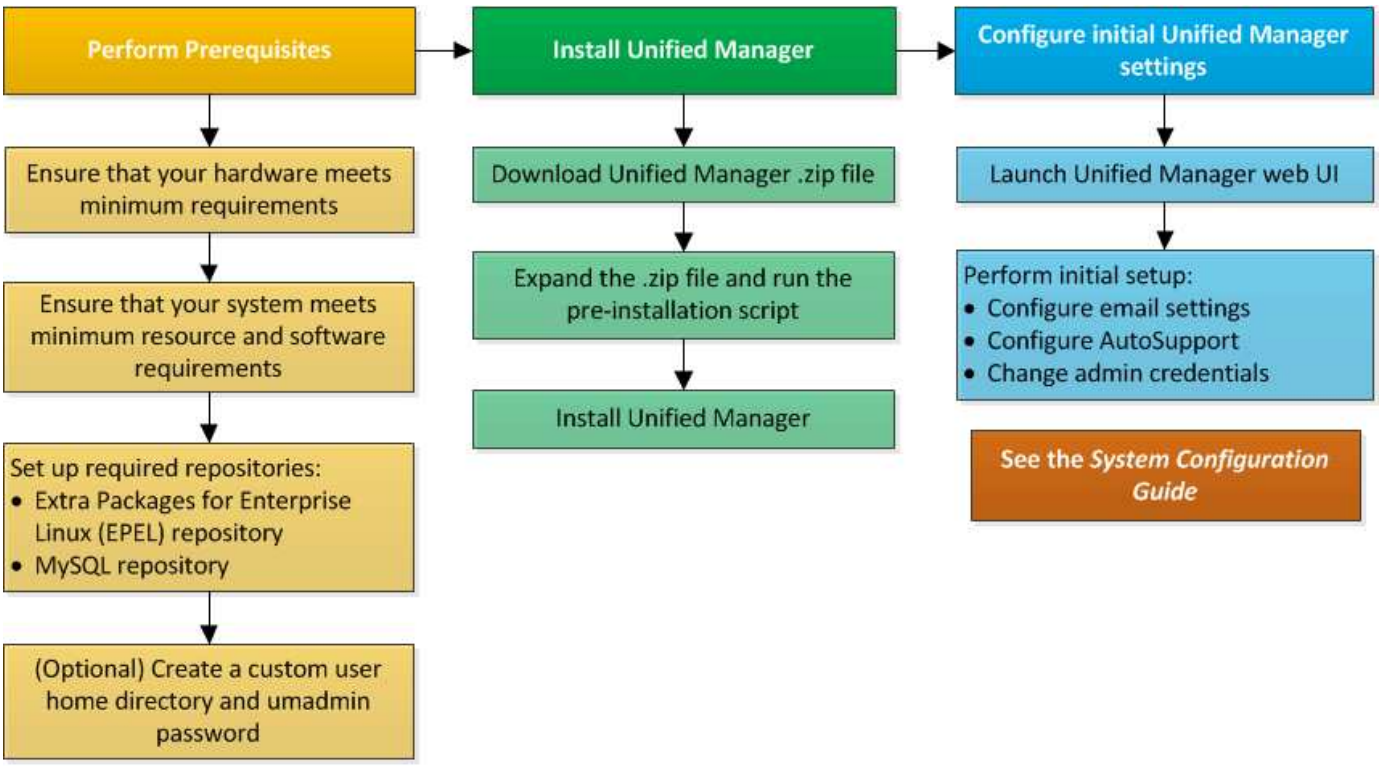
Sur les systèmes Linux, vous pouvez installer le logiciel Unified Manager, effectuer une

mise à niveau vers une version plus récente ou supprimer Unified Manager.

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

Présentation du processus d'installation

Le workflow d'installation décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.



Configuration des référentiels logiciels requis

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

Configuration manuelle du référentiel EPEL

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

Le référentiel EPEL permet d'accéder aux utilitaires tiers requis qui doivent être installés sur votre système. Que vous installiez Unified Manager sur un système Red Hat Enterprise Linux ou CentOS, vous utilisez le référentiel EPEL.

Étapes

1. Téléchargez le référentiel EPEL pour votre installation. Pour Red Hat Enterprise Linux 7, téléchargez-le à l'adresse suivante :

```
wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

Pour la version 8, téléchargez-la à l'adresse suivante :

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

2. Configurez 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.

Configuration manuelle du 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 permet d'accéder au logiciel MySQL requis qui doit être installé sur votre système.

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

Étapes

1. Téléchargez le référentiel MySQL approprié pour votre installation. Pour Red Hat Enterprise Linux 7, téléchargez-le à l'adresse suivante :

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-
community-release-el7-3.noarch.rpm
```

Pour la version 8, téléchargez-la à l'adresse suivante :

```
wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-
community-release-el8-1.noarch.rpm
```

2. Configurez le référentiel MySQL :

```
yum install mysql80-community-release-<version>.noarch.rpm
```

Pour le système Red Hat Enterprise Linux 8, si vous disposez de référentiels internes avec Java-11-openjdk, p7zip et d'autres progiciels 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 de non-concordance de clé ou de clé manquante et que l'installation échoue,

procédez comme suit :

- 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-2022
```

- Sur un système qui n'a pas de connectivité Internet, mettez à jour votre fichier de référentiel MySQL et désactivez-le `gpgcheck` en marquant `gpgcheck=0`.

Exigences SELinux sur les partages NFS et CIFS

Si vous prévoyez de monter `/opt/netapp` ou `/opt/netapp/data` sur un périphérique NAS ou SAN et que SELinux est activé, vous devez prendre en compte quelques considérations.

Si vous prévoyez de monter `/opt/netapp` ou `/opt/netapp/data` de n'importe où autre 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 dans votre environnement, procédez comme suit pour définir et confirmer le contexte SELinux correct.

Configuration du contexte SELinux lorsque `/opt/netapp/data` est monté

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

1. Exécuter cette commande pour vérifier le contexte :

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

   Exemple de sortie :

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

   > Dans ce résultat, le contexte est `default_t`. Vous devez modifier ce contexte en `mysqld_db_t`.

2. Procédez comme suit pour définir le contexte en fonction de la manière 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 devez modifier le `/etc/fstab` fichier. Pour `/opt/netapp/data/` l'option de montage, ajoutez l'étiquette MySQL comme suit :

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

c. Démonter et remonter `/opt/netapp/data/` pour activer le contexte.

d. Si vous avez 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/
```

Exemple de sortie :

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

Configuration du 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 contexte SELinux du répertoire parent `/opt/netapp` n'est pas défini sur `file_t`.

Étapes

1. Exécuter cette commande pour vérifier le contexte :

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

   Exemple de sortie :

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

   Dans ce résultat, le contexte `file_t` doit être modifié. Les commandes suivantes définissent le contexte sur `usr_t`. Vous pouvez définir le contexte sur toute valeur autre que `file_t` basée sur vos exigences de sécurité.

2. Procédez comme suit pour définir le contexte, en fonction de la manière 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 devez modifier le `/etc/fstab` fichier. Pour `/opt/netapp` l'option de montage, ajoutez l'étiquette MySQL comme suit :

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

2. Démontez, puis montez de nouveau `/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 échantillon de sortie

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

Configuration du contexte SELinux lorsque `/opt/netapp` est monté et n'est pas monté `/opt/netapp/data/` séparément

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

Étapes

1. Exécuter cette commande pour vérifier le contexte :

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

   Exemple de sortie :

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

   > Dans ce résultat, le contexte est `default_t`. Vous devez modifier ce contexte en `mysqld_db_t`.

2. Procédez comme suit pour définir le contexte en fonction de la manière 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`, modifiez le `/etc/fstab` fichier. Pour `/opt/netapp/` l'option de montage, ajoutez l'étiquette MySQL comme suit :
      `context=system_u:object_r:mysqld_db_t:s0`

c. Démontez, puis montez de nouveau `/opt/netapp/` pour activer le contexte.

d. Si vous avez 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/
```

Exemple de sortie :

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

Installation de Unified Manager sur des systèmes Linux

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

Création d'un répertoire personnel utilisateur personnalisé et d'un mot de passe umadmin avant l'installation

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

Ce dont vous aurez besoin

- Le système doit répondre aux exigences décrites à "Configuration matérielle requise"la section .
- Vous devez pouvoir vous connecter en tant qu'utilisateur root au système Red Hat Enterprise Linux ou CentOS.

L'installation par défaut de Unified Manager effectue les tâches suivantes :

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

Comme certains environnements d'installation limitent l'accès à `/home`, l'installation échoue. Vous devez créer le répertoire de base à un autre emplacement. En outre, certains sites peuvent avoir des règles sur la complexité des mots de passe ou exiger que les mots de passe soient définis par les administrateurs locaux au lieu d'être définis par le programme d'installation.

Si votre environnement d'installation nécessite que vous remplaiez ces paramètres par défaut d'installation, procédez comme suit pour créer un répertoire d'accueil personnalisé et définir le mot de passe de l'utilisateur umadmin.

Lorsque ces informations sont définies avant l'installation, le script d'installation détecte ces paramètres et

utilise les valeurs définies au lieu d'utiliser les paramètres par défaut d'installation.

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

Les stratégies de sécurité de votre environnement ne doivent pas limiter les privilèges sudo pour l'utilisateur de maintenance d'Unified Manager. Certaines opérations d'Unified Manager peuvent échouer si les privilèges sont limités. Vérifiez que vous êtes en mesure d'exécuter la commande sudo suivante lorsque vous êtes connecté en tant qu'utilisateur umadmin après avoir réussi l'installation.

```
sudo systemctl status ocie
```

Cette commande devrait renvoyer le statut approprié du service ocie sans erreur.

Étapes

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

   ```
   groupadd maintenance
   ```

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

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

4. Définissez le mot de passe umadmin :

   ```
   passwd umadmin
   ```

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

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

Téléchargement d'Unified Manager

Pour installer Unified Manager, vous devez télécharger le fichier Unified Manager `.zip` depuis le site du support NetApp.

Ce dont vous aurez besoin

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

Vous téléchargez le même package d'installation Unified Manager pour les systèmes Red Hat Enterprise Linux et CentOS.

Étapes

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

   "Site de support NetApp"

2. Sélectionnez la version requise de 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` dans un répertoire du système cible.

   - Assurez-vous de télécharger la version correcte du fichier d'installation pour votre système Red Hat Enterprise Linux. Si vous avez installé Red Hat Enterprise Linux 7 ou 8, assurez-vous de télécharger la version appropriée du fichier Unified Manager `.zip`.
   - NetApp vous recommande de télécharger le certificat de signature de code (`.pem`) et la signature numérique (`.sig`) ainsi que le `.zip` fichier.

4. Vérifiez l'intégrité de la somme de contrôle 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 à partir 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 confirme que le fichier d'installation est sûr à `Verified Ok` utiliser.

Installation de Unified Manager

Vous pouvez installer Unified Manager sur une plateforme Red Hat Enterprise Linux ou CentOS physique ou virtuelle.

Ce dont vous aurez besoin

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

  Voir "Configuration matérielle requise".

  Voir "Conditions requises pour l'installation et le logiciel Linux".

- Vous devez avoir téléchargé le fichier Unified Manager `.zip` depuis le site du support NetApp vers le système cible.
- Vous devez avoir vérifié l'intégrité du fichier téléchargé `.zip`.

- Vous devez disposer d'un navigateur Web pris en charge.
- La fonction de restauration doit être activée pour le logiciel d'émulation de terminal.

Le système Red Hat Enterprise Linux ou CentOS peut avoir toutes les versions nécessaires du logiciel de prise en charge (Java, MySQL, utilitaires supplémentaires) installé, seulement une partie du logiciel requis installé, ou peut être un système nouvellement installé sans le logiciel requis installé.

Étapes

1. Connectez-vous au serveur sur lequel vous installez Unified Manager.
2. Entrez les commandes appropriées pour évaluer le logiciel nécessitant une installation ou une mise à niveau sur le système cible afin de prendre en charge l'installation :

Logiciel requis et version minimale	Pour vérifier le logiciel et la version
OpenJDK version 11.0.21	`java -version`
MySQL 8.0.34 Community Edition	`rpm -qa
grep -i mysql`	p7zip 16.02
`rpm -qa	grep p7zip`

3. Si la version installée de MySQL est antérieure à MySQL 8.0.34 Community Edition, entrez la commande suivante pour la désinstaller :

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

   Si vous recevez des erreurs de dépendance, vous devez ajouter l' `--nodeps`option de désinstallation du composant.

4. Accédez au répertoire dans lequel vous avez téléchargé le fichier d'installation `.zip` et développez le pack Unified Manager :

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

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

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

   ```
   ls *.rpm
   ```

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

6. Exécutez le script de pré-installation pour vous assurer qu'aucun paramètre de configuration du système ou aucun logiciel installé ne peut entrer en conflit avec l'installation de 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 progiciels 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
```

7. **Facultatif:** vous ne devez effectuer l'étape 7 que 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 vous ne disposez pas des packages requis, puis téléchargez ces packages :

   a. Sur le système sur lequel vous installez Unified Manager, 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 paquets disponibles dans le répertoire actuel, et les éléments de la section « installation pour dépendances: » Sont les modules qui manquent sur votre système.

   b. Sur un système qui dispose d'un accès Internet, téléchargez les packages manquants :

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

   > 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 cette fonctionnalité pour télécharger un package sans l'installer :
   > `yum install yum-plugin-downloadonly`

   a. Copiez les modules manquants du système connecté à Internet sur votre système d'installation.

8. En tant qu'utilisateur root ou à l'aide de `sudo`, exécutez la commande suivante pour installer le logiciel :

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

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

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

   ```
   rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
   ```

   > Ne tentez pas l'installation en utilisant d'autres commandes (telles que `rpm -ivh`). Pour réussir l'installation d'Unified Manager sur un système Red Hat Enterprise Linux ou CentOS, tous les fichiers Unified Manager et les fichiers associés doivent être installés dans un ordre spécifique dans une structure de répertoires spécifique qui est automatiquement appliquée par la `yum install netapp-um<version>.x86_64.rpm` commande.

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

   L'e-mail informe l'utilisateur root de l'échec initial d'une tâche cron, 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 le message dans lequel le système affiche une adresse IP ou une URL pour l'interface utilisateur Web de Unified Manager, le nom d'utilisateur de maintenance (umin) et un mot de passe par défaut.

    Ce message est similaire à ce qui suit :

    ```
    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 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 à la section "Configuration d'Active IQ Unified Manager en cours". Il est obligatoire de modifier le mot de passe par défaut de l'utilisateur umadmin.

Utilisateurs créés lors de l'installation de Unified Manager

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

- **umadmin**

  Permet pour la première fois de vous connecter à Unified Manager. Cet utilisateur est affecté à un rôle d'utilisateur « Administrateur d'applications » et est configuré comme type « utilisateur de maintenance ». Cet utilisateur est créé par Unified Manager.

- **jboss**

  Permet d'exécuter les services Unified Manager associés à l'utilitaire JBoss. Cet utilisateur est créé par Unified Manager.

- **mysql**

  Permet d'exécuter les requêtes de base de données MySQL de 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.

Modification du mot de passe JBoss

Vous pouvez réinitialiser le mot de passe JBoss spécifique à l'instance défini lors de l'installation. Vous pouvez éventuellement réinitialiser le mot de passe si votre site requiert cette fonctionnalité de sécurité afin de remplacer le paramètre d'installation de Unified Manager. Cette opération modifie également le mot de passe que JBoss utilise pour accéder à MySQL.

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

Étapes

1. Connectez-vous en tant qu'utilisateur root sur le système.
2. Arrêter 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 modification du 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, un majuscule et des caractères minuscules, et au moins l'un des caractères spéciaux suivants :

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

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 de Unified Manager.

Mise à niveau de Unified Manager sur Red Hat Enterprise Linux ou CentOS

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

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

Si Unified Manager est associé à une instance de OnCommand Workflow Automation et que de nouvelles versions du logiciel sont disponibles pour les deux produits, vous devez déconnecter les deux produits et 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, puis vérifier que les données sont toujours acquises depuis Unified Manager.

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

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

Toutes les versions de Unified Manager ne peuvent pas effectuer de mise à niveau sans déplacement des données vers les versions ultérieures. Les mises à niveau de Unified Manager sont limitées à un modèle N-2. Ainsi, la mise à niveau ne peut être effectuée que dans les 2 versions suivantes, sur toutes les plateformes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.14 à partir d'Unified Manager 9.12 et 9.13 uniquement.

Si vous exécutez une version antérieure aux versions prises en charge, votre instance Unified Manager doit 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 la version installée est Unified Manager 9.9 et que vous souhaitez effectuer une mise à niveau vers Unified Manager 9.14, vous suivez une séquence de mises à niveau.

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.9 → 9.11
2. Mise à niveau 9.11 → 9.13
3. Mise à niveau 9.13 → 9.14

Pour plus d'informations sur la matrice de chemin de mise à niveau, reportez-vous à la section "Article de la base de connaissances (KB)" .

Mise à niveau d'Unified Manager

Vous pouvez effectuer une mise à niveau depuis Unified Manager 9.12 ou 9.13 vers 9.14 en téléchargeant et en exécutant le fichier d'installation sur la plateforme Linux.

Ce dont vous aurez besoin

- Le système sur lequel vous mettez à niveau Unified Manager doit répondre à la configuration système et logicielle requise.

  Voir "Configuration matérielle requise".

  Voir "Conditions requises pour l'installation et le logiciel Linux".

- Vous devez être abonné au Gestionnaire d'abonnement Red Hat Enterprise Linux.
- Vous devez installer ou mettre à niveau la version correcte d'OpenJDK avant de mettre à niveau Unified Manager.

  Voir "Mise à niveau de JRE sous Linux".

- Pour éviter les pertes de données, vous devez avoir créé une sauvegarde de la base de données Unified Manager en cas de problème lors de la mise à niveau. NetApp vous recommande de déplacer le fichier de sauvegarde du `/opt/netapp/data` répertoire vers un emplacement externe.
- Lors d'une mise à niveau, vous pouvez être invité à confirmer si vous souhaitez conserver les paramètres par défaut précédents pour conserver les données de performances pendant 13 mois ou à les modifier à 6 mois. A la confirmation, les données historiques de performance sont supprimées au bout de 6 mois.
- Vous devez avoir terminé toutes vos opérations en cours d'exécution, 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 la version 8.0.34, le processus de mise à niveau d'Unified Manager met automatiquement à niveau MySQL vers la version 8.0.34.

Étapes

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

   Voir "Téléchargement de Unified Manager pour Linux".

3. Accédez au répertoire cible et développez le pack 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 du système ou aucun logiciel installé ne peut 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 modules manquants sont détectés, effectuez les étapes mentionnées dans "Étapes supplémentaires à effectuer pour les packages manquants". Si aucun paquet n'est 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 et met à niveau les logiciels sous-jacentes nécessaires ainsi que les modules Unified Manager qui s'exécutent sur ceux-ci. En outre, le script de mise à niveau vérifie s'il existe des paramètres de configuration du système ou tout logiciel installé pouvant entrer en conflit avec la mise à niveau. Si le script identifie des problèmes, vous devez les corriger 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 lors de 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 le message affiche une adresse IP ou une URL pour l'interface utilisateur Web de Unified Manager, le nom d'utilisateur de maintenance (uadmin) et le mot de passe par défaut.

   Ce message est similaire à ce qui suit :

   ```
   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/
   ```

Entrez l'adresse IP ou l'URL spécifiée dans une nouvelle fenêtre d'un navigateur Web pris en charge pour démarrer l'interface utilisateur Web de Unified Manager, puis connectez-vous en utilisant le même nom d'utilisateur de maintenance (uadmin) et le même mot de passe que celui défini 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 si vous ne disposez pas des packages requis et les télécharger.

> Ces étapes doivent être effectuées après l'étape *5* de la procédure principale. Cette procédure met à niveau Unified Manager sans exécuter d'étapes supplémentaires pour les mises à niveau.

1. Afficher 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 paquets disponibles dans le répertoire actuel, et les éléments de la section « installation pour dépendances: » Sont les modules qui manquent sur votre

système.

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

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

   Les paquets sont téléchargés dans le répertoire spécifié comme `--downloaddir=`.

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

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

3. Copiez les packages téléchargés dans le répertoire dans lequel vous avez décompressé le bundle Unified Manager sur le système d'installation.
4. Modifiez les répertoires dans 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. Exécuter ces commandes :

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

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

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

Si vous avez déjà 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 8.9.

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

Dans la mesure où cette tâche nécessite la création d'une sauvegarde de 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 que Unified Manager soit hors ligne pendant une période très courte. Des lacunes dans les données collectées apparaissent dans l'interface utilisateur Unified Manager pendant la période pendant laquelle le système Red Hat Enterprise Linux 7.x est arrêté et avant le démarrage du nouveau système Red Hat Enterprise Linux 8.x.

Vérifiez "La gestion des opérations de sauvegarde et de restauration" si vous avez besoin de consulter des instructions détaillées concernant les processus de sauvegarde et de restauration.

Procédez comme suit si vous disposez d'un système de rechange sur lequel vous pouvez installer le logiciel Red Hat Enterprise Linux 8.x afin de pouvoir effectuer la restauration Unified Manager sur ce système alors 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 "Conditions requises pour l'installation et le logiciel Linux".

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

   Voir "Installation de Unified Manager sous Linux".

   Ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification lorsque l'installation est terminée. Le fichier de sauvegarde remplit ces informations lors du processus de restauration.

3. Sur le système Red Hat Enterprise Linux 7.x, dans le menu Administration de l'interface utilisateur Web, créez une sauvegarde Unified Manager, puis copiez le fichier de sauvegarde(`.7z`) et le contenu du sous-répertoire du répertoire du référentiel de base de données(`/database-dumps-repo`) 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`) de l'emplacement externe vers `/opt/netapp/data/ocum-backup/` et les fichiers du référentiel de base de données dans le `/database-dumps-repo` sous-répertoire situé sous le `/ocum-backup` répertoire.
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. Entrez l'adresse IP ou l'URL dans votre navigateur pour démarrer l'interface utilisateur Web 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

Procédez comme suit si vous ne disposez pas d'un système de rechange sur lequel vous pouvez installer le logiciel Red Hat Enterprise Linux 8.x.

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

   Voir "Conditions requises pour l'installation et le logiciel Linux".

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

   Voir "Installation de Unified Manager sous Linux".

   Ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification lorsque l'installation est terminée. Le fichier de sauvegarde remplit ces informations lors du processus de restauration.

5. Copiez le fichier de sauvegarde(`.7z`) de l'emplacement externe vers `/opt/netapp/data/ocum-backup/` et les fichiers du référentiel de base de données dans le `/database-dumps-repo` sous-répertoire situé sous le `/ocum-backup` répertoire.
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. Entrez l'adresse IP ou l'URL dans votre navigateur pour démarrer l'interface utilisateur Web Unified Manager, puis connectez-vous au système.

Mise à niveau de produits tiers après l'installation de Unified Manager

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

Les entreprises qui développent ces produits tiers signalent régulièrement des failles de sécurité. Vous pouvez effectuer la mise à niveau vers des versions plus récentes de ce logiciel à votre propre calendrier.

Mise à niveau d'OpenJDK sous Linux

Vous pouvez mettre 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.

Ce dont vous aurez besoin

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

Vous pouvez mettre à jour les versions OpenJDK dans les familles de versions. Par exemple, vous pouvez mettre à niveau OpenJDK 11.0.14 vers OpenJDK 11.0.17, mais vous ne pouvez pas mettre directement à jour 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. Arrêtez 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
```

Redémarrage de Unified Manager

Il peut s'avérer nécessaire de redémarrer Unified Manager après avoir apporté des modifications à la configuration.

Ce dont vous aurez besoin

Vous devez avoir un accès utilisateur root au serveur Red Hat Enterprise Linux ou CentOS 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 l'ordre suivant :

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Démarrez les services MySQL et Unified Manager dans l'ordre suivant :

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

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

Suppression de Unified Manager

Vous pouvez arrêter et désinstaller Unified Manager à partir de l'hôte Red Hat Enterprise Linux ou CentOS en utilisant une seule commande.

Ce dont vous aurez besoin

- 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 SELinux en "Permissive"" à l'aide de 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 de 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. Arrêter et supprimer Unified Manager du serveur :

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

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

3. **Facultatif :** si nécessaire, supprimez les modules logiciels compatibles, 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 du `/opt/netapp/data` répertoire sont déplacées vers le `/opt/netapp/data/BACKUP` dossier après la désinstallation. La désinstallation d'Unified Manager supprime également les modules Java et MySQL, sauf si les modules sont requis et utilisés par toute autre application du système. Cependant, les données MySQL ne sont pas supprimées.

Suppression de l'utilisateur umadmin personnalisé et du groupe de maintenance

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

La désinstallation standard de Unified Manager ne supprime pas un utilisateur et un compte de maintenance umadmin personnalisés. Vous devez supprimer ces éléments manuellement.

Étapes

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

   ```
   userdel umadmin
   ```

3. Supprimez le groupe de maintenance :

   ```
   groupdel maintenance
   ```

Installation de 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 seule interface. Unified Manager peut être déployé sur un serveur Linux, sur un serveur Windows ou en tant que dispositif virtuel sur un hôte VMware.

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

Informations connexes

"Matrice d'interopérabilité NetApp"

Rôle du serveur Unified Manager

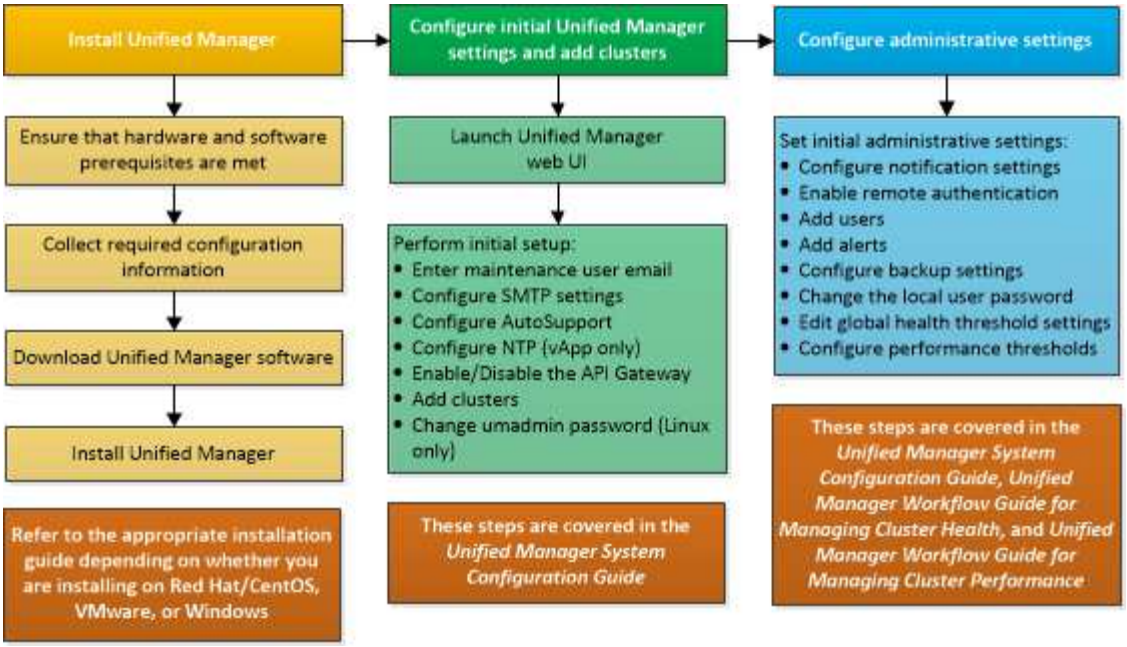
L'infrastructure de serveur Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur d'applications. Il fournit des services d'infrastructure tels que la détection, la surveillance, le contrôle d'accès basé sur des rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations sur le cluster, stocke les données dans la base de données et analyse ces données afin de voir en cas de problème au niveau du cluster.

Présentation de la séquence d'installation

Le workflow d'installation décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.

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



Conditions requises pour l'installation de 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 logiciels, de matériel, de processeur et de mémoire.

NetApp ne prend pas en charge les modifications du code de l'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 d'informations sur l'application de 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

"Matrice d'interopérabilité NetApp"

Configuration minimale requise pour l'infrastructure virtuelle et le système matériel

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

Le tableau suivant affiche les valeurs recommandées pour les ressources mémoire, processeur et espace disque. Ces valeurs ont été qualifiées pour permettre à Unified Manager de satisfaire à des niveaux de performances acceptables.

Configuration matérielle	Paramètres recommandés
RAM	12 Go (minimum requis : 8 Go)
Processeurs	4 processeurs
Capacité du cycle du processeur	9572 MHz au total (exigence minimale : 9572 MHz)
Espace disque disponible	150 Go, où la capacité est allouée 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 disposant d'une petite quantité de mémoire, mais les 12 Go recommandés de RAM garantissent qu'un volume suffisant de mémoire est disponible pour des performances optimales de façon à ce que le système puisse prendre en charge des clusters et des objets de stockage supplémentaires à mesure que votre configuration évolue. Vous ne devez pas définir de limites de mémoire sur la machine virtuelle où Unified Manager est déployé, et ne devez pas activer de fonctions (par exemple, l'option de création de bulles) qui empêchent le logiciel d'utiliser la mémoire allouée au système.

De plus, le nombre de nœuds qu'une seule instance de Unified Manager peut contrôler avant d'installer une deuxième instance de Unified Manager est limité. Pour plus d'informations, consultez le *Guide des meilleures pratiques*.

"Rapport technique 4621 : Guide des meilleures pratiques de Unified Manager"

Les échanges de pages mémoire ont un impact négatif sur les performances du système et de l'application de gestion. La concurrence pour les ressources de processeur indisponibles en raison de l'utilisation globale de l'hôte peut dégrader les performances.

Exigence pour une 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 de Unified Manager.

Besoins en espace pour les sauvegardes

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

Conditions requises pour la connectivité hôte

Le système physique ou virtuel sur lequel vous installez Unified Manager doit être configuré de manière à ce que le nom d'hôte puisse être correctement `ping` attribué à l'hôte lui-même. En cas de configuration IPv6, vérifiez que `ping6` le nom d'hôte a réussi pour vous assurer 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 pendant le déploiement, vous avez 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 du DNS.

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 sur un FQDN valide.

Conditions requises pour l'installation et le logiciel Windows

Pour une installation réussie de Unified Manager sur Windows, veillez à ce que le système sur lequel Unified Manager est installé respecte la configuration logicielle requise.

Logiciel de système d'exploitation

Vous pouvez installer Unified Manager dans les éditions Windows suivantes :

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

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

- Anglais
- Japonais
- Chinois simplifié

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

"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 de 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 afin d'éviter que l'installation ne échoue.

Logiciels tiers

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

- Microsoft Visual C++ 2015 Redistributable package version 14.26.28720,3
- Microsoft Visual C++ Redistributable Packages pour Visual Studio 2013 version 12.0.40660.0
- MySQL Community Edition version 8.0.34
- Python 3.11.6

- OpenJDK version 11.0.20
- 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, assurez-vous que :

- Il utilise le port par défaut.
- Les exemples de bases de données ne sont pas installés.
- Le nom du service est "`MYSQL8'".

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 de Unified Manager avant de mettre à niveau un logiciel tiers. Une fois l'installation du logiciel tiers terminée, vous pouvez redémarrer Unified Manager.

Conditions requises pour l'installation

- Microsoft .NET 4.5.2, ou une version ultérieure, doit être installé.
- Le `temp` 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 dans le lecteur Windows pour la mise en cache des fichiers MSI Unified Manager.
- Le serveur Microsoft Windows sur lequel vous souhaitez installer Unified Manager doit être configuré avec un nom de domaine complet (FQDN) de sorte que les réponses au nom d'hôte et au nom de domaine complet `ping` soient réussies.
- Vous devez désactiver le service mondial de publication Web Microsoft IIS et vous assurer que les ports 80 et 443 sont gratuits.
- Assurez-vous que le paramètre hôte de session de bureau à distance pour « compatibilité RDS de Windows installer » est désactivé pendant l'installation.
- Le port UDP 514 doit être libre et ne doit pas être utilisé par un autre service.
- Vous devez désactiver tous les logiciels antivirus de votre système avant d'installer Unified Manager. Une fois l'installation terminée, veillez à exclure manuellement les chemins suivants de l'analyse antivirus :
  - Répertoire de données Unified Manager, par exemple `C:\ProgramData\NetApp\OnCommandAppData\`
  - Répertoire d'installation de 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 utilisateur Web de Unified Manager, utilisez un navigateur pris

en charge.

La matrice d'interopérabilité répertorie les versions de navigateur prises en charge.

"mysupport.netapp.com/matrix"

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit que les fonctions logicielles sont affichées correctement.

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

Exigences en matière de protocoles et de ports

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

Connexions au serveur Unified Manager

Dans les installations courantes, il n'est pas nécessaire de spécifier les 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, comme Unified Manager tente toujours de s'exécuter sur son port par défaut, vous pouvez entrer à `https://<host>` la place de `https://<host>:443` .

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

Interface	Protocole	Port	Description
Interface Web Unified Manager	HTTP	80	Permet d'accéder à l'interface utilisateur Web d'Unified Manager et de la rediriger automatiquement vers le port sécurisé 443.
L'interface utilisateur et les programmes Web Unified Manager utilisant des API	HTTPS	443	Permet d'accéder de façon sécurisée à l'interface utilisateur Web d'Unified Manager ou de passer des appels d'API. Les appels d'API ne peuvent être effectués qu'à l'aide de HTTPS.
Console de maintenance	SSH/SFTP	22	Permet d'accéder à la console de maintenance et de récupérer les packs de support.

Interface	Protocole	Port	Description
Ligne de commande Linux	SSH/SFTP	22	Permet d’accéder à la ligne de commande Red Hat Enterprise Linux ou CentOS et de récupérer les packs de support.
Syslog	UDP	514	Permet d’accéder aux messages EMS basés sur un abonnement à partir des systèmes ONTAP et de créer des événements en fonction des messages.
REPOS	HTTPS	9443	Permet d’accéder aux événements EMS REST basés sur API en temps réel à partir de systèmes ONTAP authentifiés.
Base de données MySQL	MySQL	3306	Permet d’activer l’accès aux services d’API OnCommand Workflow Automation et OnCommand à Unified Manager.
Courtier QPID AMQP	TCP/IP	56072	Utilisé pour la communication de messages internes.
Courtier QPID AMQP	WebSocket sur TCP	56080	Permet d’écouter sur ce port les messages reçus de ONTAP (agent cloud).
Courtier QPID AMQP	WebSocket sur TCP	56443	Permet d’écouter sur ce port les messages reçus de ONTAP (agent cloud). La communication sur ce port prend en charge le chiffrement fourni par TLS ou SSL.
Courtier QPID AMQP	HTTP	9000	Utilisé pour lancer l’interface utilisateur de gestion AMQP sur cette page.

Le port par défaut pour MySQL, 3306, est limité à localhost uniquement 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 mise à disposition d'autres hôtes à l'aide de l' `Control access to MySQL port 3306`option de la console de maintenance. Pour plus d'informations, voir "Options de menu supplémentaires". Les ports utilisés pour les communications 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 d'Active IQ Unified Manager en cours".

Connexions à partir du serveur Unified Manager

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

Selon l'environnement du client, il est possible 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, serveurs et autres composants :

Destination	Protocole	Port	Description
Adieu les migrations de données onéreuses	HTTPS	443/TCP	Permet de surveiller et de gérer les systèmes de stockage.
Adieu les migrations de données onéreuses	NDMP	10000/TCP	Utilisée pour certaines opérations de restauration Snapshot.
Serveur AutoSupport	HTTPS	443	Permet d'envoyer des informations AutoSupport. Nécessite l'accès à 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 des communications LDAP sécurisées.	Serveur de messagerie

Destination	Protocole	Port	Description
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	Expéditeur du trap SNMP
SNMPv1 ou SNMPv3	162/UDP	Permet d'envoyer des alertes de notification des interruptions SNMP.	Serveur de fournisseur de données externe
TCP	2003	Permet d'envoyer les données de performances à un fournisseur de données externe, comme Graphite.	Serveur NTP
NTP	123/UDP	Permet de synchroniser l'heure sur le serveur Unified Manager avec un serveur de temps NTP externe. (Systèmes VMware uniquement)	Courtier QPID AMQP
TCP/IP	56072	Utilisé pour la communication de messages internes.	Courtier QPID AMQP
WebSocket sur TCP	56080	Permet d'écouter sur ce port les messages reçus de ONTAP (agent cloud).	Courtier QPID AMQP
WebSocket sur TCP	56443	Permet d'écouter sur ce port les messages reçus de ONTAP (agent cloud). La communication via ce port prend en charge le chiffrement fourni par TLS ou SSL.	Syslog

Remplir la fiche

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

Informations sur l'installation de Unified Manager

Détails requis pour installer Unified Manager.

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

Informations sur la configuration de Unified Manager

Détails de la configuration d'Unified Manager après l'installation. Certaines valeurs sont facultatives en fonction de votre configuration.

Réglage	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 d'administrateur Active Directory ou nom distinctif de liaison LDAP	

Réglage	Votre valeur
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom distinctif de la base du serveur d'authentification	
URL du fournisseur d'identités	
Métadonnées du fournisseur d'identités	
Adresses IP de l'hôte de destination de l'interruption SNMP	
Port SNMP	

Informations sur le cluster

Détails des systèmes de stockage que vous gérez à l'aide de Unified Manager.

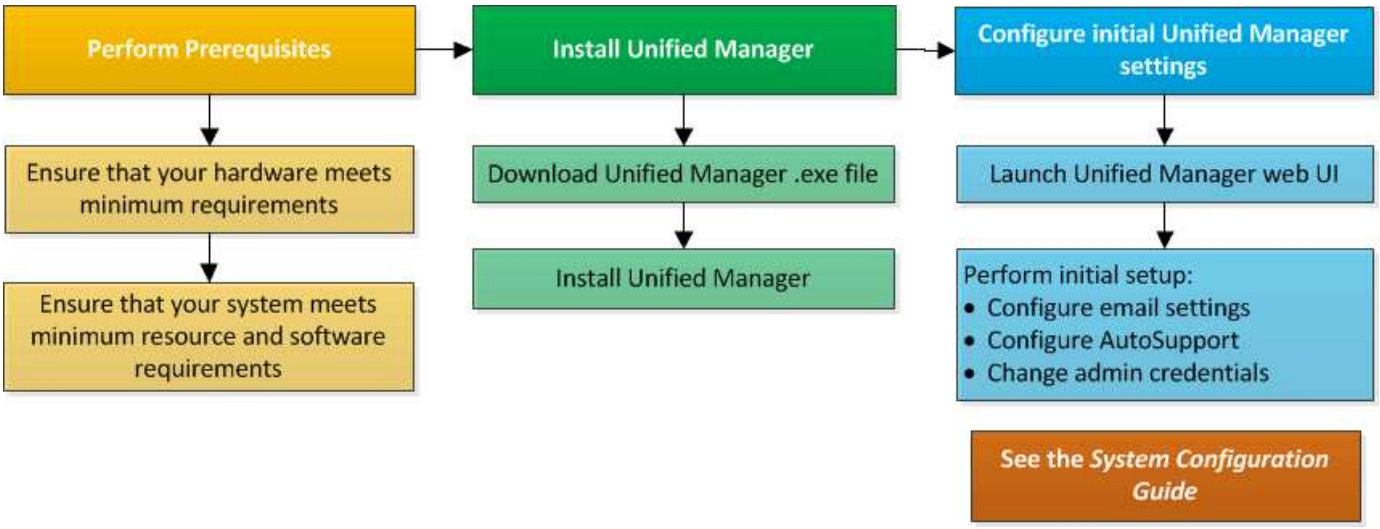
Cluster 1 de N	Votre valeur
Nom d'hôte ou adresse IP de gestion du cluster	
Nom d'utilisateur de l'administrateur ONTAP L'administrateur doit avoir reçu le rôle « admin ».	
Mot de passe administrateur ONTAP	
Protocole	HTTPS

Installation, mise à niveau et suppression du logiciel Unified Manager

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

Présentation du processus d'installation

Le workflow d'installation décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.



Installation de Unified Manager sous Windows

Il est important de comprendre la séquence des étapes à suivre pour télécharger et installer Unified Manager sur Windows.

Installation de Unified Manager

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

Ce dont vous aurez besoin

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

  Voir "Configuration matérielle requise".

  Voir "Conditions requises pour l'installation et le logiciel Windows".

  > À partir de 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 "`".
- Un navigateur Web doit être pris en charge.
- Le mot de passe de l'utilisateur de maintenance Unified Manager doit comporter entre 8 et 20 caractères, et contenir des lettres majuscules ou des 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 d'administrateur local par défaut.
2. Connectez-vous au site de support NetApp et accédez à la page de téléchargement de Unified Manager :

   "Site de support NetApp"

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

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

7. Cliquez sur **Suivant**.
8. Entrez le nom d'utilisateur et le mot de passe pour créer l'utilisateur de maintenance.
9. Dans l'Assistant connexion à la base de données, saisissez le mot de passe racine MySQL.
10. Cliquez sur **Modifier** pour spécifier un nouvel emplacement pour le répertoire d'installation 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 **Finish**.
14. Si un logiciel antivirus actif est installé sur votre système Windows, exclure manuellement les chemins suivants de l'analyse antivirus une fois l'installation terminée :
    - Répertoire des données Unified Manager
    - Répertoire d'installation de Unified Manager
    - Répertoire de données MySQL

L'installation crée plusieurs répertoires :

- Répertoire d'installation

  Il s'agit du répertoire racine de 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 les bases de données MySQL sont stockées, que vous avez spécifié 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 des données applicatives Unified Manager (AppDataDir)

  Il s'agit du répertoire dans lequel toutes les données générées par l'application sont stockées. Cela inclut les journaux, les offres groupées de support, la sauvegarde 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 d'Active IQ Unified Manager en cours".

Exécution d'une installation sans assistance de Unified Manager

Vous pouvez installer Unified Manager sans l'intervention de l'utilisateur à l'aide de l'interface de ligne de commandes. Vous pouvez effectuer l'installation sans assistance en transmettant les paramètres par paires de valeurs de clé.

Étapes

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

Option	Instructions

Si des packages tiers sont pré-installés	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"`
	
	Exemple:
	
	`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"`

Option	Instructions

Si des packages tiers ne sont pas installés	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v CompletePathForLogFile"`
	
	Exemple:
	
	`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"`

L' `/qr`option active le mode silencieux avec une interface utilisateur réduite. Une interface utilisateur de base s'affiche, indiquant la progression de l'installation. Vous n'êtes pas invité à entrer des données. Si des modules tiers tels que JRE, MySQL et 7zip ne sont pas pré-installés, vous devez utiliser l' `/qr`option. L'installation échoue si l' `/qn`option est utilisée sur un serveur sur lequel des modules tiers ne sont pas installés.

L' `/qn`option active le mode silencieux sans interface utilisateur. Aucune interface utilisateur ni aucun détail ne s'affichent pendant l'installation. Vous ne devez pas utiliser cette `/qn` option lorsque des modules tiers ne sont pas installés.

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

   `https://IP address`

Modification du mot de passe JBoss

Vous pouvez réinitialiser le mot de passe JBoss spécifique à l'instance défini lors de l'installation. Vous pouvez éventuellement réinitialiser le mot de passe si votre site requiert cette fonctionnalité de sécurité afin de remplacer le paramètre d'installation de Unified Manager. Cette opération modifie également le mot de passe que JBoss utilise pour accéder à MySQL.

Ce dont vous aurez besoin

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

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

4. Lorsque vous y êtes invité, saisissez le mot de passe 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, un majuscule et des caractères minuscules, et au moins l'un des caractères spéciaux suivants :

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

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 de Unified Manager.

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

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

Toutes les versions de Unified Manager ne peuvent pas effectuer de mise à niveau sans déplacement des données vers les versions ultérieures. Les mises à niveau de Unified Manager sont limitées à un modèle N-2. Ainsi, la mise à niveau ne peut être effectuée que dans les 2 versions suivantes, sur toutes les plateformes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.14 à partir d'Unified Manager 9.12 et 9.13 uniquement.

Si vous exécutez une version antérieure aux versions prises en charge, votre instance Unified Manager doit 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 la version installée est Unified Manager 9.9 et que vous souhaitez effectuer une mise à niveau vers Unified Manager 9.14, vous suivez une séquence de mises à niveau.

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.9 → 9.11
2. Mise à niveau 9.11 → 9.13

3. Mise à niveau 9.13 → 9.14

Pour plus d'informations sur la matrice de chemin de mise à niveau, reportez-vous à la section "Article de la base de connaissances (KB)" .

Mise à niveau d'Unified Manager

Vous pouvez mettre à niveau Unified Manager 9.12 ou 9.13 vers 9.14 en téléchargeant et en exécutant le fichier d'installation sur la plate-forme Windows.

Ce dont vous aurez besoin

- Le système sur lequel vous mettez à niveau Unified Manager doit répondre à la configuration système et logicielle requise.

  Voir "Configuration matérielle requise".

  Voir "Conditions requises pour l'installation et le logiciel Windows".

  > À partir de 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 une version ultérieure 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 la version 8.0.34, le processus de mise à niveau d'Unified Manager met automatiquement à niveau MySQL vers la version 8.0.34. Vous ne devez pas exécuter une mise à niveau autonome d'une version antérieure de MySQL vers la version 8.0.34.
- 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'identifiants valides pour vous connecter au site du support NetApp.
- Pour éviter la perte de données, vous devriez avoir créé une sauvegarde de la machine Unified Manager en cas de problème lors de la mise à niveau.
- Vous devez disposer d'un espace disque suffisant 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 si l'espace disponible est insuffisant.

- Lors d'une mise à niveau, vous pouvez être invité à confirmer si vous souhaitez conserver les paramètres par défaut précédents pour conserver les données de performances pendant 13 mois ou à les modifier à 6 mois. A la confirmation, les données historiques de performance au bout de 6 mois sont supprimées.
- Avant de procéder à la mise à niveau, fermez tous les fichiers ou dossiers ouverts dans *<InstallDir>\JDK* et *MySQL Data Directory*.
- Si un logiciel antivirus actif est installé sur votre système Windows, la mise à niveau d'Unified Manager risque d'échouer. Vous devez désactiver l'intégralité du logiciel antivirus sur votre système avant de mettre à niveau Unified Manager.

Unified Manager n'est pas disponible lors du processus de mise à niveau. Pour effectuer toute opération en cours d'exécution, vous devez effectuer la mise à niveau de Unified Manager.

Si Unified Manager est associé à une instance de OnCommand Workflow Automation et que de nouvelles versions du logiciel sont disponibles pour les deux produits, vous devez déconnecter les deux produits et 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, puis vérifier que les données sont toujours acquises depuis Unified Manager.

Étapes

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

   "Site de support NetApp".

2. Sélectionnez la version requise de Unified Manager et acceptez le contrat de licence utilisateur final (CLUF).
3. Téléchargez le fichier d'installation de Unified Manager Windows dans un répertoire cible du système Windows.
4. Cliquez avec le bouton droit de la souris et exécutez le fichier exécutable du programme d'installation de Unified Manager (.exe) en tant qu'administrateur.

   Unified Manager vous invite à message suivant :

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

5. Cliquez sur **Oui**, puis sur **Suivant**.
6. Entrez le mot de passe racine MySQL8 défini lors de l'installation, puis cliquez sur **Suivant**.
7. Lancez l'interface utilisateur Web sur une nouvelle fenêtre dans un navigateur Web pris en charge et connectez-vous pour utiliser la version mise à niveau d'Unified Manager.
8. Si un logiciel antivirus actif est installé sur votre système Windows, veillez à exclure manuellement les chemins suivants de l'analyse antivirus une fois la mise à niveau terminée :
   - Répertoire des données Unified Manager
   - Répertoire d'installation de 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"`

Mise à niveau de produits tiers

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

Les entreprises qui développent ces produits tiers signalent régulièrement des failles de sécurité. Vous pouvez

effectuer la mise à niveau vers des versions plus récentes de ce logiciel à votre propre calendrier.

Mise à niveau d'OpenJDK

Vous pouvez mettre 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.

Ce dont vous aurez besoin

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

Vous pouvez mettre à jour les versions OpenJDK dans les familles de versions. Par exemple, vous pouvez mettre à niveau OpenJDK 11.0.16 vers OpenJDK 11.0.18, mais vous ne pouvez pas mettre directement à jour 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) du site OpenJDK vers le système cible.

   Par exemple, télécharger `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 ne possédez pas de compte Oracle, allez à la "Connexion au compte Oracle" page pour en créer un.

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. Développez le `zip` fichier.
5. Copiez les répertoires et les fichiers du répertoire résultant `jdk` (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)

Redémarrage de Unified Manager

Il peut s'avérer nécessaire de redémarrer Unified Manager après avoir apporté des modifications à la configuration.

Ce dont vous aurez besoin

Vous devez disposer des privilèges d'administrateur Windows.

Étapes

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

Du…	Arrêter les services dans l'ordre suivant…
Ligne de commande	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
Microsoft Service Manager	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…	Démarrer les services dans l'ordre suivant…
Ligne de commande	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. Service de serveur de gestion NetApp Active IQ (Oncommandsvc) b. Service d'acquisition NetApp Active IQ (Ocie-au)

Désinstallation d'Unified Manager

Vous pouvez désinstaller Unified Manager à l'aide de l'Assistant programmes et fonctionnalités ou en effectuant une désinstallation automatique à partir de l'interface de ligne de commande.

Ce dont vous aurez besoin

- 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 de 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**, effectuez les opérations suivantes :
        i. Accédez à **panneau de configuration** > **Programme et fonctionnalités**.

ii. Sélectionnez Active IQ Unified Manager, puis cliquez sur **Désinstaller**.

- Si vous désinstallez Unified Manager à partir de la ligne de commande, effectuez les opérations suivantes :

  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 de ligne de commande.

Unified Manager est désinstallé de votre système.

2. Désinstallez les packages tiers et données suivants qui ne sont pas supprimés pendant la désinstallation de Unified Manager :
   - Packages tiers : JRE, MySQL, Microsoft Visual C++ 2015 Redistributable, Python, et 7zip
   - Données d'application MySQL générées par Unified Manager
   - Les journaux d'application et le contenu du répertoire des données d'application

Réaliser les tâches de configuration et d'administration

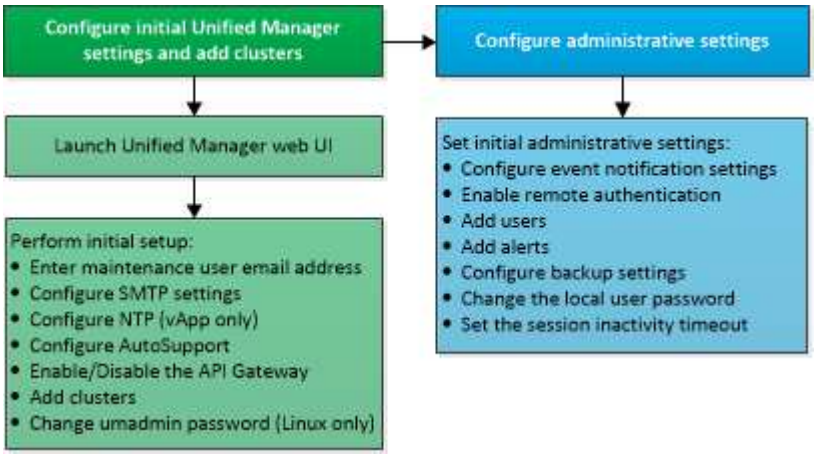
Configuration d'Active IQ Unified Manager en cours

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

La configuration initiale de votre instance Unified Manager nécessite certaines des procédures décrites dans ce manuel. D'autres procédures sont des paramètres de configuration recommandés qui sont utiles pour configurer votre nouvelle instance ou dont vous devez connaître avant de lancer le contrôle régulier de vos systèmes ONTAP.

Présentation de la séquence de configuration

Le workflow de configuration décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.



Accès à l'interface utilisateur Web de Unified Manager

Une fois Unified Manager installé, vous pouvez accéder à l'interface utilisateur Web pour configurer Unified Manager de sorte que vous puissiez commencer à surveiller vos systèmes ONTAP.

Ce dont vous aurez besoin

- Si c'est la première fois que vous accédez à l'interface utilisateur 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 sur un FQDN valide.

- Si le serveur utilise un certificat numérique auto-signé, il se peut que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez accepter le risque de continuer l'accès ou installer un certificat numérique signé par l'autorité de certification pour l'authentification du serveur.

Étapes

1. Pour démarrer l'interface utilisateur Web Unified Manager à partir de votre navigateur, utilisez l'URL affichée à la fin de l'installation. L'URL correspond à l'adresse IP ou au nom de domaine complet (FQDN) du serveur Unified Manager.

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

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

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

Configuration initiale de l'interface utilisateur Web de Unified Manager

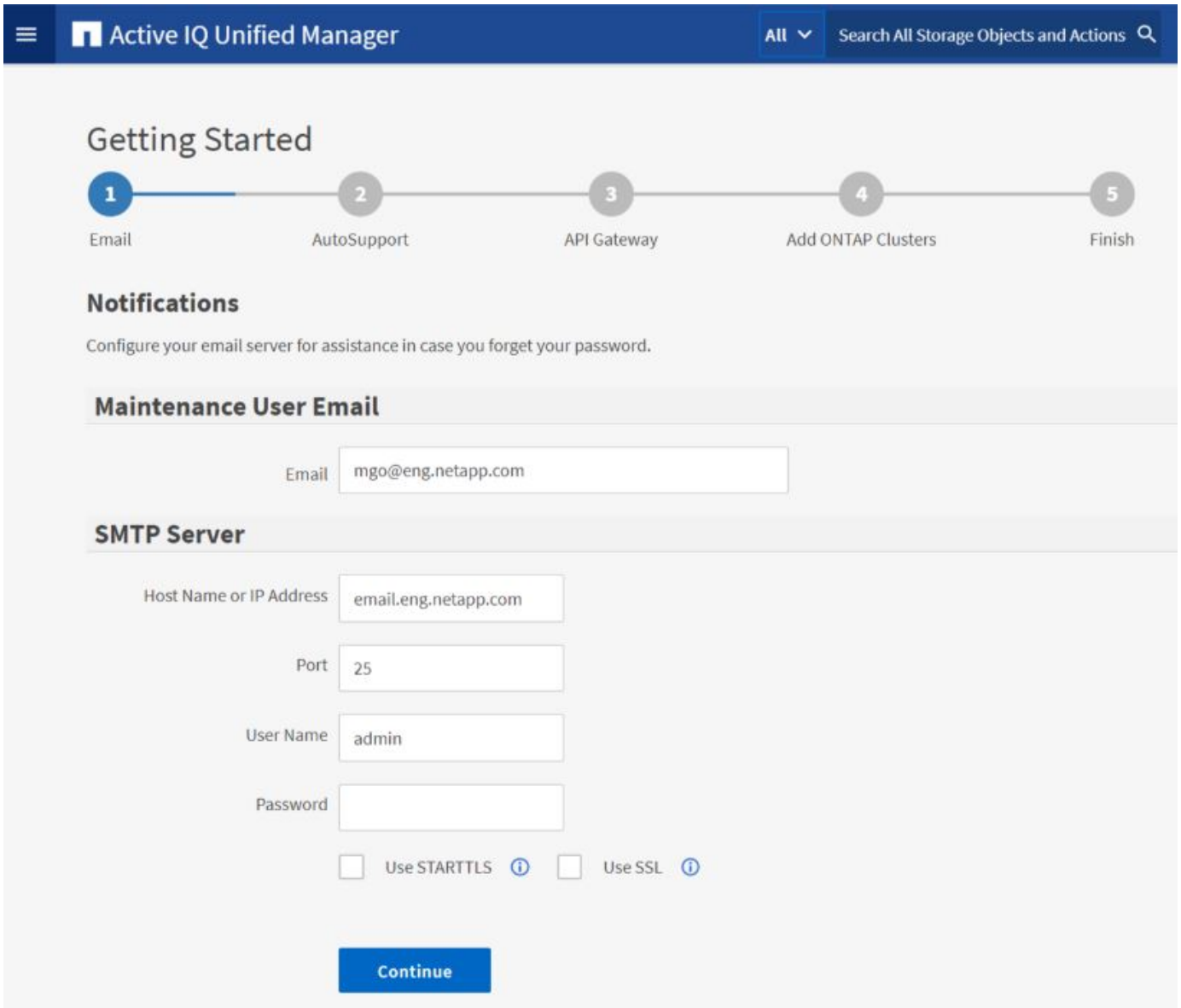
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance et l'hôte du serveur SMTP, ainsi que l'ajout de clusters ONTAP.

Ce dont vous aurez besoin

Vous devez avoir effectué les opérations suivantes :

- L'interface utilisateur Web de Unified Manager a été lancée 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 pendant l'installation

La page mise en route du Gestionnaire unifié Active IQ 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.



Si vous souhaitez modifier l'une de ces options ultérieurement, vous pouvez sélectionner votre choix dans les options générales du volet de navigation gauche de Unified Manager. Notez que le paramètre NTP n'est utilisé que pour les installations VMware et peut être modifié par la suite à l'aide de la console de maintenance Unified Manager.

Étapes

1. Dans la page Configuration initiale de Active IQ Unified Manager, entrez 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 **Use STARTTLS** ou **use SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Continuer**. Vérifiez les détails du certificat et acceptez-le pour continuer avec les paramètres de configuration initiaux de l'interface utilisateur Web.

2. Sur la page AutoSupport, cliquez sur **J'accepte et continue** pour activer l'envoi de messages AutoSupport depuis Unified Manager vers 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 et CentOS, remplacez le mot de passe utilisateur umadmin par la chaîne ""admin" par une chaîne personnalisée.
4. Dans la page configurer la passerelle d'API, indiquez si vous souhaitez utiliser la fonctionnalité de passerelle d'API qui permet à Unified Manager de gérer les clusters ONTAP que vous prévoyez de contrôler à l'aide d'API REST de ONTAP. Cliquez ensuite sur **Continuer**.

   Vous pouvez activer ou désactiver ce paramètre ultérieurement dans l'interface utilisateur Web à partir de **général** > **Paramètres de fonction** > **passerelle API**. Pour plus d'informations sur les API, reportez-vous à la section "Mise en route des API REST de Active IQ Unified Manager".

5. Ajoutez les clusters que vous souhaitez gérer Unified Manager, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez avoir le nom d'hôte ou l'adresse IP de gestion de cluster (IPv4 ou IPv6) avec le nom d'utilisateur et les identifiants de 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 **Storage Management** > **Cluster Setup**.

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

La page mise en route se ferme et la page Tableau de bord de Unified Manager s'affiche.

Ajout de clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir contrôler le cluster. Il est donc possible d'obtenir des informations sur le cluster, notamment son état, sa capacité, ses performances et sa configuration, afin de trouver et de résoudre tous les problèmes potentiels.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez disposer des 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 FQDN ou le nom court que Unified Manager utilise pour se connecter au cluster. Le nom d'hôte doit être résolu sur l'adresse IP de gestion du cluster.

    L'adresse IP de gestion du cluster doit être la LIF de gestion du cluster du serveur virtuel de stockage administratif (SVM). Si vous utilisez une LIF node-management, l'opération échoue.

  - Le cluster doit exécuter la version 9.1 du logiciel ONTAP ou une version ultérieure.
  - Nom d'utilisateur et mot de passe de l'administrateur ONTAP

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

- Le numéro de port à connecter au cluster via le protocole HTTPS (en général le port 443)
- Vous disposez des certificats requis :

  Certificat SSL (HTTPS) : ce certificat appartient à Unified Manager. Un certificat SSL (HTTPS) auto-signé par défaut est généré avec une nouvelle installation de 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 incorporent le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, reportez-vous à la section "Génération d'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 de ONTAP.

  Certificats de communication mutuelle TLS : utilisés pendant la communication mutuelle TLS entre Unified Manager et ONTAP. L'authentification basée sur le certificat est activée pour un cluster, sur la version ONTAP utilisée. Si le cluster exécutant la version ONTAP est inférieur au 9.5, l'authentification basée sur certificat n'est pas activée.

  L'authentification basée sur des certificats n'est pas activée automatiquement sur un cluster si vous mettez à jour une version antérieure 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, reportez-vous à la section "Modification des clusters".

  - Vous pouvez ajouter un cluster depuis l'interface utilisateur Web et l'authentification basée sur certificat est automatiquement activée.
  - Vous pouvez ajouter un cluster via l'interface de ligne de commandes Unified Manager ; l'authentification basée sur des certificats n'est pas activée par défaut. Si vous ajoutez un cluster via l'interface de ligne de commande d'Unified Manager, vous devez le modifier à l'aide de l'interface utilisateur d'Unified Manager. Vous pouvez voir "Commandes CLI Unified Manager prises en charge" pour ajouter un cluster à l'aide de l'interface de ligne de commande Unified Manager.
  - Si l'authentification basée sur les certificats est activée pour un cluster et que vous effectuez la sauvegarde de Unified Manager à partir d'un serveur et que vous effectuez une restauration vers un autre serveur Unified Manager où le nom d'hôte ou l'adresse IP sont modifiés, la surveillance du cluster peut échouer. Pour éviter la défaillance, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, reportez-vous à "Modification des clusters"la section .

+
Certificats de cluster : ce certificat appartient à ONTAP. Vous ne pouvez pas ajouter de 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, reportez-vous à l'article de la base de connaissances (KB) "Comment renouveler un certificat auto-signé ONTAP dans l'interface utilisateur de System Manager" .

- L'espace requis doit être adéquat sur le serveur Unified Manager. Vous ne pouvez pas ajouter un cluster au serveur lorsque plus de 90 % d'espace dans le répertoire de base de données est déjà utilisé.

Dans le cas d'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 **Storage Management** > **Cluster Setup**.
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 au format IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est indiquée dans la grille du cluster et la page de configuration du cluster une fois le cycle de surveillance suivant 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**.

   Une fois les informations de cluster enregistrées, vous pouvez afficher le certificat pour les communications TLS mutuelles pour un cluster.

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

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

> Étant donné que la collecte de données de performances sur 15 jours consomme beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters pour que les sondages de collecte de la continuité des données ne s'exécutent pas simultanément sur un trop grand nombre de clusters. En outre, si vous redémarrez Unified Manager pendant la période de collecte de la continuité des données, la collecte sera interrompue et vous verrez des écarts dans les graphiques de performances pour les périodes manquantes.

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

Informations connexes

"L'installation d'une autorité de certification a signé et renvoyé un certificat HTTPS"

Configuration de Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications vous informant des événements de votre environnement. Avant d'envoyer des notifications, vous devez configurer plusieurs autres options Unified Manager.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Une fois Unified Manager déployé 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 des événements.

Étapes

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

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

2. "Activez 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 d'utilisateurs locaux ou distants et attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous affectez un utilisateur pour recevoir les notifications d'alerte.

5. "Ajouter des alertes".

   Une fois que vous avez ajouté l'adresse e-mail pour envoyer des 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.

Configuration des paramètres de notification d'événement

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications d'alerte lorsqu'un événement est généré ou lorsqu'un événement est affecté à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour envoyer l'alerte et définir différents mécanismes de notification, par exemple, des notifications d'alerte peuvent être envoyées en tant qu'e-mails ou interruptions SNMP.

Ce dont vous aurez besoin

Vous devez disposer des informations suivantes :

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

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

- Le 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 déroutement 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 d'interruption sortante, doivent être identiques pour tous les hôtes de la liste.

Vous devez avoir le rôle Administrateur d'applications ou 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.

   Notes:

   - Si l'adresse de expéditeur est pré-remplie avec l'adresse « + ActiveIQUnifiedManager@localhost.com+ », vous devez la remplacer par une adresse e-mail réelle et opérationnelle pour vous assurer que toutes les notifications par e-mail ont été envoyées correctement.
   - 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 **Use STARTTLS** ou **use SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Save**. 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 est expiré, décochez la case **utiliser STARTTLS** ou **utiliser SSL**, enregistrez les paramètres de notification, puis cochez de nouveau la case **utiliser STARTTLS** ou **utiliser SSL** pour afficher un nouveau certificat.

Activation de 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 Unified Manager pour gérer les objets de stockage et les données.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

> 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 de 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 les communications non sécurisées et 636 comme port par défaut pour les communications sécurisées.

> 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 d'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (À l'aide de la notation LDAP appropriée) • Mot de passe administrateur • Nom distinctif de base (à l'aide de la notation LDAP appropriée)
Ouvrez LDAP	• Nom distinctif de la liaison (dans la notation LDAP appropriée) • Lier le mot de passe • Nom distinctif de base

   Si l'authentification d'un utilisateur Active Directory prend un certain temps ou plusieurs fois, le serveur d'authentification prend probablement beaucoup de temps pour 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 la connexion sécurisée pour le serveur d'authentification, Unified Manager communique avec le serveur d'authentification à l'aide du protocole SSL (Secure Sockets Layer).

4. **Facultatif :** Ajoutez des serveurs d'authentification et testez l'authentification.
5. Cliquez sur **Enregistrer**.

Désactivation des groupes imbriqués à partir de l'authentification à distance

Si l'authentification à distance est activée, vous pouvez désactiver l'authentification des groupes imbriqués de sorte que seuls les utilisateurs individuels, et non les membres du groupe, puissent s'authentifier à distance à Unified Manager. Vous pouvez désactiver les groupes imbriqués si vous souhaitez améliorer le temps de réponse de l'authentification

Active Directory.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications.
- La désactivation des groupes imbriqués n'est applicable que 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 d'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**.

Configuration des services d'authentification

Les services d'authentification permettent l'authentification d'utilisateurs distants ou de groupes distants sur un serveur d'authentification avant de leur donner 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.

Ce dont vous aurez besoin

- Vous devez avoir activé l'authentification à distance.
- Vous devez avoir le rôle Administrateur d'applications.

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, procédez comme ça…
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, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

Si vous sélectionnez…	Alors, procédez comme ça…
OpenLDAP	a. Entrez le nom distinctif de liaison 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, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.
Autres	a. Entrez le nom distinctif de liaison 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, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**. c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. d. Entrez le nom d'utilisateur, l'appartenance au groupe, le groupe d'utilisateurs et les attributs de membre.

Si vous souhaitez modifier le service d'authentification, vous devez supprimer tout serveur d'authentification existant, puis ajouter de nouveaux serveurs d'authentification.

3. Cliquez sur **Enregistrer**.

Ajout de 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 au sein du serveur d'authentification puissent accéder à Unified Manager.

Ce dont vous aurez besoin

- 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 pour que le serveur de gestion puisse authentifier les utilisateurs ou groupes distants sur le serveur d'authentification.
- Vous devez avoir le rôle Administrateur d'applications.

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. Activez ou désactivez l'option **utiliser la connexion sécurisée** :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Activez-la	a. Sélectionnez l'option **utiliser connexion sécurisée**. b. Dans la zone serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. d. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. e. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations sur le certificat, puis cliquez sur **Fermer**. f. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Oui**. Lorsque vous activez l'option **utiliser l'authentification Secure Connection**, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise 636 comme port par défaut pour les communications sécurisées et le port numéro 389 pour les communications non sécurisées.
Désactivez-le	a. Désactivez l'option **utiliser connexion sécurisée**. b. Dans la zone serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Add Authentication Server (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. d. 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.

Test de la configuration des serveurs d'authentification

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

Ce dont vous aurez besoin

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

Si le service d'authentification est défini sur Active Directory et que vous valiez l'authentification d'utilisateurs distants appartenant au groupe principal du serveur d'authentification, les informations relatives au groupe principal ne s'affichent pas dans les résultats de l'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 utilisateur de test, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom d'utilisateur du groupe distant, puis cliquez sur **Test**.

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

Ajout d'alertes

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

Ce dont vous aurez besoin

- Vous devez avoir configuré des 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 adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager à l'aide de la page scripts.
- Vous devez avoir le rôle Administrateur d'applications ou 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 de l'alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page Configuration des alertes, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter une alerte, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis 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 **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que 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 à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Evénements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel 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 affectez 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 qui a été précédemment sélectionné. En outre, 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 les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme 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 averti toutes les 15 minutes

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

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom d'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
   a. Entrez **abc** dans le champ **Name 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-la dans la zone Ressources sélectionnées.
   c. Cliquez sur **exclure**, saisissez **xyz** dans le champ **Nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Evénements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions** et saisissez **sample@domain.com** dans le champ Alert Aces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Modification du mot de passe de l'utilisateur local

Vous pouvez modifier votre mot de passe de connexion utilisateur local afin d'éviter tout risque de sécurité.

Ce dont vous aurez besoin

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 l'administrateur de votre mot de passe. Pour modifier le mot de passe de l'utilisateur de maintenance, reportez-vous à "Utilisation de la console de maintenance"la section .

Étapes

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

   L'option **Modifier le mot de passe** n'est pas affichée 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 second nœud du setup. Les deux instances doivent avoir le même mot de passe.

Définition du délai d'inactivité de la session

Vous pouvez spécifier la valeur du délai d'inactivité pour Unified Manager afin que la session soit automatiquement arrêtée au bout d'un certain temps. Par défaut, le délai est défini sur 4,320 minutes (72 heures).

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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 de fonction**.
2. Dans la page **Feature Settings**, spécifiez le délai d'inactivité en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Aucun délai défini pour que la session ne soit jamais fermée automatiquement	Dans le panneau **délai d'inactivité**, déplacez le curseur vers la gauche (désactivé) et cliquez sur **appliquer**.
Définissez un nombre spécifique de minutes comme valeur de délai d'inactivité	Dans le panneau **délai d'inactivité**, déplacez le curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes, puis cliquez sur **appliquer**.

Modification du nom d'hôte Unified Manager

Il peut être nécessaire de modifier le nom d'hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé.

Les étapes requises pour modifier le nom d'hôte sont différentes selon que Unified Manager s'exécute ou non sur un serveur VMware ESXi, sur un serveur Red Hat ou CentOS Linux, ou sur un serveur Microsoft Windows.

Modification du 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 d'hôte après le déploiement. Si vous modifiez le nom d'hôte, vous devez également régénérer le certificat HTTPS.

Ce dont vous aurez besoin

Vous devez être connecté à Unified Manager en tant qu'utilisateur de maintenance, ou avoir le 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 Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris 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.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous prévoyez d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat de sorte que le nom d'hôte du 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 n'est effectif qu'après le redémarrage de la machine virtuelle Unified Manager.

Étapes

1. Générez 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. Redémarrez la machine virtuelle Unified Manager

   Après la régénération du certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Génération d'un certificat de sécurité HTTPS

Lors de la première installation de Active IQ Unified Manager, un certificat HTTPS par défaut est installé. Vous pouvez générer un nouveau certificat de sécurité HTTPS qui remplace le certificat existant.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom unique (DN) ou si vous voulez une taille de clé plus élevée, ou 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. Pendant la régénération des certificats, vous pouvez définir la taille de la clé et la durée de validité de la clé. Si vous utilisez l' `Reset Server Certificate`option à partir de la console de maintenance, un nouveau certificat HTTPS est créé et valide pendant 397 jours. Ce certificat sera doté d'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 façon dont vous souhaitez générer le certificat :

Les fonctions que vous recherchez…	Procédez comme ça…
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option **régénérer en utilisant les attributs de certificat actuels**.

Les fonctions que vous recherchez…	Procédez comme ça…
Générez le certificat à l'aide de valeurs différentes	Cliquez sur l'option **mettre à jour les attributs de certificat actuels**. 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 entrer des valeurs, par exemple pour l'E-MAIL, LA SOCIÉTÉ, LE SERVICE, Ville, État et pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner la TAILLE DE CLÉ disponible (l'algorithme clé est « RSA ») et LA PÉRIODE DE VALIDITÉ. ⓘ • Les valeurs autorisées pour la taille de clé sont `2048`, `3072` et `4096`. • Les périodes de validité sont de 1 jour minimum à 36500 jours maximum. Même si une période de validité de 36500 jours est autorisée, il est recommandé d'utiliser une période de validité d'au plus 397 jours ou 13 mois. Puisque si vous sélectionnez une période de validité de plus de 397 jours et que vous prévoyez d'exporter une RSC pour ce certificat et de l'obtenir signé par une CA connue, la validité du certificat signé vous sera réduite à 397 jours. • Vous pouvez cocher la case « exclure les informations d'identification locales (par exemple localhost) » si vous souhaitez supprimer les informations d'identification locales du champ autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom.

4. Cliquez sur **Oui** pour régénérer le certificat.
5. Redémarrez le serveur Unified Manager afin que le nouveau certificat prenne effet.
6. Vérifiez les nouvelles informations de certificat en consultant le certificat HTTPS.

Redémarrage de la machine virtuelle Unified Manager

Vous pouvez redémarrer le serveur virtuel à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou en cas de problème avec la machine virtuelle.

Ce dont vous aurez besoin

L'appliance virtuelle est sous tension.

En tant qu'utilisateur de maintenance, vous êtes connecté à la console de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere en utilisant l'option **redémarrer invité**. Pour plus d'informations, consultez la documentation VMware.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration du système** > **redémarrer la machine virtuelle**.

Modification du nom d'hôte Unified Manager sur les systèmes Linux

À un moment donné, il peut être nécessaire de modifier le nom d'hôte de l'ordinateur Red Hat Enterprise Linux ou CentOS sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé lorsque vous répertoriez vos machines Linux.

Ce dont vous aurez besoin

Vous devez avoir 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 Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris du serveur DNS.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous envisagez 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 à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat, de sorte que le nom d'hôte du certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend pas effet tant que la machine Linux n'est pas 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. Pour arrêter le logiciel Unified Manager et le logiciel MySQL associé, saisissez la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Modifiez le nom d'hôte à l'aide de la commande Linux `hostnamectl` :

   ```
   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 peut s'envoyer par commande ping :

   ```
   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 la modification de votre nom d'hôte, redémarrez Unified Manager en entrant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

Activation et désactivation de la gestion du stockage basée sur des règles

Depuis la version 9.7 de Unified Manager, vous pouvez provisionner les charges de travail de stockage (volumes et LUN) sur vos clusters ONTAP, et gérer ces charges de travail en fonction de niveaux de service de performances attribués. Cette fonctionnalité est similaire à la création des charges de travail dans ONTAP System Manager et à l'ajout de règles de QoS. Toutefois, lorsqu'elle est appliquée à l'aide de Unified Manager, vous pouvez provisionner et gérer les charges de travail sur l'ensemble des clusters qui surveillent votre instance Unified Manager.

Vous devez avoir le rôle Administrateur d'applications.

Activation par défaut de cette option, mais désactivation 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	Emplacement
Une page pour provisionner de nouveaux workloads	Disponible à partir de **tâches courantes** > **mise en service**
Une page pour créer des règles de niveau de service de performances	Disponible à partir de **Paramètres** > **stratégies** > **niveaux de service de performance**
Une page pour créer des règles d'efficacité du stockage de performance	Disponible à partir de **Paramètres** > **stratégies** > **efficacité du stockage**
Des panneaux décrivent les performances de vos charges de travail et les IOPS de vos charges de travail actuelles	Disponible dans le tableau de bord

Pour plus d'informations sur ces pages et sur cette fonctionnalité, reportez-vous à l'aide en ligne du produit.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Paramètres de fonction**.
2. Dans la page **Feature Settings**, désactivez ou activez la gestion du stockage basée sur des règles en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Désactiver la gestion du stockage basée sur des règles	Dans le panneau gestion du stockage basée sur des règles*, déplacez le curseur vers la gauche.
Mettez en œuvre la gestion du stockage basée sur des règles	Dans le panneau gestion du stockage basée sur des règles*, déplacez le curseur vers la droite.

Configuration de la sauvegarde Unified Manager

Vous pouvez configurer la fonctionnalité de sauvegarde sur Unified Manager par le biais d'un ensemble d'étapes de configuration à effectuer sur les systèmes hôtes et sur via la console de maintenance.

Pour plus d'informations sur les étapes de configuration, reportez-vous à "La gestion des opérations de sauvegarde et de restauration"la section .

Gestion des paramètres des fonctions

La page Paramètres des fonctions vous permet d'activer et de désactiver certaines fonctions dans Active IQ Unified Manager. Cela inclut la création et la gestion d'objets de stockage basés sur des stratégies, l'activation de la passerelle d'API et de la bannière de connexion, le téléchargement de scripts pour la gestion des alertes, le timing d'une session d'interface utilisateur Web basée sur le temps d'inactivité et la désactivation de la

réception des événements de la plateforme Active IQ.

> La page Paramètres de la fonction n'est disponible que pour les utilisateurs ayant le rôle d'administrateur d'application.

Pour plus d'informations sur le téléchargement de scripts, reportez-vous à "Activation et désactivation du téléchargement des scripts"la section .

Permettre la gestion du stockage basée sur des règles

L'option **gestion du stockage basée sur des règles** permet la gestion du stockage en fonction des objectifs de niveau de service (SLO). Cette option est activée par défaut.

Lorsque vous activez 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 performance et des règles d'efficacité du stockage qui lui sont attribuées.

Vous pouvez choisir d'activer ou de désactiver cette fonction à partir de **général** > **Paramètres de fonction** > **gestion du stockage basée sur des règles**. Lors de l'activation de cette fonction, les pages suivantes sont disponibles pour le fonctionnement et la surveillance :

- Provisionnement (provisionnement de la charge de travail de stockage)
- **Stratégies** > **niveaux de service de performance**
- **Stratégies** > **efficacité du stockage**
- Charges de travail gérées par Performance Service Level sur la page de configuration des clusters
- Performances de la charge de travail sur le **Tableau de bord**

Vous pouvez utiliser les écrans pour créer des niveaux de service Performance et des règles d'efficacité du stockage et 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 qu'aux charges non conformes. Le panneau performances des charges de travail et IOPS des charges de travail vous permet également d'évaluer les performances et la capacité totales, disponibles et utilisées (IOPS) des clusters de votre data Center, basées sur les charges de travail de stockage qui y sont provisionnées.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST Unified Manager pour effectuer certaines de ces fonctions à partir de la catégorie **barre de menus** > **bouton aide** > **Documentation API** > **fournisseur de stockage**. Vous pouvez également entrer 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, reportez-vous à la section "Mise en route des API REST de Active IQ Unified Manager".

Activation de la passerelle API

La fonctionnalité de passerelle d'API permet à Active IQ Unified Manager de devenir un plan de contrôle unique depuis lequel vous pouvez gérer plusieurs clusters ONTAP sans se connecter 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 fonction à partir de **général** > **Paramètres de fonction** > **passerelle API**.

Les API REST de Unified Manager sont différentes des API REST de ONTAP. Toutes les fonctionnalités des API REST de ONTAP ne peuvent pas être disponibles via les API REST de Unified Manager. Toutefois, si vous devez accéder aux API ONTAP pour gérer des fonctionnalités spécifiques qui ne sont pas exposées à Unified Manager, vous pouvez activer la fonctionnalité de passerelle d'API et exécuter les API ONTAP. La passerelle agit comme un proxy pour le tunnel des requêtes API en maintenant les demandes d'en-tête et de corps dans le même format que dans les API ONTAP. Vous pouvez utiliser vos identifiants Unified Manager et exécuter des API spécifiques pour accéder aux clusters ONTAP et les gérer sans passer par les identifiants individuels du cluster. Unified Manager constitue un point de gestion unique pour l'exécution des API dans 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 respectives ONTAP exécutées directement depuis ONTAP.

Une fois cette fonctionnalité activée, vous pouvez exécuter les API REST Unified Manager à partir de la catégorie **barre de menus** > **bouton aide** > **Documentation API** > **passerelle**. Vous pouvez également entrer 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, reportez-vous à la section "Mise en route des API REST de Active IQ Unified Manager".

Spécification du délai d'inactivité

Vous pouvez indiquer 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 fonction ou modifier l'heure dans **général** > **Paramètres de fonction** > **délai d'inactivité**. Une fois cette fonction activée, vous devez spécifier le délai d'inactivité (en minutes) dans le champ **LOGOUT AFTER**, après lequel 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).

Activation des événements du portail Active IQ

Vous pouvez indiquer si vous souhaitez activer ou désactiver les événements du portail Active IQ. Ce paramètre permet au portail Active IQ de détecter et d'afficher d'autres événements relatifs à la configuration du système, au câblage, etc. Cette option est activée par défaut.

Lors de l'activation de 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 par rapport aux 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 et 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 fonction à partir de **général** > **Paramètres de fonction** > **événements de portail Active IQ**. Dans les sites sans accès réseau externe, vous devez télécharger manuellement les règles à partir de **Storage Management** > **Event Setup** > **Upload Rules**.

Cette fonctionnalité est activée par défaut. La désactivation de cette fonctionnalité empêche la découverte ou l'affichage des événements Active IQ sur Unified Manager. Lorsque cette option est désactivée, l'activation de

cette fonctionnalité permet à Unified Manager de recevoir les événements Active IQ sur un cluster à une heure prédéfinie de 00:15 pour le fuseau horaire du cluster.

Activation et désactivation des paramètres de sécurité à des fins de 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 sur 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 clusters et dans la vue **sécurité : toutes les VM de stockage** de la page d'inventaire des VM de stockage.

> Seuls les utilisateurs disposant d'un rôle d'administrateur peuvent modifier ces paramètres.

Les critères de sécurité de vos clusters ONTAP, machines virtuelles de stockage et volumes sont évalués en fonction des recommandations définies dans le "Guide de renforcement de la sécurité des environnements NetApp ONTAP 9". Le panneau sécurité du tableau de bord et de la page sécurité affiche 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 sont activées pour les clusters et les machines virtuelles de stockage qui ont des violations de sécurité.

Personnalisation des paramètres de sécurité

Pour personnaliser les paramètres de contrôle de conformité applicables à votre environnement ONTAP, procédez comme suit :

Étapes

1. Cliquez sur **général > Paramètres des fonctions > Tableau de bord de sécurité > Personnaliser**. La fenêtre contextuelle **Personnaliser les paramètres du tableau de bord de sécurité** s'affiche.

   > Les paramètres de conformité de sécurité que vous activez ou désactivez peuvent directement affecter les vues de sécurité par défaut, les rapports et les rapports planifiés sur les écrans clusters et ordinateurs virtuels de stockage. Si vous avez téléchargé un rapport Excel à partir de ces écrans avant de modifier les paramètres de sécurité, il se peut que les rapports Excel téléchargés soient 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 du cluster, reportez-vous à la section "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 **Storage VM**. Pour plus d'informations sur les options de personnalisation de la conformité des machines virtuelles de stockage, reportez-vous à la section "Catégories de conformité des VM de stockage".

Personnalisation des 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.

Activation et désactivation du téléchargement des scripts

La possibilité de télécharger les scripts vers Unified Manager et de les exécuter est activée par défaut. Si votre entreprise ne souhaite pas autoriser cette activité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Paramètres de fonction**.
2. Dans la page **Feature Settings**, désactivez ou activez le script en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Désactiver les scripts	Dans le panneau **script Upload**, déplacez le curseur vers la gauche.
Activez les scripts	Dans le panneau **script Upload**, déplacez le curseur vers la droite.

Ajout d'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 pendant la connexion, la déconnexion et le délai d'expiration de la session.

Utilisation de la console de maintenance

La console de maintenance vous permet de configurer les paramètres réseau, de configurer et de gérer le système sur lequel Unified Manager est installé, et d'effectuer d'autres tâches de maintenance qui vous aideront à prévenir et à résoudre d'éventuels problèmes.

Fonctionnalités offertes par la console de maintenance

La console de maintenance Unified Manager vous permet de conserver les paramètres de votre système Unified Manager et d'effectuer les modifications nécessaires afin d'éviter tout problème.

Selon le système d'exploitation sur lequel Unified Manager est installé, la console de maintenance offre les fonctions suivantes :

- Résolvez les problèmes liés à votre appliance virtuelle, notamment si l'interface Web Unified Manager n'est pas disponible
- Mise à niveau vers les dernières versions de Unified Manager
- Générez des modules de support pour envoyer au support technique
- Configurez les paramètres réseau
- Modifier le mot de passe utilisateur de maintenance
- Connectez-vous à un fournisseur de données externe pour envoyer des statistiques de performances
- Modifiez la collecte des données de performances interne
- Restaurez les paramètres de base de données et de configuration de Unified Manager à partir d'une version de sauvegarde précédente.

Rôle de l'utilisateur de maintenance

L'utilisateur de maintenance est créé lors de l'installation de Unified Manager sur un système Red Hat Enterprise Linux ou CentOS. Le nom d'utilisateur de maintenance est l'utilisateur « umadmin ». L'utilisateur de maintenance a le rôle d'administrateur d'applications dans l'interface utilisateur Web, et cet utilisateur peut créer des utilisateurs ultérieurs et leur attribuer des rôles.

L'utilisateur qui se sert de la maintenance, ou utilisateur umin, peut également accéder à la console de maintenance de Unified Manager.

Diagnostique des capacités utilisateur

L'accès au diagnostic a pour but de permettre au support technique de vous aider à résoudre les problèmes et de l'utiliser uniquement sur demande du support technique.

L'utilisateur de diagnostic peut exécuter des commandes au niveau du système d'exploitation sur demande du support technique, à des fins de dépannage.

Accès à la console de maintenance

Si l'interface utilisateur Unified Manager n'est pas en cours de fonctionnement ou si vous devez effectuer 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.

Ce dont vous aurez besoin

Vous devez avoir installé et configuré Unified Manager.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.

> Lorsqu'il est installé sur VMware, si vous 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. La procédure suivante permet d'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 à l'aide de votre nom d'utilisateur et de 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 et le mot de passe de l'utilisateur de maintenance (umadmin). c. Entrez la commande `maintenance_console` et appuyez sur entrée.
Fenêtres	a. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Entrez la commande `maintenance_console` et appuyez sur entrée.

Le menu de la console de maintenance Unified Manager s'affiche.

Accès à la console de maintenance à l'aide de la console de machine virtuelle vSphere

Si l'interface utilisateur Unified Manager n'est pas en cours de fonctionnement ou si vous devez effectuer des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour reconfigurer l'appliance virtuelle.

Ce dont vous aurez besoin

- Vous devez être l'utilisateur de maintenance.
- L'appliance virtuelle doit être mise 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 dans la fenêtre de la console pour vous connecter.

4. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de 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 des fonctionnalités spéciales et des paramètres de configuration du serveur Unified Manager.

Selon le système d'exploitation sur lequel Unified Manager est installé, la console de maintenance se compose des menus suivants :

- Mise à niveau de Unified Manager (VMware uniquement)
- Configuration réseau (VMware uniquement)
- Configuration du système (VMware uniquement)
  a. Support/Diagnostics
  b. Réinitialiser le certificat du serveur
  c. Fournisseur de données externes
  d. Sauvegarde Restauration
  e. Configuration de l'intervalle d'interrogation des performances
  f. Désactivez l'authentification SAML
  g. Afficher/modifier les ports d'application
  h. Configuration du journal de débogage
  i. Contrôlez l'accès au port MySQL 3306
  j. Quitter

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 Configuration réseau

Le menu Configuration réseau vous permet de gérer les paramètres réseau. Vous devez utiliser ce menu lorsque l'interface utilisateur de Unified Manager n'est pas disponible.

> Ce menu n'est pas disponible si Unified Manager est installé sur Red Hat Enterprise Linux, CentOS ou sur Microsoft Windows.

Les options de menu suivantes sont disponibles.

- **Paramètres d'adresse IP d'affichage**

  Affiche les paramètres réseau actuels de l'appliance virtuelle, y compris l'adresse IP, le réseau, l'adresse de diffusion, le masque de réseau, la passerelle, Et des serveurs DNS.

- **Modifier les paramètres d'adresse IP**

Permet de modifier n’importe quel paramètre réseau de l’appliance virtuelle, y compris l’adresse IP, le masque de réseau, la passerelle ou les serveurs DNS. Si vous passez des 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 effectuées.

- **Afficher les paramètres de recherche du nom de domaine**

  Affiche la liste de recherche de noms de domaine utilisée pour résoudre les noms d’hôte.

- **Modifier les paramètres de recherche de noms de domaine**

  Vous permet de modifier les noms de domaine pour lesquels vous voulez rechercher lors de la résolution des noms d’hôte. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Afficher les routes statiques**

  Affiche les routes réseau statiques actuelles.

- **Modifier les routes statiques**

  Permet d’ajouter ou de supprimer des routes réseau statiques. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

  - **Ajouter un itinéraire**

    Vous permet d’ajouter une route statique.

  - **Supprimer l’itinéraire**

    Vous permet de supprimer une route statique.

  - **Retour**

    Vous ramène au **Menu principal**.

  - **Quitter**

    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 effectuées.

- **Activer l’interface réseau**

  Active les interfaces réseau disponibles. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Valider les modifications**

  Applique les modifications apportées aux paramètres réseau de l’appliance virtuelle. Vous devez sélectionner cette option pour mettre en œuvre les modifications effectuées, sinon les modifications ne se produisent pas.

- **Ping a Host**

  Commande ping un hôte cible pour confirmer les modifications d'adresse IP ou les configurations DNS.

- **Rétablir les paramètres par défaut**

  Réinitialise tous les paramètres par défaut. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Retour**

  Vous ramène au **Menu principal**.

- **Quitter**

  Quitte la console de maintenance.

Menu Configuration du système

Le menu Configuration du système vous permet de gérer votre appliance virtuelle 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 à partir de ce menu.

Les options de menu suivantes sont disponibles :

- **Affichage de l'état du serveur**

  Affiche l'état actuel du serveur. Les options d'état incluent en cours d'exécution ou non en cours d'exécution.

  Si le serveur n'est pas en cours d'exécution, vous devrez peut-être contacter le support technique.

- **Redémarrer la machine virtuelle**

  Redémarre la machine virtuelle et arrête tous les services. Après le redémarrage, la machine virtuelle et les services redémarrent.

- **Arrêter la machine virtuelle**

  Arrête la machine virtuelle et arrête tous les services.

  Vous ne pouvez sélectionner cette option qu'à partir de la console de la machine virtuelle.

- **Modifier <utilisateur connecté> Mot de passe utilisateur**

  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) de la machine virtuelle.

- **Augmenter la taille du disque d'échange**

  Augmente la taille du disque d'échange (disque 2) de la machine virtuelle.

- **Changer fuseau horaire**

  Change le fuseau horaire en fonction de votre emplacement.

- **Changer serveur NTP**

  Modifie les paramètres du serveur NTP, tels que l'adresse IP ou le nom de domaine complet (FQDN).

- **Modifier le service NTP**

  Permet de basculer entre les `ntp` services et `systemd-timesyncd`.

- **Restaurer à partir d'une sauvegarde Unified Manager**

  Restaure les paramètres de base de données et de configuration 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.

- **Retour**

  Quitte le menu Configuration du système et revient au menu principal.

- **Quitter**

  Quitte le menu de la console de maintenance.

Menu support and Diagnostics

Le menu support and Diagnostics vous permet de générer un bundle de support que vous pouvez envoyer au support technique pour obtenir de l'aide au dépannage.

Les options de menu suivantes sont disponibles :

- **Générer ensemble support léger**

  Permet de produire un pack de support léger contenant seulement 30 jours d'enregistrements de base de données de configuration et de journaux — cela exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage de mémoire du serveur.

- **Générer un pack de support**

  Permet de créer un ensemble de support complet (fichier 7-Zip) contenant des informations de diagnostic dans le répertoire de base de l'utilisateur de diagnostic. Si votre système est connecté à Internet, vous pouvez également télécharger le pack de support à NetApp.

Le fichier contient des informations générées par un message AutoSupport, le contenu de la base de données Unified Manager, des données détaillées sur les composants internes du serveur Unified Manager et des journaux de niveau détaillé qui ne sont pas normalement inclus dans les messages AutoSupport ou dans le bundle 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 options de menu suivantes sont disponibles :

- **Réinitialiser le certificat du serveur**

  Régénère le certificat du serveur HTTPS.

  Vous pouvez régénérer le certificat de serveur dans l'interface utilisateur graphique Unified Manager en cliquant sur **général** > **certificats HTTPS** > **régénérer le certificat HTTPS**.

- **Désactiver l'authentification SAML**

  Désactive l'authentification SAML de sorte que le fournisseur d'identités ne fournit plus d'authentification d'identification pour les utilisateurs qui accèdent à l'interface graphique Unified Manager. Cette option console est généralement utilisée lorsqu'un problème de serveur IDP ou de configuration SAML empêche les utilisateurs d'accéder à l'interface graphique Unified Manager.

- **Fournisseur de données externes**

  Fournit des options pour connecter Unified Manager à un fournisseur de données externe. Une fois la connexion établie, les données relatives aux performances sont envoyées à un serveur externe afin que les experts en performance du stockage puissent créer un diagramme des indicateurs de performances à l'aide d'un logiciel tiers. Les options suivantes sont affichées :

  - **Configuration du serveur d'affichage**--affiche les paramètres de connexion et de configuration actuels pour un fournisseur de données externe.
  - **Ajouter/Modifier la connexion au serveur**--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**--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, reportez-vous aux rubriques sous "La 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 des données statistiques de performances à partir de 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 collections des grands groupes ne sont pas réalisées à temps.

- **Afficher/Modifier les ports d'application**

  La fonctionnalité offre une option permettant de modifier les ports par défaut qu'Unified Manager utilise pour les protocoles HTTP et HTTPS, si nécessaire pour la 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 à localhost uniquement lors d'une nouvelle installation de 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 si celui-ci est activé uniquement pour l'hôte local dans votre environnement, vous pouvez également rendre ce port disponible pour les hôtes distants. Sinon, lorsque cette option est activée pour tous les hôtes, vous pouvez limiter l'accès à ce port à localhost uniquement. Si l'accès était précédemment activé sur les hôtes distants, 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 basculé la visibilité du port et désactiver les paramètres du pare-feu si les paramètres sont configurés pour restreindre l'accès au port MySQL 3306.

- **Quitter**

  Quitte le menu de la console de maintenance.

Modification du mot de passe utilisateur de maintenance sous Windows

Vous pouvez modifier le mot de passe utilisateur responsable de la maintenance d'Unified Manager si nécessaire.

Étapes

1. Dans la page de connexion à l'interface utilisateur Web de 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. Entrez le nom d'utilisateur et cliquez sur **Envoyer**.

   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 **reset mot de passe** dans l'e-mail et définissez le nouveau mot de passe.
4. Revenez à l'interface utilisateur Web et connectez-vous à Unified Manager à l'aide du nouveau mot de passe.

Modification du 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 Unified Manager umadmin immédiatement après avoir terminé l'installation. Si nécessaire, vous pouvez modifier le mot de passe à nouveau ultérieurement.

Ce dont vous aurez besoin

- Unified Manager doit être installé sur un système Red Hat Enterprise Linux ou CentOS Linux.
- Vous devez disposer des informations d'identification 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. Modifier le mot de passe umadmin :

   ```
   passwd umadmin
   ```

   Le système vous invite à entrer un nouveau mot de passe pour l'utilisateur umadmin.

Changement des ports que Unified Manager utilise pour les protocoles HTTP et HTTPS

Le cas échéant, les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS peuvent être modifiés après l'installation. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

Ce dont vous aurez besoin

Vous devez disposer d'un ID 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 peut rendre le système inaccessible, ce qui vous oblige à contacter le support client pour obtenir une résolution.

L'instance de Unified Manager est redémarrée automatiquement après avoir modifié le port. Assurez-vous donc que le système est bien arrêté pendant un court laps de temps.

1. Connectez-vous en utilisant SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

   Les invites de la console de maintenance Unified Manager s'affichent.

2. Tapez le numéro de l'option de menu **Afficher/Modifier les ports d'application**, puis appuyez sur entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe utilisateur pour la maintenance.
4. Saisissez les nouveaux numéros de port pour les ports HTTP et HTTPS, puis appuyez sur entrée.

   Si vous laissez un numéro de port vide, le port par défaut du protocole est affecté.

   Vous êtes invité à modifier les ports et à redémarrer Unified Manager maintenant.

5. Tapez **y** pour modifier les ports et redémarrer Unified Manager.
6. Sortir de 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.

Ajout d'interfaces réseau

Vous pouvez ajouter de nouvelles interfaces réseau si vous devez séparer le trafic réseau.

Ce dont vous aurez besoin

Vous devez avoir ajouté l'interface réseau à l'appliance virtuelle à l'aide de vSphere.

L'appliance virtuelle 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 du système** > **redémarrer le système d'exploitation**.

   Après le redémarrage, la console de maintenance peut détecter l'interface réseau qui vient d'être 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.

   Si vous utilisez une interface statique ou si DHCP n'est pas détecté, vous êtes invité à entrer les paramètres réseau.

   Après avoir saisi 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.

Ajout d'espace disque au répertoire de base de données Unified Manager

Le répertoire de base de données Unified Manager contient toutes les données d'intégrité et de performances collectées à partir des systèmes ONTAP. Dans certaines circonstances, vous devrez peut-être augmenter la taille du répertoire de base de données.

Par exemple, le répertoire de la base de données peut devenir complet si Unified Manager collecte les données à partir d'un grand nombre de clusters où chaque cluster possède plusieurs nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de base de données est plein à 90 % et un événement

critique lorsque le répertoire est plein à 95 %.

> Aucune donnée supplémentaire n'est collectée depuis les clusters après le répertoire dans son intégralité, à 95 %.

Les étapes requises pour ajouter de la capacité au répertoire de données sont différentes selon que Unified Manager s'exécute ou non sur un serveur VMware ESXi, sur un serveur Red Hat ou CentOS Linux, ou sur un serveur Microsoft Windows.

Ajout d'espace au répertoire de données de l'hôte Linux

Si vous avez alloué un espace disque insuffisant au `/opt/netapp/data` répertoire pour prendre en charge Unified Manager lors de la configuration initiale de l'hôte Linux, puis de l'installation d'Unified Manager, vous pouvez ajouter de l'espace disque après l'installation en augmentant l'espace disque sur le `/opt/netapp/data` répertoire.

Ce dont vous aurez besoin

Vous devez avoir un accès utilisateur root à la machine Red Hat Enterprise Linux ou CentOS 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 répertoire actuel `/opt/netapp/data`.
4. Copiez le contenu et la configuration des privilèges du répertoire existant `/opt/netapp/data` dans 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 dans un dossier existant `/opt/netapp/data` :

   ```
   se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
   head -1
   ```

   Le système renvoie une confirmation similaire à ce qui suit :

```
echo $se_type
mysqld_db_t
```

a. Lancer la commande chcon pour définir le type se Linux du répertoire de sauvegarde :

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Supprimez le contenu du `/opt/netapp/data` répertoire :

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Augmentez 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 devez pas essayer de monter en `/opt/netapp/data` tant que partage NFS ou CIFS. Parce que, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` peuvent ne pas fonctionner comme prévu.

8. Vérifiez que le `/opt/netapp/data` propriétaire du répertoire (mysql) et le groupe (root) sont inchangés :

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   Le système renvoie une confirmation similaire à ce qui suit :

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. Si se Linux est activé, vérifiez que le contexte du `/opt/netapp/data` 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 ce qui suit :

   ```
   -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
   /opt/netapp/data/abc
   ```

10. Supprimez le fichier abc pour que ce fichier externe ne provoque pas d'erreur dans la base de données à l'avenir.

11. Copiez à nouveau le contenu des données de sauvegarde dans le répertoire développé `/opt/netapp/data` :

    ```
    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, démarrer 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
```

Ajout d'espace au disque de données de la machine virtuelle VMware

Si vous devez augmenter la quantité d'espace sur le disque de données de 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.

Ce dont vous aurez besoin

- Vous devez avoir accès au client vSphere.
- Aucun snapshot ne doit être stocké localement sur la machine virtuelle.
- 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`. Pour plus de détails, consultez la documentation VMware.

   Dans de rares cas, le déploiement de Unified Manager utilise « disque dur 2 » pour le disque de données au lieu de « disque dur 3 ». Si cela s'est produit au cours de votre déploiement, vous augmentez l'espace disque le plus important. 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 sur 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 du système**.
5. Dans le menu Configuration du système, entrez le numéro de l'option **augmenter la taille du disque de données**.

Ajout d'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.

Ce dont vous aurez besoin

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 de l'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 de la rubrique Microsoft : "Extension d'un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes de la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes du sujet VMware : "Augmentation de la taille d'une partition de disque"

Gestion de l'accès des utilisateurs

Vous pouvez créer des rôles et attribuer des fonctions permettant de contrôler l'accès des utilisateurs à Active IQ Unified Manager. Vous pouvez identifier les utilisateurs disposant des fonctionnalités requises pour accéder aux objets sélectionnés dans Unified Manager. Seuls les utilisateurs disposant de ces rôles et fonctionnalités peuvent gérer les objets dans Unified Manager.

Ajout d'utilisateurs

Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données à l'aide de 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 et les données de stockage à l'aide de Unified Manager ou afficher les données dans une base de données.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications.
- 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 de sorte qu'un fournisseur d'identités authentifie les utilisateurs qui accèdent à l'interface graphique, assurez-vous que ces utilisateurs sont définis comme des utilisateurs « réels ».

L'accès à l'interface utilisateur n'est pas autorisé pour les utilisateurs de type « local » ou « provenance » lorsque l'authentification SAML est activée.

Si vous ajoutez un groupe à partir de Windows Active Directory, tous les membres directs et sous-groupes imbriqués peuvent s'authentifier auprès d'Unified Manager, à moins que les sous-groupes imbriqués ne soient 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 entrez les informations requises pour l'utilisateur, vous devez spécifier une adresse électronique unique pour cet utilisateur. Vous devez éviter de spécifier des adresses e-mail partagées par plusieurs utilisateurs.

4. Cliquez sur **Ajouter**.

Création d'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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Les utilisateurs de base de données offrent une intégration à Workflow Automation et un accès à des vues de base de données spécifiques aux rapports. Les utilisateurs de base de données n'ont pas accès à l'interface utilisateur Web d'Unified Manager ou 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 **Database User** 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 **role**, sélectionnez le rôle approprié.

Si vous êtes…	Choisissez ce rôle
Connexion de Unified Manager à Workflow Automation	Schéma d'intégration
Accès aux rapports et autres vues de base de données	Schéma du rapport

6. Cliquez sur **Ajouter**.

Modification des paramètres utilisateur

Vous pouvez modifier les paramètres utilisateur, tels que l'adresse e-mail et le rôle, qui sont spécifiés par chaque utilisateur. Par exemple, vous pouvez modifier le rôle d'un utilisateur qui est un opérateur de stockage et attribuer des privilèges d'administrateur de stockage à cet utilisateur.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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 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, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue Modifier l'utilisateur, modifiez les paramètres spécifiés pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

Affichage des utilisateurs

Vous pouvez utiliser la page utilisateurs pour afficher la liste des utilisateurs qui gèrent les objets et les données de stockage à l'aide de Unified Manager. Vous pouvez afficher des détails sur les utilisateurs, tels que le nom d'utilisateur, le type d'utilisateur, l'adresse e-mail et le rôle attribué aux utilisateurs.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.

Suppression d'utilisateurs ou de groupes

Vous pouvez supprimer un ou plusieurs utilisateurs de la base de données du serveur de gestion pour empêcher certains utilisateurs d'accéder à Unified Manager. Vous pouvez également supprimer des groupes de sorte que tous les utilisateurs du groupe ne puissent plus accéder au serveur de gestion.

Ce dont vous aurez besoin

- Lorsque vous supprimez des groupes distants, vous devez avoir réaffecté les événements qui sont affectés aux utilisateurs des groupes distants.

  Si vous supprimez des utilisateurs locaux ou distants, les événements qui sont affectés à ces utilisateurs sont automatiquement affectés.

- Vous devez avoir le rôle Administrateur d'applications.

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.

En quoi consiste le RBAC

Le contrôle d'accès basé sur des rôles (RBAC) vous permet de contrôler l'accès aux différentes fonctionnalités et ressources du serveur Active IQ Unified Manager.

Rôle du contrôle d'accès basé sur des rôles

Le contrôle d'accès basé sur des 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 aux administrateurs sélectionnés, vous devez configurer des comptes d'administrateur pour eux. Si vous souhaitez limiter 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 le contrôle d'accès basé sur les rôles pour les autorisations de connexion utilisateur et de rôle. Si vous n'avez pas modifié les paramètres par défaut du serveur de gestion pour l'accès administrateur utilisateur, vous n'avez pas besoin de vous connecter pour les afficher.

Lorsque vous lancez une opération qui nécessite un Privileges spécifique, 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 d'administrateur d'application.

Définitions des types d'utilisateur

Un type d'utilisateur spécifie le type de compte que l'utilisateur détient 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 a son propre rôle, qui est attribué par un utilisateur avec le rôle Administrateur.

Les types d'utilisateurs Unified Manager sont les suivants :

- **Utilisateur de maintenance**

  Créée 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 ou CentOS, l'utilisateur chargé de la maintenance se voit attribuer le nom d'utilisateur « umadmin ».

- **Utilisateur local**

  Accède à l'interface utilisateur Unified Manager et effectue des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle d'administrateur d'applications.

- **Groupe distant**

  Groupe d'utilisateurs qui accèdent à l'interface utilisateur 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 peuvent accéder à l'interface utilisateur d'Unified Manager à l'aide de leurs identifiants individuels. Les groupes distants peuvent effectuer des fonctions en fonction de leurs rôles attribués.

- **Utilisateur distant**

  Permet d'accéder à l'interface utilisateur Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Un utilisateur distant effectue des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle d'administrateur d'applications.

- **Utilisateur de base de données**

  Possède 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 d'API.

Définitions des rôles utilisateur

L'utilisateur de maintenance ou l'administrateur d'applications 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 que vous avez attribué et des privilèges qu'il contient.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

  Affiche les informations relatives au système de stockage et les autres données collectées par Unified Manager, y compris les historiques et les tendances de la capacité. Ce rôle permet à l'opérateur de stockage d'afficher, d'affecter, d'accuser réception, de résoudre et d'ajouter des notes aux événements.

- **Administrateur de stockage**

  Configuration des opérations de gestion du stockage dans Unified Manager Ce rôle permet à l'administrateur du stockage de configurer des seuils et de créer des alertes ainsi que d'autres options et règles spécifiques à la gestion du stockage.

- **Administrateur d'applications**

  Configure des paramètres sans rapport avec la gestion du stockage. Ce rôle permet de gérer les utilisateurs, les certificats de sécurité, l'accès à la base de données et les options administratives, y compris l'authentification, SMTP, mise en réseau et AutoSupport.

> Lorsque Unified Manager est installé sur des systèmes Linux, l'utilisateur initial ayant le rôle d'administrateur d'applications est automatiquement nommé « umadmin ».

- **Schéma d'intégration**

  Ce rôle permet un accès en lecture seule aux vues de bases de données Unified Manager pour l'intégration de Unified Manager avec OnCommand Workflow Automation (WFA).

- **Schéma de rapport**

  Ce rôle permet un accès en lecture seule au reporting et à d'autres vues de base de données directement depuis la base de données Unified Manager. Les bases de données qui peuvent être affichées sont les suivantes :

  - vue_modèle_netapp
  - performances_netapp
  - ocum
  - rapport_ocum
  - ocum_report_birt
  - opm
  - scatemonitor

Fonctionnalités et rôles utilisateur de Unified Manager

En fonction du rôle d'utilisateur que vous avez 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 effectuer :

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Afficher des informations sur le système de stockage	•	•	•	•	•
Affichez d'autres données, telles que les historiques et les tendances en matière de capacité	•	•	•	•	•
Afficher, attribuer et résoudre les événements	•	•	•		

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Affichez les objets des services de stockage, tels que les associations de SVM et les pools de ressources	•	•	•		
Afficher les stratégies de seuil	•	•	•		
Gérez les objets de service de stockage, tels que les associations de SVM et les pools de ressources		•	•		
Définir des alertes		•	•		
Gérer les options de gestion du stockage		•	•		
Gérez les règles de gestion du stockage		•	•		
Gérer les utilisateurs			•		
Gérer les options administratives			•		
Définir des règles de seuil			•		
Gérer l'accès à la base de données			•		

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Gérez l'intégration avec WFA et fournissez l'accès aux vues de base de données				•	
Planifiez et enregistrez des rapports		•	•		
Exécuter les opérations « réparer » à partir des actions de gestion		•	•		
Fournir un accès en lecture seule aux vues de base de données					•

Gestion des paramètres d'authentification SAML

Une fois que vous avez configuré les paramètres d'authentification à distance, vous pouvez activer l'authentification SAML afin que les utilisateurs distants soient authentifiés par un fournisseur d'identités sécurisé avant d'accéder à l'interface utilisateur Web Unified Manager.

Notez que seuls les utilisateurs distants ont accès à l'interface utilisateur graphique 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 aucun impact sur les utilisateurs qui accèdent à la console de maintenance.

Exigences du fournisseur d'identités

Lors de la configuration d'Unified Manager pour utiliser un fournisseur d'identités (IDP) pour effectuer l'authentification SAML de tous les utilisateurs distants, vous devez connaître certains paramètres de configuration requis afin que la connexion à Unified Manager soit établie.

Vous devez entrer l'URI Unified Manager et les métadonnées dans le serveur IDP. Vous pouvez copier ces informations à partir de la page Unified ManagerSAML Authentication. Unified Manager est considéré comme le fournisseur de services dans la norme SAML.

Normes de chiffrement prises en charge

- Advanced Encryption Standard (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Des fournisseurs d'identité validés

- Hurlent
- ADFS (Active Directory Federation Services)

Configuration requise pour ADFS

- Vous devez définir trois règles de sinistre dans l'ordre suivant qui sont nécessaires à Unified Manager pour analyser les réponses SAML ADFS pour cette entrée de confiance de tiers de confiance.

Règle de réclamation	Valeur
SAM-account-name	ID nom
SAM-account-name	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 des formulaires » pour que les utilisateurs puissent recevoir une erreur lors de la déconnexion d'Unified Manager . Voici la procédure à suivre :
  a. Ouvrez la console de gestion ADFS.
  b. Cliquez sur le dossier Authentication Policies dans l'arborescence de gauche.
  c. Sous actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.
  d. Définissez la méthode d'authentification Intranet sur « authentification des formulaires » au lieu de « authentification Windows » par défaut.
- Dans certains cas, la connexion via le PDI est rejetée lorsque le certificat de sécurité Unified Manager est signé avec une autorité de certification. Il existe deux solutions pour résoudre ce problème :
  - Suivez les instructions indiquées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour les certificats CA chaînés associés à la partie de confiance :

    "Désactiver le contrôle de révocation par confiance de la partie utilisatrices"

  - Demandez au serveur CA de se trouver dans le serveur ADFS pour signer la demande d'autorisation de serveur Unified Manager.

Autres exigences de configuration

- L'inclinaison de l'horloge de Unified Manager est définie sur 5 minutes, la différence de temps entre le serveur IDP et le serveur Unified Manager ne peut pas dépasser 5 minutes, sinon l'authentification échouera.

Activation de l’authentification SAML

Vous pouvez activer l’authentification SAML (Security assertion Markup Language) pour que les utilisateurs distants soient authentifiés par un fournisseur d’identités sécurisé avant d’accéder à l’interface utilisateur Web d’Unified Manager.

Ce dont vous aurez besoin

- Vous devez avoir configuré l’authentification à distance et vérifié qu’elle a réussi.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle Administrateur d’applications.
- Le fournisseur d’identités doit être pris en charge par Unified Manager et doit être configuré.
- Vous devez disposer de l’URL IDP et des métadonnées.
- 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 le IDP n’a pas été configuré avec les informations d’hôte du serveur Unified Manager. Vous devez donc être prêt à effectuer les deux parties de la connexion avant de lancer le processus de configuration. Le IDP peut être configuré avant ou après la configuration de Unified Manager.

Seuls les utilisateurs distants ont accès à l’interface utilisateur graphique 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 aucun impact sur les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPI.

Unified Manager est redémarré automatiquement après la configuration SAML de 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 sont affichés.

3. Entrez l’URI du IDP et les métadonnées IDP requises pour connecter le serveur Unified Manager au serveur IDP.

   Si le serveur IDP est accessible directement à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IDP Metadata** après avoir saisi l’URI IDP pour remplir automatiquement le champ IDP Metadata.

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 pour le moment.

5. Cliquez sur **Enregistrer**.

   Un message s’affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants autorisés saisissent leurs identifiants sur la page de connexion du fournisseur intégré au lieu de la page de connexion de Unified Manager.

Si ce n'est pas déjà fait, accédez à votre IDP et entrez l'URI du serveur Unified Manager et les métadonnées pour terminer la configuration.

> Lorsque vous utilisez ADFS en tant que fournisseur d'identité, l'interface graphique Unified Manager ne respecte pas le délai d'attente de l'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 de fonction** > **délai d'inactivité**.

Modification du fournisseur d'identités utilisé pour l'authentification SAML

Vous pouvez modifier le fournisseur d'identités utilisé par Unified Manager pour authentifier les utilisateurs distants.

Ce dont vous aurez besoin

- Vous devez disposer de l'URL IDP et des métadonnées.
- Vous devez avoir accès au PDI.

Le nouveau IDP peut être configuré avant ou après avoir configuré Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification SAML**.
2. Entrez le nouveau URI du IDP et les métadonnées IDP requises pour connecter le serveur Unified Manager au IDP.

   Si l'IDP est accessible directement à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **extraire les métadonnées IDP** après avoir saisi l'URL IDP pour remplir automatiquement le champ métadonnées IDP.

3. Copiez l'URI des métadonnées de Unified Manager ou enregistrez les métadonnées dans un fichier texte XML.
4. Cliquez sur **Enregistrer la configuration**.

   Un message s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouveau IDP et entrez l'URI du serveur Unified Manager et les métadonnées pour terminer la configuration.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants autorisés saisissent leurs identifiants sur la nouvelle page de connexion IDP au lieu de l'ancienne page de connexion IDP.

Mise à jour des paramètres d’authentification SAML après une modification du certificat de sécurité 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 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**, entrez 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 Unified Manager à l’aide du FQDN 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/authentification**, sélectionnez l’onglet **authentification 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**.

   Un message s’affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

7. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.
8. Accédez à votre serveur IDP, puis entrez l’URI du serveur Unified Manager et les métadonnées pour terminer la configuration.

Fournisseur d'identité	Étapes de configuration
ADFS	a. Supprimez l'entrée de confiance de la partie de confiance existante dans l'interface graphique de gestion ADFS. b. Ajoutez une nouvelle entrée de confiance de partie utilisatrice à l'aide du `saml_sp_metadata.xml` à partir du serveur Unified Manager mis à jour. c. Définissez les trois règles de sinistre requises par Unified Manager pour analyser les réponses SAML ADFS pour cette entrée de confiance de tiers de confiance. d. Redémarrez le service Windows ADFS.
Hurlent	a. Mettez à jour le nouveau nom de domaine complet du serveur Unified Manager dans les `attribute-filter.xml` fichiers et `relying-party.xml`. b. Redémarrez le serveur Web Apache Tomcat et attendez que le port 8005 soit en ligne.

9. Connectez-vous à Unified Manager et vérifiez que l'authentification SAML fonctionne comme prévu via votre IDP.

Désactivation de l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs distants via un fournisseur d'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager. Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, exécutent l'authentification d'identification.

Une fois l'authentification SAML désactivée, 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 graphique.

> Unified Manager est redémarré automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification SAML**.
2. Décochez la case **Activer l'authentification SAML**.
3. Cliquez sur **Enregistrer**.

   Un message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified

Manager.

4. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants vont entrer leurs identifiants dans la page de connexion de Unified Manager au lieu de la page de connexion IDP.

Accédez à votre IDP et supprimez l'URI du serveur Unified Manager et les métadonnées.

Désactivation de l'authentification SAML à partir de la console de maintenance

Si vous n'avez pas accès à l'interface graphique Unified Manager, vous devrez peut-être désactiver l'authentification SAML à partir de la console de maintenance. Cela peut se produire en cas de mauvaise configuration ou si le IDP n'est pas accessible.

Ce dont vous aurez besoin

Comme utilisateur de maintenance, vous devez avoir accès à la console de maintenance.

Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, exécutent l'authentification d'identification. 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 est redémarré automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, entrez 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.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants vont entrer leurs identifiants dans la page de connexion de Unified Manager au lieu de la page de connexion IDP.

Si nécessaire, accédez à votre IDP et supprimez l'URL du serveur Unified Manager et les métadonnées.

Page 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'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager.

- Vous devez avoir le rôle Administrateur d'applications 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 cocher la case Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IDP**

  URI permettant d'accéder au IDP à partir du serveur Unified Manager. Les exemples d'URI sont répertoriés ci-dessous.

  Exemple d'URI ADFS :

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemple d'URI :

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Métadonnées IDP**

  Les métadonnées IDP au format XML.

  Si l'URL IDP est accessible à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **extraire les métadonnées IDP** pour remplir ce champ.

- **Système hôte (FQDN)**

  Le FQDN du système hôte Unified Manager tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI hôte**

  URI permettant d'accéder au système hôte Unified Manager à partir du IDP.

- **Métadonnées hôte**

  Métadonnées du système hôte au format XML.

Gestion de 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, reportez-vous à la section précédente sur **configurer Unified Manager pour envoyer des notifications d'alerte**.

Modification des serveurs d'authentification

Vous pouvez modifier le port utilisé par le serveur Unified Manager pour communiquer avec votre serveur d'authentification.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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 **Edit Authentication Server**, modifiez les détails du port.
5. Cliquez sur **Enregistrer**.

Suppression des 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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 **Use Secure Connection** 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 qu'il communique 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 groupes distants sont gérées 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.

Consignation d'audits

Vous pouvez détecter si les journaux d'audit ont été compromis avec l'utilisation des journaux d'audit. Toutes les activités effectuées par un utilisateur sont surveillées et consignées dans les journaux d'audit. Les audits sont effectués pour toutes les interfaces utilisateur et les fonctionnalités des API exposées publiquement de Active IQ Unified Manager.

Vous pouvez utiliser **Audit Log: File View** pour afficher et accéder à tous les fichiers journaux d'audit disponibles dans votre Active IQ Unified Manager. Les fichiers de la vue Journal d'audit : fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux d'audit qui sont enregistrés à partir de l'installation ou de la mise à niveau vers le présent dans le système. Chaque fois que vous effectuez une action dans Unified Manager, les informations sont mises à jour et disponibles dans les journaux. L'état de chaque fichier journal est capturé à l'aide de l'attribut « Etat d'intégrité des fichiers » qui est activement surveillé pour détecter la modification ou la 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 en cours de journalisation.
NORMALE	Fichier inactif, compressé et stocké dans le système.
FALSIFIÉ	Fichier compromis par un utilisateur qui a modifié manuellement le fichier.
SUPPRESSION_MANUELLE	Fichier supprimé par un utilisateur autorisé.
SUPPRESSION_DU_SURVOL	Fichier supprimé en raison de la désactivation en fonction de la stratégie de configuration de roulement.
UNEXPECTED_DELETE	Fichier supprimé pour des raisons inconnues.

La page Journal d'audit comprend les boutons de commande suivants :

- Configurer
- Supprimer

- Télécharger

Le bouton **DELETE** permet de supprimer tous les journaux d'audit répertoriés dans la vue journaux d'audit. Vous pouvez supprimer un journal d'audit et éventuellement fournir une raison de supprimer le fichier, ce qui permet à l'avenir de déterminer une suppression valide. La colonne MOTIF 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 de la table DB ne sera pas supprimée.

Vous pouvez télécharger les journaux d'audit à partir de Active IQ Unified Manager à l'aide du bouton **DOWNLOAD** de la section journaux d'audit et exporter les fichiers journaux d'audit. Les fichiers marqués « NORMAL » ou « FALSIFIÉS » sont téléchargés dans un format compressé `.gzip`.

Les fichiers journaux d'audit sont archivés régulièrement et enregistrés dans la base de données pour référence. Avant l'archivage, les journaux d'audit sont signés numériquement afin de préserver la sécurité et l'intégrité.

Lorsqu'un bundle AutoSupport complet est généré, le bundle de support inclut à la fois des 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.

Configuration des journaux d'audit

Vous pouvez utiliser le bouton **configurer** de la section journaux d'audit pour configurer la stratégie de déploiement des fichiers journaux d'audit et activer la journalisation à distance des journaux d'audit.

Vous pouvez définir les valeurs dans les JOURS de RÉTENTION du JOURNAL * **MAX ET *AUDIT LOG** en fonction de la quantité et de la fréquence de données que vous souhaitez stocker dans le système. La valeur du champ **TAILLE TOTALE DU JOURNAL D'AUDIT** est la taille totale des données du journal d'audit présentes dans le système. La stratégie de reprise est déterminée par les valeurs du champ **JOURS DE RÉTENTION DU JOURNAL D'AUDIT**, **taille DU FICHIER MAX** 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 ""Suppression de substitution"". 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 antérieur à la valeur définie dans ce champ est redéployé.

Étapes

1. Cliquez sur **journaux d'audit** > **configurer**.
2. Entrez des valeurs dans les champs **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** et **AUDIT LOG RETENTION DAYS**.

   Si vous souhaitez activer la journalisation à distance, sélectionnez **Activer la journalisation à distance**.

Activation de 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 fonction pour transférer les journaux d'audit vers un

serveur Syslog distant. Cela vous permettra de gérer vos journaux d'audit lorsqu'il existe des contraintes d'espace.

La journalisation à distance des journaux d'audit assure une sauvegarde inviolable si les fichiers journaux d'audit sur le serveur Active IQ Unified Manager sont falsités.

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 **NOM D'HÔTE** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **SERVER CA CERTIFICATE**, cliquez sur **BROWSE** pour sélectionner un certificat public du serveur cible.

   Le certificat doit être téléchargé `.pem` au format. Ce certificat doit être obtenu à partir du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le « nom d'hôte » sélectionné dans le cadre de l' `SubjectAltName`attribut (SAN).

4. Saisissez les valeurs des champs suivants : **CHARSET**, **DÉLAI DE CONNEXION**, **DÉLAI DE RECONNEXION**.

   Les valeurs doivent être exprimées en millisecondes pour ces champs.

5. Sélectionnez le format Syslog et la version du protocole TLS requis dans les champs **FORMAT** et **PROTOCOLE**.
6. Cochez la case **Activer l'authentification client** si le serveur Syslog cible nécessite une authentification par 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 requiert la création d'un <hash> du certificat à l'aide de la commande `openssl x509 -noout -hash -in cert.pem`, puis vous devez lier symboliquement le certificat d'authentification du 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 **Connection Timeout** peut affecter la configuration. Si la réponse de la configuration est plus longue que la valeur définie, elle peut entraîner une défaillance de la configuration en raison d'une erreur de connexion. Pour établir une connexion réussie, augmentez la valeur **Connection Timeout** et réessayez la configuration.

Page authentification à distance

Vous pouvez utiliser la page authentification à distance pour configurer Unified Manager pour communiquer avec votre serveur d'authentification afin d'authentifier les utilisateurs

distants qui tentent de se connecter à l'interface utilisateur Web Unified Manager.

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Après avoir sélectionné la case à cocher 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 des fournisseurs de services d'annuaire, tels qu'Active Directory, OpenLDAP ou spécifier votre propre mécanisme d'authentification. Vous pouvez spécifier un service d'authentification uniquement si vous avez activé l'authentification à distance.

  - **Active Directory**
    - Nom de l'administrateur

      Indique le nom d'administrateur du serveur d'authentification.

    - Mot de passe

      Spécifie le mot de passe pour accéder au serveur d'authentification.

    - Nom unique de base

      Indique 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, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

    - Désactiver la recherche de groupes imbriqués

      Indique 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 connexion sécurisée

      Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

  - **OpenLDAP**
    - Lier le nom unique

      Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour trouver des utilisateurs distants dans le serveur d'authentification.

    - Lier le mot de passe

      Spécifie le mot de passe pour accéder au serveur d'authentification.

    - Nom unique de base

      Indique 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, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

- Utiliser connexion sécurisée

  Spécifie que le protocole LDAP sécurisé est utilisé pour communiquer avec les serveurs d'authentification LDAP.

- **Autres**

  - Lier le nom unique

    Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour trouver des 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 unique de base

    Indique 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, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

  - Version du protocole

    Spécifie la version LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez spécifier si la version du protocole doit être automatiquement détectée 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 utilisateur 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 groupeOfUniqueNames dans le serveur d'authentification, cette option vous permet d'affecter l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet groupeOfUniqueNames.

  - Désactiver la recherche de groupes imbriqués

    Indique 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

    Indique le nom d'attribut utilisé par votre serveur d'authentification pour stocker des informations sur les membres individuels d'un groupe.

- Classe d’objets 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 identiques à celles ajoutées dans vos configurations Active Directory, OpenLDAP et LDAP. Dans le cas contraire, l’authentification pourrait échouer.

- Utiliser 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 tout serveur d’authentification existant et d’ajouter de nouveaux serveurs d’authentification.

Zone serveurs d’authentification

La zone serveurs d’authentification affiche les serveurs d’authentification avec lesquels le serveur de gestion communique pour trouver et authentifier les utilisateurs distants. Les informations d’identification des utilisateurs ou groupes distants sont gérées par le serveur d’authentification.

- **Boutons de commande**

  Permet d’ajouter, de modifier ou de supprimer des serveurs d’authentification.

  - Ajouter

    Permet d’ajouter un serveur d’authentification.

  Si le serveur d’authentification que vous ajoutez fait partie d’une paire haute disponibilité (à l’aide de 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

    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.

- **Test d’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.

Gestion des certificats de sécurité

Vous pouvez configurer HTTPS sur le serveur Unified Manager pour surveiller et gérer les clusters via une connexion sécurisée.

Affichage du certificat de sécurité HTTPS

Vous pouvez comparer les détails du certificat HTTPS au certificat récupéré dans votre navigateur pour vous assurer que la connexion chiffrée de votre navigateur à Unified Manager n’est pas interceptée.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d’applications ou administrateur de stockage.

L’affichage du certificat vous permet de vérifier le contenu d’un certificat régénéré ou d’afficher les noms des objets (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 s’affiche en haut de la page

Si vous avez besoin d’afficher des informations plus détaillées sur le certificat de sécurité par rapport à ce qui s’affiche sur la page certificat HTTPS, vous pouvez afficher le certificat de connexion dans votre navigateur.

Téléchargement d’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 à signer. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l’homme du milieu et offre une meilleure protection contre la sécurité qu’un certificat auto-signé.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d’applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
2. Cliquez sur **Télécharger demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

Vous pouvez fournir le fichier à une autorité de certification pour signer, puis installer le certificat signé.

L'installation d'une autorité de certification a signé et renvoyé un certificat HTTPS

Vous pouvez télécharger et installer un certificat de sécurité une fois qu'une autorité de certification l'a signé et l'a 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 contribue à prévenir les attaques de l'homme au milieu et offre une meilleure protection contre la sécurité qu'un certificat auto-signé.

Ce dont vous aurez besoin

Vous devez avoir effectué les actions suivantes :

- A téléchargé le fichier de demande de signature de certificat et l'a signé par une autorité de certification
- Enregistré la chaîne de certificats au format PEM
- Inclus tous les certificats de la chaîne, du certificat du serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

Vous devez avoir le rôle Administrateur d'applications.

> Si la validité du certificat pour lequel une RSC a été créée est supérieure à 397 jours, la validité sera réduite à 397 jours par l'AC avant de signer et de retourner 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 le fichier…** pour localiser le fichier à télécharger.
4. Sélectionnez le fichier, puis cliquez sur **installer** pour l'installer.

   Pour plus d'informations, voir "Installation d'un certificat HTTPS généré à l'aide d'outils externes".

Exemple de chaîne de certificat

L'exemple suivant montre comment le fichier de chaîne de certificats peut s'afficher :

```
-----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-----
```

Installation d'un certificat HTTPS généré à l'aide d'outils externes

Vous pouvez installer des certificats qui sont auto-signés ou qui sont générés à l'aide d'un outil externe tel que 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 par l'extérieur. Les algorithmes de paire de clés autorisés sont « RSA » et « EC ». L'option **installer le certificat HTTPS** est disponible dans la page certificats HTTPS de la section général. Le fichier que vous téléchargez doit avoir le 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 autorités de certification en sens inverse 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 « sept-4r1 ». 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.

Vérifie lors du téléchargement de certificats générés en externe

Le système effectue des vérifications pendant le chargement d'un certificat généré à l'aide d'outils externes. Si l'une des vérifications échoue, le certificat est rejeté. Il existe également une validation pour les certificats générés à partir de la RSC dans le produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée de l'entrée est validée par rapport au certificat hôte dans l'entrée.
- Le nom commun (CN) du certificat hôte est vérifié par rapport au FQDN de l'hôte.

- Le nom commun (CN) du certificat 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 ultérieure et la date d'expiration de validité du certificat ne doit pas être antérieure.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être ultérieure et la date d'expiration de la validité ne doit pas être antérieure.

> La clé privée de l'entrée ne doit pas être chiffrée. Si des clés privées sont 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 : "ActiveIQ Unified Manager ne parvient pas à installer un certificat généré en externe"

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 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 permettent d'effectuer les opérations suivantes :

- **Télécharger 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 pour que vous puissiez fournir le fichier à une autorité de certification à signer.

- **Installer le certificat HTTPS**

  Vous permet de télécharger et d'installer un certificat de sécurité une fois qu'une autorité de certification a signé et renvoyé ce certificat. Le nouveau certificat est 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 est 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 sur le 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**

  Obligatoire. Le nom de domaine complet (FQDN) que vous souhaitez sécuriser.

  Dans les configurations haute disponibilité Unified Manager, utilisez l'adresse IP virtuelle.

- **Courriel**

  Facultatif. Une adresse e-mail pour contacter votre organisation, généralement l'adresse e-mail de l'administrateur de certificat ou DU service INFORMATIQUE.

- **Société**

  Facultatif. Généralement le nom incorporé de votre société.

- **Ministère**

  Facultatif. Le nom du service de votre entreprise.

- **Ville**

  Facultatif. La ville de votre entreprise.

- **État**

  Facultatif. L'emplacement de l'État ou de la province, non abrégé, de votre entreprise.

- **Pays**

  Facultatif. Pays de votre entreprise. Il s'agit généralement d'un code ISO à deux lettres du pays.

- **Noms alternatifs**

  Obligatoire. Noms de domaine supplémentaires non primaires pouvant être utilisés pour accéder à ce serveur en plus de l'hôte local existant ou d'autres adresses réseau. Séparez les différents noms 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 autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom.

- **TAILLE DE CLÉ (ALGORITHME CLÉ : RSA)**

  L'algorithme clé est défini sur RSA. Vous pouvez choisir parmi l'une des tailles de touches : 2048, 3072 ou 4096 bits. La taille de clé par défaut est de 2048 bits.

- * PÉRIODE 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 peut changer.

Pour plus d'informations, voir "Génération de certificats HTTPS".

Surveillance et gestion du 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 seule interface.

Unified Manager offre les fonctionnalités suivantes :

- Découverte, surveillance et notifications pour les systèmes installés avec le logiciel ONTAP.
- Tableau de bord permettant d'afficher la capacité, la sécurité et les performances de l'environnement.
- Alertes améliorées, événements et infrastructure de seuils.
- Affiche des graphiques détaillés qui correspondent à l'activité des charges de travail dans le temps, notamment les IOPS (opérations), les Mbit/s (débit), la latence (temps de réponse), l'utilisation la capacité de performance et le ratio cache.
- Identifie les charges de travail qui surutilisent 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 exécutées pour résoudre certains incidents et événements, et un bouton « Fix it » pour certains événements afin de résoudre le problème immédiatement.
- S'intègre avec OnCommand Workflow Automation pour exécuter des flux de travail de protection automatisés.
- Possibilité de créer de nouvelles charges de travail, par exemple une LUN ou un partage de fichiers, directement dans Unified Manager et d'attribuer un niveau de service de performances afin de définir les objectifs de performance et de stockage auxquels les utilisateurs qui accèdent à l'application via cette charge de travail.

Présentation de 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 de serveur Unified Manager offre évolutivité, compatibilité et fonctionnalités avancées de contrôle et de notification.

Il offre de nombreuses fonctionnalités : surveillance, alerte, gestion de la disponibilité et de la capacité des clusters, gestion des fonctionnalités de protection et regroupement des données de diagnostic et envoi au support technique.

Vous pouvez utiliser Unified Manager pour surveiller vos clusters. Lorsqu'un problème se produit au sein du cluster, Unified Manager vous informe des détails de ces problèmes par le biais d'événements. Certains événements vous fournissent également une action corrective que vous pouvez effectuer pour corriger ces problèmes. Vous pouvez configurer les alertes pour les événements afin que lorsque des problèmes se produisent, vous être averti par e-mail et des interruptions SNMP.

Unified Manager vous permet de gérer les objets de stockage de votre environnement en les associant à des annotations. Vous pouvez créer des annotations personnalisées et associer de façon dynamique des clusters, des machines virtuelles de stockage 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 santé et de capacité pour l'objet de cluster respectif.

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 désigne les blocs physiques utilisés dans le volume. La capacité physique utilisée est généralement inférieure à la capacité logique utilisée en raison de la réduction des données provenant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- Capacité logique : espace logique désigne l'espace utilisable (blocs logiques) dans un volume. L'espace logique désigne la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats obtenus grâce à la déduplication ou à la compression. L'espace logique utilisé est 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 semble souvent plus importante que la capacité physique utilisée, car elle ne reflète pas la compression des données et d'autres réductions de l'espace physique. La capacité logique totale peut donc être supérieure à l'espace provisionné.

Unités de mesure de la capacité

Unified Manager calcule la capacité de stockage en fonction des unités binaires de 1024 (2^{10}) octets. Dans ONTAP 9.10.0 et versions antérieures, ces unités étaient affichées sous la forme Ko, Mo, Go, To et PB. À partir de ONTAP 9.10.1, ces objets sont affichés dans Unified Manager comme Kio, Mio, Gio, Tio et Pio.

> Les unités utilisées pour le débit continuent d'être de kilo-octets par seconde (Kbit/s), mégaoctets par seconde (Mbit/s), gigaoctets par seconde (Gbit/s) ou téraoctets par seconde (Tbit/s), 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	Kio	1024	1024 octets
MO	Mio	1024 * 1024	1 048 576 octets
GO	Gio	1024 * 1024 * 1024	1 073 741 824 octets
TO	Tio	1024 * 1024 * 1024 * 1024	1 099 511 627 776 octets

Présentation de la surveillance des performances Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) fournit des fonctions de contrôle des performances et d'analyse de la source des événements pour les systèmes exécutant le logiciel NetApp ONTAP.

Unified Manager vous aide à identifier les charges de travail qui surutilisent les composants du cluster et à réduire les performances des autres charges de travail sur le cluster. En définissant des règles de seuil de performances, vous pouvez également spécifier des valeurs maximales pour certains compteurs de performances afin que les événements soient générés lorsque le seuil est dépassé. Unified Manager vous alerte concernant ces événements de performance, afin de mettre en place des actions correctives et de rétablir les performances normales. Vous pouvez afficher et analyser les événements dans l'interface utilisateur Unified Manager.

Unified Manager surveille les performances de deux types de charges de travail :

- Les charges de travail définies par l'utilisateur

  Ces charges de travail sont constituées de volumes FlexVol et de volumes FlexGroup que vous avez créés dans votre cluster.

- Les charges de travail définies par le système

  Ces workloads sont constitués d'une activité système interne.

Grâce aux API REST de Unified Manager

Active IQ Unified Manager 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 les objets de stockage en fonction de règles.

Vous pouvez également exécuter des API ONTAP sur tous les clusters gérés par ONTAP à l'aide de la passerelle d'API prise en charge par Unified Manager.

Pour plus d'informations sur les API REST d'Unified Manager, consultez"Démarrer avec les API REST Active IQ Unified Manager" .

Rôle du serveur Unified Manager

L'infrastructure de 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 détection, la surveillance, le contrôle d'accès basé sur des rôles (RBAC), l'audit et la journalisation.

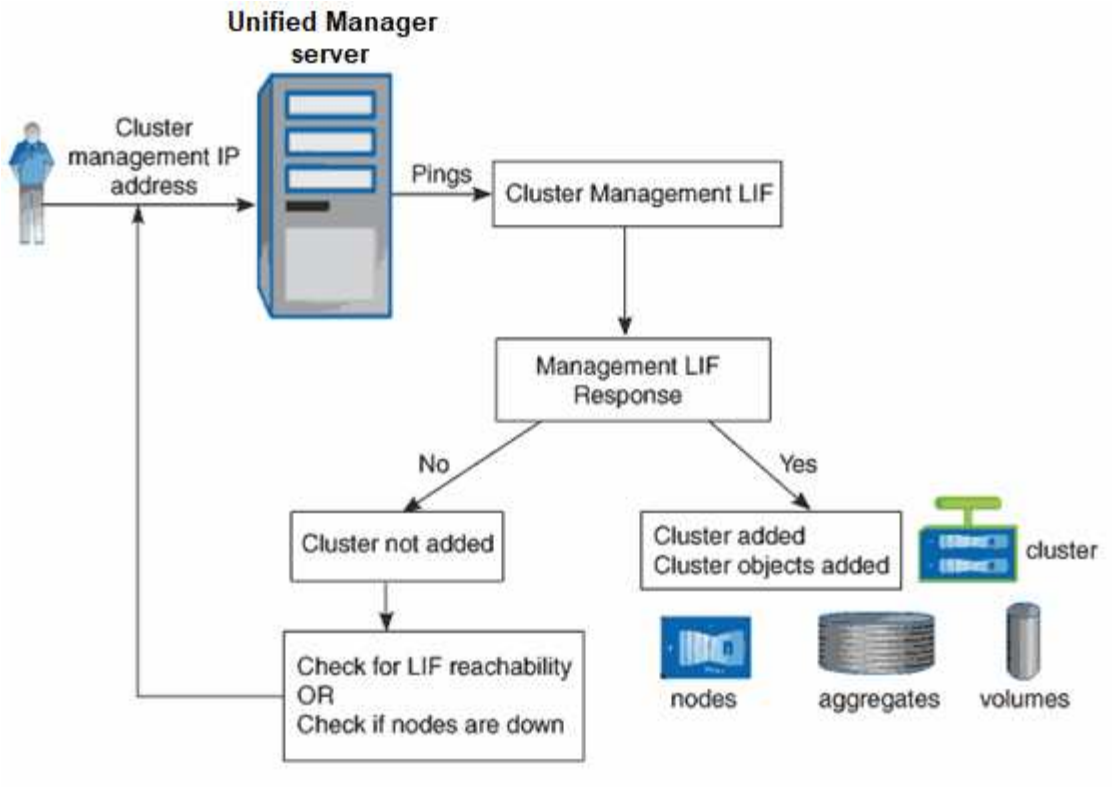
Unified Manager collecte les informations sur le cluster, stocke les données dans la base de données et analyse ces données afin de voir en cas de problème au niveau du cluster.

Fonctionnement du processus de découverte

Une fois le cluster ajouté à Unified Manager, le serveur détecte les objets du cluster et les ajoute à sa base de données. Le fonctionnement du processus de découverte vous permet de gérer les clusters de votre entreprise et leurs objets.

L'intervalle de contrôle par défaut est de 15 minutes : si vous avez ajouté un cluster à un serveur Unified Manager, il faut 15 minutes pour afficher les détails du cluster dans l'interface utilisateur Unified Manager.

L'image suivante illustre le processus de détection dans Active IQ Unified Manager :



Présentation de l’interface utilisateur

L’interface utilisateur de Unified Manager se compose principalement d’un tableau de bord offrant une vue d’ensemble des objets surveillés. L’interface utilisateur permet également d’accéder à l’affichage de tous les objets du cluster.

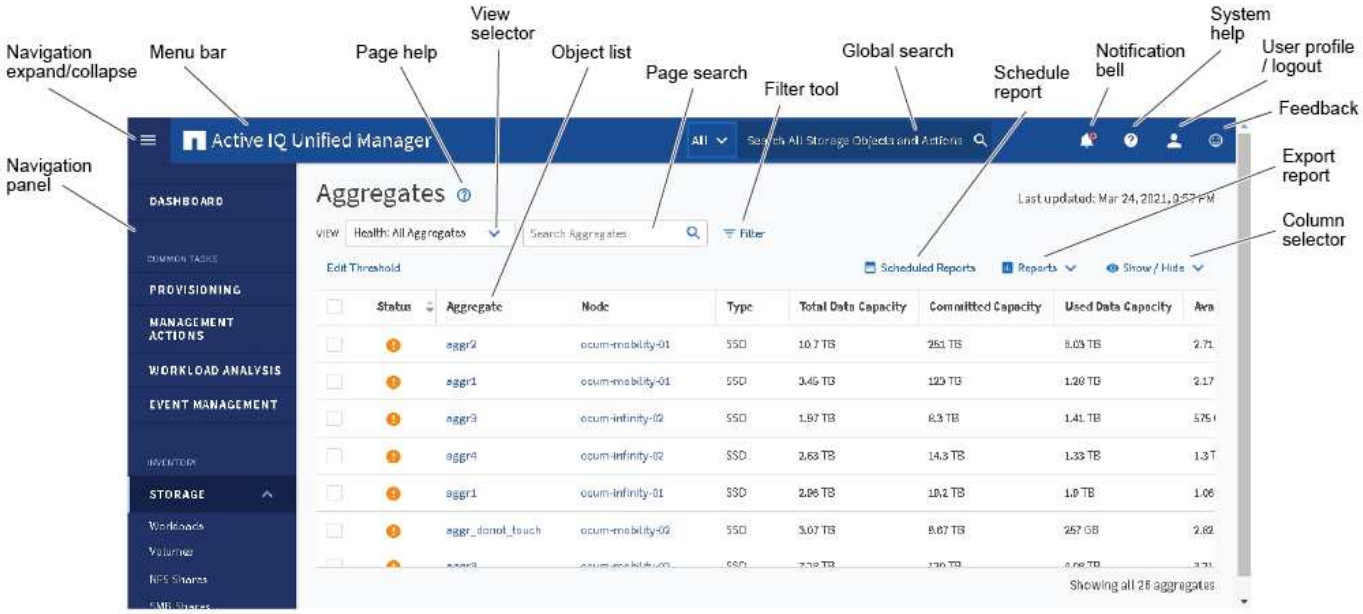
Vous pouvez sélectionner une vue préférée et utiliser les boutons d’action si nécessaire. Votre configuration d’écran est enregistrée dans un espace de travail de sorte que toutes les fonctionnalités nécessaires soient disponibles lorsque vous démarrez Unified Manager. Cependant, lorsque vous naviguez d’une vue à l’autre, puis naviguez vers l’arrière, la vue peut ne pas être la même.

Dispositions de fenêtre types

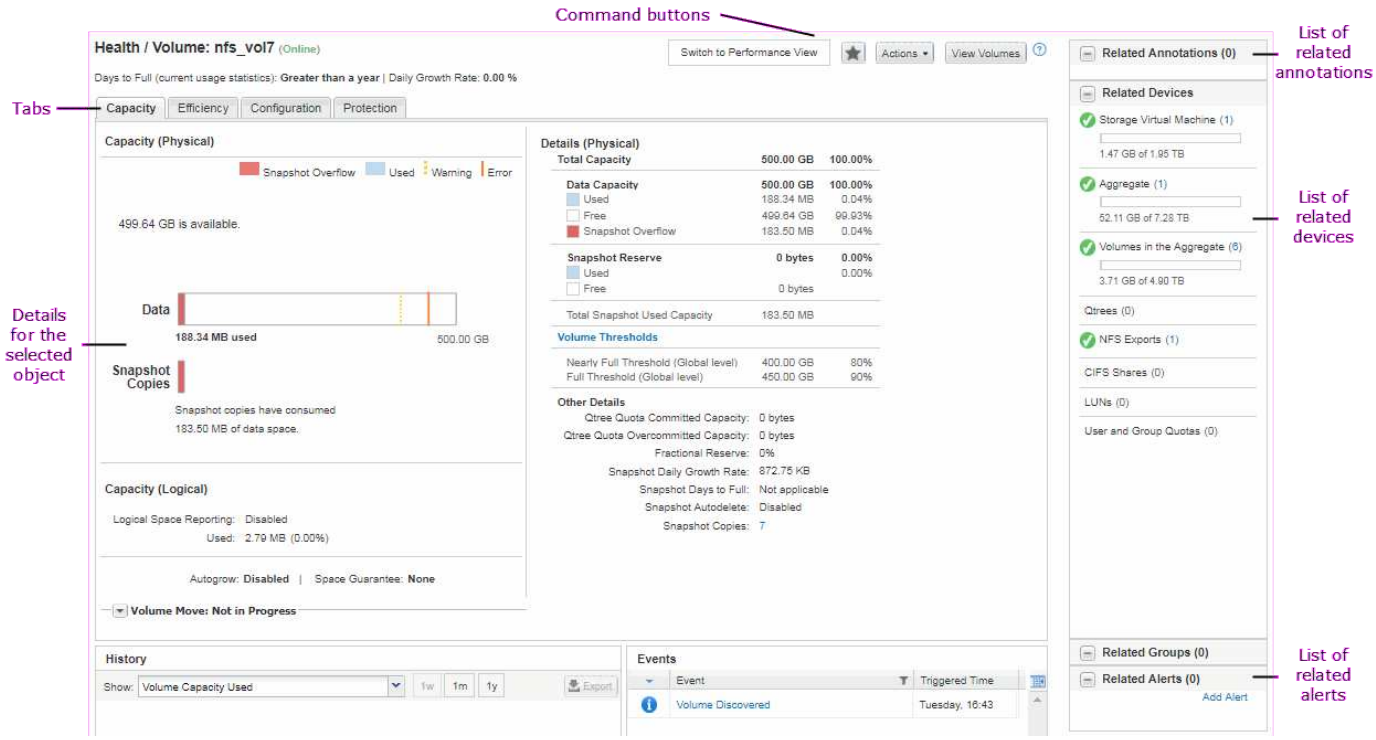
La compréhension des dispositions de fenêtre types vous permet de naviguer et d’utiliser Active IQ Unified Manager efficacement. La plupart des fenêtres Unified Manager sont similaires à l’une des deux présentations générales : liste d’objets ou détails. Le paramètre d’affichage recommandé est d’au moins 1280 x 1024 pixels.

Toutes les fenêtres ne contiennent pas tous les éléments des schémas suivants.

Disposition de la fenêtre de liste d’objets



Disposition de la fenêtre 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 réseau et de stockage. En personnalisant les fenêtres, vous pouvez contrôler les données qui sont affichées et la façon dont elles 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.

- **Filtrage**

  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 de sorte 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.

  Dans toute liste, les colonnes relatives à la capacité affichent toujours les données de capacité dans les unités appropriées arrondies à deux décimales. Cela s'applique également lors du filtrage des colonnes de capacité. Par exemple, si vous utilisez le filtre de la colonne capacité totale des données dans la vue Santé : tous les agrégats pour filtrer des 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 des données inférieures à 20.45 Go, la capacité réelle de 20.449 Go s'affiche sous la forme 20.45 Go.

  Si vous utilisez le filtre de la colonne % de données disponibles dans la vue Santé : tous les agrégats pour filtrer des données supérieures à 20.45 %, la capacité réelle de 20.454 % s'affiche sous la forme 20.45 %. De même, si vous filtrez des données inférieures à 20.45 %, la capacité réelle de 20.449 % s'affiche à 20.45 %.

- **Masquage ou affichage des colonnes**

  Vous pouvez cliquer sur l'icône d'affichage de colonne (**Afficher/Masquer**) pour sélectionner les colonnes à 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 de vous aider à affiner la liste des éléments de la page d'inventaire. Par exemple, vous pouvez entrer « cloud » pour affiner la liste des volumes de la page d'inventaire des volumes afin de voir tous les volumes dont le mot « cloud » est « cloud ».

- **Exportation de données**

  Vous pouvez cliquer sur le bouton **Rapports** (ou sur le bouton **Exporter**) pour exporter des données vers un fichier de valeurs séparées par des virgules, `(.pdf)` un document ou un `(.csv)`` fichier Microsoft Excel ``(.xlsx)` et utiliser les données exportées pour générer des rapports.

Utilisation de l'aide de Unified Manager

L'aide contient des informations sur toutes les fonctions 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 fonctions et leur utilisation.

L'aide est disponible sur chaque onglet et dans la barre de menus de l'interface utilisateur de 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 le contenu de l'aide, cliquez sur * ? **> *aide/Documentation** dans la barre de menus.

  Pour obtenir des informations plus détaillées, développez n'importe quelle partie de la table des matières dans le volet de navigation.

- Pour effectuer une recherche dans 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, puis cliquez sur **Go!**
- Pour imprimer des rubriques d'aide, cliquez sur l'icône de l'imprimante.

Création de signets pour vos rubriques d'aide préférées

Dans l'onglet Favoris de l'aide, vous pouvez ajouter fréquemment des rubriques d'aide aux signets. Les signets permettent d'accéder rapidement à vos sujets favoris.

Étapes

1. Accédez à la rubrique d'aide que vous souhaitez ajouter en tant que favori.
2. Cliquez sur **Favoris**, puis sur **Ajouter**.

Recherche d'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 menus. 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 classés par type d'objet de stockage et vous pouvez les filtrer davantage par objet à l'aide du menu déroulant.

Ce dont vous aurez besoin

- Pour effectuer cette tâche, vous devez avoir l'un des rôles suivants : opérateur, administrateur d'applications ou administrateur de stockage.
- Une recherche valide doit contenir au moins trois caractères.

Lorsque vous utilisez la valeur de 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 dans un type d'objet spécifique. Dans ce cas, la liste retournée n'est pas limitée aux 25 objets supérieurs.

Les types d'objet que vous pouvez rechercher sont les suivants :

- Clusters
- Nœuds
- Machines virtuelles de stockage
- 64 bits
- Volumes
- Qtrees
- Partages SMB

- Partages NFS
- Quotas d'utilisateur ou de groupe
- LUN
- Espaces de noms NVMe
- Groupes d'initiateurs
- Initiateurs
- Groupe de cohérence

La saisie d'un nom de charge de travail renvoie la liste des charges de travail dans la catégorie volumes ou LUN appropriés.

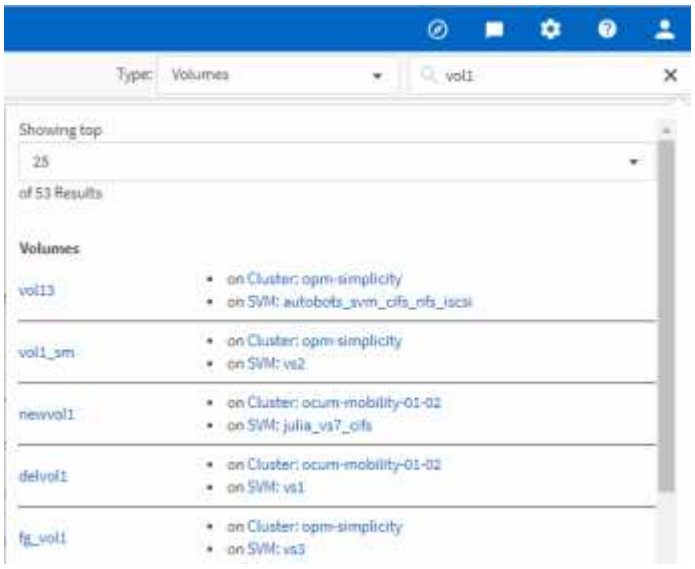
Vous pouvez cliquer sur n'importe quel objet dans les résultats de la recherche pour accéder à la page Détails de l'état de santé de cet objet. S'il n'existe pas de page d'intégrité directe pour un objet, la page Santé de l'objet parent s'affiche. Par exemple, lors d'une recherche de LUN spécifique, la page des détails du SVM sur laquelle réside la LUN s'affiche.

Les ports et les LIFs ne sont pas interrogeables 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, le type d'objet volumes est sélectionné dans la zone déroulante. La saisie de "vol1" dans le champ **Rechercher tous les objets de stockage** affiche la liste de tous les volumes dont les noms contiennent ces caractères.



Exportation des 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, si 10 événements

critiques n'ont pas été résolus, vous pouvez exporter les données depuis la page d'inventaire Event Management pour créer un rapport, puis envoyer le rapport aux administrateurs capables de résoudre les problèmes.

Vous pouvez exporter des données vers un fichier, `.xlsx` un fichier ou `.pdf` un `.csv` document à partir des pages d'inventaire **Storage** et **Network** et utiliser les données exportées pour générer des rapports. Il existe d'autres emplacements dans le produit où seuls les `.csv` fichiers ou `.pdf` peuvent être générés.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour exporter…	Procédez comme ça…
Détails de l'inventaire des objets de stockage	Cliquez sur **Storage** ou **Network** dans le menu de navigation 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 sur le groupe de règles de qualité de service	Cliquez sur **Storage** > **QoS Policy Groups** dans le menu de navigation gauche.
Détails de l'historique de la capacité de stockage et de la protection	Cliquez sur **Storage** > **Aggregates** ou **Storage** > **volumes**, puis sélectionnez un seul agrégat ou volume.
Détails de l'événement	Cliquez sur **Event Management** dans le menu de navigation gauche.
Les performances des 10 principaux objets de stockage sont détaillées	Cliquez sur **Storage** > **clusters** > **Performance:tous les clusters**, puis sélectionnez un cluster et choisissez l'onglet **meilleurs exécutants**. Sélectionnez ensuite un objet de stockage et le 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.

   Dans l'onglet Top Performers, vous pouvez choisir de télécharger un rapport des statistiques pour le cluster 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 Health/clusters"

"Planification d'un rapport"

Filtrage du contenu de la page d'inventaire

Vous pouvez filtrer les données de page d'inventaire dans Unified Manager pour localiser rapidement des données en fonction de critères spécifiques. Vous pouvez utiliser le filtrage pour affiner le contenu des pages Unified Manager afin d'afficher uniquement les résultats qui vous intéressent. Ceci fournit une méthode très efficace pour n'afficher que les données qui vous intéressent.

Utilisez **Filtering** pour personnaliser la vue de grille en fonction de vos préférences. Les options de filtre disponibles sont basées sur le type d'objet affiché 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**.
Numéro	Les opérateurs sont **supérieurs à**, **inférieurs à**, **dans le dernier** et **entre**.
Enum (texte)	Les opérateurs sont **is** et **n'est pas**.

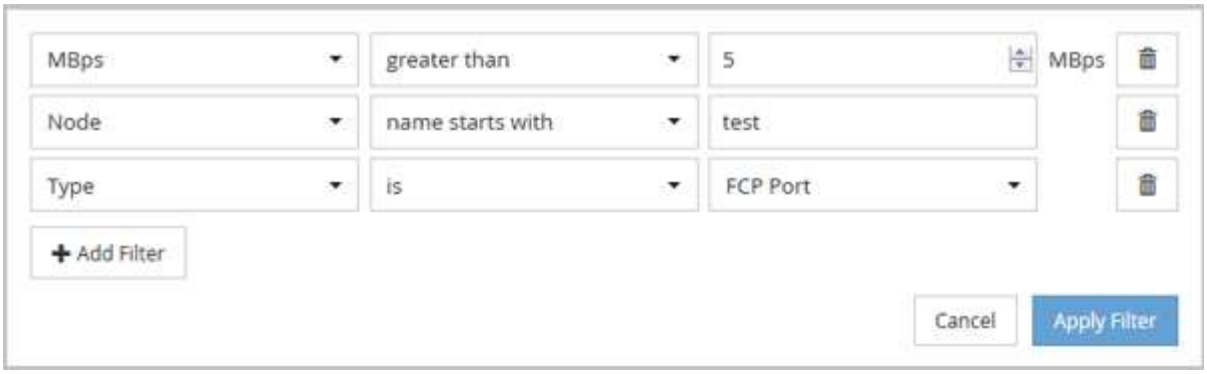
Les champs colonne, opérateur et valeur sont requis pour chaque filtre ; les filtres disponibles reflètent les colonnes filtrables de la page actuelle. Le nombre maximal de filtres que vous pouvez appliquer est de quatre. Les résultats filtrés sont basés sur des paramètres de filtre combinés. Les résultats 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 **Filter**. 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 entrez une valeur pour compléter le filtre de cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Ajouter filtre**. Un champ de filtre supplémentaire s'affiche. Effectuez ce filtre en suivant la procédure décrite dans les étapes précédentes. Notez que lors de l'ajout de votre quatrième filtre, le bouton **+Ajouter 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 s'affiche à droite du bouton filtre.
7. Utilisez le panneau filtrage pour supprimer des filtres individuels en cliquant sur l'icône de corbeille située 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 filtrage avec trois filtres. Le bouton **+Ajouter filtre** s'affiche lorsque vous avez moins de quatre filtres que le maximum.



Après avoir cliqué sur **appliquer le filtre**, le panneau filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Affichage des événements actifs à partir du signal sonore 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 visualiser 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 derniers jours 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 est inaccessible, 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 l'espace faible ou la RAM sur la station de gestion, sont également affichés sur cette page.

Étapes

1. Dans la barre de menus, cliquez sur .
2. Pour afficher les détails de l'un des événements actifs, cliquez sur le lien texte de l'événement, tel que « 2 Capacity » ou « 4 Performance ».

Contrôle et gestion des clusters depuis le tableau de bord

Le tableau de bord fournit des informations cumulées d'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 la sécurité des clusters que vous surveillez.

En outre, certains problèmes ONTAP peuvent être résolus directement depuis l'interface utilisateur d'Unified Manager, au lieu d'utiliser ONTAP System Manager ou l'interface de ligne de commande d'ONTAP.

En haut du tableau de bord, vous pouvez indiquer 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 informations détaillées vers chacun d'eux lorsque vous le souhaitez.

> Certains des panneaux répertoriés ci-dessous peuvent ne pas apparaître sur la page en fonction de votre configuration.

Panneaux	Description
Actions de gestion	Lorsque Unified Manager peut diagnostiquer et déterminer une résolution unique pour un problème, ces résolutions s'affichent dans ce panneau avec un bouton **Fix it**.
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 et performances	Affiche la valeur de la capacité de performances pour chaque cluster, ainsi que le nombre de jours jusqu'à ce que la capacité de performances atteigne la limite supérieure.
IOPS des workloads	Affiche le nombre total de charges de travail actuellement exécutées dans une certaine plage d'IOPS.
Performances des workloads	Affiche le nombre total de charges de travail conformes et non conformes affectées à chaque niveau de service de performances défini.
Sécurité	Affiche le nombre de clusters conformes ou non, le nombre de SVM conformes ou non, et le nombre de volumes chiffrés.
La 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.
Présentation de l'utilisation	Affiche les clusters triés par rapport aux IOPS les plus élevées, au débit le plus élevé (Mbit/s) ou à la capacité physique la plus utilisée.

Page de tableau de bord

La page Tableau de bord comporte des « panneaux » qui indiquent le niveau élevé de capacité, de performances et de sécurité des clusters que vous surveillez. Cette page fournit également un panneau actions de gestion qui répertorie les correctifs que 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 décider des clusters que vous devrez analyser davantage pour résoudre les événements. Un clic sur les événements affiche les principaux événements et fournit un lien vers la page d'inventaire Event Management

filtrée pour afficher les événements actifs dans cette catégorie.

En haut du tableau de bord, vous pouvez indiquer 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 informations détaillées vers chacun d'eux lorsque vous le souhaitez.

> Certains panneaux répertoriés ci-dessous apparaissent sur le tableau de bord en fonction de votre configuration.

Panneau actions de gestion

Unified Manager effectue un diagnostic approfondi et permet sa résolution unique. Lorsqu'elles sont disponibles, ces résolutions sont affichées dans ce panneau avec un bouton **Fix it** ou **Fix All**. Vous pouvez corriger ces problèmes immédiatement à partir d'Unified Manager au lieu d'utiliser ONTAP System Manager ou l'interface de ligne de commande de ONTAP. Pour afficher tous les problèmes, cliquez sur Voir "Résolution des problèmes ONTAP directement dans 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 du stockage) et la capacité physique disponible (sans tenir compte des économies potentielles en termes d'efficacité du stockage) pour chaque cluster, le nombre de jours avant que les disques ne soient pleins, Et le taux de réduction des données (sans copies Snapshot) basé sur les paramètres d'efficacité du stockage ONTAP configurés. Elle répertorie également la capacité utilisée pour tous les niveaux cloud configurés. Cliquez sur le graphique à barres pour accéder à la page d'inventaire des agrégats correspondant à ce cluster. Lorsque vous cliquez sur le texte « jours avant complets », un message s'affiche, indiquant l'agrégat dont il reste le nombre de jours de capacité minimum. Cliquez sur le nom de l'agrégat pour en savoir plus.

Lorsque vous affichez un seul cluster, ce panneau affiche la capacité physique utilisée et la capacité physique disponible pour les agrégats de données, triés par 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 Performance Capacity

Lorsque vous affichez tous les clusters, ce panneau affiche la valeur de capacité des performances pour chaque cluster (moyenne sur l'heure précédente) et le nombre de jours jusqu'à ce que la capacité des performances atteigne la limite supérieure (basée sur le taux de croissance quotidien). Cliquez sur le graphique à barres pour accéder à la page d'inventaire des nœuds de ce cluster. Notez que la page d'inventaire des nœuds affiche la capacité de performance moyenne sur les 72 heures précédentes. Lorsque vous cliquez sur le texte « jours avant complets », un message indiquant le nœud correspondant au moins au nombre de jours de capacité en performance restants s'affiche. Cliquez sur le nom du nœud pour en savoir plus.

Lorsque vous affichez un seul cluster, ce panneau affiche les valeurs relatives à la capacité de performance du cluster utilisée : pourcentage, IOPS totales et débit total (Mbit/s), ainsi que le nombre de jours jusqu'à ce que chacune de ces trois mesures atteigne sa limite supérieure.

Panneau des IOPS des workloads

Lorsque vous affichez un seul cluster, ce volet affiche le nombre total de charges de travail actuellement exécutées dans une certaine plage d'opérations d'E/S par seconde. Il indique le nombre de chaque type de

disque lorsque vous positionnez le curseur de votre souris sur le graphique.

Panneau Performance des workloads

Ce volet affiche le nombre total de charges de travail conformes et non conformes affectées à chaque politique de niveau de service de performance (PSL). Elle affiche également le nombre de charges de travail qui ne sont pas affectées à un PSL. Dans un graphique à barres, vous accédez aux charges de travail conformes attribuées à cette règle sur la page des charges de travail. Cliquez sur le nombre qui suit le graphique à barres pour accéder aux charges de travail conformes et non conformes attribuées à cette règle.

Panneau de sécurité

Le panneau sécurité présente l'état de sécurité de haut niveau pour tous les clusters ou un seul cluster, selon votre vue actuelle. Ce panneau affiche :

- liste des événements de sécurité reçus au cours des 24 dernières 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)
- État de sécurité des machines virtuelles de stockage (nombre de machines virtuelles de stockage conformes et non conformes)
- statut du chiffrement de volume (nombre des volumes chiffrés ou non chiffrés)
- statut anti-ransomware du volume (nombre de volumes avec protection contre les ransomwares 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 cryptés et des volumes anti-ransomwares pour accéder aux pages respectives et afficher les informations de sécurité des clusters filtrés, des machines virtuelles de stockage et des volumes.

La conformité est basée sur le "Guide NetApp sur le renforcement de la sécurité des environnements 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 pour les clusters et les VM de stockage".

Panneau protection des données

Ce panneau affiche le récapitulatif de la protection des données pour un seul ou l'ensemble des clusters d'un data Center. Il affiche le nombre total d'événements liés à la protection des données, les événements MetroCluster et le nombre d'événements actifs soulevés au cours des dernières 24 heures dans ONTAP. Cliquez sur le lien de chacun de ces événements pour accéder 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 gestion des événements. Le panneau affiche :

- Nombre de volumes dans un cluster ou de tous les clusters d'un data Center protégé par les copies Snapshot.
- Le nombre de volumes dans un cluster ou l'ensemble des clusters d'un data Center protégé 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 l'ensemble des clusters d'un data Center protégé par une configuration MetroCluster sur IP ou FC.
- Le nombre de relations de volume avec l'objectif de point de récupération (RPO) SnapMirror est basé sur l'état du décalage.

Vous pouvez positionner le curseur de la souris pour afficher les comptages et légendes respectifs. Vous pouvez cliquer sur la flèche droite en haut du panneau pour afficher les détails d'un ou de tous les clusters sur la page protection des données. Vous pouvez également cliquer sur :

- Les graphiques à barres des volumes et volumes non protégés par les copies Snapshot permettent d'accéder à la page volumes et d'afficher les détails.
- Les graphiques à barres des clusters protégés ou non par la configuration MetroCluster permettent d'accéder à la page clusters et d'afficher les détails.
- Les graphiques à barres permettant d'accéder à la page relations, où les détails sont filtrés en fonction du groupe source.

Pour plus d'informations, voir "Affichage de l'état de protection du volume".

Panneau vue d'ensemble de l'utilisation

Lorsque vous affichez tous les clusters, vous pouvez choisir d'afficher les clusters triés par ordre d'IOPS, de débit le plus élevé (Mbit/s) ou de capacité physique la plus élevée utilisée.

Lorsque vous affichez un seul cluster, vous pouvez choisir d'afficher les charges de travail triées par IOPS plus élevées, par débit (Mbit/s) ou par capacité logique la plus élevée utilisée.

Informations connexes

"Résolution des problèmes à l'aide des résolutions automatiques de Unified Manager"

"Affichage des informations relatives aux événements de performances"

"Gestion des performances grâce à la capacité en termes de performances et aux informations d'IOPS disponibles"

"Page de détails sur le volume / la santé"

"Analyse et notification des événements de performance"

"Description des types de gravité d'événement"

"Sources des événements de performance"

"Gestion des objectifs de sécurité des clusters"

"Contrôle des performances des clusters à partir de la page d'accueil Performance Cluster"

"Surveillance des performances à l'aide des pages d'inventaire des performances"

Gestion des problèmes ou des fonctionnalités d'ONTAP directement à partir d'Unified Manager

Vous pouvez corriger certains problèmes ONTAP ou gérer certaines fonctionnalités ONTAP directement depuis l'interface utilisateur d'Unified Manager, au lieu d'utiliser ONTAP System Manager ou l'interface de ligne de commande d'ONTAP. L'option « actions de gestion » fournit des correctifs à un certain nombre de problèmes ONTAP qui ont déclenché des événements d'Unified Manager.

Vous pouvez corriger 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 des événements et de la sélection analyse de la charge de travail dans le menu de navigation de gauche.

Unified Manager effectue un diagnostic approfondi et permet sa résolution unique. Pour certaines fonctionnalités de ONTAP, telles que la surveillance anti-ransomwares, Unified Manager effectue des vérifications internes et recommande des actions spécifiques. Lorsqu'elles sont disponibles, ces résolutions sont affichées dans les actions de gestion avec un bouton **Fix it**. Cliquez sur le bouton **Fix it** pour résoudre le problème. Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Unified Manager envoie les commandes ONTAP au cluster pour effectuer le correctif demandé. Lorsque la réparation est terminée, l'événement est obsolète.

Certaines actions de gestion vous permettent de résoudre le même problème sur plusieurs objets de stockage à l'aide du bouton **Fix All**. Par exemple, il peut y avoir 5 volumes qui ont l'événement "Volume Space Full" qui pourrait être résolu en cliquant sur l'action de gestion **Fix All** pour "Enable volume Autogrow". 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, reportez-vous à "Problèmes pouvant être résolus par Unified Manager"la section .

Quelles sont les options qui s'offrent lorsque je vois le bouton réparer ou réparer tout

La page actions de gestion vous fournit le bouton **Fix it** ou **Fix all** pour résoudre les problèmes dont Unified Manager a été informé par le biais d'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 :

Que souhaitez-vous faire ?	Action
Demandez à Unified Manager de corriger le problème sur tous les objets identifiés.	Cliquez sur le bouton **réparer tout**.
Ne corrigez pas le problème pour l'un des objets identifiés à ce stade et ne masquez pas cette action de gestion jusqu'à ce que l'événement soit à nouveau déclenché.	Cliquez sur la flèche vers le bas et cliquez sur **rejeter tout**.
Corrigez le problème uniquement sur certains des objets identifiés.	Cliquez sur le nom de l'action de gestion pour développer la liste et afficher toutes les actions individuelles **Fix it**.Suivez ensuite les étapes de résolution ou de rejet des actions de gestion individuelles.

Que souhaitez-vous faire ?	Action
Demandez à Unified Manager de résoudre le problème.	Cliquez sur le bouton **Fix it**.

Que souhaitez-vous faire ?	Action
Ne corrigez pas le problème à ce stade et ne masquez pas cette action de gestion tant que l'événement n'est pas à nouveau déclenché.	Cliquez sur la flèche vers le bas et cliquez sur **rejeter**.
Affichez les détails de cet événement pour mieux comprendre le problème.	• Cliquez sur le bouton **Fix it** et vérifiez le correctif qui sera appliqué dans la boîte de dialogue résultante. • Cliquez sur la flèche vers le bas et cliquez sur **Afficher les détails de l'événement** pour afficher la page Détails de l'événement. Cliquez ensuite sur **Fix it** dans l'une ou l'autre de ces pages si vous souhaitez résoudre le problème.
Affichez les détails de cet objet de stockage pour mieux comprendre le problème.	Cliquez sur le nom de l'objet de stockage pour afficher des détails dans la page Performance Explorer ou Health Details.

Dans certains cas, la correction est reflétée dans l'interrogation de configuration de 15 minutes suivante. Dans d'autres cas, il peut prendre jusqu'à plusieurs heures pour que la modification de configuration soit vérifiée et pour l'événement à rendue obsolète.

Pour afficher la liste des actions de gestion terminées ou en cours, cliquez sur l'icône de filtre et sélectionnez **terminé** ou **en cours**.

Corriger toutes les opérations s'exécutent en série. Ainsi, lorsque vous affichez le panneau **en cours**, certains objets auront l'état **en cours** alors que d'autres auront l'état **programmé**, ce qui signifie qu'ils sont toujours en attente d'être implémentés.

Affichage de l'état des actions de gestion que vous avez choisies pour corriger

Vous pouvez afficher l'état de toutes les actions de gestion que vous avez choisies de corriger dans la page actions de gestion. La plupart des actions s'affichent sous la forme **terminé** assez rapidement après l'envoi de la commande ONTAP par Unified Manager au cluster. Toutefois, certaines actions, telles que le déplacement d'un volume, peuvent prendre plus de temps.

Trois filtres sont disponibles sur la page actions de gestion :

- **Terminé** affiche les deux actions de gestion qui ont abouti et celles qui ont échoué. **Les actions échoués** fournissent une raison pour l'échec afin que vous puissiez résoudre le problème manuellement.
- **En cours** montre à la fois les actions de gestion qui sont mises en œuvre et celles qui sont prévues à mettre en œuvre.
- **Recommandé** affiche toutes les actions de gestion actuellement actives pour tous les clusters surveillés.

Étapes

1. Cliquez sur **Management actions** dans le volet de navigation de gauche. Vous pouvez également cliquer ⋮ en haut du panneau **actions de gestion** sur le **Tableau de bord** et sélectionner la vue que vous

souhaitez voir.

La page actions de gestion s'affiche.

2. Vous pouvez cliquer sur l'icône caret en regard de l'action de gestion dans le champ **Description** pour afficher les détails du problème et de la commande utilisée pour résoudre le problème.
3. Pour afficher les actions qui ont **échoué**, triez dans la colonne **État** de la vue **terminé**. Vous pouvez utiliser l'outil **Filter** pour ce 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 le détail de l'événement** dans la zone développée après avoir cliqué sur l'icône caret en regard de l'action de gestion. Un bouton **Fix it** est disponible à partir de cette page.

Problèmes pouvant être résolus par Unified Manager

En utilisant la fonctionnalité de correction automatique d'Active IQ Unified Manager, vous pouvez choisir de résoudre certains problèmes liés à ONTAP ou de gérer certaines fonctionnalités ONTAP, telles que la surveillance anti-ransomwares, efficacement via Unified Manager.

Ce tableau décrit ces problèmes ou fonctionnalités ONTAP que vous pouvez gérer directement via le bouton **Fix it** ou **Fix All** de l'interface utilisateur Web d'Unified Manager.

Nom et description de l'événement	Action de gestion	Opération « réparer »
Espace de volume plein Le volume est presque à court d'espace et sa capacité est atteinte au seuil maximal. Ce seuil est défini par défaut sur 90 % de la taille du volume.	Activer la croissance automatique de volumes	Unified Manager détermine que la croissance automatique du volume n'est pas configurée pour ce volume. Elle active donc cette fonctionnalité afin que le volume augmente en capacité en cas de besoin.
Inodes plein Ce volume est à court d'inodes et ne peut accepter de nouveaux fichiers.	Augmenter le nombre d'inodes sur le volume	Augmente le nombre d'inodes sur le volume de 2 %.
Discordance des règles de niveau de stockage détectée Le volume dispose de nombreuses données inactives, et la règle de Tiering actuelle est définie sur « Snapshot uniquement » ou sur « aucune ».	Tiering automatisé dans le cloud	Le volume réside déjà dans une FabricPool, mais la règle de Tiering est définie sur « automatique » afin que les données inactives soient déplacées vers le Tier cloud à moindre coût.

Nom et description de l'événement	Action de gestion	Opération « réparer »
Discordance de niveau de stockage détectée De nombreuses données inactives sont stockées dans le volume, mais elles ne résident pas sur un Tier de stockage cloud (FabricPool).	Modifier le niveau de stockage de volumes	Déplace le volume vers un Tier de stockage cloud et définit la règle de Tiering sur « automatique » pour déplacer les données inactives vers le Tier cloud.
Journal d'audit désactivé Le journal d'audit n'est pas activé pour la machine virtuelle de stockage	Activez la journalisation des audits pour la machine virtuelle de stockage	Active la journalisation des audits sur la machine virtuelle de stockage. Notez que la machine virtuelle de stockage doit déjà disposer d'un emplacement de journal d'audit local ou distant configuré.
Bannière de connexion désactivée La bannière de connexion du cluster doit être activée pour renforcer la sécurité en appliquant des restrictions d'accès claires.	Définissez la bannière de connexion du cluster	Définit la bannière de connexion du cluster sur « accès restreint aux utilisateurs autorisés ».
Bannière de connexion désactivée La bannière de connexion de la machine virtuelle de stockage doit être activée pour renforcer la sécurité en appliquant clairement les restrictions d'accès.	Définissez la bannière de connexion de la machine virtuelle de stockage	Définit la bannière de connexion de la machine virtuelle de stockage sur « accès limité aux utilisateurs autorisés ».
SSH utilise des Ciphers non sécurisés Les chiffrements avec le suffixe "-cbc" sont considérés comme non sécurisés.	Supprimez les chiffrements non sécurisés du cluster	Supprime le chiffrement non sécurisé — tel qu'aes192-cbc et aes128-cbc — du cluster.
SSH utilise des Ciphers non sécurisés Les chiffrements avec le suffixe "-cbc" sont considérés comme non sécurisés.	Supprimez les chiffrements non sécurisés de la machine virtuelle de stockage	Supprime le chiffrement non sécurisé — tel qu'aes192-cbc et aes128-cbc — de la machine virtuelle de stockage.

Nom et description de l'événement	Action de gestion	Opération « réparer »
Transport AutoSupport HTTPS désactivé Le protocole de transport utilisé pour envoyer des messages AutoSupport au support technique doit être chiffré.	Définissez HTTPS comme protocole de transport des messages AutoSupport	Configure HTTPS comme le protocole de transport des messages AutoSupport sur le cluster.
Seuil de déséquilibre de charge du cluster dépassé Indique que la charge est déséquilibrée entre les nœuds du cluster. Cet événement est généré lorsque la variance de performance utilisée est supérieure à 30 % entre les nœuds.	Équilibrez les charges de travail en cluster	Unified Manager identifie le volume le mieux à déplacer d'un nœud vers l'autre pour réduire le déséquilibre, puis déplace le volume.
Seuil de déséquilibre de la capacité du cluster dépassé Indique que la capacité est déséquilibrée entre les agrégats du cluster. Cet événement est généré lorsque la variance de capacité utilisée est supérieure à 70 % entre les agrégats.	Équilibrez la capacité du cluster	Unified Manager identifie le volume le mieux à déplacer d'un agrégat à un autre pour réduire le déséquilibre, puis déplace le volume.
Seuil de capacité utilisée - performances dépassé Indique que la charge sur le nœud peut devenir surutilisée si vous ne réduisez pas l'utilisation d'une ou de plusieurs charges de travail hautement 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 dont les IOPS sont les plus élevées et applique une règle de QoS en utilisant l'historique des niveaux d'IOPS attendus et les niveaux de pic pour réduire la charge sur le nœud.
Seuil d'avertissement d'événement dynamique dépassé Indique que le nœud fonctionne déjà dans un état surchargé en raison de la charge anormalement élevée de certaines charges de travail.	Réduire la surcharge dans le nœud	Unified Manager identifie le volume dont les IOPS sont les plus élevées et applique une règle de QoS en utilisant l'historique des niveaux d'IOPS attendus et les niveaux de pic pour réduire la charge sur le nœud.

Nom et description de l'événement	Action de gestion	Opération « réparer »
Basculement impossible Le basculement est actuellement désactivé, afin de limiter l'accès aux ressources du nœud en cas de panne ou de redémarrage, jusqu'à ce que le nœud devienne disponible à nouveau.	Activez le basculement de nœud	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 peut provoquer un problème sur les systèmes configurés en haute disponibilité.	Activation du basculement en cas d'incident	Unified Manager envoie la commande appropriée au cluster pour modifier ce paramètre sur **on**.
Désactivez l'option nodeshell snapmirror.enable L'ancienne option de nodeshell « snapmirror.enable » est définie sur **on**, ce qui peut entraîner un problème au démarrage après la mise à niveau vers ONTAP 9.3 ou version ultérieure.	Définissez 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.	Désactivez Telnet	Unified Manager envoie la commande appropriée au cluster pour désactiver Telnet.

Nom et description de l'événement	Action de gestion	Opération « réparer »
Configurer l'apprentissage anti-ransomwares des VM de stockage Vérifie régulièrement si les clusters sont dotés de licences pour assurer la surveillance contre les ransomwares. Confirme qu'une VM de stockage ne prend en charge que les volumes NFS ou SMB dans un tel cluster	Mettez vos machines virtuelles de stockage en `learning` mode de surveillance anti-ransomware	Unified Manager définit la fonction de surveillance anti-ransomware sur `learning` l'état des machines virtuelles de stockage via la console de gestion des clusters. La surveillance anti-ransomwares sur tous les nouveaux volumes créés sur le VM de stockage sont automatiquement déplacés en mode d'apprentissage. Grâce à cette activation, ONTAP peut apprendre le modèle d'activité sur les volumes et détecter les anomalies dues à d'éventuelles attaques malveillantes.
Configurer l'apprentissage anti-ransomware des volumes Vérifie régulièrement si les clusters sont dotés de licences pour assurer la surveillance contre les ransomwares. Confirme qu'un volume ne prend en charge que les services NFS ou SMB dans un tel cluster	Mettez les volumes en `learning` mode de surveillance anti-ransomware	Unified Manager définit la fonction de surveillance anti-ransomware sur `learning` l'état des volumes via la console de gestion des clusters. Grâce à cette activation, ONTAP peut apprendre le modèle d'activité sur les volumes et détecter les anomalies dues à d'éventuelles attaques malveillantes.
Activation d'une protection contre les ransomwares de volume Vérifie régulièrement si les clusters sont dotés de licences pour assurer la surveillance contre les ransomwares. Détecte si les volumes sont en `learning` mode de surveillance anti-ransomware pendant plus de 45 jours et détermine le cas échéant la perspective de les mettre en mode actif.	Mettez les volumes en `active` mode de surveillance anti-ransomware	Unified Manager définit la fonction de surveillance anti-ransomware sur `active` 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	Action de gestion	Opération « réparer »
Désactivation de l'anti-ransomware des volumes Vérifie régulièrement si les clusters sont dotés de licences pour assurer la surveillance contre les ransomwares. Détecte les notifications répétitives lors de la surveillance active anti-ransomware sur les volumes (par exemple, plusieurs avertissements de ransomware potentiels sont renvoyés sur 30 jours)	Désactiver la surveillance anti-ransomwares sur les volumes	Unified Manager désactive la surveillance anti-ransomwares sur les volumes via la console de gestion du cluster.

Remplacement des actions de gestion via des scripts

Vous pouvez créer des scripts personnalisés et les associer à des alertes afin de prendre des actions spécifiques pour des événements spécifiques. Vous n'êtes pas non plus en accord avec les actions de gestion par défaut qui leur sont disponibles sur la page des actions de gestion ou sur le tableau de bord Unified Manager.

Si vous souhaitez effectuer des actions spécifiques pour un type d'événement et choisir de ne pas les corriger dans le cadre de l'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 prendre en charge 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 le tableau de bord Unified Manager.

Gestion des clusters

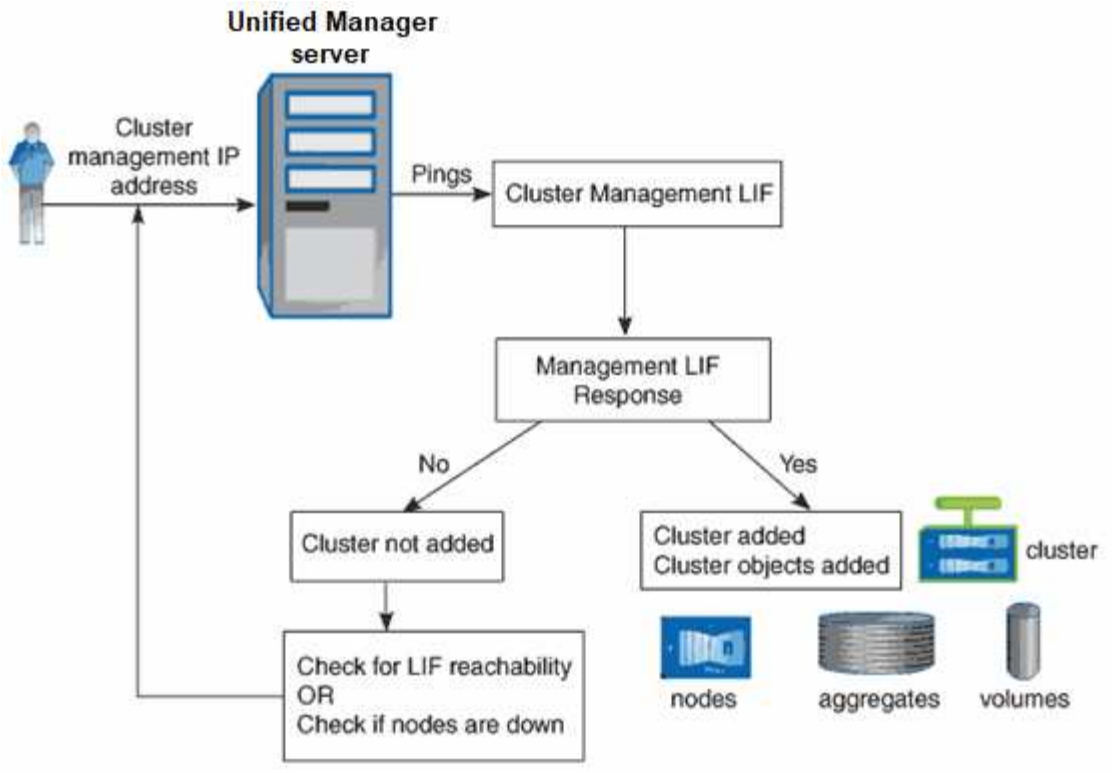
Vous pouvez gérer les clusters ONTAP à l'aide d'Unified Manager afin de surveiller, d'ajouter, de modifier et de supprimer des clusters.

Fonctionnement du processus de détection du cluster

Une fois que vous avez ajouté un cluster à Unified Manager, le serveur détecte les objets du cluster et les ajoute à sa base de données. Le fonctionnement du processus de découverte vous permet de gérer les clusters de votre entreprise et leurs objets.

L'intervalle de contrôle permettant de collecter les informations de configuration du cluster est de 15 minutes. Par exemple, une fois que vous avez ajouté un cluster, il faut 15 minutes pour afficher les objets de cluster dans l'interface utilisateur Unified Manager. Cette période est également vraie lorsque vous apportez des modifications à un cluster. Par exemple, si vous ajoutez deux nouveaux volumes à un SVM dans un cluster, ces nouveaux objets s'affichent dans l'interface utilisateur après l'intervalle d'interrogation suivant, qui peut prendre jusqu'à 15 minutes.

L'image suivante illustre le processus de détection :



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

> Étant donné que la collecte de données de performances sur 15 jours consomme beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters pour que les sondages de collecte de la continuité des données ne s'exécutent pas simultanément sur un trop grand nombre de clusters.

Afficher la liste des clusters surveillés

Vous pouvez utiliser la page Cluster Setup pour afficher l'inventaire de vos clusters. Vous pouvez afficher des détails sur les clusters, tels que leur nom ou leur adresse IP et l'état de la communication.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.

   Tous les clusters de votre environnement de stockage géré par Unified Manager sont affichés.la liste des clusters est triée par colonne du niveau de gravité de l'état de collecte. Vous pouvez cliquer sur un en-tête de colonne pour trier les clusters par différentes colonnes.

Ajout de clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir contrôler le cluster. Il est donc possible d'obtenir des informations sur le cluster, notamment son état, sa capacité, ses performances et sa configuration, afin de trouver et de résoudre tous les problèmes potentiels.

Ce dont vous aurez besoin

- Vous devez disposer du rôle Administrateur d'applications ou Administrateur stockage.
- Vous devez disposer des 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.

    Lorsque vous utilisez le nom d'hôte, il doit résoudre l'adresse IP de gestion du cluster pour la LIF de gestion du cluster. Si vous utilisez une LIF de node-management, 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 accès à l'application défini sur *ontapi*, *console* et *http*.
  - Vous devez connaître le numéro de port à connecter au cluster à l'aide du protocole HTTPS (généralement le port 443).
  - Le cluster doit exécuter la version 9.1 du logiciel ONTAP ou une version ultérieure.
  - L'espace requis doit être adéquat sur le serveur Unified Manager. Vous n'avez pas besoin d'ajouter un cluster au serveur lorsque plus de 90 % de l'espace est déjà utilisé.
  - Vous disposez des certificats requis :

    Certificat SSL (HTTPS) : ce certificat appartient à Unified Manager. Un certificat SSL (HTTPS) auto-signé par défaut est généré avec une nouvelle installation de 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 incorporent le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, reportez-vous à la section "Génération d'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 de ONTAP.

    Certificats de communication mutuelle TLS : utilisés pendant la communication mutuelle TLS entre Unified Manager et ONTAP. L'authentification basée sur le certificat est activée pour un cluster, sur la version ONTAP utilisée. Si le cluster exécutant la version ONTAP est inférieur au 9.5, l'authentification basée sur certificat n'est pas activée.

    L'authentification basée sur des certificats n'est pas activée automatiquement sur un cluster si vous mettez à jour une version antérieure 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, reportez-vous à la section "Modification des clusters".

- Vous pouvez ajouter un cluster depuis l'interface utilisateur Web et l'authentification basée sur certificat est automatiquement activée.
- Vous pouvez ajouter un cluster via l'interface de ligne de commandes Unified Manager ; l'authentification basée sur des certificats n'est pas activée par défaut. Si vous ajoutez un cluster via l'interface de ligne de commande d'Unified Manager, vous devez le modifier à l'aide de l'interface utilisateur d'Unified Manager. Vous pouvez voir "Commandes CLI Unified Manager prises en charge" pour ajouter un cluster à l'aide de l'interface de ligne de commande Unified Manager.
- Si l'authentification basée sur les certificats est activée pour un cluster et que vous effectuez la sauvegarde de Unified Manager à partir d'un serveur et que vous effectuez une restauration vers un autre serveur Unified Manager où le nom d'hôte ou l'adresse IP sont modifiés, la surveillance du cluster peut échouer. Pour éviter la défaillance, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, reportez-vous à "Modification des clusters"la section .
- 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 de 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, reportez-vous à l'article de la base de connaissances (KB) "Comment renouveler un certificat auto-signé ONTAP dans l'interface utilisateur de System Manager" .

- Une instance unique de Unified Manager peut prendre en charge un nombre spécifique de nœuds. Si vous devez contrôler un environnement qui dépasse le nombre de nœuds pris en charge, vous devez installer une instance supplémentaire de Unified Manager pour surveiller certains clusters. Pour afficher la liste du nombre de nœuds pris en charge, reportez-vous à la "Guide des meilleures pratiques de Unified Manager".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs requises, puis cliquez sur **Envoyer**.
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**.

   Une fois les informations de cluster enregistrées, vous pouvez afficher le certificat pour les communications TLS mutuelles pour un cluster.

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

Une fois que tous les objets d'un nouveau cluster sont découverts, Unified Manager commence à collecter les données d'historique de performances des 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité fournit des informations de performance sur plus de deux semaines pour un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données en temps réel des performances du cluster 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 ne permettant pas d'ajouter le cluster, vérifiez si les problèmes suivants existent :

- Si les horloges sur les deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS de Unified Manager est postérieure à la date sur le cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide du protocole 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"

"L'installation d'une autorité de certification a signé et renvoyé un certificat HTTPS"

Modification des clusters

Vous pouvez modifier les paramètres d'un cluster existant, comme 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.

Ce dont vous aurez besoin

Vous devez disposer du rôle Administrateur d'applications ou Administrateur stockage.

Depuis Unified Manager 9.7, vous pouvez ajouter des clusters en utilisant HTTPS uniquement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Sur la page **Cluster Setup**, sélectionnez le cluster à modifier, puis cliquez sur **Edit**.
3. Dans la boîte de dialogue **Edit Cluster**, modifiez les valeurs comme requis. + si vous avez modifié les détails d'un cluster ajouté à Unified Manager, vous pouvez afficher les détails du certificat pour les communications TLS mutuelles, en fonction de la version de ONTAP. Pour plus d'informations sur la version de ONTAP, reportez-vous à "Certificats de communication mutuelle TLS"la section . + 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 de Unified Manager en utilisant la page Cluster Setup. Par exemple, vous pouvez supprimer un cluster si la détection d'un cluster échoue ou si vous souhaitez désaffecter un système de stockage.

Ce dont vous aurez besoin

Vous devez disposer du rôle Administrateur d'applications ou Administrateur stockage.

Cette tâche supprime le cluster sélectionné de Unified Manager. Après le retrait d'un cluster, il n'est plus surveillé. De même, l'instance de Unified Manager enregistrée avec le cluster supprimé n'est pas enregistrée du cluster.

La suppression d'un cluster supprime également tous ses objets de stockage, ses données historiques, les services de stockage et tous les événements associés à partir d'Unified Manager. Ces changements sont reflétés sur les pages d'inventaire et les pages de détails après le prochain cycle de collecte des données.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Sur la page Cluster Setup (Configuration du cluster), sélectionnez le cluster à supprimer et cliquez sur **Remove** (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"

Détection des clusters à nouveau

Vous pouvez redécouvrir manuellement un cluster à partir de la page de configuration des clusters afin d'obtenir les dernières informations sur l'état de santé, la surveillance de l'état et les performances du cluster.

Vous pouvez redécouvrir manuellement un cluster lorsque vous souhaitez mettre à jour le cluster, par exemple

en augmentant la taille d'un agrégat lorsque l'espace est insuffisant, et vous souhaitez qu'Unified Manager détecte les modifications que vous apportez.

Lorsque Unified Manager est associé à OnCommand Workflow Automation (WFA), le couplage déclenche la reacquisition des données mises en cache par WFA.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Sur la page **Cluster Setup**, cliquez sur **redécouvrir**.

   Unified Manager détecte de nouveau le cluster sélectionné et affiche le dernier état de santé et de performances.

Informations connexes

"Affichage de la liste et des détails des clusters"

Surveillance de l'infrastructure virtuelle VMware

Active IQ Unified Manager offre une visibilité sur les machines virtuelles (VM) de votre infrastructure virtuelle et permet d'effectuer la surveillance et la résolution des problèmes de stockage et de performances dans votre environnement virtuel. Vous pouvez l'utiliser pour déterminer tout problème de latence dans votre environnement de stockage ou lorsqu'un événement de performances est signalé sur votre serveur vCenter.

Un déploiement d'infrastructure virtuelle standard sur ONTAP comporte divers composants répartis sur les couches de calcul, de réseau et de stockage. Tout ralentissement des performances dans une application VM peut survenir en raison de la combinaison de latences rencontrées par les différents composants au niveau des couches respectives. Cette fonctionnalité est utile pour les administrateurs du stockage et vCenter Server, ainsi que les informaticiens généralistes qui doivent analyser un problème de performance dans un environnement virtuel et identifier quel composant le problème est survenu.

Vous pouvez désormais accéder à vCenter Server à partir du menu vCenter de la section VMware. La vue d'aperçu de chaque machine virtuelle répertoriée contient le lien **VCENTER SERVER** dans la VUE TOPOLOGIQUE qui lance le serveur vCenter dans un nouveau navigateur. Vous pouvez également utiliser le bouton **Expand Topology** pour lancer vCenter Server et cliquer sur le bouton **View in vCenter** pour afficher les datastores dans vCenter Server.

Unified Manager présente le sous-système sous-jacent d'un environnement virtuel dans une vue topologique afin de déterminer si un problème de latence a eu lieu dans le nœud de calcul, le réseau ou le stockage. La vue indique également l'objet spécifique qui provoque le décalage des performances lors de la réalisation des étapes correctives et de la résolution du problème sous-jacent.

Une infrastructure virtuelle déployée sur un système de stockage ONTAP comprend les objets suivants :

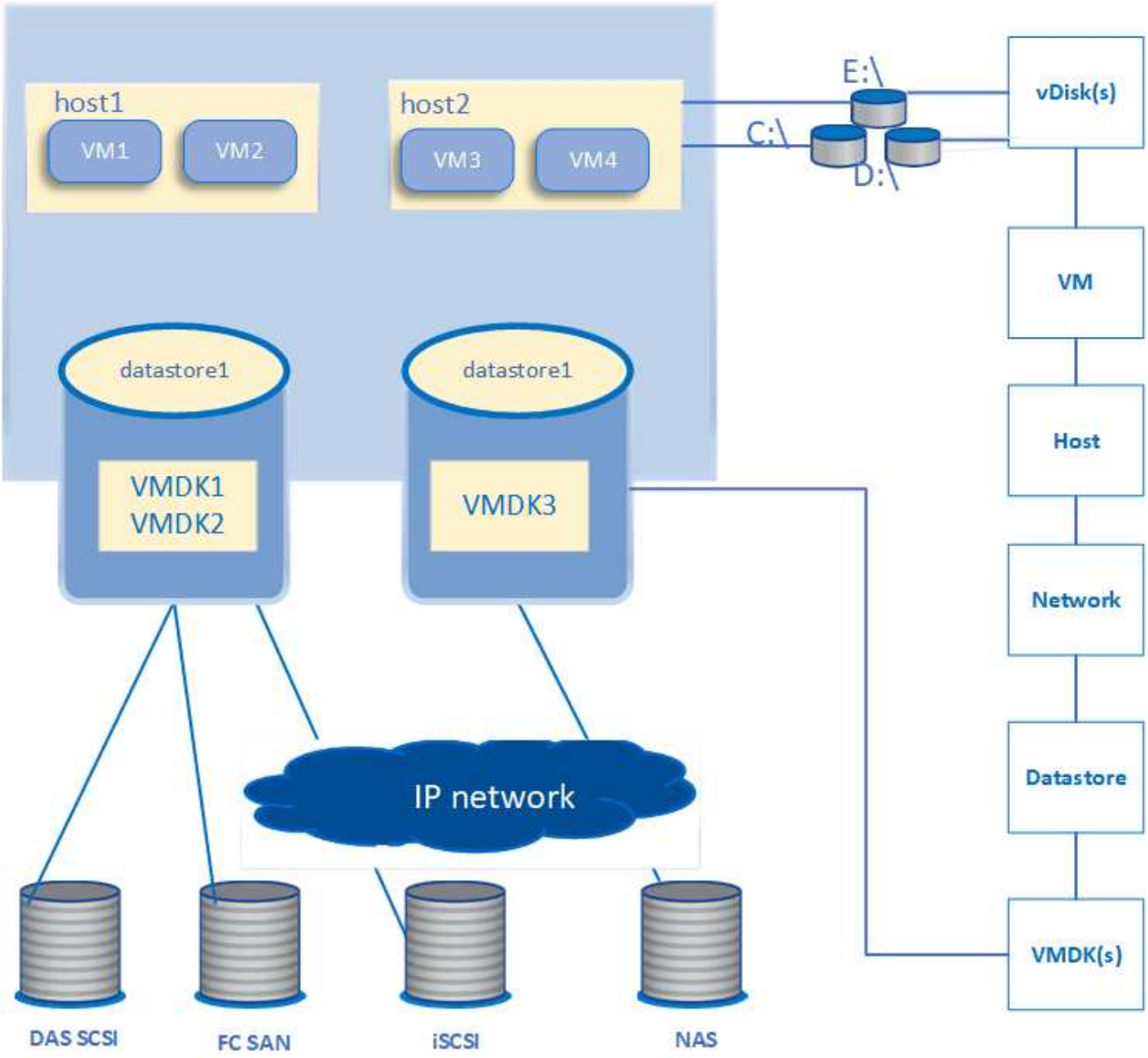
- VCenter Server : plan de contrôle centralisé pour la gestion des machines virtuelles VMware, des hôtes ESXi et de tous les composants associés dans un environnement virtuel. Pour plus d'informations sur vCenter Server, consultez la documentation VMware.
- Hôte : système physique ou virtuel qui exécute ESXi, le logiciel de virtualisation de VMware et héberge la machine virtuelle.
- Datastore : les datastores sont des objets de stockage virtuel connectés aux hôtes ESXi. Les datastores

sont des entités de stockage de ONTAP, telles que des LUN ou des volumes, utilisées comme référentiel pour les fichiers de machines virtuelles, tels que des fichiers journaux, des scripts, des fichiers de configuration et des disques virtuels. Ils sont connectés aux hôtes de l'environnement via une connexion réseau SAN ou IP. Les datastores hors ONTAP mappés à vCenter Server ne sont pas pris en charge ni affichés sur Unified Manager.

- VM : machine virtuelle VMware.
- Disques virtuels : disques virtuels sur des datastores appartenant aux VM ayant une extension au format VMDK. Les données d'un disque virtuel sont stockées sur le VMDK correspondant.
- VMDK : disque de machine virtuelle situé sur le datastore qui fournit de l'espace de stockage pour les disques virtuels. Pour chaque disque virtuel, il existe un VMDK correspondant.

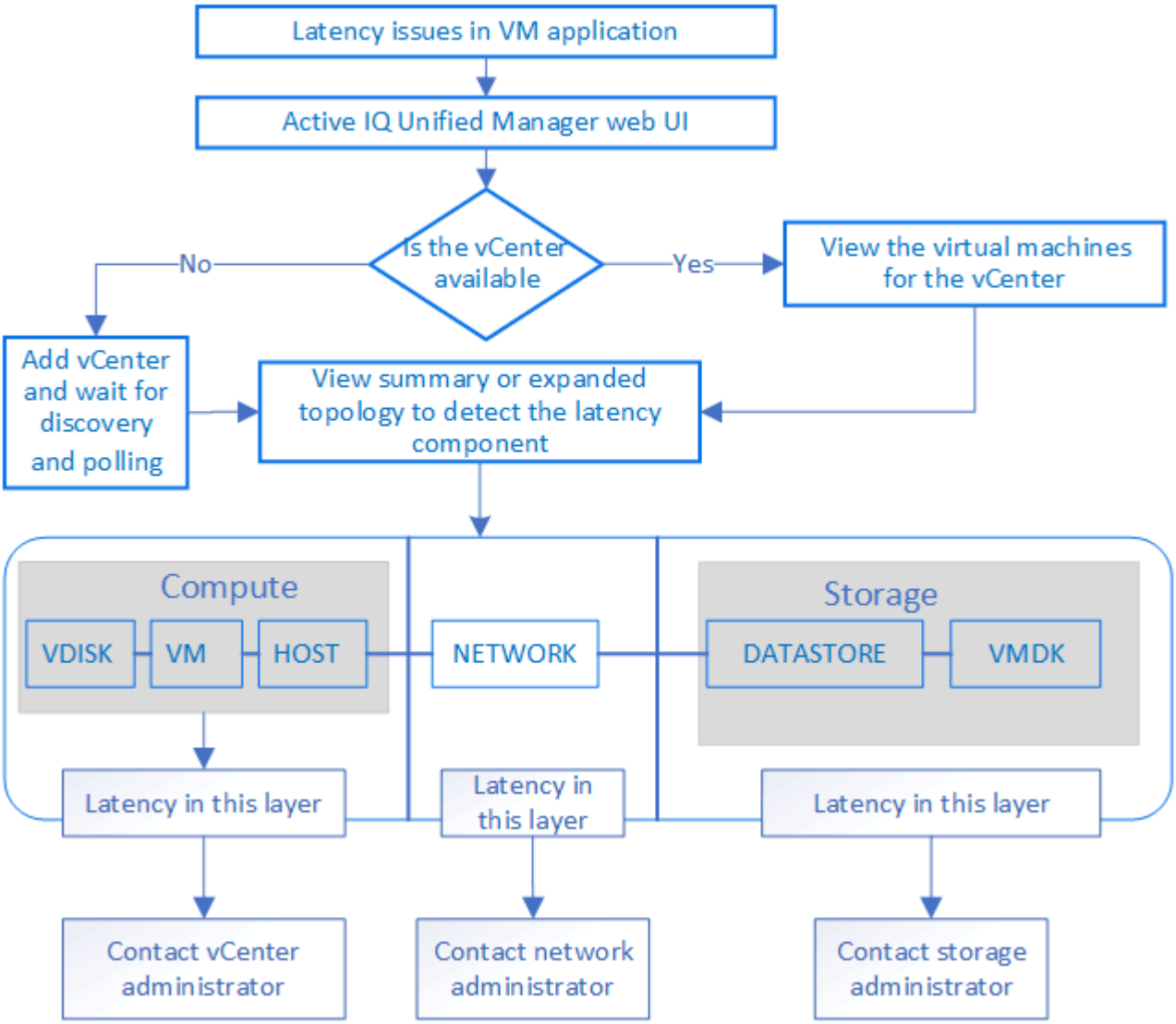
Ces objets sont représentés dans une vue topologique de VM.

Virtualisation VMware sur ONTAP



Flux de travail utilisateur

Le schéma suivant présente un cas d'utilisation typique de la vue topologique de la machine virtuelle :



Ce qui n'est pas pris en charge

- Les datastores hors ONTAP et mappés vers les instances de vCenter Server ne sont pas pris en charge par Unified Manager. Les machines virtuelles contenant des disques virtuels sur ces datastores ne sont pas non plus prises en charge.
- Un datastore qui s'étend sur plusieurs LUN n'est pas pris en charge.
- Les datastores utilisant la traduction d'adresse réseau (NAT) pour le mappage des LIF de données (point de terminaison d'accès) ne sont pas pris en charge.
- L'exportation de volumes ou de LUN en tant que datastores sur différents clusters avec les mêmes adresses IP dans une configuration comportant plusieurs LIF n'est pas prise en charge, car Unified Manager ne peut pas identifier le datastore qui appartient à quel cluster.

  Exemple : supposons que le cluster A possède le datastore A. le datastore A est exporté via la LIF de données avec la même adresse IP x.x.x.x et que la machine virtuelle A est créée sur ce datastore. De même, le cluster B possède le datastore B. le datastore B est exporté via la LIF de données avec la même adresse IP x.x.x.x et la machine virtuelle B est créée sur le datastore B. UM ne peut pas mapper le

datastore A pour la topologie de la machine virtuelle A sur le volume/LUN ONTAP correspondant ni mapper la machine virtuelle B.

- Seuls les volumes NAS et SAN (iSCSI et FCP pour VMFS) sont pris en charge en tant que datastores, 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 pour analyser les performances des différents composants.
- Pour la configuration de reprise sur incident des machines virtuelles de stockage (VM de stockage) prise en charge pour seule infrastructure virtuelle sur Unified Manager, il convient de modifier manuellement la configuration dans vCenter Server afin de désigner les LUN actifs dans les scénarios de basculement et de rétablissement. Sans intervention manuelle, les datastores deviennent inaccessibles.

Affichage et ajout de vCenter Server

Pour afficher et dépanner les performances des machines virtuelles, vous devez ajouter les serveurs vCenter associés à votre instance Active IQ Unified Manager.

Ce dont vous aurez besoin

Avant d'ajouter ou d'afficher des serveurs vCenter, vérifiez les points suivants :

- Vous connaissez les noms des serveurs vCenter.
- Vous connaissez l'adresse IP de vCenter Server et possédez les informations d'identification requises. Les identifiants doivent être d'un administrateur vCenter Server ou d'un utilisateur root disposant d'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 for VMware ESXi et de vCenter Server est disponible en anglais et en japonais.

- Le paramètre de collecte de données dans vCenter Server est défini sur le niveau de statistiques de `Level 3`, garantissant le niveau requis de collecte de metrics 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, reportez-vous à la section « niveaux de collecte des données » du document *vSphere Monitoring and Performance Guide* de 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 du datastore 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 FQDN, 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` fichier.
- L'heure actuelle de vCenter Server est en cours de synchronisation avec le fuseau horaire de vCenter Server.
- VCenter Server est accessible pour une découverte réussie.
- Vous disposez de l'accès en lecture au SDK VMware lorsque vous ajoutez vCenter Server à Unified

Manager. Ceci est requis pour l'interrogation de la configuration.

Pour chaque serveur vCenter ajouté et découvert, Unified Manager collecte les données de configuration, telles que les informations des serveurs vCenter Server et ESXi, le mappage ONTAP, les détails des datastores et le nombre de machines virtuelles hébergées. Elle collecte en outre les mesures de performances des composants.

Étapes

1. Accédez à **VMWARE** > **vCenter** et vérifiez si votre serveur vCenter est disponible dans la liste.

   Si votre serveur vCenter 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 un 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 détection réussie, un certificat de serveur s'affiche pour vous permettre d'accepter.

   Lorsque vous acceptez le certificat, vCenter Server est ajouté à la liste des serveurs vCenter disponibles. L'ajout du périphérique n'entraîne pas la collecte de données pour les machines virtuelles associées, et la collecte s'effectue aux intervalles programmés.

2. Si votre serveur vCenter est disponible sur la page **vCenters**, vérifiez son état en plaçant votre souris sur le champ **Status** pour afficher si votre serveur vCenter fonctionne comme prévu ou s'il y a un avertissement ou une erreur.

   Ajout de vCenter Server vous permet d'afficher les États suivants. Toutefois, les données de performances et de latence des VM correspondantes peuvent prendre jusqu'à une heure après l'ajout de vCenter Server.

   - Vert : « normal », indiquant que vCenter Server a été découvert et que les mesures de performances ont été recueillies avec succès
   - Jaune : « avertissement » (par exemple, lorsque le niveau de statistiques de vCenter Server n'a pas été défini sur 3 ou plus pour obtenir des statistiques pour chaque objet)
   - Orange : « ERROR » (indique toute erreur interne, telle qu'une exception, un échec dans la collecte des données de configuration ou un serveur vCenter inaccessible) vous pouvez cliquer sur l'icône d'affichage de colonne (**Afficher/Masquer**) pour afficher le message d'état d'un serveur vCenter 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 du serveur vCenter

VCenter Server collecte des échantillons de données de performances en temps réel de 20 secondes et les transfère jusqu'à des échantillons de 5 minutes. La planification de la collecte des données de performances

de Unified Manager repose sur les paramètres par défaut de vCenter Server. Unified Manager traite les échantillons de 5 minutes provenant de vCenter Server et calcule la moyenne horaire des IOPS et de la latence des disques virtuels, des machines virtuelles et des hôtes. Pour les datastores, Unified Manager calcule la moyenne horaire des IOPS et de la latence à partir des échantillons provenant de ONTAP. Ces valeurs sont disponibles en haut de l'heure. Les mesures de performance ne sont pas disponibles immédiatement après l'ajout de vCenter Server et ne sont disponibles qu'au démarrage de l'heure suivante. L'interrogation des données de performances commence par la fin d'un cycle de collecte des données de configuration.

Pour l'interrogation des données de configuration de vCenter Server, Unified Manager suit la même planification que pour la collecte des données de configuration du cluster. Pour plus d'informations sur la planification de la collecte des données de performances et de configuration de vCenter Server, reportez-vous à la section « activité de collecte des données de configuration du cluster et de performances ».

Informations connexes

"Activité de collecte des données sur la configuration et les performances du cluster"

Suppression de vCenter Server

Vous pouvez supprimer des serveurs vCenter de votre instance Active IQ Unified Manager. Par exemple, vous pouvez supprimer un serveur vCenter si la découverte de vCenter Server échoue ou si elle n'est plus nécessaire.

La suppression d'un serveur vCenter 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, avec les objets associés et les données historiques. Ces modifications seront répercutées sur vCenter et les pages d'inventaire des machines virtuelles.

Ce dont vous aurez besoin

Avant de supprimer des serveurs vCenter, vérifiez les points suivants :

- Vous disposez du rôle d'administrateur d'applications ou d'administrateur du stockage.
- Vous devez connaître les noms des serveurs vCenter et leurs adresses IP respectives.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **VMWARE>vCenter**.
2. Sur la page vCenters, sélectionnez le serveur vCenter à supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Supprimer vCenter**, cliquez sur **OK** pour confirmer la demande de suppression.

Surveillance des machines virtuelles

En cas de 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 serveur vCenter 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, du datastore et de l'hôte sont affichées. Pour une machine virtuelle prenant en

charge plusieurs datastores, la grille affiche les mesures du datastore ayant la plus faible latence, avec une icône astérisque (*) indiquant d'autres datastores. Si vous cliquez sur l'icône, les mesures du datastore supplémentaire s'affichent. Certaines de ces colonnes ne sont pas disponibles pour le tri et le filtrage.

> Pour afficher un serveur virtuel et ses détails, la découverte (interrogation ou collecte de metrics) du cluster ONTAP doit être terminée. Si le cluster est retiré du Unified Manager, la machine virtuelle n'est plus disponible, après le cycle suivant de détection.

Cette page vous permet également d'afficher la topologie détaillée d'une machine virtuelle et d'afficher les composants auxquels elle est associée, par exemple, l'hôte, le disque virtuel et le datastore qui y est connecté. La vue topologique affiche les composants sous-jacents dans leurs couches spécifiques, dans l'ordre suivant : **disque virtuel** > **VM** > **hôte** > **réseau** > **datastore** > **VMDK**.

Vous pouvez déterminer le chemin d'E/S et les latences au niveau des composants à partir d'un aspect topologique, afin d'identifier si le stockage est à l'origine du problème de performances. La vue résumée de la topologie affiche le chemin d'E/S et met en évidence le composant présentant des problèmes d'IOPS et de latence pour vous aider à décider des étapes de dépannage. Vous pouvez également disposer d'une vue développée de la topologie décrivant 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 couches.

Affichage de la topologie résumée

Pour déterminer les problèmes de performances, consultez les VM dans une topologie récapitulative :

1. Accédez à **VMWARE** > **machines virtuelles**.
2. Recherchez votre VM en saisissant son nom dans la zone de recherche. Vous pouvez également filtrer les résultats de votre recherche en fonction de critères spécifiques en cliquant sur le bouton **Filter**. Cependant, si vous ne trouvez pas votre VM, assurez-vous que le serveur vCenter correspondant a été ajouté et découvert.

   > Les serveurs vCenter autorisent des caractères spéciaux (tels que %, &, *, $, #, @, !, \, / :, *, ?, "», <, >, |, ;, ') dans les noms d'entités vSphere, telles que VM, cluster, datastore, dossier, ou fichier. VMware vCenter Server et ESX/ESXi Server n'échappent pas aux caractères spéciaux utilisés dans les noms d'affichage. En revanche, lorsque le nom est traité dans Unified Manager, il s'affiche différemment. Par exemple, une machine virtuelle nommée `%$VC_AIQUM_clone_191124%`dans vCenter Server s'affiche comme `%25$VC_AIQUM_clone_191124%25` dans Unified Manager. Vous devez garder une note de ce problème lorsque vous effectuez une requête sur un VM portant un nom comportant des caractères spéciaux.

3. Vérifier l'état de la VM. Les États VM sont récupérés à partir de vCenter Server. Les États suivants sont disponibles. Pour plus d'informations sur ces États, reportez-vous à la documentation VMware.
   - Normale
   - Avertissement
   - Alerte
   - Non surveillé
   - Inconnu
4. Cliquez sur la flèche vers le bas en regard de la machine virtuelle pour afficher la vue résumée de la topologie des composants au niveau des couches de calcul, de réseau et de stockage. Le nœud

présentant des problèmes de latence est mis en évidence. La vue résumée présente la pire latence des composants. Par exemple, si une machine virtuelle possède plusieurs disques virtuels, cette vue affiche le disque virtuel qui présente la latence la plus faible parmi tous les disques virtuels.

5. Pour analyser la latence et le débit du datastore sur une période donnée, cliquez sur le bouton **Workload Analyzer** situé en haut de l'icône de l'objet datastore. 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 datastore. Pour plus d'informations sur l'analyseur de charge de travail, reportez-vous à la section *Dépannage des charges de travail à l'aide de l'analyseur de charge de travail*.

Affichage de la topologie étendue

Vous pouvez explorer chaque composant séparément en visualisant la topologie étendue de la machine virtuelle.

Étapes

1. Dans la vue topologique récapitulative, cliquez sur **développer topologie**. La topologie détaillée de chaque composant s'affiche séparément avec les numéros de latence de chaque objet. Si une catégorie contient plusieurs nœuds, par exemple plusieurs nœuds dans le datastore ou VMDK, le nœud présentant la latence la plus faible est surligné en rouge.
2. Pour vérifier le chemin d'E/S d'un objet spécifique, cliquez sur cet objet pour afficher le chemin d'E/S et le mappage correspondant. Par exemple, pour afficher le mappage d'un disque virtuel, cliquez sur le disque virtuel pour afficher son mappage mis en surbrillance sur le disque VMDK correspondant. Si ces latences de performances décalage sont dues à des composants, vous pouvez collecter davantage de données à partir d'ONTAP et résoudre le problème.

> Les mesures ne sont pas signalées pour les VMDK. Dans la topologie, seuls les noms VMDK sont affichés, et non les metrics.

Informations connexes

"Dépannage des workloads à l'aide de l'analyseur de charge de travail"

Visualisation d'une infrastructure virtuelle dans une configuration de reprise après incident

Vous pouvez afficher les mesures de configuration et de performances des datastores hébergés dans une configuration MetroCluster ou une configuration de reprise après incident de SVM (Storage Virtual machine).

Sur Unified Manager, vous pouvez afficher les volumes NAS ou les LUN dans une configuration MetroCluster rattachés en tant que datastores dans vCenter Server. Les datastores hébergés en configuration MetroCluster sont représentés dans la même vue topologique qu'un datastore dans un environnement standard.

Vous pouvez également afficher les volumes NAS ou les LUN dans une configuration de reprise après incident des machines virtuelles de stockage mappée aux datastores de vCenter Server.

Affichage des datastores dans la configuration MetroCluster

Notez les prérequis suivants avant de afficher les datastores dans une configuration MetroCluster :

- En cas de basculement et de rétablissement, la découverte des clusters principaux et secondaires de la paire haute disponibilité et des serveurs vCenter doit être achevée.

- Les clusters principaux et secondaires de la paire haute disponibilité 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 de ONTAP et vCenter.

  "Centre de documentation ONTAP 9"

Pour afficher les datastores, procédez comme suit :

1. Sur la page **VMWARE** > **Virtual machines**, cliquez sur la VM qui héberge le datastore. Cliquez sur le lien **Workload Analyzer** ou sur l'objet datastore. Dans le scénario standard, lorsque le site principal hébergeant le volume ou la LUN fonctionne comme prévu, vous pouvez afficher les détails du cluster du SVM du site primaire.
2. En cas d'incident et pour un basculement consécutif vers le site secondaire, la liaison du datastore pointe vers les mesures de performances du volume ou de la LUN du cluster secondaire. Cela est reflétée après la fin du cycle suivant de clusters et de la découverte du SVM (acquisition).
3. Une fois le rétablissement réussi, la liaison du datastore reflète à nouveau les mesures de performances du volume ou de la LUN dans le cluster principal. Cela est reflétée après la fin du cycle suivant de clusters et de la découverte du SVM.

Affichage des datastores dans la configuration de reprise d'activité des machines virtuelles de stockage

Notez les prérequis suivants avant de visualiser les datastores dans une configuration de reprise d'activité de VM de stockage :

- En cas de basculement et de rétablissement, la découverte des clusters principaux et secondaires de la paire haute disponibilité et des serveurs vCenter doit être achevée.
- Les pairs de clusters source et de destination doivent être gérés par Unified Manager.
- La configuration requise doit être effectuée sur ONTAP et vCenter Server.
  - Pour les datastores NAS (NFS et VMFS), en cas d'incident, il convient de mettre en place la machine virtuelle de stockage secondaire, vérifier les LIFs et les routes des données, établir les connexions perdues sur vCenter Server et démarrer les VM.

    Pour un rétablissement sur le site primaire, les données entre les volumes doivent être synchronisées avant que le site primaire ne commence à transmettre les données.

  - Pour les datastores SAN (iSCSI et FC pour VMFS), vCenter Server formate le LUN monté au format VMFS. En cas d'incident, la procédure comprend l'installation de la machine virtuelle de stockage secondaire, la vérification des LIFs et des routes des données. Si les adresses IP cibles iSCSI sont différentes des LIF primaires, elles doivent être ajoutées manuellement. Les nouvelles 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 datastores VMFS avec les nouvelles LUN doivent être créés et les anciennes machines virtuelles enregistrées avec de nouveaux noms. Les machines virtuelles doivent être opérationnelles.

    En cas de restauration, les données entre les volumes doivent être synchronisées. Les nouveaux datastores 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 l'installation, reportez-vous à la documentation relative à ONTAP et à

vCenter Server.

"Centre de documentation ONTAP 9"

Pour afficher les datastores, procédez comme suit :

1. Sur la page **VMWARE** > **Virtual machines**, cliquez sur l'inventaire VM qui héberge le datastore. Cliquez sur le lien objet datastore. Le scénario standard vous permet de voir les données de performances des volumes et des LUN dans la VM de stockage primaire.
2. En cas d'incident et pour un basculement consécutif vers la machine virtuelle de stockage secondaire, la liaison du datastore pointe vers les mesures de performances du volume ou de la LUN du VM de stockage secondaire. Cela est reflétée après la fin du cycle suivant de clusters et de la découverte du SVM (acquisition).
3. Une fois le rétablissement réussi, la liaison du datastore reflète à nouveau les mesures de performances du volume ou du LUN sur la machine virtuelle de stockage principale. Cela est reflétée après la fin du cycle suivant de clusters et de la découverte du SVM.

Scénarios non pris en charge

- Pour une configuration MetroCluster, noter les limites suivantes :
  - Les clusters dans les États et `SWITCHOVER` uniquement `NORMAL` sont pris en compte. Les autres États, tels que `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK`, et `NOT_REACHABLE` ne sont pas pris en charge.
  - Sauf si le basculement automatique (ASO) est activé, si le cluster principal est en panne, le cluster secondaire ne peut pas être découvert et la topologie continue de pointer vers le volume ou la LUN du cluster principal.
- Pour une configuration de reprise après incident de VM de stockage, notez les limites suivantes :
  - Une configuration avec site Recovery Manager (SRM) ou Storage Replication adapter (SRA) activée pour un environnement de stockage SAN n'est pas prise en charge.

Provisionner et gérer les workloads

La fonction de gestion active de Active IQ Unified Manager offre les niveaux de service en matière de performance, les règles d'efficacité du stockage et les API des fournisseurs de stockage pour le provisionnement, la surveillance et la gestion des charges de travail de stockage dans un data Center.

> Unified Manager fournit cette fonctionnalité par défaut. Vous pouvez le désactiver à partir de **Storage Management** > **Feature Settings** si vous ne prévoyez pas d'utiliser cette fonctionnalité.

Lorsque cette option est activée, vous pouvez provisionner les charges de travail sur les clusters ONTAP gérés par votre instance de Unified Manager. Vous pouvez également attribuer des règles, comme des niveaux de service performances et des règles d'efficacité du stockage aux charges de travail, et gérer votre environnement de stockage en fonction de ces règles.

Cette fonction permet d'utiliser les fonctions suivantes :

- La découverte automatique des charges de travail de stockage sur les clusters ajoutés, ce qui facilite

l'évaluation et le déploiement 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 performances et des règles d'efficacité du stockage
- Assignation des niveaux de service de performances et des règles d'efficacité du stockage aux charges de travail de stockage

Les options **Provisioning**, **Storage** > **workloads** et **Policies** du volet gauche de l'interface utilisateur vous permettent de modifier diverses configurations.

Vous pouvez exécuter les fonctions suivantes à l'aide des options suivantes :

- Affichez les charges de travail de stockage sur la page **Storage** > **workloads**
- Créez des workloads de stockage à partir de la page provisionner les workloads
- Création et gestion de niveaux de service de performances à partir de règles
- Créez et gérez des règles d'efficacité du stockage à partir de règles
- Attribuez des règles aux charges de travail de stockage depuis la page charges de travail

Informations connexes

"Gestion du stockage basée sur des règles"

Présentation des charges de travail

Une charge de travail (workload) représente les opérations d'entrée/sortie (I/O) d'un objet de stockage, telles qu'un volume ou une LUN. La méthode de provisionnement du stockage repose sur les exigences des charges de travail attendues. Les statistiques de charge de travail sont uniquement suivies par Active IQ Unified Manager après le trafic vers et depuis l'objet de stockage. Par exemple, les valeurs d'IOPS et de latence de la charge de travail sont disponibles lorsque les utilisateurs ont commencé à utiliser une application de base de données ou de messagerie.

La page charges de travail affiche un récapitulatif des charges de travail de stockage des clusters ONTAP gérés par Unified Manager. Il fournit des informations cumulées d'un coup d'œil sur les charges de travail de stockage conformes au niveau de service performances, ainsi que sur les charges de travail de stockage non conformes. Elle vous permet également d'évaluer la capacité et les performances totales, disponibles et utilisées (IOPS) des clusters de votre data Center.

> Il est recommandé d'évaluer le nombre de charges de travail de stockage non conformes, non disponibles ou non gérées par un niveau de service Performance, et de prendre les mesures nécessaires pour assurer la conformité, l'utilisation de la capacité et le nombre d'opérations d'entrée/sortie par seconde.

La page workloads contient les deux sections suivantes :

- Présentation des charges de travail : offre une vue d'ensemble du nombre de charges de travail de stockage sur les clusters ONTAP gérés par Unified Manager.

- Présentation du data Center : présente la capacité et les IOPS des charges de travail de stockage dans le data Center. Les données pertinentes sont affichées au niveau du centre de données et pour chaque .

Les charges de travail

La section vue d'ensemble des charges de travail fournit des informations cumulées d'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 affectés et non attribués.

- **Assigné** : les États suivants sont signalés pour les charges de travail de stockage sur lesquelles des niveaux de service de performance ont été attribués :
  - **Conformité** : les performances des charges de travail de stockage sont basées sur les niveaux de service de performances qui leur sont affectés. Si les charges de travail de stockage se situent dans la latence seuil définie dans les niveaux de services de performance associés, elles sont désignées par le terme « conformité ». Les charges de travail conformes sont indiquées en bleu.
  - **Non-conformité** : pendant la surveillance des performances, les charges de travail de stockage sont marquées d'un « non-conformité » si la latence des charges de travail de stockage dépasse le seuil défini dans le niveau de services de performances associé. Les charges de travail non conformes sont signalées en orange.
  - **Indisponible** : les charges de travail de stockage sont marquées comme « non disponibles » s'elles sont hors ligne ou si le cluster correspondant est inaccessible. Les charges de travail non disponibles sont marquées en rouge.
- **Non affectées** : les charges de travail de stockage qui ne leur sont pas attribuées un niveau de service de performance sont signalées comme « non affectées ». 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 affectées et non affectées.

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 Conformance by Performance Service Levels affiche le nombre total de charges de travail de stockage disponibles :

- Conformité à chaque type de niveau de service Performance
- Pour laquelle il existe une incohérence entre les niveaux de service performances attribués et recommandés

Présentation du data Center

La section présentation du data Center représente sous forme graphique la capacité disponible et utilisée et les IOPS de tous les clusters du data Center. Ces données vous permettront de gérer la capacité et les IOPS des charges de travail de stockage. Cette section affiche également les informations suivantes pour les charges de travail de stockage sur tous les clusters :

- Total, disponible et capacité utilisée pour tous les clusters de votre data Center
- Le total, la disponibilité et les IOPS utilisées pour tous les clusters de votre data Center
- Capacité disponible et utilisée en fonction de chaque niveau de service Performance
- Les IOPS disponibles et utilisées sont basées sur chaque niveau de service de performance
- Espace total et IOPS utilisés par les charges de travail pour lesquelles aucun niveau de service de performance n'est attribué

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.

Le nombre d'IOPS disponibles est calculé en fonction de la latence attendue et des niveaux de service de performances recommandés sur les nœuds. Elle inclut les IOPS disponibles pour tous les niveaux de services de performances dont la latence prévue est inférieure ou égale à la latence attendue.

La capacité disponible est calculée en fonction du temps de latence attendu et des niveaux de service de performances recommandés pour les agrégats. Elle inclut la capacité disponible pour tous les niveaux de services de performances dont la latence prévue est inférieure ou égale à la latence attendue.

Affichage des charges de travail

Lorsque vous ajoutez des clusters à Unified Manager, les charges de travail de stockage de chaque cluster sont automatiquement découvertes et affichées sur la page des charges de travail.

Unified Manager commence à analyser les charges de travail à des fins de recommandation (PSLs recommandés) uniquement après le démarrage des opérations d'E/S sur les charges de travail de stockage.

Les volumes FlexGroup et ses composants sont exclus.

Présentation des charges de travail

La page vue d'ensemble des charges de travail présente les charges de travail du data Center, ainsi que le résumé de l'espace et des performances du data Center.

- **Panneau Aperçu des charges de travail** : affiche le nombre total de charges de travail et le nombre de charges de travail avec ou sans PSLs qui leur sont affectées. La répartition du nombre de charges de travail pour chaque PSL s'affiche également. En cliquant sur le nombre, 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 aux recommandations du système et leur affecter les PSLs recommandés par le système en cliquant sur le bouton **affecter les PSLs** recommandés par le système.
- **Panneau Présentation du centre de données** : affiche l'espace disponible et utilisé (TIB) 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.

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.

Concernant les charges de travail de stockage récemment découvertes sur lesquelles il n'y a pas d'opérations d'E/S, l'état est « en attente d'E/S ». Une fois les opérations d'E/S traitées sur les charges de travail de stockage, Unified Manager commence l'analyse et l'état des charges de travail devient « apprentissage… ». Une fois l'analyse terminée (dans les 24 heures suivant le début des opérations d'E/S), les PSLs recommandés sont affichés pour les charges de travail de stockage.

La page vous permet également d'attribuer des politiques d'efficacité du stockage (PPE) et des niveaux de service de performances (PSLs) aux charges de travail de stockage. Vous pouvez effectuer plusieurs tâches :

- Ajout ou provisionnement de workloads de stockage
- Afficher et filtrer la liste des charges de travail
- Attribuez des PSLs aux charges de travail de stockage
- Évaluez les SLS recommandées par le système et affectez-les aux charges de travail
- Attribuez des PPE 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 aux LUN prises en charge (prise en charge des protocoles iSCSI et FCP), aux partages de fichiers NFS et aux partages SMB.

Étapes

1. Cliquez sur **stockage > charges de travail > toutes les charges de travail > Créer**.
2. Créer des workloads Pour plus d'informations, voir "Provisionner et gérer les workloads".

Afficher et filtrer les workloads

Sur l'écran toutes les charges de travail, vous pouvez afficher toutes les charges de travail de votre data Center ou rechercher des charges de travail de stockage spécifiques en fonction de leurs PSLs ou de leurs noms. Vous pouvez utiliser l'icône de filtre pour entrer des conditions spécifiques à votre recherche. Vous pouvez effectuer une recherche selon différentes conditions de filtre, par exemple par le cluster hôte ou la machine virtuelle de stockage. L'option **Capacity Total** permet de filtrer en fonction de la capacité totale des charges de travail (par Mo). Toutefois, le nombre de workloads renvoyés peut varier car la capacité totale est comparée à un niveau d'octet.

Pour chaque charge de travail, des informations, telles que le cluster hôte et la machine virtuelle de stockage, s'affichent, ainsi que les informations PSL et SEP attribuées.

Cette page vous permet également d'afficher les performances détaillées 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 / Commander les colonnes** et en sélectionnant des colonnes spécifiques à afficher. La colonne vue des performances affiche les IOPS moyennes et maximales d'une charge de travail. Vous pouvez cliquer sur l'icône de l'analyseur de workloads pour afficher l'analyse détaillée des IOPS.

L'analyse des critères de performances et de capacité d'une charge de travail

Le bouton **analyser charge de travail** de la fenêtre contextuelle **analyse d'IOPS** vous permet d'accéder à la page analyse de charge de travail, où vous pouvez sélectionner une plage de temps 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 flux de travail, reportez-vous à "Dépannage des charges de travail à l'aide de l'analyseur de workloads"la section .

Vous pouvez afficher les informations de performances d'une charge de travail pour faciliter le dépannage en cliquant sur l'icône du graphique à barres dans la colonne **Affichage des performances**. Pour afficher les graphiques de performances et de capacité sur la page analyse de la charge de travail pour analyser l'objet, cliquez sur le bouton **analyser la charge de travail**.

Pour plus d'informations, voir "Données affichées par l'analyseur de flux de travail".

L'attribution de règles aux workloads

Vous pouvez affecter des politiques d'efficacité du stockage (PPE) et des niveaux de

service de performance aux charges de travail de stockage à partir de la page toutes les charges de travail en utilisant les différentes options de navigation.

L'assignation de règles à un seul workload

Vous pouvez affecter un PSL ou un SEP ou les deux à une seule charge de travail. Voici la procédure à suivre :

1. Sélectionnez la charge de travail.
2. Cliquez sur l'icône d'édition située à côté de la ligne, puis cliquez sur **Modifier**.

   Les champs **niveau de service de performances attribué** et **Stratégie d'efficacité du stockage** sont activés.

3. Sélectionnez la PSL ou SEP requise, 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 affecter les stratégies.

Attribuez des règles à plusieurs workloads de stockage

Vous pouvez affecter un PSL ou un SEP à plusieurs charges de travail de stockage ensemble. Voici la procédure à suivre :

1. Cochez les cases correspondant aux charges de travail auxquelles vous souhaitez attribuer la règle ou sélectionnez toutes les charges de travail de votre data Center.
2. Cliquez sur **plus d'actions**.
3. Pour attribuer une PSL, sélectionnez **attribuer un niveau de service de performances**. Pour attribuer un SEP, sélectionnez **attribuer une stratégie d'efficacité du stockage**. Une fenêtre contextuelle s'affiche pour vous permettre de sélectionner la stratégie.
4. Sélectionnez la stratégie appropriée et cliquez sur **appliquer**. Le nombre de charges de travail attribuées aux règles s'affiche. Les charges de travail sur lesquelles les règles ne sont pas attribuées sont également répertoriées, en entraînant la cause.

> L'application de règles à des charges de travail en bloc peut prendre un certain temps selon le 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 groupée terminée, vous pouvez afficher l'état d'achèvement. Si vous appliquez une PSL sur plusieurs charges de travail, vous ne pouvez pas déclencher une autre demande lorsque la tâche précédente d'affectation en bloc est en cours d'exécution.

Attribution des SLS recommandées par le système aux charges de travail

Vous pouvez affecter des SLR recommandés par le système à ces charges de travail de stockage dans un centre de données ne disposant pas de SLP, ou les SLS attribuées ne correspondent pas aux recommandations du système. Pour utiliser cette fonctionnalité, cliquez sur le bouton **affecter les PSLs** recommandés par le système. Vous n'avez pas besoin de sélectionner des workloads spécifiques.

Cette recommandation est déterminée en interne par l'analyse du système et est ignorée pour les charges de

travail dont les IOPS et les autres paramètres ne coïncident pas avec les définitions de tout PSL disponible. Les workloads de stockage avec `Waiting for I/O` statut et d'apprentissage sont également exclus.

> Unified Manager recherche des mots-clés spéciaux dans le nom de la charge de travail pour ignorer l'analyse du système et recommander une autre PSL pour la charge de travail. Lorsque la charge de travail porte les lettres « ora » dans le nom, la **Extreme Performance** PSL est recommandée. Et lorsque la charge de travail a les lettres « vm » dans le nom, la **Performance** PSL est recommandée.

Consultez également l'article de la base de connaissances "ActiveIQ Unified Manager « attribuer le niveau de service de performances recommandé par le système » n'est pas adaptable à une charge de travail extrêmement variable"

Provisionnement des volumes de partage de fichiers

Vous pouvez créer des volumes de partage de fichiers qui prennent en charge les protocoles CIFS/SMB et NFS, sur un cluster existant et sur Storage Virtual machine (VM de stockage) à partir de la page provisionner les workloads.

Ce dont vous aurez besoin

- La VM de stockage doit disposer d'espace pour le provisionnement du volume de partage de fichiers.
- Les services SMB et NFS doivent être activés sur la machine virtuelle de stockage.
- Pour sélectionner et attribuer le niveau de service de performances (PSL) et la stratégie d'efficacité du stockage (SEP) sur la charge de travail, les règles 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 à créer, puis sélectionnez le cluster dans la liste disponible.
2. En fonction du cluster sélectionné, le champ **Storage VM** filtre les machines virtuelles de stockage disponibles pour ce cluster. Sélectionnez la VM de stockage requise dans la liste.

   En fonction des services SMB et NFS pris en charge sur la VM 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 la PSL, et éventuellement un SEP pour la charge de travail.

   Les spécifications du SEP sont affectées à la LUN et les définitions de la 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'affectation 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 performances et de capacité définis dans la politique correspondante. Par exemple, si une charge de travail est affectée « PSL Extreme Performance «, l'agrégat sur lequel la charge de travail est provisionnée doit avoir la capacité de soutenir les objectifs de performances et de capacité de la stratégie « Extreme Performance », comme le stockage SSD.

> Sauf si vous cochez cette case, la PSL n'est pas appliquée à la charge de travail et l'état de la charge de travail sur le tableau de bord apparaît comme non affecté.

5. Sélectionnez l'option **NAS**.

   Si l'option **NAS** n'est pas 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 cocher les cases **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 entrer des valeurs séparées par des virgules pour plusieurs hôtes.

   Lors de l'ajout de l'adresse IP de l'hôte, une vérification interne vérifie la correspondance des détails de l'hôte avec le VM de stockage et l'export policy pour cet hôte est créée, ou lorsqu'une règle existante est utilisée, elle est réutilisée. Si plusieurs partages NFS sont créés pour le même hôte, une export policy disponible pour le même hôte avec des règles correspondantes est réutilisée pour tous les partages de fichiers. La fonction de définition de règles spécifiques à chaque règle ou de réutilisation de règles s'effectue en fournissant des clés de règles spécifiques lorsque vous provisionnez le partage NFS à l'aide d'API.

7. Pour un partage SMB, spécifiez quels utilisateurs ou groupes d'utilisateurs 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 qui prennent en charge les protocoles CIFS/SMB et NFS, sur un cluster existant et sur une machine virtuelle de stockage (VM de stockage) à partir de la page provisionner les charges de travail.

Ce dont vous aurez besoin

- La machine virtuelle de stockage doit disposer d'espace pour le provisionnement de la LUN.
- ISCSI et FCP doivent être activés sur la VM de stockage sur laquelle vous créez la LUN.
- Pour sélectionner et attribuer le niveau de service de performances (PSL) et la stratégie d'efficacité du stockage (SEP) sur la charge de travail, les règles 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 à créer, puis sélectionnez le cluster dans la liste disponible.

   En fonction du cluster 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 la PSL, et éventuellement le SEP pour la charge de travail.

   Les spécifications du SEP sont affectées à la LUN et les définitions de la 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'affectation 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 performances et de capacité définis dans la politique correspondante. Par exemple, si une charge de travail se voit attribuer la PSL « Extreme Performance », l'agrégat sur lequel la charge de travail doit être provisionnée doit avoir la capacité de respecter les objectifs de performances et de capacité de la politique Extreme Performance, comme le stockage SSD.

   > Sauf si vous cochez 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 s'affiche comme `unassigned`.

5. Sélectionnez l'option **SAN**. Si l'option **SAN** n'est pas 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 à la LUN. Vous pouvez affecter des groupes initiateurs existants ou définir et mapper de nouveaux groupes initiateurs.

   > Si vous créez un nouveau groupe initiateur lors du provisionnement de la LUN, vous devez attendre le cycle de détection suivant (jusqu'à 15 minutes) pour l'utiliser. Il est donc recommandé d'utiliser un groupe initiateur existant dans la liste des igroups disponibles.

   Si vous souhaitez créer un nouveau groupe initiateur, sélectionnez le bouton **Créer un nouveau groupe initiateur**, puis entrez les informations du groupe initiateur.

8. Cliquez sur **Enregistrer**.

   La LUN est ajoutée à la liste des charges de travail de stockage.

Niveaux de services de performances

Un niveau de service de performances (PSL) vous permet de définir les objectifs de performances et de stockage d'une charge de travail. Vous pouvez affecter un PSL à une charge de travail lors de la création initiale de la charge de travail ou par la suite en modifiant la charge de travail.

La gestion et la surveillance des ressources de stockage reposent sur des objectifs de niveau de service (SLO). Les SLO sont définis par des contrats 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 un système de stockage NetApp. Les services de stockage sont différenciés en fonction des performances et de

l'utilisation des ressources sous-jacentes. Une 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 régie par les IOPS minimales maximales, attendues et absolues, ainsi que la latence attendue.

Unified Manager offre les types de PSLs suivants :

- **System-defined** : Unified Manager fournit quelques stratégies prédéfinies qui ne peuvent pas être modifiées. Ces SLS prédéfinies sont les suivantes :

  - Performances exceptionnelles
  - Performances
  - Valeur

    Les SLS Extreme Performance, Performance et Value s'appliquent à la plupart des charges de travail de stockage courantes d'un data Center.

  Unified Manager propose également trois niveaux de service haute performance pour les applications de base de données. Il s'agit de PSLs hautes performances qui prennent en charge les IOPS en rafales et qui sont adaptées aux applications de base de données présentant le débit le plus élevé.

  - Extrême pour les journaux de base de données
  - Extrême pour les données partagées de bases de données
  - Extrême pour les données de base de données
- **Défini par l'utilisateur** : si les niveaux de service de performances prédéfinis ne répondent pas à vos exigences, vous pouvez créer de nouveaux SLS pour répondre à vos besoins. Pour plus d'informations, voir "Création et modification de niveaux de service Performance".
- **Au-delà de Extreme** : au-delà des PSLs extrêmes, les PSLs recommandés par le système sont ceux recommandés pour les charges de travail qui exigent des IOPS supérieures à celles du système Extreme. Les charges de travail sont analysées en interne en fonction de leurs IOPS, de leur capacité et de leur latence. Au-delà de la norme PSL extrême, il est recommandé d'utiliser un modèle au-delà de la norme **stockage > charges de travail > toutes les charges de travail**. Vous pouvez appliquer les PSLs aux charges de travail pour assurer des performances optimales.

  Les paramètres d'IOPS des charges de travail sont générés de façon dynamique, 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 doit avoir les valeurs d'IOPS maximales et prévues `37929` respectivement, la valeur d'IOPS `106345` au-delà de la limite extrême générée pour la charge de travail est nommée `Beyond Extreme 106345 37929`. Bien que ces LSIPs soient recommandés par le système, lorsque vous les attribuez à des charges de travail, ces LSIPs sont étiquetés comme `User-defined` de type.

Gérer les charges de travail en attribuant des SLS

Vous pouvez accéder aux PSLs à partir de la page **Policies** > **Performance Service Levels** et à l'aide des API du fournisseur de stockage. Il est très pratique de gérer les charges de travail de stockage en leur affectant des PSLs, car il n'est pas nécessaire de gérer individuellement les charges de travail de stockage. Toutes les modifications peuvent également être gérées en réaffectant un autre PSL plutôt que de les gérer individuellement. Unified Manager vous aide à attribuer des SLP à vos charges de travail en fonction de

l'évaluation interne et des recommandations.

Pour plus d'informations sur l'attribution de LSIPs recommandés par le système à des charges de travail, reportez-vous à la section "Attribution des SLS recommandées par le système aux charges de travail"

La page niveaux de service de performances répertorie les politiques de 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 qui est actuellement affecté à une charge de travail. Vous ne pouvez pas supprimer un fichier PSL qui est affecté à une charge de travail ou s'il s'agit du seul fichier PSL disponible.

Cette page affiche les informations suivantes :

Champ	Description
Nom	Nom de la PSL.
Type	Indique si la règle est définie par le système ou par l'utilisateur.
IOPS/To attendu	Nombre minimal d'IOPS qu'une application doit exécuter sur une LUN ou un partage de fichiers. Les IOPS attendues indiquent la quantité minimale d'IOPS allouées, en fonction de la taille allouée à l'objet de stockage.
Pic d'IOPS/To	Nombre maximal d'IOPS qu'une application peut exécuter sur une LUN ou un partage de fichiers. Les IOPS en pics indiquent les IOPS maximales allouées, en fonction de la taille de l'objet de stockage ou de la taille de l'objet de stockage utilisé. Les pics d'activité d'IOPS sont basés sur une règle d'allocation. La règle d'allocation est l'espace alloué ou l'espace utilisé. Lorsque la règle d'allocation est définie sur l'espace alloué, les IOPS de pointe sont calculées en fonction de la taille de l'objet de stockage. Lorsque la règle d'allocation est définie sur l'espace utilisé, les IOPS maximales sont calculées en fonction de la quantité de données stockées dans l'objet de stockage, en tenant compte des fonctionnalités d'efficacité du stockage. Par défaut, la règle d'allocation est définie sur l'espace utilisé.

Champ	Description
IOPS minimales absolues	La valeur d'IOPS minimale absolue est utilisée comme valeur prioritaire lorsque la valeur d'IOPS attendue est inférieure à cette valeur. Les valeurs par défaut des SLS définies par le système sont les suivantes : • Performances extrêmes : si le nombre d'IOPS attendu est supérieur à 6144/To, la valeur d'IOPS minimale absolue est égale à 1000 • Performances : si les IOPS prévues sont >= 2048/To et < 6144/To, la valeur d'IOPS minimale absolue est égale à 500 • Valeur : si IOPS attendu >= 128/To et < 2048/To, la valeur d'IOPS minimale absolue est égale à 75 Les valeurs par défaut des PSLs de la base de données définie par le système sont les suivantes : • Extreme pour les journaux de base de données : si attendue d'IOPS >= 22528, alors la valeur d'IOPS minimale absolue est égale à 4000 • Extrême pour les données partagées de bases de données : si le nombre d'IOPS attendu est supérieur à 16384, la valeur d'IOPS minimale absolue est égale à 2000 • Extrême pour les données de base de données : si le nombre d'IOPS attendu est supérieur à 12288, la valeur d'IOPS minimale absolue est égale à 2000 La valeur la plus élevée de la valeur minimale absolue pour les PSLs personnalisés peut être de 75000 au maximum. La valeur la plus faible est calculée comme suit : 1000/latence attendue
Latence attendue	Latence attendue pour les IOPS de stockage en millisecondes par opération (ms/opération).
Capacité	Capacité totale disponible et utilisée dans les clusters.
Charges de travail	Nombre de charges de travail de stockage qui ont reçu la PSL.

Pour plus d'informations sur la manière dont les pics d'IOPS et les valeurs d'IOPS attendues permettent d'obtenir des performances cohérentes et différenciées sur les clusters ONTAP, consultez l'article de la base de connaissances suivant : "Qu'est-ce que la budgétisation des performances ?"

Les événements générés pour les charges de travail enfreindre le seuil défini par les SLS

Si des charges de travail dépassent la valeur de latence prévue pour 30 % de la durée de l'heure précédente, Unified Manager génère l'un des événements suivants pour vous informer d'un problème de performance potentiel :

- Seuil de latence du volume de la charge de travail dépassé, tel que défini par la règle de niveau de service de performances
- Seuil de latence de la LUN de charge de travail dépassé, tel que défini par la règle de niveau de service de performances.

Vous pouvez 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 règle de seuil de performances est enfreinte"
- "Comment Unified Manager utilise une latence de charge de travail pour identifier les problèmes de performance"
- "En quoi sont les événements de performances"

SLS définies par le système

Le tableau suivant fournit des informations sur les SLS définies par le système :

Niveau de service de performances	Description et cas d'utilisation	Latence attendue (ms/opérations)	IOPS en pic	IOPS attendues	IOPS minimales absolues
Performances exceptionnelles	Offre un débit extrêmement élevé à une latence très faible Idéal pour les applications sensibles à la latence	1	12288	6144	1000
Performances	Garantit un débit élevé à une faible latence Idéal pour les bases de données et les applications virtualisées	2	4096	2048	500

Niveau de service de performances	Description et cas d'utilisation	Latence attendue (ms/opérations)	IOPS en pic	IOPS attendues	IOPS minimales absolues
Valeur	Fournit une capacité de stockage élevée et une latence modérée Idéal pour les applications haute capacité telles que la messagerie, le contenu web, les partages de fichiers et les cibles de sauvegarde	17	512	128	75
Extrême pour les journaux de base de données	Assure un débit maximal à la latence la plus faible. Idéal pour les applications de base de données prenant en charge les journaux de base de données Ce PSL fournit le débit le plus élevé car les journaux de base de données sont extrêmement en rafales et la consignation est constamment à la demande.	1	45056	22528	4000

Niveau de service de performances	Description et cas d'utilisation	Latence attendue (ms/opérations)	IOPS en pic	IOPS attendues	IOPS minimales absolues
Extrême pour les données partagées de bases de données	Fournit un débit très élevé avec la latence la plus faible. Idéal pour les données d'applications de bases de données stockées dans un datastore commun, mais partagées entre bases de données.	1	32768	16384	2000
Extrême pour les données de base de données	Fournit un débit élevé à 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

Création et modification de niveaux de service Performance

Lorsque les niveaux de services de performances définis par le système ne correspondent pas aux exigences de vos workloads, vous pouvez créer vos propres niveaux de services de performance optimisés pour vos charges de travail.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications.
- 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 accèdent au stockage.

> Vous ne pouvez pas modifier un niveau de service de performances s'il est actuellement affecté à une charge de travail.

Étapes

1. Dans le volet de navigation de gauche sous **Paramètres**, sélectionnez **stratégies** > **niveaux de service de performance**.
2. Dans la page **niveaux de service de performances**, cliquez sur le bouton approprié selon que vous souhaitez créer un nouveau niveau de service de performances ou modifier un niveau de service de performances existant.

Pour…	Suivez ces étapes…
Créer un nouveau niveau de service de performance	Cliquez sur **Ajouter**.
Modifiez un niveau de service de performances existant	Sélectionnez un niveau de service de performances 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 performances en spécifiant les objectifs de performances, puis cliquez sur **Submit** pour enregistrer le niveau de service de performances.

Vous pouvez appliquer le nouveau niveau de service de performances ou modifié aux charges de travail (LUN, partages de fichiers NFS et partages CIFS) à partir de la page des charges de travail ou lors du provisionnement d'un nouveau workload.

Gestion des règles d'efficacité du stockage

Une stratégie d'efficacité du stockage (SEP) vous permet de définir les caractéristiques d'efficacité du stockage d'une charge de travail. Vous pouvez affecter 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 comprend plusieurs technologies, telles que le provisionnement fin, la déduplication et la compression des données, qui augmentent l'utilisation du stockage et diminuent les coûts du stockage. Lors de la création de PPE, vous pouvez utiliser ces technologies de gain d'espace, individuellement ou conjointement, pour obtenir une efficacité de stockage maximale. Lorsque vous associez les règles à vos charges de travail de stockage, les paramètres de règles spécifiés leur sont affectés. Unified Manager vous permet d'attribuer des PPE définies par le système et par l'utilisateur afin d'optimiser les ressources de stockage de votre centre de données.

Unified Manager fournit deux PPE définies par le système : haute et basse. Ces PPE sont applicables à la plupart des charges de travail de stockage d'un centre de données. Toutefois, vous pouvez créer vos propres politiques si les PPE définies par le système ne répondent pas à vos exigences.

Vous ne pouvez pas modifier un SEP défini par le système ou actuellement affecté à une charge de travail. Vous ne pouvez pas supprimer un SEP affecté à une charge de travail, ou s'il s'agit du seul SEP disponible.

La page règles d'efficacité du stockage répertorie les PPE disponibles et vous permet d'ajouter, de modifier et de supprimer des PPE personnalisées. Cette page affiche les informations suivantes :

Champ	Description
Nom	Nom de la SEP.
Type	Indique si la règle est définie par le système ou par l'utilisateur.
Réserve d'espace	Indique si le volume a un provisionnement fin ou non fin.
Déduplication	Si la déduplication est activée sur la charge de travail : • À la volée : la déduplication a lieu lors de l'écriture sur la charge de travail • Arrière-plan : la déduplication a lieu 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 : • À la volée : la compression des données a lieu lors de l'écriture sur la charge de travail • Arrière-plan : la compression des données a lieu 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 attribuées au SEP

Instructions de création d'une stratégie d'efficacité du stockage personnalisée

Si les PPE existantes ne répondent pas aux exigences de la politique pour vos charges de travail de stockage, vous pouvez créer une SEP personnalisée. Toutefois, il est recommandé d'utiliser les PPE définies par le système pour vos charges de travail de stockage et de créer uniquement des PPE personnalisées si nécessaire.

Vous pouvez afficher le SEP affecté aux charges de travail dans la page toutes les charges de travail et dans la page Détails du volume / intégrité. Vous pouvez afficher le taux de réduction des données au niveau du cluster (sans copies Snapshot) en fonction de ces gains d'efficacité du stockage dans le volet capacité du tableau de bord et dans la vue capacité : tous les clusters.

Création et modification de règles Storage Efficiency

Lorsque les règles d'efficacité du stockage définies par le système ne répondent pas aux exigences de vos workloads, vous pouvez créer vos propres règles d'efficacité du stockage optimisées pour vos charges de travail.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications.
- Le nom de la stratégie 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 politiques personnalisées d'efficacité du stockage à partir de la page règles d'efficacité du stockage en définissant les caractéristiques d'efficacité de stockage requises pour les applications qui accèdent au stockage.

> Vous ne pouvez pas modifier une stratégie d'efficacité du stockage s'il est actuellement affecté à une charge de travail.

Étapes

1. Dans le volet de navigation de gauche sous **Paramètres**, sélectionnez **stratégies** > **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 si vous souhaitez modifier une stratégie d'efficacité du stockage existante.

Pour…	Suivez ces étapes…
Créez une nouvelle politique d'efficacité du stockage	Cliquez sur **Ajouter**
Modifiez une stratégie d'efficacité du stockage existante	Sélectionnez une stratégie d'efficacité du stockage existante et cliquez sur **Modifier**

   La page permettant d'ajouter ou de modifier une stratégie d'efficacité du stockage s'affiche.

3. Personnalisez la stratégie d'efficacité du stockage en spécifiant les caractéristiques d'efficacité du stockage, puis cliquez sur **Submit** pour enregistrer la stratégie d'efficacité du stockage.

Vous pouvez appliquer la nouvelle règle d'efficacité du stockage ou la version modifiée aux charges de travail (LUN, partages de fichiers NFS et partages CIFS) à partir de la page des charges de travail ou lors du provisionnement d'un nouveau workload.

Gestion et contrôle des configurations MetroCluster

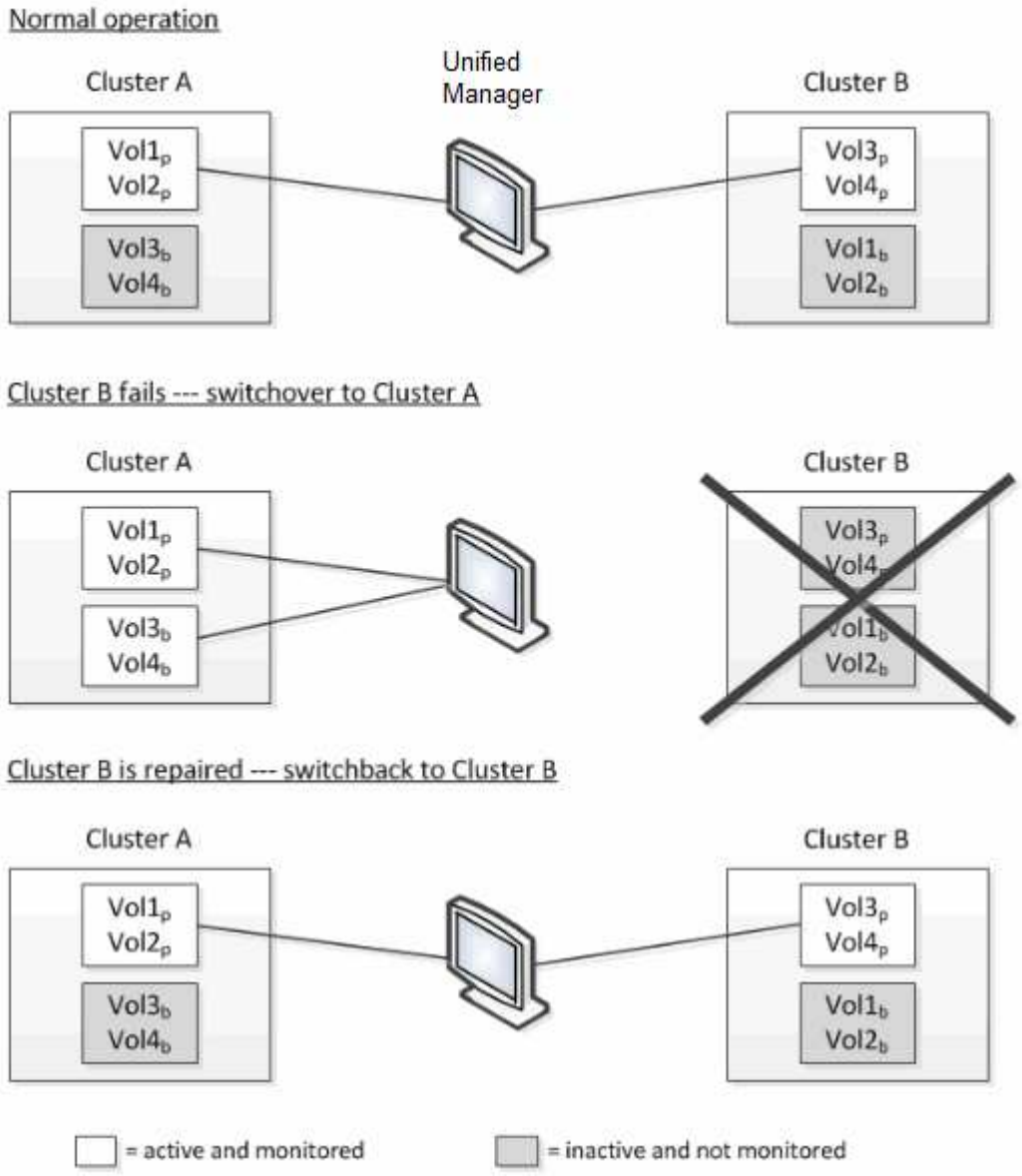
La prise en charge de la surveillance des configurations MetroCluster dans l'interface utilisateur Web Unified Manager vous permet de vérifier la présence de problèmes de

connectivité dans vos configurations MetroCluster over FC et IP. La détection précoce d'un problème de connectivité vous permet de gérer efficacement vos configurations MetroCluster.

Comportement des volumes lors du basculement et du rétablissement

Les événements qui déclenchent un basculement ou un rétablissement entraînent le déplacement des volumes actifs d'un cluster vers l'autre cluster du groupe de reprise sur incident. Les volumes du cluster qui étaient actifs et devaient transmettre des données aux clients sont arrêtés, et les volumes de l'autre cluster sont activés et commencent à transmettre les données. Unified Manager surveille uniquement les volumes actifs et en cours d'exécution.

Comme les volumes sont déplacés d'un cluster à l'autre, il est recommandé de contrôler les deux clusters. Une seule instance de Unified Manager peut contrôler les deux clusters dans une configuration MetroCluster, mais parfois la distance entre les deux sites nécessite l'utilisation de deux instances Unified Manager pour surveiller les deux clusters. La figure suivante présente une seule instance de Unified Manager :



Les volumes portant la référence p indiquent les volumes primaires, et les volumes dont l'noms est b sont des volumes de sauvegarde en miroir créés par SnapMirror.

En fonctionnement normal :

- Le cluster A a deux volumes actifs : Vol1p et Vol2p.
- Le cluster B a deux volumes actifs : Vol3p et Vol4p.
- Cluster A comporte deux volumes inactifs : Vol3b et Vol4b.
- Le cluster B a 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 recueillies par le Cluster B.

Après une défaillance majeure, entraîne le basculement des volumes actifs du Cluster B vers le Cluster A :

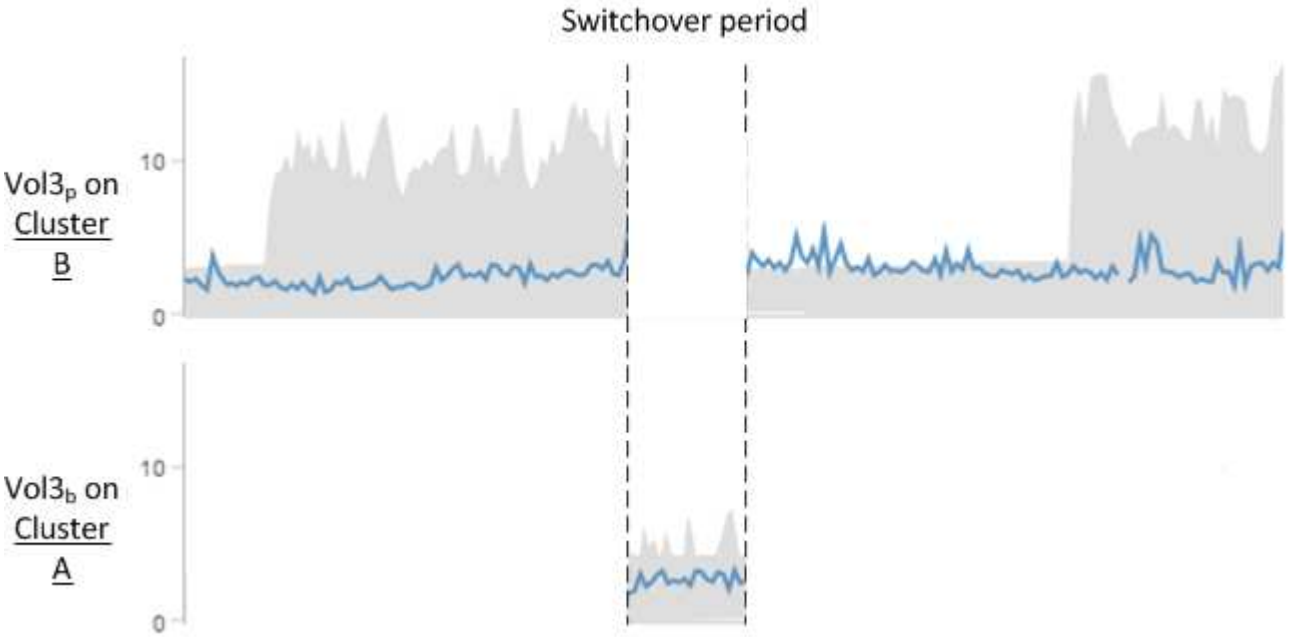
- Cluster A contient quatre volumes actifs : Vol1p, Vol2p, Vol3b et Vol4b.
- Le cluster B a quatre volumes inactifs : Vol3p, Vol4p, Vol1b et Vol2b.

Comme pendant le 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 recueillies par le Cluster A, et les statistiques Vol3b et Vol4b sont également recueillies 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 contenues dans Unified Manager pour Vol3p ne sont pas les mêmes que Vol3b :

- Lors du basculement vers le Cluster A, les statistiques et les événements Vol3p ne sont pas visibles.
- Lors du premier basculement, Vol3b ressemble à un nouveau volume sans informations historiques.

Lorsque le Cluster B est réparé et qu'un rétablissement est effectué, Vol3p est de nouveau actif sur le Cluster B, avec les statistiques historiques et un intervalle de statistiques correspondant à la période de basculement. Vol3b n'est pas visible depuis le Cluster A tant qu'un autre basculement se produit :



- Ainsi, les volumes MetroCluster inactifs, Vol3b sur le Cluster A après rétablissement, sont identifiés par le message « ce volume a été supprimé ». Le volume n'est pas supprimé, mais n'est actuellement pas surveillé par Unified Manager, car il ne s'agit pas du volume actif.
- Lorsqu'un seul Unified Manager contrôle les deux clusters dans une configuration MetroCluster, la recherche de volume renvoie les informations correspondant au volume actif à ce moment-là. Par exemple, une recherche « Vol3 » renvoie des statistiques et des événements pour Vol3b sur le Cluster A si un basculement s'est produit et Vol3 est activé sur le Cluster A.

Définitions d'état de la connectivité des clusters pour la configuration MetroCluster over FC

La connectivité entre les clusters d'une configuration MetroCluster over FC peut être l'un des États suivants : optimal, impacté ou inactif. La présentation des États de connectivité vous permet de gérer efficacement vos configurations MetroCluster.

État de la connectivité	Description	Icône affichée
Optimale	La connectivité entre les clusters dans la configuration MetroCluster est normale.	
Sont concernés	Une ou plusieurs erreurs compromettent l'état de la disponibilité du basculement. Toutefois, les deux clusters de la configuration MetroCluster sont toujours en service. Par exemple, lorsque la liaison ISL est en panne, lorsque la liaison IP intercluster est en panne ou lorsque le cluster partenaire est inaccessible.	
Vers le bas	La connectivité entre les clusters de la configuration MetroCluster est en panne, car l'un des clusters ou les deux sont en panne ou en mode de basculement. Par exemple, lorsque le cluster partenaire est hors service à cause d'un incident ou lorsqu'un basculement est planifié à des fins de test.	Basculement par erreur : Basculement réussi :

Définitions de l'état de la mise en miroir des données pour MetroCluster sur FC

Les configurations MetroCluster sur FC assurent la mise en miroir des données et offrent la possibilité supplémentaire de lancer un basculement en cas d'indisponibilité de la totalité d'un site. L'état de la mise en miroir des données entre les clusters d'une configuration MetroCluster over FC peut être Normal ou mise en miroir indisponible. La compréhension de cet état permet de gérer efficacement les configurations MetroCluster.

État de la mise en miroir des données	Description	Icône affichée
Normale	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 de la configuration MetroCluster est indisponible en raison du basculement. Par exemple, lorsque le cluster partenaire est hors service à cause d'un incident ou lorsqu'un basculement est planifié à des fins de test.	Basculement par erreur : Basculement réussi :

Contrôle des configurations MetroCluster

Vous pouvez surveiller les problèmes de connectivité dans votre configuration MetroCluster. Ces détails incluent l'état des composants, la connectivité dans un cluster et l'état de connectivité entre les clusters dans la configuration MetroCluster. Vous apprendrez à surveiller les problèmes de connectivité dans les clusters protégés par les configurations MetroCluster over FC et MetroCluster over IP.

Vous pouvez contrôler les configurations MetroCluster à partir des vues suivantes à partir du volet de navigation de gauche de Active IQ Unified Manager :

- **Stockage** > **clusters** > **protection : vue MetroCluster**
- **Protection** > **relations** > **relation : MetroCluster** vue

Unified Manager utilise des alertes d'intégrité du système pour indiquer l'état des composants et la connectivité dans la configuration MetroCluster.

Ce dont vous aurez besoin

- Les clusters locaux et distants dans 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, il doit être configuré et ajouté au cluster par l'API correspondante.
- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Surveiller les problèmes de connectivité dans la configuration MetroCluster over FC

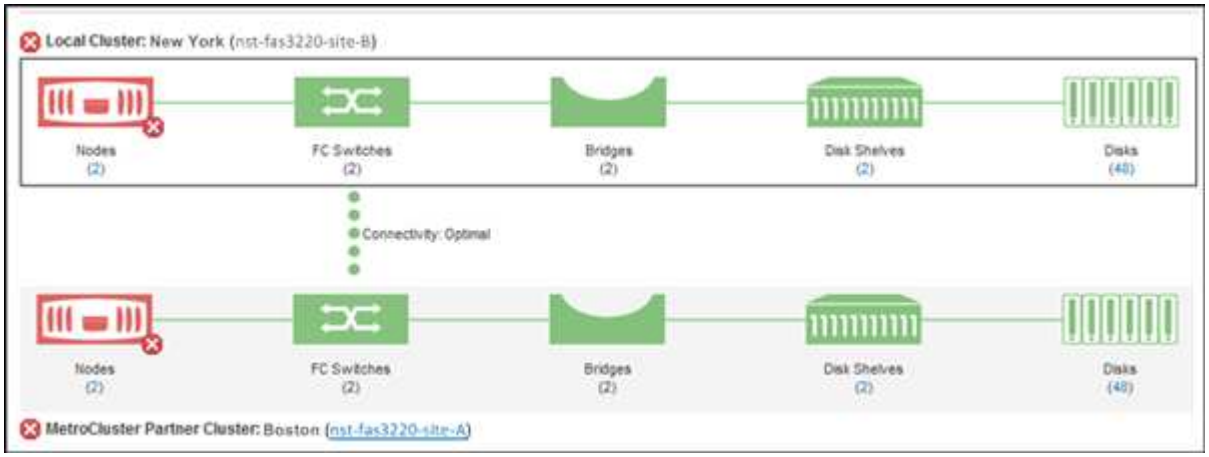
Pour les clusters d'une configuration MetroCluster sur FC, les graphiques de connectivité sont affichés sur la page **Cluster / Santé**. Effectuez la procédure suivante.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.

   La 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 la configuration MetroCluster sur FC. Vous pouvez également filtrer les clusters par configuration MetroCluster.
3. Dans la page **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 s'affiche dans la zone d'objet cluster correspondante. Vous pouvez utiliser les informations affichées sur la page Cluster / Health Details pour corriger tout problème de connectivité. Par exemple, si la connectivité entre le nœud et le commutateur d'un cluster est inactive, l'icône suivante est affichée :

Si vous déplacez le pointeur sur l'icône, vous pouvez afficher des informations détaillées sur l'événement généré.

Si vous détectez les problèmes de connectivité dans votre configuration MetroCluster, vous devez vous connecter à System Manager ou accéder à l'interface de ligne de commandes de ONTAP pour résoudre les problèmes.

Pour plus d'informations sur la détermination de l'intégrité du cluster, reportez-vous à "Détermination de l'état du cluster dans la configuration MetroCluster sur FC"la section .

Surveiller les problèmes de connectivité dans la configuration MetroCluster over IP

Pour les clusters d'une configuration MetroCluster sur IP, les diagrammes de connectivité s'affichent sur la page **clusters**. Effectuez la procédure suivante.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.

   La 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 la configuration MetroCluster sur IP. Vous pouvez également filtrer les clusters par configuration MetroCluster.
3. Développez la ligne en cliquant sur l'icône caret `v`. L'icône caret s'affiche uniquement pour un cluster protégé par la configuration MetroCluster over IP.

   Vous pouvez afficher la topologie des sites source et miroir, ainsi que le médiateur, le cas échéant, utilisé pour la connexion. Vous pouvez afficher les informations suivantes :

   - Connectivité sur l'ensemble des sites
   - Problèmes de santé et de disponibilité, le cas échéant, sur les deux sites
   - Questions relatives à un médiateur
   - Problèmes liés à la réplication.

   > Les États suivants sont signalés : critique ( ), erreur ( ) ou Normal ( ) . Vous pouvez également afficher l'état de réplication des données de l'agrégat des données primaires et en miroir dans une 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 contenant la définition de l'erreur s'affiche. Si un événement a été signalé pour le problème dans votre configuration MetroCluster sur IP, vous pouvez cliquer sur le bouton **Afficher l'événement** du message et afficher les détails de l'événement. Lorsque vous avez résolu le

problème et l'événement, l'icône d'état de cette topologie devient normal ( ).

5. Vous pouvez afficher d'autres détails de configuration dans les sections **Présentation MetroCluster** et **protection** de l'onglet **Configuration** de la page **Cluster / Santé**.

> Uniquement pour une configuration MetroCluster sur IP, vous pouvez afficher la topologie de cluster sur la page **clusters**. Pour les clusters d'une configuration MetroCluster sur FC, la topologie s'affiche dans l'onglet **connectivité MetroCluster** de la page **Cluster / Santé**.

Informations connexes

- "Page Cluster / Health Details"
- Pour plus d'informations sur la vue **Relationship:MetroCluster**, voir "Contrôle des configurations MetroCluster".
- Pour plus d'informations sur la vue **Relationship: Last 1 Month Transfer Status**, voir "Relation : vue État transfert du dernier mois".
- Pour plus d'informations sur la vue **relation : taux de transfert du dernier mois**, voir "Relation : vue du taux de transfert du dernier mois".
- Pour plus d'informations sur la vue **relation : toutes les relations**, voir "Relation : vue de toutes les relations".

Contrôle de la réplication MetroCluster

Vous pouvez contrôler et diagnostiquer l'état de santé général des connexions logiques tout en symétrisant les données. Vous pouvez identifier les problèmes ou tout risque qui interrompt la mise en miroir des composants de 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.

Ce dont vous aurez besoin

Le cluster local et distant en configuration MetroCluster doivent être ajoutés à Unified Manager

Affichage de la réplication pour les configurations MetroCluster sur IP

Dans le cas des configurations MetroCluster sur IP, l'état de la réplication des données s'affiche dans la vue topologique des clusters protégés par MetroCluster sur IP à partir des vues suivantes du volet de navigation de Unified Manager gauche :

- **Stockage** > **clusters** > **protection : vue MetroCluster**
- **Protection** > **relations** > **relation : MetroCluster** vue

Pour plus d'informations, voir "Surveiller les problèmes de connectivité dans MetroCluster sur IP".

Affichage de la réplication pour les configurations MetroCluster sur FC

Suivez ces étapes pour déterminer les éventuels problèmes dans la réplication des données pour la configuration MetroCluster over FC.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.

   La 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 la réplication MetroCluster. Sur la page **Détails de cluster / 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'objets du cluster correspondante, avec les informations relatives au 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 sur la page Cluster / Health Details pour corriger tout problème de réplication. Si vous détectez les problèmes de mise en miroir dans votre configuration MetroCluster, vous devez vous connecter à System Manager ou accéder à l'interface de ligne de commandes de ONTAP pour résoudre les problèmes.

Informations connexes

"Page Cluster / Health Details"

Gestion des 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 des 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 des quotas

Les limites des quotas utilisateur sont des valeurs que le serveur Unified Manager utilise pour évaluer si la consommation de l'espace par un utilisateur approche de la limite ou a atteint la limite définie par le quota de l'utilisateur. Si la limite soft est traversée ou si la limite hard est atteinte, le serveur Unified Manager génère des événements de quotas d'utilisateurs.

Par défaut, le serveur Unified Manager envoie un e-mail de notification aux utilisateurs qui ont franchi la limite soft quota ou qui ont atteint la limite Hard quota et pour lesquels les événements de quota utilisateur sont configurés. Les utilisateurs disposant du rôle Administrateur d'applications peuvent configurer des alertes qui informent les destinataires spécifiés des événements de quota d'utilisateur ou de groupe d'utilisateurs.

Vous pouvez spécifier des limites de quota à l'aide de ONTAP System Manager ou de l'interface de ligne de commande de ONTAP.

Affichage des quotas d'utilisateurs et de groupes d'utilisateurs

La page d'informations Storage VM / Health 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 fichier utilisés et l'adresse e-mail de notification.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Storage VM**.
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"

Création de 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 SVM (Storage Virtual machine), aux volumes, aux qtrees, aux utilisateurs ou aux groupes d'utilisateurs. Une notification est envoyée à l'adresse e-mail spécifiée lorsqu'une violation de quota est constatée.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir passé en revue les directives de la page règles de génération de l'adresse 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 violations 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 pour les règles que vous avez spécifiées n'est satisfait, 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** > **quota Email Rules**.
2. Saisissez la règle en fonction de vos critères.
3. Cliquez sur **Validate** 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 **Validate**.

4. Cliquez sur **Enregistrer**.

5. Vérifiez que l'adresse e-mail que vous avez créée s'affiche dans l'onglet **quotas d'utilisateurs et de groupes** de la page Détails Storage **VM / Health**.

Création d'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 à un quota (limite souple dépassée ou limite stricte atteinte).

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **quota Email format**.
2. Saisissez ou modifiez les détails dans les champs **de**, **sujet** et **Détails de l'adresse électronique**.
3. Cliquez sur **Aperçu** pour afficher un aperçu de 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**.

Modification des adresses e-mail des quotas d'utilisateur et de groupe

Vous pouvez modifier les adresses e-mail en fonction des quotas d'utilisateurs associés aux clusters, aux SVM (Storage Virtual machine), 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 des règles spécifiées dans la boîte de dialogue règles de génération d'adresse e-mail de quota utilisateur et de groupe.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Vous devez avoir examiné le "instructions pour la création de règles".

Si vous modifiez une adresse e-mail, les règles permettant de générer les adresses e-mail des quotas d'utilisateur et de groupe ne sont plus applicables 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 **Storage** > **SVM**.
2. Dans la vue **Santé : toutes les machines virtuelles de stockage**, sélectionnez un SVM, puis cliquez sur l'onglet **quotas d'utilisateur et de groupe**.
3. Cliquez sur **Modifier l'adresse électronique** sous la ligne d'onglets.
4. Dans la boîte de dialogue **Modifier 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 est affichée 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 permettant de générer les adresses e-mail des quotas d'utilisateur et de groupe ne sont plus applicables au quota.

En savoir plus sur les quotas

Comprendre les concepts relatifs aux quotas vous aide à gérer efficacement vos quotas d'utilisateurs et vos quotas de groupes d'utilisateurs.

Présentation du processus de quotas

Les quotas peuvent être conditionnels ou inconditionnels. Lors du dépassement de limites définies, les quotas conditionnels entraînent l'envoi d'une notification par ONTAP, tandis que les quotas inconditionnels empêcheront toute opération d'écriture.

Lorsqu'ONTAP reçoit une demande d'un utilisateur ou d'un groupe d'utilisateurs d'écrire sur un volume FlexVol, il vérifie si les quotas sont activés sur ce volume pour l'utilisateur ou le groupe d'utilisateurs et détermine les éléments suivants :

- Indique si la limite stricte sera atteinte

  Si oui, l'opération d'écriture échoue lorsque la limite stricte est atteinte et que la notification de quota stricte est envoyée.

- Indique si la limite soft sera enfreinte

  Si oui, l'opération d'écriture réussit lorsque la limite soft est dépassée et que la notification soft quota est envoyée.

- Indique si une opération d'écriture ne dépassera pas la limite soft

  Si oui, l'opération d'écriture réussit et aucune notification n'est envoyée.

À propos des quotas

Les quotas permettent de limiter ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree. Vous spécifiez des quotas à l'aide du `/etc/quotas` fichier. Les quotas group sont appliqués à un volume ou qtree spécifique.

Pourquoi utilisez des quotas

Vous pouvez utiliser les quotas pour limiter l'utilisation des ressources dans les volumes FlexVol, fournir des notifications lorsque l'utilisation des ressources atteint des niveaux spécifiques ou 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 qui peuvent être utilisés par un utilisateur ou un groupe, ou qui peut être contenue par un un qtree
- Pour suivre la quantité d'espace disque ou le nombre de fichiers utilisés par un utilisateur, un groupe ou qtree, sans imposer une limite
- Pour avertir les utilisateurs lorsque leur utilisation du disque ou de l'utilisation du fichier est élevé

Description des boîtes de dialogue quotas

Vous pouvez utiliser l'option appropriée dans l'onglet quotas d'utilisateur et de groupe de la vue Santé : tous les ordinateurs virtuels de stockage pour configurer le format de la notification par e-mail envoyée lorsqu'un problème lié au quota se produit et pour configurer des règles pour spécifier des adresses e-mail en fonction du quota d'utilisateur.

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 lorsqu'il existe un problème lié à un quota (limite souple dépassée ou limite stricte atteinte).

La notification par e-mail est envoyée uniquement lorsque les événements de quota d'utilisateur ou de groupe d'utilisateurs suivants sont générés : Quota utilisateur ou Groupe limite matérielle d'espace disque enfreinte, limite logicielle de nombre de fichiers de quota utilisateur ou de groupe dépassée, limite matérielle de quota utilisateur ou de groupe atteinte ou limite matérielle de nombre de fichiers de quota utilisateur ou de groupe atteinte.

- **À partir de**

  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 électronique indiquée sur la page Notifications.

- **Sujet**

  Affiche l'objet de l'e-mail de notification.

- **Détails de courriel**

Affiche le texte de l'e-mail de notification. Vous pouvez modifier le texte en fonction de vos exigences. Par exemple, vous pouvez fournir des informations relatives aux attributs de quota et réduire le nombre de mots-clés. Toutefois, vous ne devez pas modifier les mots clés.

Les mots clés valides sont les suivants :

- $NOM_ÉVÉNEMENT

  Indique le nom de l'événement à l'origine de la notification par e-mail.

- $QUOTA_TARGET

  Spécifie le qtree ou le volume sur lequel le quota est applicable.

- $QUOTA_UTILISÉ_POURCENTAGE

  Indique le pourcentage de limite matérielle du disque, la limite logicielle du disque, la limite matérielle du fichier ou la limite logicielle du fichier utilisée 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 :

  - Quota utilisateur ou groupe limite matérielle d'espace disque atteinte
  - Quota utilisateur ou de groupe - limite logicielle d'espace disque atteinte
  - Limite matérielle de nombre de fichiers de quota utilisateur ou de groupe atteinte
  - Limite logicielle de nombre de fichiers de quota utilisateur ou de groupe atteinte

- $QUOTA_UTILISÉ

  Indique 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 d'afficher un aperçu, 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.

- **Rétablir les paramètres par défaut**

  Permet de restaurer le format de notification aux valeurs par défaut.

- **Enregistrer**

  Enregistre les modifications apportées au format de notification.

Règles de génération de la page adresse e-mail de quota d'utilisateur et de groupe

La page règles de génération 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 des quotas d'utilisateur associés aux clusters, SVM, volumes, qtrees, utilisateurs, ou groupes d'utilisateurs. Une notification est envoyée à l'adresse e-mail spécifiée lorsqu'un quota est dépassé.

Domaine règles

Vous devez définir les règles pour une adresse e-mail de quota. Vous pouvez également ajouter des commentaires pour expliquer les règles.

Comment définir des règles

Vous devez entrer 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 en fonction de cette règle. Si le critère n'est pas satisfait, alors le critère de la règle suivante est pris en compte, et ainsi de suite. Chaque ligne liste 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 violations de quota pour qtre1 et utiliser l'adresse e-mail admin@xyz.com pour tous les autres qtrees, les règles doivent être répertoriées dans l'ordre suivant :

- Si ($QTREE == 'qtre1') puis qtree1@xyz.com
- Si ($QTREE == *), admin@xyz.com

Si aucun des critères pour les règles que vous avez spécifiées n'est satisfait, 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 la forme de valeurs séparées par des virgules et les règles ne sont pas applicables pour le 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 liste 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`

  si est un mot-clé et est en minuscules. L'opérateur est ==. L'ID e-mail peut contenir n'importe quel caractère, les variables valides $USER_OR_GROUP, $USER ou $GROUP, ou une combinaison de tout caractère et des variables valides $USER_OR_GROUP, $USER ou $GROUP. Le nom de domaine peut contenir n'importe quel caractère, la variable valide $DOMAINE ou une combinaison de tout caractère et de la variable valide $DOMAINE. Les variables valides peuvent être en majuscules ou 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`

  si est un mot-clé et est en minuscules. L'opérateur peut contenir ou ==. L'ID e-mail peut contenir n'importe quel caractère, les variables valides $USER_OR_GROUP, $USER ou $GROUP, ou une combinaison de tout caractère et des variables valides $USER_OR_GROUP, $USER ou $GROUP. Le nom de domaine peut contenir n'importe quel caractère, la variable valide $DOMAINE ou une combinaison de tout caractère et de la variable valide $DOMAINE. Les variables valides peuvent être en majuscules ou 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 d'enregistrer, de valider ou d'annuler les règles créées :

- **Valider**

  Valide la syntaxe de la règle créée. En cas d'erreurs lors de la validation, la règle qui génère l'erreur s'affiche avec un message d'erreur.

- **Rétablir les paramètres par défaut**

  Permet de restaurer les règles d'adresse aux valeurs par défaut définies en usine.

- **Enregistrer**

  Valide la syntaxe de la règle et enregistre la règle en l'absence d'erreurs. En cas d'erreurs lors de la validation, la règle qui génère l'erreur s'affiche avec un message d'erreur.

Dépannage

Les informations de dépannage vous permettent d'identifier et de résoudre les problèmes que vous rencontrez lors de l'utilisation de Unified Manager.

Ajout d'espace disque au répertoire de base de données Unified Manager

Le répertoire de base de données Unified Manager contient toutes les données d'intégrité et de performances collectées à partir des systèmes ONTAP. Dans certaines circonstances, vous devrez peut-être augmenter la taille du répertoire de base de données.

Par exemple, le répertoire de la base de données peut devenir complet si Unified Manager collecte les données à partir d'un grand nombre de clusters où chaque cluster possède plusieurs nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de base de données est plein à 90 % et un événement critique lorsque le répertoire est plein à 95 %.

> Aucune donnée supplémentaire n'est collectée depuis les clusters après le répertoire dans son intégralité, à 95 %.

Les étapes requises pour ajouter de la capacité au répertoire de données sont différentes selon que Unified Manager s'exécute ou non sur un serveur VMware ESXi, sur un serveur Red Hat ou CentOS Linux, ou sur un serveur Microsoft Windows.

Ajout d'espace au disque de données de la machine virtuelle VMware

Si vous devez augmenter la quantité d'espace sur le disque de données de 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.

Ce dont vous aurez besoin

- Vous devez avoir accès au client vSphere.
- Aucun snapshot ne doit être stocké localement sur la machine virtuelle.
- 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`. Pour plus de détails, consultez la documentation VMware.

   Dans de rares cas, le déploiement de Unified Manager utilise le "disque dur 2" pour le disque de données au lieu du "disque dur 3". Si cela s'est produit au cours de votre déploiement, vous augmentez l'espace disque le plus important. 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 sur 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 du système**, entrez le numéro de l'option **augmenter la taille du disque de données**.

Ajout d'espace au répertoire de données de l'hôte Linux

Si vous avez alloué un espace disque insuffisant au `/opt/netapp/data` répertoire pour prendre en charge Unified Manager lors de la configuration initiale de l'hôte Linux, puis de l'installation d'Unified Manager, vous pouvez ajouter de l'espace disque après l'installation en augmentant l'espace disque sur le `/opt/netapp/data` répertoire.

Ce dont vous aurez besoin

Vous devez avoir un accès utilisateur root à la machine Red Hat Enterprise Linux ou CentOS 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 répertoire actuel `/opt/netapp/data`.
4. Copiez le contenu et la configuration des privilèges du répertoire existant `/opt/netapp/data` dans 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 dans un dossier existant `/opt/netapp/data` :

   ```
   se_type=`ls -Z /opt/netapp/data| awk '{print $4}'| awk -F: '{print $3}'|
   head -1
   ```

   Le système renvoie une confirmation similaire à ce qui suit :

```
echo $se_type
mysqld_db_t
```

   a. Lancer `chcon` la commande pour définir le type se Linux du répertoire de sauvegarde :

   ```
   chcon -R --type=mysqld_db_t /backup-data
   ```

6. Supprimez le contenu du `/opt/netapp/data` répertoire :
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Augmentez 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 devez pas essayer de monter en `/opt/netapp/data` tant que partage NFS ou CIFS. Parce que, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` peuvent ne pas fonctionner comme prévu.

8. Vérifiez que le `/opt/netapp/data` propriétaire du répertoire (mysql) et le groupe (root) sont inchangés :

```
ls -ltr /opt/netapp/ | grep data
```

   Le système renvoie une confirmation similaire à ce qui suit :

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. Si se Linux est activé, vérifiez que le contexte du `/opt/netapp/data` 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 ce qui suit :

```
-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 de `backup-data` retour vers le répertoire développé `/opt/netapp/data` :

    ```
    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, démarrer 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
    ```

Ajout d'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.

Ce dont vous aurez besoin

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 de l'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 de la rubrique Microsoft : "Extension d'un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes de la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes du sujet VMware : "Augmentation de la taille d'une partition de disque"

Modification de l'intervalle de collecte des statistiques de performances

L'intervalle de collecte par défaut des statistiques de performances est de 5 minutes. Vous pouvez modifier cet intervalle à 10 ou 15 minutes si vous constatez que les collections des grands groupes ne se termine pas dans l'heure par défaut. Ce paramètre a un impact sur la collecte des statistiques de tous les clusters contrôlant cette instance de Unified Manager.

Ce dont vous aurez besoin

Vous devez disposer d'un ID utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

La question des collections de statistiques de performance qui ne se terminent pas à temps est indiquée par les messages de la bannière `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

Vous devez modifier l'intervalle de collecte uniquement 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 défaut de 5 minutes peut affecter le nombre et la fréquence des événements de performances générés par Unified Manager. Par exemple, les seuils de performance définis par le système déclenchent des événements lorsque la règle est dépassée pendant 30 minutes. Lorsque vous utilisez des collections de 5 minutes, la police doit être dépassée pour six collections consécutives. Pour les collections de 15 minutes, la police doit être dépassée pour seulement deux périodes de collecte.

Un message en bas de la page Cluster Setup indique l'intervalle de collecte des données statistiques actuel.

Étapes

1. Connectez-vous en utilisant SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

   Les invites de la console de maintenance Unified Manager s'affichent.

2. Saisissez le numéro de l'option de menu **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 utilisateur pour la maintenance.
4. Saisissez le numéro du nouvel intervalle d'interrogation que vous souhaitez définir, puis appuyez sur entrée.

Si vous avez modifié l'intervalle de collecte de Unified Manager à 10 ou 15 minutes et que vous disposez d'une connexion actuelle à un fournisseur de données externe (Graphite, par exemple), vous devez modifier l'intervalle de transmission du fournisseur de données de façon à ce qu'il soit supérieur ou égal à l'intervalle de collecte Unified Manager.

Modification de la durée pendant laquelle Unified Manager conserve les données relatives aux événements et aux performances

Par défaut, Unified Manager stocke les données d'événements et de performances pendant 6 mois pour l'ensemble des clusters surveillés. Après cette période, les données plus anciennes sont automatiquement supprimées pour faire place aux nouvelles données. Cette durée de conservation par défaut fonctionne parfaitement dans la plupart des configurations, mais de très grandes configurations comprenant plusieurs clusters et nœuds peuvent être nécessaires pour réduire la période de conservation afin que Unified Manager fonctionne de façon optimale.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Vous pouvez modifier les périodes de conservation de ces deux types de données dans la page conservation des données. Ces paramètres ont un impact sur la conservation des données depuis tous les clusters qui surveillent cette instance de Unified Manager.

> Unified Manager collecte les statistiques de performances toutes les 5 minutes. Chaque jour, les statistiques de 5 minutes sont résumées en statistiques de performance horaire. Il conserve 30 jours de données historiques de performances de 5 minutes et 6 mois de données résumées de la performance horaire (par défaut).

La durée de conservation doit être réduite uniquement si votre espace est insuffisant ou si la sauvegarde et d'autres opérations prennent beaucoup de temps. La réduction de la période de rétention 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 dans l'interface utilisateur.
- Les emplacements dans l'interface utilisateur où les statistiques de performance horaire sont affichées sont vides avant la période de conservation.
- Si la période de conservation des événements dépasse la période de rétention des données de performances, un message s'affiche sous le curseur de performances, vous avertissant que les événements de performance plus anciens peuvent ne pas contenir de données de sauvegarde dans leurs graphiques associés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Policies** > **Data Retention**.
2. Dans la page **Data Retention**, sélectionnez l'outil curseur dans la zone conservation des événements ou conservation des données de performances et déplacez-le au nombre de mois pendant lesquels les données doivent être conservées, puis cliquez sur **Enregistrer**.

Erreur d'authentification inconnue

Lorsque vous effectuez une opération d'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 survenir si vous avez défini une valeur incorrecte pour les options suivantes :

- Nom d'administrateur du service d'authentification Active Directory
- BIND Nom unique du service d'authentification OpenLDAP
- Action 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 Nom d'administrateur ou Nom unique.
  3. Cliquez sur **Tester l'authentification** pour tester l'authentification avec les détails que vous avez spécifiés.
  4. Cliquez sur **Enregistrer**.

Utilisateur introuvable

Lorsque vous effectuez une opération d'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 survenir si l'utilisateur existe dans le serveur AD ou le serveur LDAP et si vous avez défini le nom distinctif de base sur une valeur incorrecte.

- Action corrective*
  1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
  2. Entrez les informations appropriées pour le nom distinctif de base.
  3. Cliquez sur **Enregistrer**.

Problème d'ajout de LDAP à l'aide d'autres services d'authentification

Lorsque vous sélectionnez autres comme service d'authentification, l'utilisateur et la classe d'objet de groupe conservent les valeurs du modèle précédemment sélectionné. Si le serveur LDAP n'utilise pas les mêmes valeurs, l'opération risque d'échouer.

Cause

Les utilisateurs ne sont pas configurés correctement dans OpenLDAP.

- Action corrective*

Vous pouvez résoudre manuellement ce problème en utilisant l'une des solutions suivantes.

Si votre classe d'objet utilisateur LDAP et votre classe d'objet de groupe sont respectivement utilisateurs et groupes, effectuez les opérations suivantes :

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. Complétez les champs de texte.

Si votre classe d'objet utilisateur LDAP et votre classe d'objet de groupe sont posixAccount et posixGroup, respectivement, procédez comme suit :

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Dans le menu déroulant **Authentication Service**, sélectionnez **OpenLDAP**, puis **autres**.
3. Complétez les champs de texte.

Si les deux premières solutions de contournement ne s'appliquent pas, appelez l' `option-set`API et définissez les options et `auth.ldap.groupObjectClass` sur les `auth.ldap.userObjectClass` valeurs correctes.

Gestion des événements et des alertes

Gestion des événements

Les événements vous aident à identifier les problèmes qui se produisent dans les clusters surveillés.

Sont les événements sur la plateforme Active IQ

Unified Manager peut afficher les événements détectés 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 contrôlés par Unified Manager.

Pour plus d'informations, voir "Génération des événements de la plateforme Active IQ".

Unified Manager recherche automatiquement un nouveau fichier de règles et ne télécharge un nouveau fichier que lorsqu'il existe de nouvelles règles. Dans les sites sans accès réseau externe, vous devez télécharger manuellement les règles à partir de **Storage Management** > **Event Setup** > **Upload Rules**.

Ces événements Active IQ ne se chevauchent pas dans les événements Unified Manager existants et ils identifient les incidents ou les risques liés à la configuration du système, au câblage, aux meilleures pratiques et à la disponibilité.

Pour plus d'informations sur l'activation des événements de plate-forme, reportez-vous à la section "Activation des événements du portail Active IQ". Pour plus d'informations sur le téléchargement du fichier de règles, reportez-vous à la section "Téléchargement d'un nouveau fichier de règles Active IQ".

NetApp Active IQ est un service cloud qui offre des analyses prédictives et un support proactif pour optimiser les opérations des systèmes de stockage dans le cloud hybride NetApp. Voir "NetApp Active IQ" pour plus d'informations.

Quels sont les événements Event Management System

Le système de gestion des événements (EMS) collecte les données d'événements de différentes parties du noyau ONTAP et fournit des mécanismes de transfert d'événements. Ces événements ONTAP peuvent être signalés comme des événements EMS dans Unified Manager. La surveillance et la gestion centralisées facilitent la configuration des événements EMS stratégiques et des notifications d'alerte basées sur ces événements EMS.

L'adresse Unified Manager est ajoutée en tant que 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 automatiquement signalés.
- Vous pouvez vous abonner pour recevoir des événements EMS individuels.

Les événements EMS générés par Unified Manager sont signalés différemment selon la méthode dans

laquelle l'événement a été généré :

Fonctionnalité	Messages EMS automatiques	Messages EMS auxquels vous êtes abonné
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 point de l'événement EMS réel
Messages reçus	Dès que le cluster a été découvert	Après l'ajout de chaque événement EMS requis à Unified Manager et au terme du cycle d'interrogation de 15 minutes suivant
Cycle de vie de l'événement	Identique à d'autres événements Unified Manager : États nouveaux, acquittés, résolus et Obsolète	L'événement EMS est mis hors service après la mise à jour du cluster, au bout de 15 minutes, à partir de la création de l'événement
Capture des événements pendant le temps d'indisponibilité de Unified Manager	Oui, lorsque le système démarre, il communique avec chaque cluster pour acquérir des événements manquants	Non
Détails de l'événement	Suggestions d'actions correctives sont importées directement depuis ONTAP pour fournir des résolutions cohérentes	Actions correctives non disponibles sur la page Détails de l'événement

Certains des nouveaux événements EMS automatiques sont des événements informationnels qui indiquent qu'un incident précédent a été résolu. Par exemple, l'événement d'information « État de l'espace des composants FlexGroup OK » indique que l'événement d'erreur « les composants 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 d'autres types de gravité d'événement. Cependant, l'événement est automatiquement obsolète si le même volume reçoit un autre événement d'erreur "`problèmes de vitesse'".

Événements EMS ajoutés automatiquement à Unified Manager

Les événements ONTAP EMS suivants sont ajoutés automatiquement à Unified Manager. Ces événements sont générés lorsqu'ils sont déclenchés sur un cluster que Unified Manager surveille.

Les événements EMS suivants sont disponibles lors de la surveillance des clusters exécutant ONTAP 9.5 ou une version supérieure du logiciel :

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
Accès au niveau cloud refusé pour le transfert d'agrégats	arl.netra.ca.check.failed	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation des agrégats pendant le basculement du stockage	gb.netra.ca.check.failed	Agrégat	Erreur
Resynchronisation de la réplication des miroirs FabricPool terminée	wafl.ca.resync.complete	Cluster	Erreur
Espace FabricPool presque plein	fabritpool.presque.plein	Cluster	Erreur
Le délai NVMe-of Grace a commencé	nvmf.graceperiod.start	Cluster	Avertissement
Délai de grâce NVMe-of actif	nvmf.graceperiod.active	Cluster	Avertissement
Délai de grâce NVMe-of expiré	nvmf.graceperiod.expired	Cluster	Avertissement
LUN supprimée	lun.destroy	LUN	Informations
MetaDataConnFail dans le cloud AWS	Cloud.aws.metadataConnFail	Nœud	Erreur
Cloud AWS IAMCredentistesExrequis	Cloud.aws.iamCredentistesExpired	Nœud	Erreur
Identifiants iAMCredentistspour Cloud AWS non valides	Cloud.aws.iamCredsinvalide	Nœud	Erreur
Des informations iAMCredentistsNotFound pour Cloud AWS	Cloud.aws.iamCredentisNotFound	Nœud	Erreur
Cloud AWS IAMCredentistsNotInitialized	Cloud.aws.iamNotInitialized	Nœud	Informations

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
IAMRleInvalid Cloud AWS	Cloud.aws.iamRoleinvalid e	Nœud	Erreur
L'IAMRleNotFound Cloud AWS	Cloud.aws.iamRoleNotFo und	Nœud	Erreur
L'hôte Cloud Tier ne peut pas être résolu	objstore.host.non résolu	Nœud	Erreur
Interface réseau intercluster de Cloud Tier down	objstore.interclusterlifDow n	Nœud	Erreur
Demander une signature de niveau de cloud différente	osc.signatureMismatch	Nœud	Erreur
Un des pools NFSv4 épuisés	Nblade.nfsV4PoolExhaust	Nœud	Primordial
QoS Monitor mémoire portée en mémoire	qos.monitor.memory.capa cité maximale	Nœud	Erreur
Mémoire du moniteur QoS saturée	qos.monitor.memory.abat ed	Nœud	Informations
Détruire NVMeNS	NVMeNS.destroy	Espace de noms	Informations
NVMeNS en ligne	NVMeNS.offline	Espace de noms	Informations
NVMeNS hors ligne	NVMeNS.online	Espace de noms	Informations
NVMeNS hors de l'espace	NVMeNS.out.of.space	Espace de noms	Avertissement
Réplication synchrone hors synchronisation	sms.status.out.of.sync	Relation SnapMirror	Avertissement
Réplication synchrone restaurée	sms.status.in.sync	Relation SnapMirror	Informations
Échec de la resynchronisation automatique de la réplication synchrone	sms.resynchronisation.ten tative.échec	Relation SnapMirror	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
De nombreuses connexions CIFS	Nibd.cifsManyAuths	SVM	Erreur
Connexion CIFS maximale dépassée	NBlade.cifsMaxOpenSametiFile	SVM	Erreur
Le nombre maximal de connexions CIFS par utilisateur a été dépassé	NBlade.cifsMaxSessPerUsrConn	SVM	Erreur
Conflit de nom NetBIOS CIFS	NBlade.cifsNbNameConflitt	SVM	Erreur
Tentatives de connexion sans partage CIFS	NBlade.cifsNoPrivShare	SVM	Primordial
Échec de l'opération CIFS Shadow Copy	cifs.shadowcopy.failure	SVM	Erreur
Virus détecté par le serveur AV	NBlade.vscanVirusDetected	SVM	Erreur
Aucune connexion au serveur AV pour virus Scan	NBlade.vscanNoScannerConn	SVM	Primordial
Aucun serveur AV enregistré	NBlade.vscanNoRegdScanner	SVM	Erreur
Pas de connexion au serveur AV réactive	NBlade.vscanConnInactif	SVM	Informations
Serveur AV trop occupé pour accepter une nouvelle demande de numérisation	NBlade.vscanConnBackPressure	SVM	Erreur
Un utilisateur non autorisé tente d'utiliser le serveur AV	NBlade.vscanBadUserPrivAccess	SVM	Erreur
Les composants FlexGroup présentent des problèmes d'espace	flexgroup.constituants.have.space.issues	Volumétrie	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
État de l'espace des composants FlexGroup OK	flexgroup.commettants.space.status.all.ok	Volumétrie	Informations
Les composants FlexGroup présentent des problèmes d'inodes	flexgroup.constituents.have.inodes.issues	Volumétrie	Erreur
État des inodes des composants FlexGroup OK	flexgroup.constituents.inodes.status.all.ok	Volumétrie	Informations
Espace logique du volume presque plein	monitor.vol.nearFull.inc.sav	Volumétrie	Avertissement
Espace logique du volume plein	monitor.vol.full.inc.sav	Volumétrie	Erreur
Volume Logical Space Normal	monitor.vol.one.ok.inc.sav	Volumétrie	Informations
Échec de la taille automatique du volume WAFL	wafl.vol.autoSize.fail	Volumétrie	Erreur
Taille automatique du volume WAFL terminée	wafl.vol.autoSize.done	Volumétrie	Informations
WAFL - délai d'attente de l'opération de FICHIER DE REMADDIR	wafl.readdir.expiré	Volumétrie	Erreur

Abonnement aux événements ONTAP EMS

Vous pouvez vous abonner aux événements EMS (Event Management System) générés par les systèmes installés avec le logiciel ONTAP. Un sous-ensemble d'événements EMS est automatiquement signalé à Unified Manager, mais des événements EMS supplémentaires ne sont signalés que si vous êtes abonné à ces événements.

Ce dont vous aurez besoin

Ne vous abonnez pas aux événements EMS déjà ajoutés automatiquement à Unified Manager, car ils peuvent être source de confusion lors de la réception de deux événements pour le même problème.

Vous pouvez vous abonner à un certain nombre d'événements EMS. Tous les événements auxquels vous êtes abonné 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* dans la page Documentation produit de ONTAP 9 pour obtenir la liste des événements applicables.

"Bibliothèque de produits ONTAP 9"

Vous pouvez configurer les alertes relatives aux événements EMS ONTAP auxquels vous êtes abonné et créer des scripts personnalisés à exécuter pour ces événements.

> Si vous ne recevez pas les événements EMS ONTAP auxquels vous êtes abonné, il peut y avoir un problème de 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. Cette opération permet de vider les événements EMS en attente du serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Event Setup**.
2. Dans la page Configuration des événements, 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 EMS ONTAP auquel vous souhaitez vous abonner.

   Pour afficher les noms des événements EMS auxquels vous pouvez vous abonner, vous pouvez utiliser la commande (avant ONTAP 9) ou la commande (ONTAP 9 ou version ultérieure) dans le shell de `event catalog show` cluster ONTAP `event route show`.

   "Comment configurer et recevoir des alertes de l'abonnement aux événements EMS ONTAP dans Active IQ Unified Manager"

4. Cliquez sur **Ajouter**.

   L'événement EMS est ajouté à la liste des événements EMS auxquels vous êtes abonné, mais la colonne applicable au cluster affiche l'état « Inconnu » pour l'événement EMS que vous avez ajouté.

5. Cliquez sur **Enregistrer et fermer** pour enregistrer l'abonnement aux événements EMS avec le cluster.
6. Cliquez de nouveau sur **Abonnez-vous aux événements EMS**.

   L'état « 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 EMS ONTAP. Si le nom n'est pas saisi correctement, vous devez supprimer l'événement incorrect, puis ajouter à nouveau l'événement.

Lorsque l'événement EMS ONTAP se produit, l'événement s'affiche sur la page événements. Vous pouvez sélectionner l'événement pour afficher les détails de l'événement EMS sur la page Détails de l'événement. Vous pouvez également gérer la disposition de l'événement ou créer des alertes pour cet événement.

Que se passe-t-il lorsqu'un événement est reçu

Lorsqu'Unified Manager reçoit un événement, celui-ci s'affiche sur la page Tableau de bord, dans la page d'inventaire de la gestion des événements, dans les onglets Summary et Explorer de la page Cluster/Performance, ainsi que dans la page d'inventaire

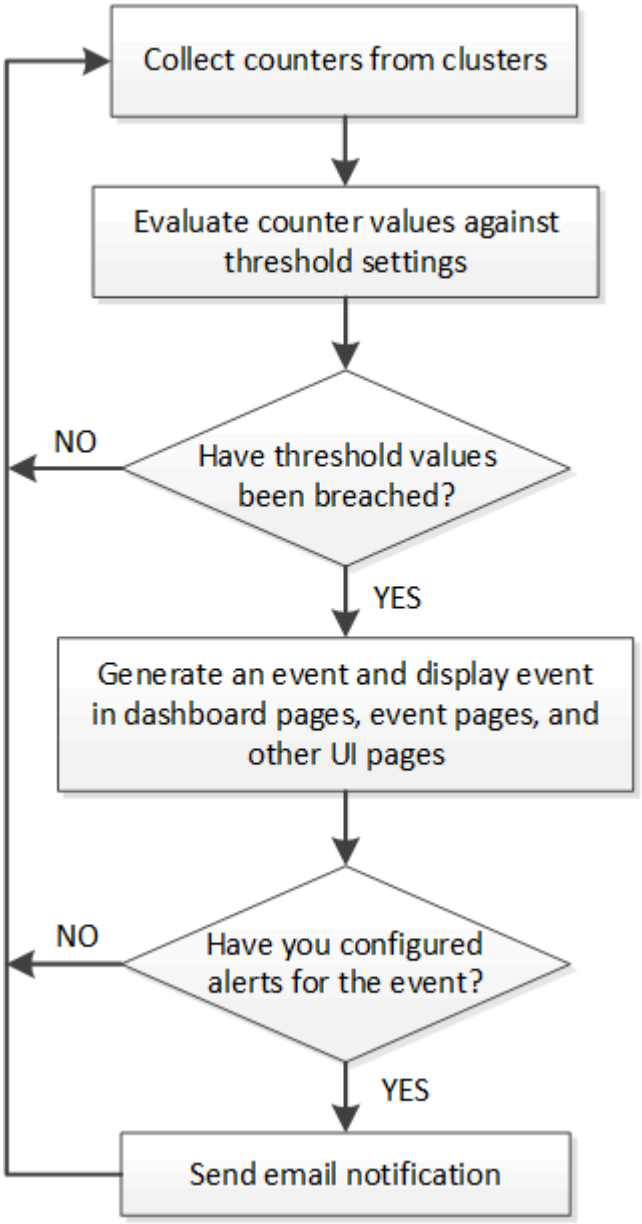
spécifique à chaque objet (par exemple, la page d'inventaire volumes/Health).

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.

En fonction de la configuration des paramètres dans la page Configuration des alertes, vous pouvez avertir d'autres utilisateurs de ces événements. L'alerte entraîne le lancement des actions suivantes :

- Un e-mail sur l'événement peut être envoyé à tous les utilisateurs d'Unified Manager Administrator.
- L'événement peut être envoyé à d'autres destinataires de courrier électronique.
- Une interruption SNMP peut être envoyée au récepteur d'interruption.
- Un script personnalisé peut être exécuté pour exécuter une action.

Ce flux de travail est présenté dans le schéma suivant.



Affichage des événements et des détails des événements

Vous pouvez afficher les détails d'un événement déclenché par Unified Manager pour effectuer une action corrective. Par exemple, si un événement de santé est hors ligne, vous pouvez cliquer sur cet événement pour afficher les détails et effectuer les actions correctives nécessaires.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Les détails de l'événement incluent des informations telles que la source de l'événement, la cause de l'événement et toute note liée à l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.

   Par défaut, la vue tous les événements actifs affiche les événements nouveaux et acquittés (actifs) qui ont été générés au cours des 7 derniers jours ayant un niveau d'impact d'incident ou de risque.

2. Si vous souhaitez afficher une catégorie particulière d'événements, par exemple, les événements de capacité ou les événements de performances, cliquez sur **Afficher** et sélectionnez 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 s'affichent sur la page Détails de l'événement.

Affichage des événements non assignés

Vous pouvez afficher les événements non attribués, puis les affecter à un utilisateur qui peut les résoudre.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.

   Par défaut, les événements nouveaux et acquittés sont affichés sur la page d'inventaire gestion des événements.

2. Dans le volet **filtres**, sélectionnez l'option de filtre **non affecté** dans la zone **affecté à**.

Confirmation et résolution des événements

Vous devez accuser réception d'un événement avant de commencer à travailler sur le problème qui a généré l'événement afin de ne pas continuer à recevoir de notifications d'alerte répétées. Après avoir effectué une action corrective pour un événement particulier, vous devez marquer l'événement comme résolu.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez accepter et résoudre plusieurs événements simultanément.

> Vous ne pouvez pas accuser réception d'événements d'information.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.
2. Dans la liste des événements, effectuez les opérations suivantes pour accuser réception des événements :

Les fonctions que vous recherchez…	Procédez comme ça…
Accuser réception et marquer un seul événement comme résolu	a. Cliquez sur le nom de l'événement. b. Dans la page Détails de l'événement, déterminez la cause de l'événement. c. Cliquez sur **Acknowledge**. d. Prendre les mesures correctives appropriées. e. Cliquez sur **Marquer comme résolu**.
Accuser réception et marquer plusieurs événements comme résolus	a. Déterminez la cause des événements à partir de la page Détails de l'événement correspondant. b. Sélectionnez les événements. c. Cliquez sur **Acknowledge**. d. Prenez les mesures correctives appropriées. e. Cliquez sur **Marquer comme résolu**.

   Une fois que l'événement est 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 façon dont vous avez traité l'événement, puis cliquez sur **Post**.

Attribution d'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 réattribuer des événements à un autre utilisateur, si nécessaire. Par exemple, en cas de problèmes fréquents sur un objet de stockage, vous pouvez attribuer les événements associés à ces problèmes à l'utilisateur qui gère cet objet.

Ce dont vous aurez besoin

- Le nom et l'ID e-mail de l'utilisateur doivent être configurés correctement.
- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.
2. Dans la page d'inventaire **Event Management**, sélectionnez un ou plusieurs événements à attribuer.
3. Attribuez l'événement en choisissant l'une des options suivantes :

Si vous souhaitez affecter l'événement à…	Alors, procédez comme ça…
Vous-même	Cliquez sur **attribuer à** > **Me**.
Un autre utilisateur	a. Cliquez sur **affecter 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 sélectionnez un utilisateur dans la liste déroulante et cliquez sur **affecter**, l'événement reste non affecté.

Désactivation des événements indésirables

Tous les événements sont activés par défaut. Vous pouvez désactiver globalement les événements pour empêcher la génération de notifications pour les événements qui ne sont pas importants dans votre environnement. Vous pouvez activer les événements désactivés lorsque vous souhaitez reprendre la réception de notifications pour eux.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Lorsque vous désactivez des événements, les événements générés précédemment dans le système sont signalés comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications de ces événements sont générées à partir du cycle de surveillance suivant.

Lorsque vous désactivez un événement pour un objet (par exemple, l' `vol offline`événement), puis que vous l'activez ultérieurement, Unified Manager ne génère pas de nouveaux événements pour les objets qui se sont mis hors ligne lorsque l'événement était à l'état Désactivé. Unified Manager génère un nouvel événement uniquement lorsqu'il y a une modification de l'état de l'objet après la réactivation de l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Event Setup**.

2. Dans la page **Event Setup**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
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 Matching Events, sélectionnez les événements que vous souhaitez désactiver en fonction de la gravité de l'événement, puis cliquez sur la flèche de droite pour déplacer ces événements vers la colonne Disable Events. d. Cliquez sur **Enregistrer et fermer**. e. Vérifiez que les événements que vous avez désactivés s'affichent dans la vue 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**.

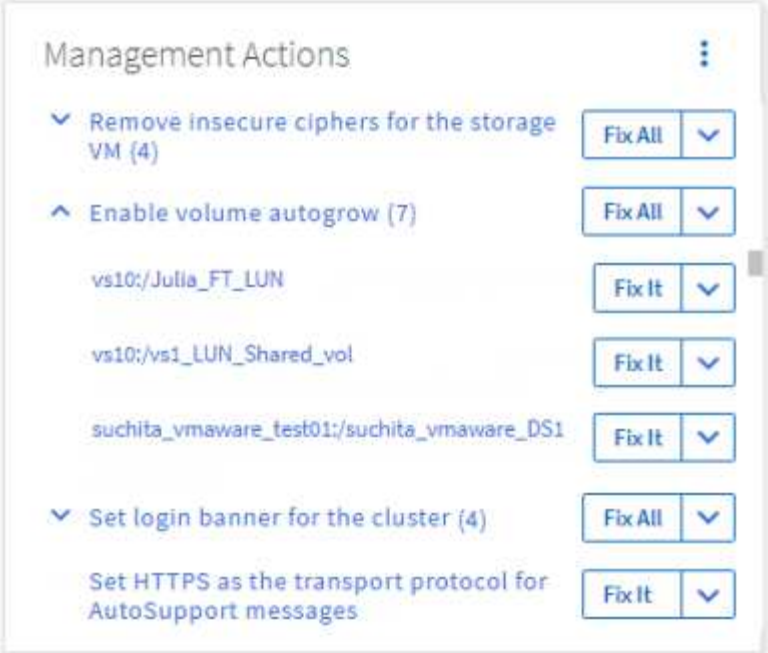
Résolution des problèmes à l'aide de la correction automatique de Unified Manager

Unified Manager peut diagnostiquer en profondeur certains événements et fournir une résolution unique à l'aide du bouton **Fix it**. Lorsqu'elles sont disponibles, ces résolutions sont affichées dans le tableau de bord, à partir de la page Détails de l'événement et dans la sélection analyse de la charge de travail du menu de navigation gauche.

La plupart des événements ont différentes résolutions possibles qui s'affichent sur la page des détails d'événement. Vous pouvez ainsi implémenter la solution la plus adaptée à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP. 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 **Dashboard**, cliquez sur **Dashboard**.



2. Pour résoudre les problèmes que Unified Manager peut résoudre, cliquez sur le bouton **Fix it**. Pour résoudre un problème qui existe sur plusieurs objets, cliquez sur le bouton **réparer tout**.

Pour plus d'informations sur les problèmes pouvant être résolus par la correction automatique, reportez-vous à "Problèmes pouvant être résolus par Unified Manager"la section .

Activation et désactivation du reporting des événements Active IQ

Les événements liés à la plateforme Active IQ sont générés et affichés par défaut dans l'interface utilisateur Unified Manager. Si vous constatez que ces événements sont trop « bruyants » ou que vous ne souhaitez pas afficher ces événements dans Unified Manager, vous pouvez les désactiver. Vous pouvez les activer ultérieurement si vous souhaitez reprendre la réception de ces notifications.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Lorsque vous désactivez cette fonctionnalité, Unified Manager cesse de recevoir immédiatement les événements liés à la plateforme Active IQ.

Lorsque vous activez cette fonctionnalité, Unified Manager commence à recevoir des événements sur la plateforme Active IQ peu après minuit, sur le fuseau horaire du cluster. L'heure de début est basée sur l'heure à laquelle Unified Manager reçoit des messages AutoSupport de chaque cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Paramètres de fonction**.
2. Dans la page **Paramètres de la fonction**, désactivez ou activez les événements de plate-forme Active IQ en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Désactiver les événements de la plate-forme Active IQ	Dans le panneau **Active IQ Portal Events**, déplacez le curseur vers la gauche.
Activez les événements sur la plateforme Active IQ	Dans le panneau **Active IQ Portal Events**, déplacez le curseur vers la droite.

Téléchargement d'un nouveau fichier de règles Active IQ

Unified Manager recherche automatiquement un nouveau fichier Active IQ Events (règles) et télécharge un nouveau fichier dès qu'il existe de nouvelles règles. 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 d'un site sans connectivité réseau, les règles Active IQ fournies sont automatiquement disponibles en téléchargement. Toutefois, il est recommandé de télécharger un nouveau fichier de règles environ une fois par mois sur le site de support NetApp afin de garantir la génération d'événements mis à jour et le fonctionnement optimal de vos systèmes de stockage.

Ce dont vous aurez besoin

- Le reporting sur les événements affectant le portail Active IQ doit être activé. 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 depuis le site de support NetApp.

  Le fichier de règles se trouve à l'adresse suivante : 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 le fichier de règles actuel `.zip`.

   Le pack de règles inclut le référentiel de règles, les sources de données et un article de la base de connaissances NetApp.

   > Sur les systèmes Windows, dans 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* à partir du site d'assistance et le télécharger pour voir 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 de la zone sécurisée.
3. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Event Setup**.
4. Dans la page **Event Setup**, cliquez sur le bouton **Upload Rules**.

5. Dans la boîte de dialogue **règles de téléchargement**, accédez au fichier de règles que vous avez téléchargé et sélectionnez-le `.zip`, puis cliquez sur **Télécharger**.

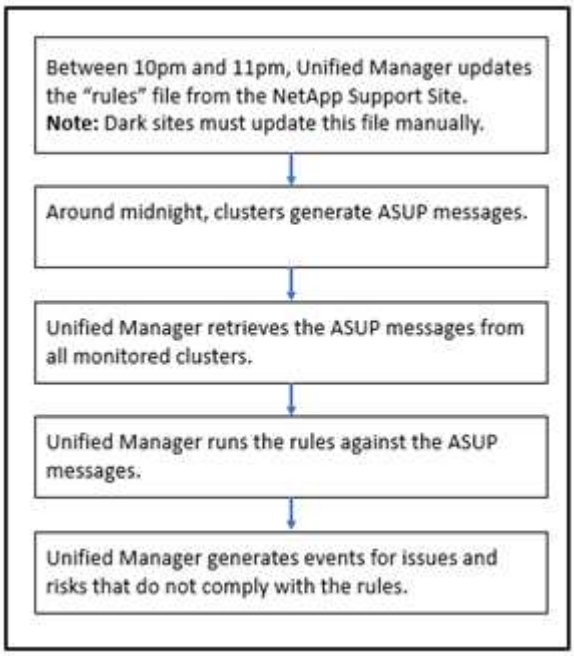
   Ce processus peut prendre quelques minutes.

Le fichier de règles est décompressé sur le serveur Unified Manager. Une fois que vos clusters gérés ont généré un fichier AutoSupport après minuit, Unified Manager vérifie les clusters par rapport au fichier de règles et génère de nouveaux risques et incidents, le cas échéant.

Pour plus d'informations, consultez l'article suivant de la base de connaissances : "Comment mettre à jour les règles AIQCASecure manuellement dans Active IQ Unified Manager".

Génération des événements de la plateforme Active IQ

Les incidents et les risques liés à la plateforme Active IQ sont convertis en événements Unified Manager, comme illustré dans le diagramme ci-dessous.

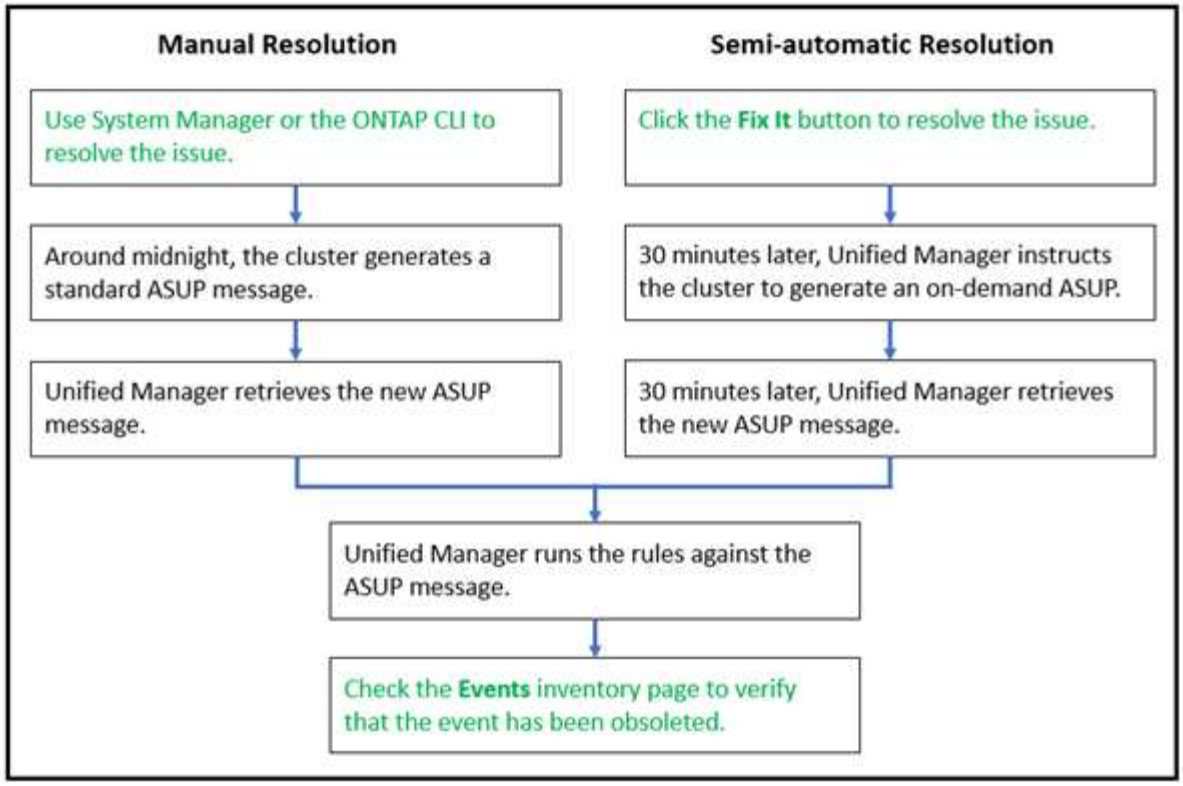


Comme vous pouvez le voir, le fichier de règles compilé sur la plateforme Active IQ est actualisé et les messages AutoSupport de cluster sont générés quotidiennement. Unified Manager met à jour la liste d'événements.

Résoudre les événements relatifs à la plateforme Active IQ

Les risques et incidents liés à la plateforme Active IQ sont similaires aux autres événements affectant Unified Manager. En effet, ils peuvent être affectés à des fins de résolution et ont le même état disponible. Toutefois, lorsque vous résolvez ces types d'événements à l'aide du bouton **Fix it**, vous pouvez vérifier la résolution en quelques heures.

Le diagramme suivant présente les actions à effectuer (en vert) et les actions à effectuer par Unified Manager (en noir) lors de la résolution des événements générés à partir de la plateforme Active IQ.



Pour effectuer une résolution manuelle, vous devez vous connecter à System Manager ou à l'interface de ligne de commandes ONTAP pour corriger le problème. Vous pourrez vérifier le problème uniquement après la génération d'un nouveau message AutoSupport à minuit.

Lors de l'exécution d'une résolution semi-automatique à l'aide du bouton **Fix it**, vous pouvez vérifier que le correctif a réussi en quelques heures.

Configuration des paramètres de conservation des événements

Vous pouvez indiquer le nombre de mois pendant lequel un événement est conservé dans le serveur Unified Manager avant d'être supprimé automatiquement.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

La conservation d'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** > **Data Retention**.
2. Dans la page **Data Retention**, sélectionnez le curseur dans la zone Event Retention (conservation des événements) et déplacez-le au nombre de mois pendant lesquels les événements doivent être conservés, puis cliquez sur **Save** (Enregistrer).

Qu'est-ce qu'une fenêtre de maintenance Unified Manager

Vous définissez une fenêtre de maintenance Unified Manager afin de supprimer les événements et les alertes d'une période spécifique lorsque vous avez planifié la

maintenance du cluster et que vous ne souhaitez pas recevoir un grand nombre de notifications non souhaitées.

Lorsque la fenêtre de maintenance démarre, un événement « fenêtre de maintenance d'objet démarrée » est affiché sur la page d'inventaire de gestion d'événements. Cet événement est automatiquement obsolète lorsque la fenêtre de maintenance se termine.

Lors d'une fenêtre de maintenance, les événements liés à tous les objets du cluster sont toujours générés, mais ils n'apparaissent sur aucune page de l'interface utilisateur et aucune alerte ou tout autre type de notification n'est envoyée pour ces événements. Vous pouvez cependant afficher les événements générés pour tous les objets de stockage pendant une fenêtre de maintenance en sélectionnant l'une des options d'affichage de la page d'inventaire gestion des événements.

Vous pouvez planifier l'ouverture d'une fenêtre de maintenance. Vous pouvez modifier les heures de début et de fin d'une fenêtre de maintenance planifiée et annuler une fenêtre de maintenance planifiée.

Planification d'une fenêtre de maintenance pour désactiver les notifications d'événements du cluster

Si vous avez un temps d'indisponibilité planifié 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 ce délai en planifiant une fenêtre de maintenance Unified Manager.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Lors d'une fenêtre de maintenance, les événements liés à tous les objets du cluster sont toujours générés, mais ils n'apparaissent pas sur la page d'événement. En outre, aucune alerte ou tout autre type de notification n'est envoyée pour ces événements.

L'heure saisie pour la fenêtre de maintenance est basée sur l'heure sur le serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Dans la colonne **Maintenance mode** du cluster, sélectionnez le bouton coulissant et déplacez-le vers la droite.

   La fenêtre de 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 » s'affiche à côté du bouton coulissant.

Lorsque l'heure de début est atteinte, le cluster passe en mode maintenance et un événement « Object Maintenance Window Started » est généré.

Modification ou annulation d'une fenêtre de maintenance planifiée

Si vous avez configuré une fenêtre de maintenance Unified Manager pour qu'elle s'effectue à l'avenir, vous pouvez modifier les heures de début et de fin ou annuler la fenêtre de maintenance.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

L'annulation d'une fenêtre de maintenance en cours d'exécution est utile si la maintenance du cluster est terminée avant l'heure de fin de la fenêtre de maintenance planifiée et que vous souhaitez recevoir à nouveau des événements et des alertes à partir du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Dans la colonne **Maintenance mode** du cluster :

Les fonctions que vous recherchez…	Effectuer cette étape…
Modifier le délai d'une fenêtre de maintenance planifiée	a. Cliquez sur le texte « planifié » à côté du bouton du curseur. b. Modifiez la date et l'heure de début et/ou de fin et cliquez sur **appliquer**.
Allonger la longueur d'une fenêtre de maintenance active	a. Cliquez sur le texte « actif » en regard 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.

Affichage des événements qui se sont produits lors d'une fenêtre de maintenance

Si nécessaire, vous pouvez afficher les événements générés pour tous les objets de stockage au cours d'une fenêtre de maintenance Unified Manager. La plupart des événements apparaissent à l'état Obsolète une fois la fenêtre de maintenance terminée et toutes les ressources système sont sauvegardées et en cours d'exécution.

Ce dont vous aurez besoin

Au moins une fenêtre de maintenance doit avoir été effectuée avant que des événements soient disponibles.

Les événements qui se sont produits 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 **Evénements**.

   Par défaut, tous les événements actifs (nouveaux et acquittés) sont affichés sur la page d'inventaire gestion des événements.

2. Dans le volet Affichage, sélectionnez l'option **tous les événements générés pendant la maintenance**.

   La liste des événements trigés au cours des 7 derniers jours à partir de toutes les sessions de la fenêtre de maintenance et de tous les clusters s'affiche.

3. Si plusieurs fenêtres de maintenance ont été disponibles pour un seul cluster, vous pouvez cliquer sur l'icône du calendrier **déclenché Time** et sélectionner la durée des événements de la fenêtre de maintenance que vous souhaitez afficher.

Gestion des événements de 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 affichés sous forme de messages de bannière dans la partie supérieure de l'interface utilisateur.

Les événements de Management Station indiquent un problème avec le système hôte sur lequel Unified Manager est installé. Les problèmes liés à la station de gestion incluent l'espace disque insuffisant sur le système hôte, Unified Manager manquant d'un cycle régulier de collecte de données et l'absence d'achèvement, ou fin tardive, de l'analyse statistique car le prochain sondage de collecte a été lancé.

Contrairement à tous les autres messages d'événement Unified Manager, ces messages d'avertissement et événements critiques particuliers de la station de gestion s'affichent dans des bannières.

Étape

1. Pour afficher les informations d'événement de station de gestion, effectuez les opérations suivantes :

Les fonctions que vous recherchez…	Procédez comme ça…
Afficher les détails de l'événement	Cliquez sur la bannière de l'événement pour afficher la page Détails de l'événement qui contient des suggestions de solutions pour le problème.
Afficher tous les événements de station de gestion	a. Dans le volet de navigation de gauche, cliquez sur **Event Management**. b. Dans le volet filtres de la page d'inventaire de gestion des événements, cliquez sur la zone de la station de gestion dans la liste Type de source.

Présentation des événements

La compréhension des concepts relatifs aux événements vous permet de gérer efficacement les clusters et les objets de cluster, et de définir les alertes de manière appropriée.

Définitions d'état d'événement

L'état d'un événement vous aide à déterminer si une action corrective appropriée est nécessaire. Un événement peut être Nouveau, accusé de réception, résolu ou Obsolète. Notez que les événements nouveaux et acquittés sont considérés comme des événements actifs.

Les États d'événement sont les suivants :

- **Nouveau**

  État d'un nouvel événement.

- **Reconnu**

  État d'un événement lorsque vous l'avez reconnu.

- **Résolu**

  État d'un événement lorsqu'il est marqué comme résolu.

- **Obsolète**

  État d'un événement lorsqu'il est automatiquement corrigé ou lorsque la cause de l'événement n'est plus valide.

  > Vous ne pouvez pas accepter 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 inaccessible 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 effectué une action corrective adéquate, vous devez marquer l'événement comme résolu. L'état de l'événement devient alors résolu.

Si l'événement Cluster inaccessible est généré en raison d'une panne de courant, lorsque l'alimentation est restaurée, le cluster démarre sans intervention de l'administrateur. Par conséquent, l'événement Cluster inaccessible n'est plus valide et l'état de l'événement passe à Obsolète dans le cycle de surveillance suivant.

Unified Manager envoie une alerte lorsqu'un événement est à l'état Obsolète ou résolu. La ligne d'objet de l'e-mail et le contenu de l'e-mail d'une alerte fournissent des informations sur l'état de l'événement. Un trap SNMP contient également des informations relatives à l'état d'événement.

Description des types de gravité d'événement

Chaque événement est associé à un type de gravité pour vous aider à hiérarchiser les événements nécessitant une action corrective immédiate.

- **Critique**

  Un problème peut entraîner une interruption des services si des mesures correctives ne sont pas prises

immédiatement.

Les événements stratégiques de performance sont envoyés uniquement à partir de seuils définis par l'utilisateur.

- **Erreur**

  La source de l'événement est toujours en cours d'exécution. Toutefois, une action corrective est nécessaire pour éviter toute interruption de service.

- **Avertissement**

  La source d'événement a rencontré un événement que vous devez connaître ou qu'un compteur de performances pour un objet de cluster est hors de la plage normale et doit être surveillé pour vérifier qu'il n'atteint pas la gravité critique. Les événements de ce niveau de gravité n'entraînent pas d'interruption des services, mais une action corrective immédiate peut ne pas être nécessaire.

  Les événements d'avertissement de performance 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 exécutée. Par exemple, lorsqu'un objet de stockage est supprimé ou en cas de modification de la configuration, l'événement contenant des informations de type de gravité est généré.

  Les événements d'informations sont envoyés directement depuis ONTAP lorsqu'il détecte une modification de configuration.

Description des niveaux d'impact d'événement

Chaque événement est associé à un niveau d'impact (incident, risque, événement ou mise à niveau) pour vous aider à hiérarchiser les événements nécessitant une action corrective immédiate.

- **Incident**

  Un incident est un ensemble d'événements pouvant entraîner l'arrêt du service des données au client et un manque d'espace pour le stockage des données. Les événements ayant un niveau d'impact de l'incident sont les plus graves. Une action corrective immédiate doit être prise pour éviter toute perturbation du service.

- **Risque**

  Un risque est un ensemble d'événements pouvant entraîner l'arrêt du service des données au client et le manque d'espace pour le stockage des données. Les événements ayant un impact sur le niveau de risque peuvent entraîner des perturbations du service. Une action corrective peut être nécessaire.

- **Événement**

  Un événement est un changement d'état ou d'état des objets de stockage et de leurs attributs. Les événements ayant un niveau d'impact de l'événement sont informatifs et ne nécessitent pas d'action 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 liés à la résolution des problèmes lorsque vous devez mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les conseils de sécurité). Vous pouvez effectuer une action corrective immédiatement pour certains de ces problèmes, alors que d'autres peuvent attendre la prochaine maintenance planifiée.

Description des zones d'impact de l'événement

Les événements sont classés en six catégories 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 lorsqu'un objet de stockage est hors ligne, si un service de protocole est défaillant, en cas de basculement du stockage ou si un problème survient au niveau du matériel.

- **Capacité**

  Les événements de capacité vous avertissent lorsque vos agrégats, volumes, LUN ou espaces de noms sont proches 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 détection, 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'événement et un type d'information de gravité.

- **Performance**

  Les événements de performances vous avertissent des conditions de ressources, de configuration ou d'activité sur votre cluster qui peuvent nuire à la vitesse des entrées et des récupérations du stockage de données pour vos objets de stockage surveillés.

- **Protection**

  Les événements de protection vous signalent les incidents et les risques impliquant des relations SnapMirror, des problèmes de capacité de destination, des problèmes avec les relations SnapVault ou des problèmes de protection. Tout objet ONTAP (notamment les agrégats, les volumes et les SVM) hébergeant des volumes secondaires et des relations de protection est classé dans la zone d'impact sur la protection.

- **Sécurité**

  Les événements de sécurité vous informent de la manière dont la sécurité de vos clusters ONTAP, de vos machines virtuelles de stockage (SVM) et de vos volumes repose sur les paramètres définis dans le "Guide NetApp sur le renforcement de la sécurité des environnements ONTAP 9".

  De plus, ce domaine inclut des événements de mise à niveau signalés sur la plateforme Active IQ.

Mode de calcul de l'état de l'objet

L'état de l'objet est déterminé par l'événement le plus grave qui détient actuellement un état Nouveau ou reconnu. Par exemple, si l'état d'un objet est erreur, l'un des événements de l'objet a un type de gravité erreur. Une fois l'action corrective effectuée, l'état d'événement passe à résolu.

Détails du graphique d'événements de performances dynamiques

Pour les événements de performance dynamiques, la section System Diagnosis (diagnostic du système) de la page Event Details (Détails des événements) répertorie les principaux workloads présentant la latence ou l'utilisation la plus élevée du composant de cluster en conflit.

Les statistiques de performance sont basées sur l'heure à laquelle 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 pour le composant de cluster en conflit.

Par exemple, vous pouvez identifier les charges de travail avec une utilisation élevée d'un composant afin de déterminer la charge de travail à déplacer vers un composant moins utilisé. Le déplacement de la charge de travail réduirait le travail sur le composant actuel, ce qui aurait probablement pour effet de démettre le composant en conflit. En haut de cette section se trouve la plage d'heure et de date lorsqu'un événement a été détecté et la dernière analyse. Pour les événements actifs (nouveaux ou acquittés), la dernière analyse est mise à jour.

Les graphiques latence et activité affichent les noms des principales charges de travail lorsque vous positionnez le curseur de votre souris sur le graphique. En cliquant sur le menu Type de charge de travail à droite du graphique, vous pouvez trier les charges de travail en fonction de leur rôle dans l'événement, notamment *requins*, *bullies* ou *victimes*. Il affiche également 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 savoir quand la charge de travail se trouvait en dehors de la plage prévue de latence ou d'utilisation. Pour plus d'informations, voir "Types de charges de travail surveillés par Unified Manager".

> Lorsque vous triez par écart de latence en fonction des pics, les workloads définis par système ne s'affichent pas dans le tableau, car la latence s'applique uniquement aux workloads définis 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 performances dynamiques, reportez-vous à "Analyse des événements à partir de seuils de performances dynamiques"la section .

Pour plus d'informations sur la manière dont Unified Manager classe les charges de travail et détermine l'ordre de tri, reportez-vous à la section "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 analyse de l'événement. 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 impliquer un événement après la détection de l'événement. Ses statistiques de performances peuvent donc ne pas correspondre aux valeurs lors de la détection d'événement. Par défaut, les workloads sont triés par écart de latence maximal (le plus élevé).

> Dans la mesure où Unified Manager conserve un maximum de 30 jours de données historiques de performances et d'événements de 5 minutes, si l'événement est âgé de plus de 30 jours, aucune donnée de performance n'est affichée.

- **Colonne Tri de la charge de travail**
  - **Tableau de latence**

    Affiche l'impact de l'événement sur la latence de la charge de travail au cours de la dernière analyse.
  - **Colonne utilisation des composants**

    Affiche des détails sur l'utilisation de la charge de travail du composant de cluster dans les conflits. Dans les graphiques, l'utilisation réelle est une ligne bleue. Une barre rouge met en évidence la durée de l'événement, de l'heure de détection à la dernière heure analysée. Pour plus d'informations, voir "Valeurs de mesure des performances des charges de travail".

    > Pour le composant réseau, car les statistiques de performances du réseau proviennent de l'activité hors du cluster, cette colonne n'est pas affichée.
  - **Utilisation des composants**

    Affiche l'historique d'utilisation, en pourcentage, des composants du traitement réseau, du traitement des données et de l'agrégat, ou l'historique d'activité, en pourcentage, du composant du groupe de règles de QoS. Le graphique ne s'affiche pas pour les composants réseau ou d'interconnexion. Vous pouvez pointer vers les statistiques pour afficher les statistiques d'utilisation à un point dans le temps spécifique.
  - **Total écrire Mo/s Historique**

    Pour le composant Ressources MetroCluster uniquement, la indique le débit d'écriture total, en mégaoctets par seconde (Mbit/s), pour toutes les charges de travail de volume qui sont mises en miroir sur le cluster partenaire dans une configuration MetroCluster.
  - **Historique des événements**

    Affiche des lignes grisées en rouge pour indiquer les événements historiques du composant en conflit. Pour les événements obsolètes, le graphique affiche les événements survenus avant la détection de l'événement sélectionné et après sa résolution.

Modifications de configuration détectées par Unified Manager

Unified Manager surveille vos clusters pour modifier la configuration, ce qui vous permet de déterminer si une modification a pu être causée ou contribué 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 auxquelles la modification a été détectée.

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 affecté les performances de l'objet de cluster sélectionné. Si la modification a été détectée en même temps qu'un événement de performance ou à peu près, la modification peut avoir contribué au problème, qui a déclenché

l'alerte d'événement.

Unified Manager peut détecter les événements de modification suivants, classés dans la catégorie « événements d'information » :

- Un volume est déplacé entre agrégats.

  Unified Manager peut détecter lorsque le déplacement est en cours, terminé ou échoué. Lorsqu'Unified Manager est inactif pendant le déplacement d'un volume, lors de sa sauvegarde, il détecte le déplacement de volume et affiche un événement de modification pour celui-ci.

- Le débit (Mbit/s ou IOPS) d'un groupe de règles de QoS contenant un ou plusieurs changements de charge de travail surveillés.

  La modification de la limite d'un groupe de règles peut entraîner des pics intermittents de latence (temps de réponse), qui peuvent également déclencher des événements pour le groupe de règles. La latence revient progressivement à la normale et tous les événements provoqués par les pics deviennent obsolètes.

- Un nœud d'une paire haute disponibilité prend le relais ou renvoie le stockage de son nœud partenaire.

  Unified Manager peut détecter la fin de l'opération de basculement, de basculement partiel ou de rétablissement. Si le basculement est causé par un nœud paniqué, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de restauration de ONTAP a été effectuée correctement.

  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 avec les catégories d'événements, les noms d'événements et le type de gravité de chaque événement que vous pouvez afficher dans Unified Manager. Les événements sont répertoriés par ordre alphabétique par catégorie d'objet.

Agréger les événements

Les événements d'agrégat fournissent des informations sur l'état des agrégats, qui vous permettent de surveiller en cas de problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine 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
Agrégat hors ligne(ocumEvtAggregateStateOffline)	Gestion des	Agrégat	Primordial
L'agrégat a échoué(ocumEvtagrégeStateFaitStateFaitStateFailed)	Gestion des	Agrégat	Primordial
Agrégat Restricted (ocumEvtAggregateStateRestricted)	Risques	Agrégat	Avertissement
Reconstruction d'agrégats(ocumEvtAggregateRaidStateReconstructing)	Risques	Agrégat	Avertissement
Agrégat dégradé(ocumEvtAggregateRaidStateDegraded)	Risques	Agrégat	Avertissement
Cloud Tier partiellement accessible(ocumEventCloudTierPartiallyRelixiaccessible)	Risques	Agrégat	Avertissement
Cloud Tier inaccessible(ocumEventCloudTierUnreaccessible)	Risques	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation d'agrégats *(arlNetraChecked Failed)	Risques	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation des agrégats pendant le basculement du stockage *(gbNetraChecked)	Risques	Agrégat	Erreur

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Agrégat MetroCluster laissé derrière(ocumEvtMetroClusterAggregatede gauche)	Risques	Agrégat	Erreur
Mise en miroir des agrégats MetroCluster dégradé (ocumEvtMetroClusterAggréateMirrorDegret)	Risques	Agrégat	Erreur

Zone d'impact : capacité

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Espace total quasiment plein (ocumEvtagrégeNearyFull)	Risques	Agrégat	Avertissement
Espace total de l'agrégat (ocumEvtAggregateFull)	Risques	Agrégat	Erreur
Agréger les jours jusqu'au total (ocumEvtAggregateDays UntilFullSoon)	Risques	Agrégat	Erreur
Surallocation des agrégats (ocumEvtAggregateOverd éterminé)	Risques	Agrégat	Erreur
Agrégat presque surengagé(ocumEvtAggregateAlmostOverdéterminé)	Risques	Agrégat	Avertissement
Réserve Snapshot totale de l'agrégat (ocumEvtAggregateSnap ReserveFull)	Risques	Agrégat	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Taux de croissance global anormal (ocumEvtagrégeRegeTrowthRateAbnormal)	Risques	Agrégat	Avertissement

Zone d'impact : configuration

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Agrégat découvert (non applicable)	Événement	Agrégat	Informations
Agrégat renommé (non applicable)	Événement	Agrégat	Informations
Agrégat supprimé (non applicable)	Événement	Nœud	Informations

Zone d'impact : performances

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS global dépassé (ocumagrégeIopsincident)	Gestion des	Agrégat	Primordial
Seuil d'avertissement d'IOPS global dépassé(ocumagrégeIops Avertissement)	Risques	Agrégat	Avertissement
Seuil critique cumulé en Mo/s dépassé(ocumAggregate Mbpsincident)	Gestion des	Agrégat	Primordial
Seuil d'avertissement global MB/s dépassé (ocumAggregateMbpsWarning)	Risques	Agrégat	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil critique de latence globale dépassé(ocumagrégeReg eLatenceincident)	Gestion des	Agrégat	Primordial
Seuil d'avertissement de latence globale dépassé (ocumAggregateLatAvertis sement)	Risques	Agrégat	Avertissement
Performance de l'agrégat capacité seuil critique utilisé dépassé(ocumagrégeCon tretRequeContretcapacité s effectiveUsedincident)	Gestion des	Agrégat	Primordial
Performance globale seuil d'avertissement utilisé - capacité rompues (suite à l'agrégation de donnéesEntiqueContretue ContreteContretuseeCont retuseedu)	Risques	Agrégat	Avertissement
Seuil critique d'utilisation des agrégats (ocumagrégeUtilationincid ent)	Gestion des	Agrégat	Primordial
Seuil d'avertissement d'utilisation des agrégats dépassé (avertissement concernant l'agrégation de l'agrégationUtilationWarni ng)	Risques	Agrégat	Avertissement
Dépassement du seuil lors de la surutilisation des disques agrégés (ocumAgregateDiskOverU tilizedWarning)	Risques	Agrégat	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil dynamique d'agrégat dépassé (ocumAggregateDynamicEventWarning)	Risques	Agrégat	Avertissement

Événements de cluster

Les événements de cluster fournissent des informations sur l'état des clusters, ce qui vous permet de contrôler les clusters pour identifier des problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement, le nom de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Le cluster ne dispose pas de disques de rechange (ocumEvtDisksNoSpares)	Risques	Cluster	Avertissement
Cluster inaccessible(ocumEvtClusterUnreaccessible)	Risques	Cluster	Erreur
Echec de la surveillance du cluster(oocumEvtClusterMonitoringFailé)	Risques	Cluster	Avertissement
Limites de capacité de la licence Cluster FabricPool enfreintes précédemment (ocumEvtExternalcapacityTierSpaceplein)	Risques	Cluster	Avertissement
Début de la période de grâce NVMe-of *(nvmfGracePeriodStart)	Risques	Cluster	Avertissement
Période de grâce active NVMe-of *(nvmfGracePeriodActive)	Risques	Cluster	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Délai de grâce NVMe-of expiré *(nvmfGracePeriodExpired)	Risques	Cluster	Avertissement
Fenêtre de maintenance de l'objet démarrée(objectMaintenanceStarted)	Événement	Cluster	Primordial
Fin de la fenêtre de maintenance de l'objet(objectMaintenance Fenêtre fenêtré)	Événement	Cluster	Informations
Disques de rechange MetroCluster laissés derrière (ocumEvtSpareDiskgauches Behind)	Risques	Cluster	Erreur
Basculement automatique non planifié désactivé dans MetroCluster (fonction ocumEvtccAutomaticUnplanndSwitchOverDisabled)	Risques	Cluster	Avertissement
Mot de passe utilisateur du cluster modifié *(cluster.passwd.changed)	Événement	Cluster	Informations

Zone d'impact : capacité

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil de déséquilibre de la capacité du cluster dépassé(ocumConformanceNodeImbalanceWarning)	Risques	Cluster	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Planification des niveaux de cluster Cloud (clusterCloudTierPlaningAvertissement)	Risques	Cluster	Avertissement
Resynchronisation de la réplication des miroirs FabricPool terminée * (date de préexécution)	Événement	Cluster	Avertissement
Espace FabricPool presque complet * (fabrication NearpoolyFull)	Risques	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	Informations
Nœud supprimé (non applicable)	Événement	Cluster	Informations
Suppression du cluster (non applicable)	Événement	Cluster	Informations
Échec de l'ajout du cluster (non applicable)	Événement	Cluster	Erreur
Nom de cluster modifié (non applicable)	Événement	Cluster	Informations
EMS d'urgence reçu (non applicable)	Événement	Cluster	Primordial
EMS critique reçu (non applicable)	Événement	Cluster	Primordial
Alerte EMS reçue (non applicable)	Événement	Cluster	Erreur

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Erreur EMS reçue (non applicable)	Événement	Cluster	Avertissement
Avertissement reçu EMS (non applicable)	Événement	Cluster	Avertissement
EMS de débogage reçu (non applicable)	Événement	Cluster	Avertissement
Avis EMS reçu (non applicable)	Événement	Cluster	Avertissement
Informations fournies par le SGE (non applicable)	Événement	Cluster	Avertissement

Les événements EMS ONTAP sont classés en trois niveaux de sévérité des événements dans Unified Manager.

Niveau de sévérité des événements Unified Manager	Niveau de sévérité des événements EMS ONTAP
Primordial	Urgence Primordial
Erreur	Alerte
Avertissement	Erreur Avertissement Débogage Avertissement Informatif

Zone d'impact : performances

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil de déséquilibre de charge du cluster dépassé()	Risques	Cluster	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS du cluster dépassé (ocumClusterIopsincident)	Gestion des	Cluster	Primordial
Seuil d'avertissement d'IOPS du cluster dépassé (ocumClusterIopsWarning)	Risques	Cluster	Avertissement
Saturation du seuil critique du cluster MB/s (ocumClusterMbpsincident)	Gestion des	Cluster	Primordial
Seuil d'avertissement MB/s du cluster dépassé(avertissement ocumClusterMbpsWarning)	Risques	Cluster	Avertissement
Seuil dynamique de cluster dépassé (ocumClusterDynamicEventWarning)	Risques	Cluster	Avertissement

Zone d'impact : sécurité

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Transport HTTPS AutoSupport désactivé (ocumClusterASUPHttsConfigredDisabled)	Risques	Cluster	Avertissement
Le transfert de journal n'est pas crypté(ocumClusterAuditLogUncrypté)	Risques	Cluster	Avertissement
Utilisateur Admin local par défaut activé (ocumClusterDefaultAdminEnabled)	Risques	Cluster	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Mode FIPS désactivé (fonction ocumClusterFipsDisabled)	Risques	Cluster	Avertissement
Bannière de connexion désactivée (oocumClusterLoginBannerDisabled)	Risques	Cluster	Avertissement
Bannière de connexion modifiée(ocumClusterLoginBannerChanged)	Risques	Cluster	Avertissement
Destinations de transfert de journal modifiées (ocumLogForwarddesmodes Changed)	Risques	Cluster	Avertissement
Modification des noms de serveur NTP (ocumNtpServerNamesChanged)	Risques	Cluster	Avertissement
Le nombre de serveurs NTP est faible (securityConfigNTPServerCountLowRisk)	Risques	Cluster	Avertissement
Les communications des pairs de cluster ne sont pas cryptées(octaPeerEncryptionDisabled)	Risques	Cluster	Avertissement
SSH utilise des Ciphers non sécurisés (ocumClusterSSHInSecure)	Risques	Cluster	Avertissement
Protocole Telnet activé (ocumClusterTelnetEnabled)	Risques	Cluster	Avertissement

Nom de l'événement(Nom du piège)	Niveau d'impact	Type de source	Gravité
Les mots de passe de certains comptes utilisateur ONTAP utilisent la fonction de hachage MD5 moins sécurisée (ocumClusterMD5PasswordHashUsed)	Risques	Cluster	Avertissement
Le cluster utilise un certificat auto-signé (ocumClusterSelfSignedCertificate)	Risques	Cluster	Avertissement
Cluster Remote Shell est activé (ocumClusterRshDisabled)	Risques	Cluster	Avertissement
Certificat de cluster sur le point d'expirer(ocumEvtClusterCertificate AboutToExpire)	Risques	Cluster	Avertissement
Certificat de cluster expiré(ocumEvtClusterCertificateExpired)	Risques	Cluster	Erreur

Événements des disques

Les événements de disque 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 de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Disques Flash – blocs de rechange presque consommés (ocumEvtClusterFlashDiskFewerSpareBlockError)	Risques	Cluster	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Disques Flash - pas de blocs de rechange (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Gestion des	Cluster	Primordial
Certains disques non affectés(ocumEvtClusterUnassignedDisksSome)	Risques	Cluster	Avertissement
Certains disques défaillants(ocumEvtDisksUnsUnsUnsFailed)	Gestion des	Cluster	Primordial

Événements des armoires

Les armoires fournissent des informations sur l'état des armoires de tiroirs disques dans votre data Center, afin que vous puissiez contrôler l'éventualité d'un problème. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Échec des ventilateurs du tiroir disque (octaumEvtShelfFanFailed)	Gestion des	Tiroir de stockage	Primordial
Échec des blocs d'alimentation du tiroir disque (tiroir à tiroir disque, alimentation en panne)	Gestion des	Tiroir de stockage	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Tiroir disque Multipath non configuré(ocumDiskShelfConnectivtyNotInMultiPath) Cet événement ne s'applique pas aux : • Clusters qui font partie d'une configuration MetroCluster • Les plateformes suivantes : FAS2554, FAS2552, FAS2520 et FAS2240	Risques	Nœud	Avertissement
Défaillance du chemin du tiroir disque (octumDiskShelfConnectivtyPathFailure)	Risques	FAS NetApp	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Tiroir disque détecté (non applicable)	Événement	Nœud	Informations
Tiroirs disques supprimés (non applicables)	Événement	Nœud	Informations

Événements fans

Les événements ventilateurs fournissent des informations sur l'état des ventilateurs sur les nœuds de votre data Center, afin que vous puissiez surveiller les éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Un ou plusieurs ventilateurs défaillants(ocumEvtFansOneOrMoreFailed)	Gestion des	Nœud	Primordial

Événements de carte Flash

Les événements de carte Flash fournissent des informations sur l'état des cartes Flash installées sur les nœuds de votre data Center, afin de pouvoir surveiller l'éventuelle présence de problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Cartes Flash hors ligne (ocumEvtFlashCardOffline)	Gestion des	Nœud	Primordial

Inode événements

Les événements d'inode fournissent des informations lorsque l'inode est plein ou presque plein afin que vous puissiez surveiller tout problème potentiel. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Inodes presque plein (ocumEvtInodesAlmostFull)	Risques	Volumétrie	Avertissement
Inodes complet (ocumEvtInodesFull)	Risques	Volumétrie	Erreur

Événements liés à l'interface réseau (LIF)

Les événements de l'interface réseau fournissent des informations sur l'état de votre interface réseau (LIFS), qui vous permettent de surveiller les problèmes potentiels. Les

événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
État de l'interface réseau Down (ocumEvtLifStatusDown)	Risques	Interface	Erreur
Statut de l'interface réseau FC/FCoE arrêté (ocumEvtFCLIfStatusDown)	Risques	Interface	Erreur
Basculement de l'interface réseau impossible (ocumEvtLiftFailOverNoble)	Risques	Interface	Avertissement
L'interface réseau n'est pas à Home Port (ocumEvtLiftNoteAHomePort)	Risques	Interface	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Route de l'interface réseau non configurée (non applicable)	Événement	Interface	Informations

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil critique de l'interface réseau MB/s (ocumNetworkLifMbpsincident)	Gestion des	Interface	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil d'avertissement de l'interface réseau MB/s dépassé(ocumNetworkLifMbpsWarning)	Risques	Interface	Avertissement
Brèche dans le seuil critique de l'interface réseau FC MB/s (ocumFcpLifMbpsincident)	Gestion des	Interface	Primordial
Seuil d'avertissement de l'interface réseau FC MB/s dépassé(ocumFcpLifMbpsWarning)	Risques	Interface	Avertissement
Interface réseau FC NVMf MB/s Critical Threshold rompues(ocumNvmfFcLifMbpsincident)	Gestion des	Interface	Primordial
Interface réseau FC NVMf MB/s seuil d'avertissement dépassé(ocumNvmfFcLifMbpsWarning)	Risques	Interface	Avertissement

Événements LUN

Les événements de LUN fournissent des informations sur l'état de vos LUN, ce qui vous permet de contrôler s'il y a des problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
LUN hors ligne(ocumEvtLunOffline)	Gestion des	LUN	Primordial
LUN détruite * (déjeuner)	Événement	LUN	Informations

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
LUN mappée avec un système d'exploitation non pris en charge dans le groupe initiateur(macusPrunsupportedOsType)	Gestion des	LUN	Avertissement
Chemin actif unique pour accéder à la LUN (ocumEvtLunSingleActivePath)	Risques	LUN	Avertissement
Aucun chemin actif pour accéder à la LUN (ocumEvtLunNotRelixivisible)	Gestion des	LUN	Primordial
Pas de chemins optimisés pour accéder aux LUN (ocumEvtLunOptimizedPathInactif)	Risques	LUN	Avertissement
Aucun chemin d'accès aux LUN depuis un partenaire de haute disponibilité (ocumEvtLunHaPathInactif)	Risques	LUN	Avertissement
Chemin d'accès LUN à partir d'un nœud dans paire HA(ocumEvtLunNodePathStatusDown)	Risques	LUN	Erreur

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Espace insuffisant pour la copie Snapshot de LUN (ocumEvtLunSnapshotNotPossible)	Risques	Volumétrie	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
LUN mappée avec un système d'exploitation non pris en charge dans le groupe initiateur(macusPrunsupportedOsType)	Risques	LUN	Avertissement

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS LUN dépassé (ocumLunIopsincident)	Gestion des	LUN	Primordial
Seuil d'avertissement d'IOPS de la LUN dépassé (ocumlunIopsWarning)	Risques	LUN	Avertissement
Seuil critique de LUN Mo/s dépassé (ocumLunmMbpsincident)	Gestion des	LUN	Primordial
Seuil d'avertissement de LUN Mo/s dépassé(ocumLunmpsWarning)	Risques	LUN	Avertissement
Seuil critique de latence ms/op du LUN dépassé (ocumLunLatenincident)	Gestion des	LUN	Primordial
Seuil d'avertissement ms/op de latence de LUN dépassé (avertissement relatif à l'ocumLunlateAvertissement)	Risques	LUN	Avertissement
Latence des LUN et seuil critique d'IOPS dépassé(ocumLunLatencyIopsincident)	Gestion des	LUN	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil de latence LUN et d'avertissement d'IOPS dépassé(ocumLunLatencyIopsWarning)	Risques	LUN	Avertissement
Latence des LUN et seuil critique MB/s dépassé(ocumLunlacyMbpsincident)	Gestion des	LUN	Primordial
Latence des LUN et seuil d'avertissement MB/s dépassé(ocumLunLatcyMbpsWarning)	Risques	LUN	Avertissement
Latence du LUN et performances globales capacité utilisée seuil critique dépassé(ocumLunagenceEngraregPerfeCapacitéUsedincident)	Gestion des	LUN	Primordial
Latence du LUN et performances de l'agrégat seuil d'avertissement de capacité utilisée dépassé(ocumLunagenceEngraregcapacitéUsedWarning)	Risques	LUN	Avertissement
Latence du LUN et utilisation des agrégats seuil critique dépassé(ocumLunlateagrégationUtilitéincident)	Gestion des	LUN	Primordial
Seuil d'avertissement de latence du LUN et d'utilisation des agrégats dépassé(ocumLunlateagrégationUtilitéAvertissement)	Risques	LUN	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Latence du LUN et performances du nœud capacité utilisée seuil critique dépassé(ocumLunlateNodePerf2eUsedincident)	Gestion des	LUN	Primordial
Latence du LUN et performances du nœud seuil d'avertissement de capacité utilisée dépassé(ocumLunlationNodePerf2eContretuseeAvertissement)	Risques	LUN	Avertissement
Latence du LUN et performances du nœud capacité utilisée – seuil critique de basculement violé(ocumLunagenceContreteContreteContreteContretedessurincident)	Gestion des	LUN	Primordial
Latence du LUN et performances du nœud utilisation - seuil d'avertissement de basculement dépassé(ocumLuntyAgrégeContreteContreteContreteContretedesousContretoussuintardesousContretousde l'avertissement)	Risques	LUN	Avertissement
Latence du LUN et utilisation du nœud seuil critique dépassé(ocumLunLatencyNodeUtizationincident)	Gestion des	LUN	Primordial
Seuil d'avertissement de latence des LUN et d'utilisation des nœuds dépassé(ocumLunLatcyNodeUtilAvertissement)	Risques	LUN	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil d'avertissement IOPS max. De la LUN QoS dépassé (ocumQosLunMaxIopsWarning)	Risques	LUN	Avertissement
Seuil d'avertissement QoS LUN max. Mo/s dépassé(ocumQosLunMaxMbpsWarning)	Risques	LUN	Avertissement
Seuil de latence des LUN de charge de travail dépassé, tel que défini par la règle de niveau de service de performance(ocumConformanceLatenceWarning)	Risques	LUN	Avertissement

Événements de station de gestion

Les événements de Management Station vous fournissent des informations sur l'état du serveur sur lequel Unified Manager est installé afin de pouvoir surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Espace disque du serveur de gestion presque plein (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risques	Station de gestion	Avertissement
Espace disque du serveur de gestion plein (ocumEvtUnifiedManagerDiskSpaceplein)	Gestion des	Station de gestion	Primordial
Serveur de gestion mémoire faible (ocumEvtUnifiedManagerMemoryLow)	Risques	Station de gestion	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Serveur de gestion presque mémoire(ocumEvtUnifiedManagerMemoryAlmostOut)	Gestion des	Station de gestion	Primordial
Taille du fichier journal MySQL augmentée ; redémarrage requis (ocumEvtMysqlLogFileSizeWarning)	Gestion des	Station de gestion	Avertissement
L'allocation totale de la taille du journal d'audit est sur le point d'être complète	Risques	Station de gestion	Avertissement
Le certificat du serveur syslog arrive à expiration	Risques	Station de gestion	Avertissement
Le certificat du serveur syslog a expiré	Risques	Station de gestion	Erreur
Fichier journal d'audit altéré	Risques	Station de gestion	Avertissement
Fichier journal d'audit supprimé	Risques	Station de gestion	Avertissement
Erreur de connexion au serveur syslog	Risques	Station de gestion	Erreur
Configuration du serveur syslog modifiée	Événement	Station de gestion	Avertissement

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
L'analyse des données de performances est impactée (ocumEvtUnifiedManagerDataMissingAnalyze)	Risques	Station de gestion	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
La collecte des données de performances est impactée (ocumEvtUnifiedManager DataMsingCollection)	Gestion des	Station 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 le nouvel état, et que vous effectuez une mise à niveau vers une version plus récente du logiciel Unified Manager, ces événements ne sont pas supprimés automatiquement. Vous devrez déplacer les événements à l'état résolu manuellement.

Événements du pont MetroCluster

Les événements Bridge MetroCluster fournissent des informations sur l'état des ponts, ce qui vous permet de surveiller les éventuels problèmes dans une configuration MetroCluster over FC. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Pont inaccessible(ocumEvtBridgeUnreaccessible)	Gestion des	Pont MetroCluster	Primordial
Température du pont anormale(ocumEvtBridgeTemperatureAbnormal)	Gestion des	Pont MetroCluster	Primordial

Événements de la connectivité MetroCluster

Les événements de connectivité fournissent des informations sur la connectivité entre les composants d'un cluster et entre les clusters dans les configurations MetroCluster over FC et MetroCluster over IP, ce qui permet de contrôler les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Événements communs dans les deux configurations

Ces événements de connectivité sont courants à la fois pour les configurations MetroCluster over FC et MetroCluster over IP.

Domaine d’impact : disponibilité

Nom de l’événement (nom de l’argument)	Niveau d’impact	Type de source	Gravité
Tous les liens entre les partenaires MetroCluster Down(ocumEvtMetroClusterAllLinksBetweenisDown)	Gestion des	Relation MetroCluster	Primordial
Les partenaires MetroCluster ne sont pas accessibles via le réseau de peering(ocumEvtMetroClusterPartenairesNotReachableOverPeeringNetwork)	Gestion des	Relation MetroCluster	Primordial
Fonctionnalité de reprise après incident MetroCluster impactée (ocumEvtMetroClusterDRStatusImpacted)	Risques	Relation MetroCluster	Primordial
Commutation de la configuration MetroCluster(ocumEvtMetroClusterDRStatusImpaced)	Risques	Relation MetroCluster	Avertissement

Configuration MetroCluster sur FC

Ces événements sont en rapport avec les configurations MetroCluster sur FC.

Domaine d’impact : disponibilité

Nom de l’événement (nom de l’argument)	Niveau d’impact	Type de source	Gravité
Toutes les liaisons inter-commutateurs Down (ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Gestion des	Connexion inter-commutateurs MetroCluster	Primordial
Lien descendant entre la passerelle FC-SAS et la pile de stockage (ocumEvtBridgeSasPortDown)	Gestion des	Connexion de la pile de pont MetroCluster	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Configuration MetroCluster partiellement commutée(ocumEvtMetroClusterDRStatusPartiallyImpaced)	Risques	Relation MetroCluster	Erreur
Switch nœud à FC tous les liens d'interconnexion FC-VI Down(ocumEvtMccNodeSwitchFcviLinksDown)	Gestion des	Connexion du switch de nœud MetroCluster	Primordial
Lien nœud vers commutateur FC une ou plusieurs liaisons FC-Initiator Down (ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risques	Connexion du switch de nœud MetroCluster	Avertissement
Switch Node to FC tous les liens FC-Initiator Down(ocumEvtMccNodeSwitchFcLinksDown)	Gestion des	Connexion du switch de nœud MetroCluster	Primordial
Basculer vers FC Bridge FC Link Down (ocumEvtMccSwitchBridgeFcLinksDown)	Gestion des	Connexion du pont du commutateur MetroCluster	Primordial
Inter Node All FC VI Interconnect Links Down (ocumEvtMccInterNodeLinksDown)	Gestion des	Connexion inter-nœuds	Primordial
Inter Node, une ou plusieurs liaisons d'interconnexion VI FC (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risques	Connexion inter-nœuds	Avertissement
Lien nœud vers pont descendant (ocumEvtMccNodeBridgeLinksDown)	Gestion des	Connexion de pont de nœud	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Nœud vers stockage tous les liens SAS vers le bas (ocumEvtMccNodeStackLinksDown)	Gestion des	Connexion à la pile de nœuds	Primordial
Nœud à pile de stockage une ou plusieurs liaisons SAS vers le bas (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risques	Connexion à la pile de nœuds	Avertissement

Configuration MetroCluster sur IP

Ces événements sont en rapport avec les configurations MetroCluster sur IP.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Le statut de la connectivité intersite IP de MetroCluster est « en panne » (mccIntersiteconnectivityStatusDown)	Risques	Relation MetroCluster	Primordial
MetroCluster-IP connexion du nœud au commutateur hors ligne (mccIpPortStatusOffline)	Risques	Nœud	Erreur

Événements des commutateurs MetroCluster

Les événements des commutateurs MetroCluster pour les configurations MetroCluster sur FC fournissent des informations sur l'état des commutateurs MetroCluster, ce qui vous permet de surveiller les éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Température du commutateur anormale(ocumEvtTemperSwitchatureAbnormal)	Gestion des	Commutateur MetroCluster	Primordial
Commutateur inaccessible(oocumEvtSwitchUnreaccessible)	Gestion des	Commutateur MetroCluster	Primordial
Echec des ventilateurs du commutateur(ocumEvtSwitchFansOneOrMoreFailed)	Gestion des	Commutateur MetroCluster	Primordial
Échec des blocs d'alimentation du commutateur (panne de l'option ocumEvtSwitchPowerSupplésOneOrMoreFailed)	Gestion des	Commutateur MetroCluster	Primordial
Défaillance des capteurs de température du commutateur (ocumEvtTemperSwitchatureSensorFailed) Cet événement s'applique uniquement aux commutateurs Cisco.	Gestion des	Commutateur MetroCluster	Primordial

Événements de l'espace de noms NVMe

Les événements d'espace de noms NVMe fournissent des informations sur l'état de vos espaces de noms, afin que vous puissiez surveiller certains problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, 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.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
NVMeNS hors ligne *(nvmeNamespaceStatus hors ligne)	Événement	Espace de noms	Informations
NVMeNS en ligne *(nvmeNamespaceStatus Online)	Événement	Espace de noms	Informations
NVMeNS hors de l'espace *(nvmeNamespaceOutOf Space)	Risques	Espace de noms	Avertissement
NVMeNS Destroy *(nvmeNamespaceDesroy)	Événement	Espace de noms	Informations

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS dans l'espace de noms NVMe(ocumNvmeNames paceIopsincident)	Gestion des	Espace de noms	Primordial
Seuil d'avertissement d'IOPS pour l'espace de noms NVMe dépassé(ocumNmeName spaceIopsWarning)	Risques	Espace de noms	Avertissement
Seuil critique de l'espace de noms NVMe (ocumNvmeNamespaceM bpsincident)	Gestion des	Espace de noms	Primordial
Seuil de saturation de l'espace de noms NVMe (ocumNvmeNamespaceM bpsWarning)	Risques	Espace de noms	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Latence de l'espace de noms NVMe ms/op critique seuil dépassé(ocumNmeNamespaceLatenceincident)	Gestion des	Espace de noms	Primordial
Seuil de latence ms/op de l'espace de noms NVMe dépassé(ocumNmeNamespaceAvertissement)	Risques	Espace de noms	Avertissement
Latence de l'espace de noms NVMe et seuil critique d'IOPS brèche (ocumNvmeNamespaceLatenceIopsincident)	Gestion des	Espace de noms	Primordial
Latence de l'espace de noms NVMe et seuil d'avertissement d'IOPS dépassé(ocumNvmeNamespaceLatenceIopsAvertissement)	Risques	Espace de noms	Avertissement
Latence de l'espace de noms NVMe et seuil critique b/s dépassé(ocumNvmeNamespaceLatenceMbpsincident)	Gestion des	Espace de noms	Primordial
Latence de l'espace de noms NVMe et seuil de saturation des Mo/s (ocumNvmeNamespaceLatenceMbpsWarning)	Risques	Espace de noms	Avertissement

Événements du nœud

Les événements du nœud vous fournissent des informations sur l'état du nœud, ce qui vous permet de contrôler l'éventualité d'un problème. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, 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.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Espace du volume racine du nœud presque plein (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risques	Nœud	Avertissement
Cloud AWS MetaDataConnFail * (ocumCloudAwsMetadaConnFail)	Risques	Nœud	Erreur
Cloud AWS IAMCredeExceExcired *(ocumCloudAwsCredentistesExpired)	Risques	Nœud	Erreur
Cloud AWS IAMCredsInvalidate *(ocumCloudAwsCredentistsInvalides)	Risques	Nœud	Erreur
Des IAMCredentisNotFound dans Cloud AWS *(ocumCloudAwsIamCredentisNotFound)	Risques	Nœud	Erreur
Cloud AWS IAMCredentistsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Événement	Nœud	Informations
IAMROOROBnon valide *(ocumCloudAwsIamRoleInvalid)	Risques	Nœud	Erreur
L'IAMRRoleNotFound dans le cloud AWS *(ocumCloudAwsIamRoleNotFound)	Risques	Nœud	Erreur
Hôte Cloud Tier non résolu * (ocumObjstoreHostinsoluble)	Risques	Nœud	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Panne de l'interface réseau intercluster Cloud Tier * (ocumObjstoreInterClusterLifDown)	Risques	Nœud	Erreur
Un des pools NFSv4 épuisés *(nblaadeNfsv4PoolEXhaust)	Gestion des	Nœud	Primordial
Demande de signature de niveau de Cloud discordant * (SignatureMismatch)	Risques	Nœud	Erreur

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Mémoire du moniteur QoS max. *(ocumQosMonitorMemoryMembed)	Risques	Nœud	Erreur
Mémoire du moniteur QoS abated * (ocumQosMonitorMemoryAbated)	Événement	Nœud	Informations

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Nœud renommé (non applicable)	Événement	Nœud	Informations

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS du nœud dépassé (ocumNodeIopsincident)	Gestion des	Nœud	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil d'avertissement d'IOPS du nœud dépassé (ocumNodeIopsWarning)	Risques	Nœud	Avertissement
Seuil critique du nœud Mo/s dépassé(ocumNodeMbpsincident)	Gestion des	Nœud	Primordial
Seuil d'avertissement du nœud MB/s dépassé(ocumNodeMbpsWarning)	Risques	Nœud	Avertissement
Latence du nœud ms/op critique Threshold brèche (ocumNodeLatcyincident)	Gestion des	Nœud	Primordial
Seuil d'avertissement ms/op de latence du nœud dépassé(ocumNodeLattionWarning)	Risques	Nœud	Avertissement
Performances du nœud violation du seuil critique utilisé(ocumNodePerfcapacityUsedincident)	Gestion des	Nœud	Primordial
Seuil d'avertissement de capacité utilisée du nœud de performance dépassé(ocumNodePerfcapacityUsedAvertissement)	Risques	Nœud	Avertissement
Capacité du nœud utilisée – seuil critique de basculement dépassé(ocumNodePerftyUseTakouverincident)	Gestion des	Nœud	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Capacité du nœud utilisée – seuil d'avertissement de basculement dépassé(ocumNodePerfanceUseeprenne un niveau de prise en compte)	Risques	Nœud	Avertissement
Seuil critique d'utilisation du nœud dépassé (cas d'incident liés à l'utilisation du nœud)	Gestion des	Nœud	Primordial
Seuil d'avertissement d'utilisation du nœud dépassé (avertissement relatif à l'ocumNodeUtiliationWarning)	Risques	Nœud	Avertissement
Seuil surexploité par la paire HA du nœud (ocumNodeHaPairOverUtilizedinformation)	Événement	Nœud	Informations
Seuil de fragmentation du disque du nœud dépassé (ocumNodeDiskFragmentWarning)	Risques	Nœud	Avertissement
Dépassement du seuil minimal de capacité utilisée en matière de performances (ocumNodeOverUtilizedWarning)	Risques	Nœud	Avertissement
Seuil dynamique du nœud dépassé (ocumNodeDynamicEventWarning)	Risques	Nœud	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
ID d'avis : NTAP-<*Advisory ID*>(ocumx)	Risques	Nœud	Primordial

Événements de la batterie NVRAM

Les événements relatifs à la batterie NVRAM fournissent des informations sur l'état des 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 de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Batterie NVRAM faible (batterie ocumEvtNvramyLow)	Risques	Nœud	Avertissement
Batterie NVRAM déchargée (batterie ocumEvtNvramyDischargée)	Risques	Nœud	Erreur
Batterie NVRAM trop chargée (batterie ocumEvtNvramyOverCharged)	Gestion des	Nœud	Primordial

Événements de port

Les événements de port fournissent le statut des ports du cluster, de sorte que vous puissiez surveiller les modifications ou les problèmes sur le port, comme si le port est en panne.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Etat du port Down (ocumEvtPortStatusDown)	Gestion des	Nœud	Primordial

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil critique de port réseau MB/s dépassé(ocumNetworkPortMbpsincident)	Gestion des	Port	Primordial
Seuil d'avertissement MB/s du port réseau dépassé(oocumNetworkPortMbpsWarning)	Risques	Port	Avertissement
Seuil critique du port FCP MB/s dépassé(ocumFcpPortMbpsincident)	Gestion des	Port	Primordial
Seuil d'avertissement de port FCP MB/s dépassé(ocumFcpPortMbpsWarning)	Risques	Port	Avertissement
Violation du seuil critique d'utilisation des ports réseau (incident liés à l'ocusNetworkUtilazationincident)	Gestion des	Port	Primordial
Seuil d'avertissement d'utilisation des ports réseau dépassé (avertissement concernant l'oocusNetworkUtilazationWarning)	Risques	Port	Avertissement
Seuil critique d'utilisation du port FCP dépassé (ocumFcpPortUtilizinciden t)	Gestion des	Port	Primordial
Seuil d'avertissement d'utilisation du port FCP dépassé (avertissement concernant l'ocumFcpPortUtilizationWarning)	Risques	Port	Avertissement

Événements d'alimentation

Les événements des blocs d'alimentation 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 de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Un ou plusieurs blocs d'alimentation défectueux (module d'alimentation défaillant)OnOrMoreFailed	Gestion des	Nœud	Primordial

Événements de protection

Les événements de protection vous indiquent si un travail a échoué ou a été abandonné pour que vous puissiez surveiller les problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Echec du travail de protection(ocumEvtProtectionJobTasked)	Gestion des	Volume ou service de stockage	Primordial
Travail de protection abandonné(ocumEvtProtectionJobAborted)	Risques	Volume ou service de stockage	Avertissement

Événements qtree

Les événements qtree fournissent des informations sur la capacité qtree, sur les limites de fichiers et de disques, afin de pouvoir surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Espace qtree presque plein (ocumEvtQtréeNeareSpacelyFull)	Risques	Qtree	Avertissement
Espace qtree plein (ocumEvtQtreeSpaceFull)	Risques	Qtree	Erreur
Espace qtree normal(ocumEvtQtreeSpaceseuil de seuil Ok)	Événement	Qtree	Informations
Limite stricte atteinte des fichiers qtree (ocumEvtQtréeFilesHardLiitReached)	Gestion des	Qtree	Primordial
Qtree Files Soft Limit Breached(ocumEvtQtréeFilesSoftLimitBreached)	Risques	Qtree	Avertissement
Limite matérielle de l'espace qtree atteinte (ocumEvtQtreeSpaceHardLiitReached)	Gestion des	Qtree	Primordial
Qtree Space Soft Limit Breached (ocumEvtQtreeSpaceSoftLimitBreached)	Risques	Qtree	Avertissement

Événements du processeur de service

Les événements du processeur de service fournissent des informations sur l'état de votre processeur de service, ce qui vous permet de contrôler l'éventualité d'un problème. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Processeur de service non configuré(ocumEvtServiceProcessorNotConfigred)	Risques	Nœud	Avertissement
Processeur de service hors ligne(ocumEvtServiceProcessorOffline)	Risques	Nœud	Erreur

Événements liés à la relation SnapMirror

Les événements de relation SnapMirror fournissent des informations sur l'état de vos relations SnapMirror asynchrones et synchrones qui vous permettent de surveiller l'incident. Des événements de relation SnapMirror asynchrone sont générés à la fois pour les machines virtuelles de stockage et les volumes, mais les événements de relation SnapMirror synchrone sont générés uniquement pour les relations de volume. Aucun événement n'est généré pour les volumes composants faisant partie des relations de reprise sur incident des machines virtuelles de stockage. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, 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, qui sont protégées par la reprise après incident des machines virtuelles de stockage, mais pas pour les relations d'objets constitutifs.

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Réplication miroir défectueuse(ocumEvtSnapmirrorRelationshipUnHealthy)	Risques	Relation SnapMirror	Avertissement
Coupure de la réplication en miroir (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risques	Relation SnapMirror	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Échec de l'initialisation de la réplication du miroir (ocumEvtSnapmirrorRelationInitializeFailé)	Risques	Relation SnapMirror	Erreur
Échec de la mise à jour de la réplication miroir (ocumEvtSnapmirrorRelationshipUpdateFailed)	Risques	Relation SnapMirror	Erreur
Erreur de décalage de réplication du miroir (ocumEvtSnapMirrorRelationshipLagError)	Risques	Relation SnapMirror	Erreur
Avertissement de délai de réplication en miroir (ocumEvtSnapMirrorRelationshipLagWarning)	Risques	Relation SnapMirror	Avertissement
Échec de la resynchronisation de la réplication en miroir (ocumEvtSnapmirrorRelationshipResyncFailed)	Risques	Relation SnapMirror	Erreur
Réplication synchrone hors synchronisation * (syncSnapmirrorRelationshipOutfisync)	Risques	Relation SnapMirror	Avertissement
Réplication synchrone restaurée * (syncSnapmirrorRelationshipInSync)	Événement	Relation SnapMirror	Informations
Échec de la resynchronisation automatique de la réplication synchrone * (syncSnapmirrorRelationshipAutoSyncRetryFairyed)	Risques	Relation SnapMirror	Erreur
Un médiateur ONTAP est ajouté sur le cluster (snapmirrorMediatorAdded)	Événement	Cluster	Informations

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Le médiateur ONTAP est retiré du cluster (snapmirrorMediatorRemoved)	Événement	Cluster	Informations
ONTAP Mediator n'est pas accessible depuis le cluster (snapmirrorMediatorUnreastable)	Risques	Médiateur	Avertissement
Le Mediator ONTAP n'est pas accessible depuis le cluster (snapmirrorMediatorMisConfigured)	Risques	Médiateur	Erreur
La connectivité du médiateur ONTAP a été rétablie, et elle est redéfinie et prête pour la synchronisation active SnapMirror (snapmirrorMediatorInquorum)	Événement	Médiateur	Informations

Événements de relation de mise en miroir asynchrone et de coffre-fort

Les événements de relation SnapMirro et Vault vous fournissent des informations sur l'état de vos relations SnapMirror et Vault asynchrones, qui vous permettent de surveiller et contrôler les éventuels problèmes. Les événements de relation de mise en miroir asynchrone et de copie en miroir sont pris en charge pour les relations de protection des volumes et des machines virtuelles de stockage. Mais seules les relations de coffre-fort ne sont pas prises en charge pour la reprise sur incident de la machine virtuelle de stockage. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, 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 reprise après incident des machines virtuelles de stockage, mais pas pour les relations d'objet constituantes.

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Asynchrone Mirror et Vault malsains (ocumEvtMirrorVaultRelationshipHealthy)	Risques	Relation SnapMirror	Avertissement
Désactivation du miroir asynchrone et du coffre-fort (ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risques	Relation SnapMirror	Erreur
Échec de l'initialisation du miroir asynchrone et du coffre-fort (ocumEvtMirrorVaultRelationshipInitializeFailed)	Risques	Relation SnapMirror	Erreur
Échec de la mise à jour asynchrone du miroir et du coffre-fort (ocumEvtMirrorVaultRelationshipUpdateFailed)	Risques	Relation SnapMirror	Erreur
Erreur de décalage asynchrone du miroir et du coffre-fort (ocumEvtMirrorVaultRelationshipLagError)	Risques	Relation SnapMirror	Erreur
Avertissement : mise en miroir asynchrone et décalage du coffre-fort (ocumEvtMirrorVaultRelationshipLagWarning)	Risques	Relation SnapMirror	Avertissement
Échec de la resynchronisation asynchrone du miroir et du coffre-fort (ocumEvtMirrorVaultRelationshipResyncFailed)	Risques	Relation SnapMirror	Erreur

L'événement « échec de la mise à jour SnapMirror » est déclenché par le portail Active IQ (Config Advisor).

Événements Snapshot

Les événements Snapshot fournissent des informations sur l'état des snapshots, qui vous permettent de surveiller ces snapshots en cas de problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement, le nom de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Suppression automatique de l'instantané désactivée (non applicable)	Événement	Volumétrie	Informations
Suppression automatique de l'instantané activée (non applicable)	Événement	Volumétrie	Informations
Configuration de suppression automatique de snapshot modifiée (non applicable)	Événement	Volumétrie	Informations

Événements liés aux relations SnapVault

Les événements de relation SnapVault fournissent des informations sur l'état de vos relations SnapVault, ce qui vous permet de surveiller l'apparition de problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Vault asynchrone malsain(ocumEvtSnapVaultRelationshipUnHealthy)	Risques	Relation SnapMirror	Avertissement
Coupure asynchrone du coffre-fort (ocumEvtSnapVaultRelationshipStateBrokenoff)	Risques	Relation SnapMirror	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Échec de l'initialisation asynchrone du coffre-fort (ocumEvtSnapVaultRelationshipInitializeFailed)	Risques	Relation SnapMirror	Erreur
Echec de la mise à jour asynchrone du coffre-fort (ocumEvtSnapVaultRelationshipUpdateFailed)	Risques	Relation SnapMirror	Erreur
Erreur de décalage asynchrone du coffre-fort (ocumEvtSnapVaultRelationshipLagError)	Risques	Relation SnapMirror	Erreur
Avertissement de décalage asynchrone du coffre-fort (ocumEvtSnapVaultRelationshipLagWarning)	Risques	Relation SnapMirror	Avertissement
Échec de la resynchronisation asynchrone du coffre-fort (ocumEvtSnapvaultRelationshipResyncFailed)	Risques	Relation SnapMirror	Erreur

Événements relatifs aux paramètres de basculement du stockage

Les événements de basculement du stockage (SFO) vous fournissent des informations sur la désactivation ou l'absence de configuration de votre basculement du stockage, afin de pouvoir surveiller l'éventuelle des problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Storage Failover Interconnect une ou plusieurs liaisons Down (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risques	Nœud	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Basculement du stockage désactivé (fonction ocumEvtSfoSettingsDisabled)	Risques	Nœud	Erreur
Basculement du stockage non configuré(ocumEvtSfoSettingsNotConfigred)	Risques	Nœud	Erreur
Storage Failover State - Takeover(ocumEvtSfoStateTakover)	Risques	Nœud	Avertissement
Storage Failover State - Partial back(ocumEvtSfoStatePartialGiveback)	Risques	Nœud	Erreur
Statut du nœud de basculement du stockage en baisse (ocumEvtSfoNodeStatusDown)	Risques	Nœud	Erreur
Basculement de stockage impossible (ocumEvtSfoTakeoverNotPossible)	Risques	Nœud	Erreur

Événements des services de stockage

Les événements des services de stockage vous fournissent des informations sur la création et l'abonnement des services de stockage, ce qui vous permet de surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Service de stockage créé (non applicable)	Événement	Service de stockage	Informations

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Service de stockage souscrit (non applicable)	Événement	Service de stockage	Informations
Service de stockage non souscrit (non applicable)	Événement	Service de stockage	Informations

Zone d'impact : protection

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Suppression inattendue de la relation SnapMirror manageryardesokumEvtStorageServiceUprise en charge RelationshipSuppression	Risques	Service de stockage	Avertissement
Suppression inattendue du volume membre du service de stockage(otumEvtStorageServiceUnexpectedVolumeDeletion)	Gestion des	Service de stockage	Primordial

Événements du tiroir de stockage

Les événements du tiroir de stockage vous indiquent si votre tiroir de stockage est anormal pour contrôler les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Plage de tension anormale (ocumEvtShelfVoltageAbnormal)	Risques	Tiroir de stockage	Avertissement
Plage de courant anormale (ocumEvtShelfCurrentAbnormal)	Risques	Tiroir de stockage	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Température anormale(ocumEvtShelfTemperatureAbnormal)	Risques	Tiroir de stockage	Avertissement

Événements des VM de stockage

Les événements des machines virtuelles de stockage (SVM), également appelés SVM, vous fournissent des informations sur l'état de vos VM de stockage afin de pouvoir surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, 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.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Arrêt du service CIFS de la machine virtuelle de stockage (ocumEvtVserverCifsServiceStatusDown)	Gestion des	SVM	Primordial
Service SVM CIFS non configuré (non applicable)	Événement	SVM	Informations
Tentatives de connexion sans partage CIFS * (nbladeCifsNoPrivShare)	Gestion des	SVM	Primordial
Conflit de nom NetBIOS CIFS *(nbladeCifsNbNameConflitt)	Risques	SVM	Erreur
Échec de l'opération CIFS Shadow Copy * (cifsShadowCopyFailure)	Risques	SVM	Erreur
Nombreuses connexions CIFS * (nbladeCifsManyAuths)	Risques	SVM	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Connexion CIFS max. Dépassée * (nbladeCifsMaxOpenSametiFile)	Risques	SVM	Erreur
Nombre maximum de connexions CIFS par utilisateur dépassé *(nbladeCifsMaxSessPerUsrConn)	Risques	SVM	Erreur
Panne du service SVM FC/FCoE (ocumEvtVserverFcServiceStatusDown)	Gestion des	SVM	Primordial
SVM iSCSI Service Down (ocumEvtVserverIscsiServiceStatusDown)	Gestion des	SVM	Primordial
Arrêt du service NFS de la machine virtuelle de stockage (ocumEvtVserverNfsServiceStatusDown)	Gestion des	SVM	Primordial
Service SVM FC/FCoE non configuré (non applicable)	Événement	SVM	Informations
Service SVM iSCSI non configuré (non applicable)	Événement	SVM	Informations
Service SVM NFS non configuré (non applicable)	Événement	SVM	Informations
Serveur virtuel de stockage arrêté (ocumEvtVserverDown)	Risques	SVM	Avertissement
Serveur AV trop occupé pour accepter une nouvelle demande d'acquisition * (nbladeVscanConnBackPressure)	Risques	SVM	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Aucune connexion au serveur AV pour virus Scan *(nbladeVscanNoScannerConn)	Gestion des	SVM	Primordial
Aucun serveur AV enregistré *(nbladeVscanNoRegdScanner)	Risques	SVM	Erreur
Pas de connexion au serveur AV réactive *(nbladeVscanConninactive)	Événement	SVM	Informations
Tentative d'utilisateur non autorisée vers le serveur AV *(nbladeVscanBadUserPrivAccess)	Risques	SVM	Erreur
Virus détecté par le serveur AV *(nbladeVscanVirusDetected)	Risques	SVM	Erreur

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
SVM découvert (non applicable)	Événement	SVM	Informations
SVM supprimé (non applicable)	Événement	Cluster	Informations
SVM renommé (non applicable)	Événement	SVM	Informations

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS du SVM dépassé (ocumSvmIopsincident)	Gestion des	SVM	Primordial
Seuil d'avertissement d'IOPS de la SVM dépassé (ocumSvmIopsWarning)	Risques	SVM	Avertissement
Seuil critique de la SVM Mo/s violé(ocumSmMbpsincident)	Gestion des	SVM	Primordial
Seuil d'avertissement de SVM Mo/s dépassé(ocumSmMbpsWarning)	Risques	SVM	Avertissement
Seuil critique de latence SVM dépassé(ocumSvmLatencyincident)	Gestion des	SVM	Primordial
Seuil d'avertissement de latence SVM dépassé(ocumSvmLaten Avertissement)	Risques	SVM	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Journal d'audit désactivé(ocumVserverAuditLogDisabled)	Risques	SVM	Avertissement
Bannière de connexion désactivée(ocumVserverLoginBannerDisabled)	Risques	SVM	Avertissement
SSH utilise des Ciphers non sécurisés (ocumVserverSSHInSecure)	Risques	SVM	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Bannière de connexion modifiée(ocumVserverLoginBannerChanged)	Risques	SVM	Avertissement
La surveillance anti-ransomwares des VM de stockage est désactivée (antiRansomwareSvmStateDisabled)	Risques	SVM	Avertissement
Activation de la surveillance anti-ransomwares des VM de stockage (mode d'apprentissage) (antiRansomwareSvmStateDryrun)	Événement	SVM	Informations
Machine virtuelle de stockage adaptée à la surveillance anti-ransomwares (Learning mode) (ocumEvtSvmArwCandidate)	Événement	SVM	Informations

Événements de quota d'utilisateur et de groupe

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 fichiers et de disques afin de pouvoir surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Quota utilisateur ou de groupe espace disque limite souple dépassée(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risques	Quota d'utilisateur ou de groupe	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Quota utilisateur ou groupe limite matérielle de l'espace disque atteinte(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Gestion des	Quota d'utilisateur ou de groupe	Primordial
Quota utilisateur ou Groupe nombre de fichiers limite souple dépassée(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risques	Quota d'utilisateur ou de groupe	Avertissement
Quota utilisateur ou Groupe nombre de fichiers limite stricte atteinte(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Gestion des	Quota d'utilisateur ou de groupe	Primordial

Événements de volume

Les événements de volume fournissent des informations sur l'état des volumes qui vous permettent de surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement, le nom de l'interruption, 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.

Domaine d'impact : disponibilité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Volume restreint (ocumEvtVolumeRestricted)	Risques	Volumétrie	Avertissement
Volume hors ligne (ocumEvtVolumeOffline)	Gestion des	Volumétrie	Primordial
Volume partiellement disponible(ocumEvtVolumePartiallyAvailable)	Risques	Volumétrie	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Volume démonté (non applicable)	Événement	Volumétrie	Informations
Montage en volume (non applicable)	Événement	Volumétrie	Informations
Volume remonté (non applicable)	Événement	Volumétrie	Informations
Chemin de jonction de volume inactif (ocumEvtJuncVolumePathInactif)	Risques	Volumétrie	Avertissement
Taille automatique du volume activée (non applicable)	Événement	Volumétrie	Informations
Taille automatique du volume désactivée (non applicable)	Événement	Volumétrie	Informations
Capacité maximale de la taille automatique du volume modifiée (non applicable)	Événement	Volumétrie	Informations
Taille d'incrément de taille automatique du volume modifiée (non applicable)	Événement	Volumétrie	Informations

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Espace Volume à provisionnement fin en péril (provisionnement fin)ProvisionVolumeSpaceAtRisk)	Risques	Volumétrie	Avertissement
Erreur de fonctionnement de l'efficacité du volume (OcumEvtVolumeEfficiencyOperationError)	Risques	Volumétrie	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Espace du volume plein (ocumEvtVolumeFull)	Risques	Volumétrie	Erreur
Espace du volume presque plein (ocumEvtNearVolumelyFull)	Risques	Volumétrie	Avertissement
Volume Logical Space Full * (Volume LogicalSpaceFull)	Risques	Volumétrie	Erreur
Espace logique du volume presque plein * (volume LogicalSpaceNearyFull)	Risques	Volumétrie	Avertissement
Volume Logical Space Normal * (volume LogicalSpaceAllOK)	Événement	Volumétrie	Informations
Espace de réserve Snapshot du volume saturé (ocumEvtSnapshotFull)	Risques	Volumétrie	Avertissement
Trop de copies Snapshot (ocumEvtSnapshotTooMoany)	Risques	Volumétrie	Erreur
Volume qtree quota overengagé(ocumEvtVolumeQtreeQuotaOverengagé)	Risques	Volumétrie	Erreur
Quota qtree volume presque overengagé(ocumEvtVolumeQtreeQuotaAlmostOverdéterminé)	Risques	Volumétrie	Avertissement
Taux de croissance du volume anormal (ocumEvtVolumeGrowthRateAbnormal)	Risques	Volumétrie	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Nombre de jours jusqu'à la fin (ocumEvtVolumeDaysUntilFullSoon)	Risques	Volumétrie	Erreur
Garantie d'espace sur le volume désactivée (non applicable)	Événement	Volumétrie	Informations
Garantie d'espace sur volume activée (non applicable)	Événement	Volumétrie	Informations
Garantie d'espace Volume modifiée (non applicable)	Événement	Volumétrie	Informations
Jours de réserve Snapshot du volume jusqu'à la version complète (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risques	Volumétrie	Erreur
Les composants FlexGroup présentent des problèmes d'espace * (flexGroupConstituentsHaveSpaceIsles)	Risques	Volumétrie	Erreur
État de l'espace des composants FlexGroup OK *(flexGroupConstituentsSpaceStatusAllOK)	Événement	Volumétrie	Informations
Les composants FlexGroup ont des problèmes d'inodes * (flexGroupConstituentsHaveInodesIssues)	Risques	Volumétrie	Erreur

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
État des inodes des composants FlexGroup OK * (flexGroupConstituentsInodesStatusAllOK)	Événement	Volumétrie	Informations
Échec de la taille automatique du volume WAFL * (waflVolAutoSizeFail)	Risques	Volumétrie	Erreur
Taille automatique du volume WAFL effectuée * (waflVolAutoSizeDone)	Événement	Volumétrie	Informations
Volume FlexGroup utilisé à plus de 80 %*	Gestion des	Volumétrie	Erreur
Volume FlexGroup utilisé à plus de 90 %*	Gestion des	Volumétrie	Primordial
Anomalie de l'efficacité du stockage volume (cimVolumeCfficationAvertissement)	Risques	Volumétrie	Avertissement
Volume Snapshot Reserve sous-utilisé (Volume SnaphovReserveUnderutilizedWarning)	Événement	Volumétrie	Avertissement
Volume Snapshot Reserve sous-utilisé (Volume SnaphotsReserveUnderutilizedClean)	Événement	Volumétrie	Avertissement

Zone d'impact : configuration

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Volume renommé (non applicable)	Événement	Volumétrie	Informations

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Volume découvert (non applicable)	Événement	Volumétrie	Informations
Volume supprimé(non applicable)	Événement	Volumétrie	Informations

Zone d'impact : performances

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Seuil d'avertissement IOPS max du volume QoS dépassé (ocumQosVolumeMaxIopsWarning)	Risques	Volumétrie	Avertissement
Seuil d'avertissement de volume QoS max. Mo/s dépassé (ocumQosVolumeMaxMbpsWarning)	Risques	Volumétrie	Avertissement
Seuil d'avertissement maximal IOPS/To du volume QoS dépassé (ocumQosVolumeMaxIopsPerTbWarning)	Risques	Volumétrie	Avertissement
Seuil de latence du volume de la charge de travail dépassé, tel que défini par la politique de niveau de service de performance(ocumConformanceLatenceWarning)	Risques	Volumétrie	Avertissement
Seuil critique d'IOPS du volume dépassé (nombre d'octets VolumeIopsincident)	Gestion des	Volumétrie	Primordial
Seuil d'avertissement IOPS du volume dépassé (nombre d'octets VolumeIopsAvertissement)	Risques	Volumétrie	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Nombre de Mo/s de seuil critique dépassé (ocumVolumeMbpsincident)	Gestion des	Volumétrie	Primordial
Seuil d'avertissement du volume MB/s dépassé(AocumVolumeMbpsWarning)	Risques	Volumétrie	Avertissement
Seuil critique de latence du volume dépassé (ocumVolumeLatencyincident)	Gestion des	Volumétrie	Primordial
Seuil d'avertissement de latence du volume dépassé (avertissement cumVolumeLatencyWarning)	Risques	Volumétrie	Avertissement
Rapport volume cache Miss ratio (seuil critique dépassé) (ocumVolumeCacheMissa incident)	Gestion des	Volumétrie	Primordial
Seuil d'avertissement de taux de Miss du cache volume dépassé (ocumVolumeCachemissile RatioWarning)	Risques	Volumétrie	Avertissement
Latence du volume et seuil critique d'IOPS dépassé (ocumVolumeLatenceIops incident)	Gestion des	Volumétrie	Primordial
Latence du volume et seuil d'avertissement d'IOPS dépassé (ocumVolumeLatenceIops Avertissement)	Risques	Volumétrie	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Latence du volume et seuil critique en Mo/s dépassé (ocumVolumeLatenceMbpsincident)	Gestion des	Volumétrie	Primordial
Latence du volume et seuil d'avertissement MB/s rompues (ocumVolumeLatenceMbpsWarning)	Risques	Volumétrie	Avertissement
Latence du volume et performances globales utilisation de la capacité critique franchissement du seuil critique (ocumVolumeAgrégeContreteContreteÉvolutivité des capacitéUsedincident)	Gestion des	Volumétrie	Primordial
Latence du volume et performances de l'agrégat seuil d'avertissement de capacité utilisée dépassé(ocumVolumeAgrégeContreteContreteContreteÉvolutivité des capacitéUsedAvertissement)	Risques	Volumétrie	Avertissement
Latence du volume et utilisation des agrégats seuil critique dépassé (ocumVolumeLatengeAgrégeUtilationincident)	Gestion des	Volumétrie	Primordial
Seuil d'avertissement de latence du volume et d'utilisation des agrégats dépassé (ocumVolumeLatengeAgrégeUtilAvertissement)	Risques	Volumétrie	Avertissement

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Latence du volume et performance du nœud capacité utilisée seuil critique dépassé(ocumVolumeCPerfContrettyEnseUsedincident)	Gestion des	Volumétrie	Primordial
Latence du volume et performances du nœud seuil d'avertissement de capacité utilisée dépassé(ocumVolumeCPerfContreteContretcapacités UsedAvertissement)	Risques	Volumétrie	Avertissement
Latence du volume et performance du nœud capacité utilisée : seuil critique de basculement dépassé (ocumVolumeAgrégeContreteContreteContreteContretedessurincidents)	Gestion des	Volumétrie	Primordial
Latence du volume et performances du nœud utilisation - seuil d'avertissement de basculement dépassé(ocumVolumeAgrégeContreteContreteContreteContreteContretousContreteousContretousde l'espace de stockage)	Risques	Volumétrie	Avertissement
Latence du volume et utilisation du nœud seuil critique dépassé (ocumVolumeLatenceNodeUtiationincident)	Gestion des	Volumétrie	Primordial
Latence du volume et seuil d'avertissement d'utilisation du nœud dépassé(ocumVolumeLatenceAvertissement de nœud)	Risques	Volumétrie	Avertissement

Zone d'impact : sécurité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
La surveillance anti-ransomware des volumes est activée (mode actif) (antiRansomwareVolumeStateEnabled)	Événement	Volumétrie	Informations
La surveillance anti-ransomwares des volumes est désactivée (antiRansomwareVolumeStateDisabled)	Risques	Volumétrie	Avertissement
Activation de la surveillance anti-ransomware des volumes (mode d'apprentissage) (antiRansomwareVolumeStateDryrun)	Événement	Volumétrie	Informations
La surveillance des volumes anti-ransomwares est mise en pause (mode d'apprentissage) (antiRansomwareVolumeStateDryrunPaow)	Risques	Volumétrie	Avertissement
La surveillance anti-ransomware des volumes est mise en pause (mode actif) (antiRansomwareVolumeStateEnablePaused)	Risques	Volumétrie	Avertissement
Désactivation de la surveillance des volumes anti-ransomwares (antiRansomwareVolumeStateDisableInProgress)	Risques	Volumétrie	Avertissement
Activité ransomware (callHomeRansomwareActivitySeen)	Gestion des	Volumétrie	Primordial

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Volume adapté à la surveillance anti-ransomwares (Learning mode) (ocumEvtVolumeArwCandidate)	Événement	Volumétrie	Informations
Volume adapté pour la surveillance anti-ransomwares (Active mode) (ocumVolumeSuiteForActiveRansomwaredétection)	Risques	Volumétrie	Avertissement
Volume présentant des alertes anti-ransomware bruyantes (antiRansomwareFeatureNoisyVolume)	Risques	Volumétrie	Avertissement

Zone d'impact : protection des données

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
Volume dont la protection par snapshots locaux est insuffisante (VolumeLacksLocalProtectionWarning)	Risques	Volumétrie	Avertissement
Le volume a une protection snapshots locale insuffisante (Volume : LacksLocalProtectionClean)	Risques	Volumétrie	Avertissement

Événements d'état de déplacement de volumes

Les événements d'état de déplacement de volume vous indiquent l'état de déplacement de volume afin de pouvoir surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et de l'interruption, le niveau d'impact, le type de source et la gravité.

Zone d'impact : capacité

Nom de l'événement (nom de l'argument)	Niveau d'impact	Type de source	Gravité
État du déplacement du volume : en cours (non applicable)	Événement	Volumétrie	Informations
Etat du déplacement du volume - échec (ocumEvtVolumeMoveFailed)	Risques	Volumétrie	Erreur
Statut de déplacement de volume : terminé (non applicable)	Événement	Volumétrie	Informations
Déplacement de volume - report du basculement (oocumEvtVolumeMoveCutOverreporté)	Risques	Volumétrie	Avertissement

Description des fenêtres d'événement et des boîtes de dialogue

Cet événement vous signale tout problème rencontré au sein de votre environnement. Vous pouvez utiliser la page d'inventaire gestion des événements et la page 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 qu'il envoie des notifications lorsqu'un événement est généré ou lorsqu'il est affecté à un utilisateur. Vous pouvez également configurer les mécanismes de notification. Par exemple, des notifications peuvent être envoyées sous forme d'e-mails ou de traps SNMP.

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

E-mail

Cette zone vous permet de configurer les paramètres d'e-mail suivants pour la notification d'alerte :

- **De l'adresse**

  Spécifie l'adresse e-mail à partir de laquelle la notification d'alerte est envoyée. Cette valeur est également utilisée comme adresse de 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 permet de configurer les paramètres suivants du serveur SMTP :

- **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 le SMTPUTH est activé sur le serveur SMTP.

- **Mot de passe**

  Spécifie le mot de passe SMTP. Le nom d'utilisateur SMTP est requis uniquement lorsque le SMTPUTH 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**

  Cette case permet une communication sécurisée entre le serveur SMTP et le serveur de gestion à l'aide des protocoles TLS/SSL (également appelés start_tls et StartTLS).

- **Utiliser SSL**

  Cette case permet une communication sécurisée entre le serveur SMTP et le serveur de gestion à l'aide du protocole SSL.

SNMP

Cette zone vous permet de configurer les paramètres d'interruption SNMP suivants :

- **Version**

  Spécifie la version SNMP que vous souhaitez utiliser en fonction du type de sécurité dont vous avez besoin. Les options disponibles sont la version 1, la version 3, la version 3 avec authentification et la version 3 avec authentification et chiffrement. La valeur par défaut est version 1.

- **Hôte destination Trap**

  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 sortant », doivent être identiques pour tous les hôtes de la liste.

- **Port de déroutement sortant**

  Spécifie le port par lequel le serveur SNMP reçoit les interruptions envoyées par le serveur de gestion.

  La valeur par défaut est 162.

- **Communauté**

  Chaîne de communauté pour accéder à l'hôte.

- **ID moteur**

  Spécifie l'identifiant unique de l'agent SNMP et est automatiquement généré par le serveur de gestion. L'ID de 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 traps SNMP, vous pouvez télécharger le depuis le "MIB Active IQ Unified Manager"site de support NetApp.

Page d'inventaire gestion des événements

La page d'inventaire gestion des événements vous permet d'afficher une liste des événements en cours et leurs propriétés. Vous pouvez effectuer des tâches telles que la

validation, la résolution et l'attribution d'événements. Vous pouvez également ajouter une alerte pour des événements spécifiques.

Les informations de cette page sont automatiquement actualisées toutes les 5 minutes pour s'assurer que les nouveaux événements les plus récents sont affichés.

Composants du filtre

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 Affichage pour faire votre choix dans une liste prédéfinie de sélections de filtres.

  Cela inclut des éléments tels que tous les événements actifs (nouveaux et acquittés), les événements de performances actifs, les événements qui m'ont été 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.
- Le bouton filtre qui lance le volet filtres vous permet de sélectionner tous les champs et attributs de champ disponibles pour affiner la liste des événements.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Affecter à**

  Vous permet de sélectionner l'utilisateur auquel l'événement est affecté. Lorsque vous affectez un événement à un utilisateur, le nom d'utilisateur et l'heure à laquelle vous avez affecté l'événement sont ajoutés dans la liste des événements pour les événements sélectionnés.

  - Moi

    Attribue l'événement à l'utilisateur actuellement connecté.

  - Un autre utilisateur

    Affiche la boîte de dialogue attribuer un propriétaire qui vous permet d'affecter ou de réaffecter l'événement à d'autres utilisateurs. Vous pouvez également annuler l'affectation d'événements en laissant le champ de propriété vide.

- **Acknowledge**

  Acquitte 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 accuser réception d'événements d'information.

- **Marquer comme résolu**

  Vous permet de changer l'état de l'événement en 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 les mesures correctives nécessaires à l'événement, vous devez marquer l'événement comme résolu.

- **Ajouter alerte**

  Affiche la boîte de dialogue Ajouter une alerte qui vous permet d'ajouter des alertes pour les événements sélectionnés.

- **Rapports**

  Permet d'exporter les détails de la vue d'événement en cours vers un fichier de valeurs séparées par des virgules (.csv) ou un document PDF.

- **Afficher/Masquer le sélecteur de colonne**

  Vous permet de choisir les colonnes qui s'affichent sur la page et de sélectionner l'ordre dans lequel elles sont affichées.

Liste des événements

Affiche les détails de tous les événements commandés par heure déclenchée.

Par défaut, la vue tous les événements actifs s'affiche pour afficher les événements nouveaux et acquittés des sept jours précédents ayant un niveau d'impact d'incident ou de risque.

- **Temps déclenché**

  Heure à laquelle l'événement a été généré.

- **Gravité**

  Gravité de l'événement : critique ( ), erreur ( ), Avertissement ( ) et informations ( ).

- **État**

  État de l'événement : nouveau, validé, résolu ou Obsolète.

- **Niveau d'impact**

  Niveau d'impact des événements : incident, risque, événement ou mise à niveau.

- **Zone d'impact**

  Domaine de l'impact de l'événement : disponibilité, capacité, performances, protection, configuration, Ou la sécurité.

- **Nom**

  Nom de l'événement. Vous pouvez sélectionner le nom pour afficher la page Détails de l'événement pour cet événement.

- **Source**

  Nom de l'objet sur lequel l'événement s'est produit. Vous pouvez sélectionner le nom pour afficher la page

d’informations de santé ou de performances de cet objet.

Lorsqu’une violation de la politique de 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 règle s’affichent dans la page Détails de l’événement.

- **Type de source**

  Type d’objet (par exemple, Storage VM, Volume ou qtree) auquel l’événement est associé.

- **Affecté à**

  Nom de l’utilisateur auquel l’événement est affecté.

- **Origine de l’événement**

  Qu’il s’agisse du « portail Active IQ » ou directement de « Active IQ Unified Manager »,

- **Nom d’annotation**

  Nom de l’annotation qui est attribuée à l’objet de stockage.

- **Notes**

  Nombre de notes ajoutées pour un événement.

- **Jours en suspens**

  Nombre de jours depuis la génération initiale de l’événement.

- **Temps attribué**

  Temps écoulé depuis l’affectation de l’événement à un utilisateur. Si le temps écoulé dépasse une semaine, l’heure à laquelle l’événement a été attribué à un utilisateur s’affiche.

- **Reconnu par**

  Nom de l’utilisateur qui a reconnu l’événement. Le champ est vide si l’événement n’est pas validé.

- **Heure reconnue**

  Temps écoulé depuis l’accusé de réception de l’événement. Si le temps écoulé dépasse une semaine, l’heure à laquelle l’événement a été reconnu s’affiche.

- **Résolu par**

  Nom de l’utilisateur qui a résolu l’événement. Le champ est vide si l’événement n’est pas résolu.

- **Temps résolu**

  Temps écoulé depuis la résolution de l’événement. Si le temps écoulé dépasse une semaine, l’heure à laquelle l’événement a été résolu s’affiche.

- **Obsolète**

  Heure à laquelle l’état de l’événement est devenu Obsolète.

Page de détails de l'événement

Dans la page Détails des événements, vous pouvez afficher les détails d'un événement sélectionné, tels que la gravité d'événement, le niveau d'impact, la zone d'impact et la source d'événement. Vous pouvez également afficher des informations supplémentaires sur les résolutions possibles pour résoudre le problème.

- **Nom de l'événement**

  Nom de l'événement et heure de la dernière vue de l'événement.

  Pour les événements sans performances, alors que l'événement est à l'état Nouveau ou validé, les dernières informations affichées ne sont pas connues et sont donc masquées.

- **Description de l'événement**

  Brève description de l'événement.

  Dans certains cas, une raison pour l'événement déclenché est fournie dans la description de l'événement.

- **Composant en conflit**

  Pour les événements de performances dynamiques, cette section affiche les icônes qui représentent les composants logiques et physiques du cluster. Si un composant est en conflit, son icône est entourée et mise en surbrillance rouge.

  Voir *Cluster components et pourquoi ils peuvent être dans contention* pour une description des composants qui sont affichés ici.

Les sections informations sur les événements, diagnostic du système et actions suggérées sont décrites dans d'autres rubriques.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Icône Notes**

  Permet d'ajouter ou de mettre à jour une note concernant l'événement et de consulter toutes les notes laissées par les autres utilisateurs.

Menu actions

- **Attribuer à moi**

  Vous affecte l'événement.

- **Affecter à d'autres**

  Ouvre la boîte de dialogue attribuer un propriétaire qui permet d'affecter ou de réaffecter 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 affecté sont ajoutés dans la liste des événements pour les événements sélectionnés.

Vous pouvez également annuler l'affectation d'événements en laissant le champ de propriété vide.

- **Acknowledge**

  Acquitte les événements sélectionnés pour ne pas continuer à recevoir de 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 (acquittés par) pour les événements sélectionnés. Lorsque vous reconnaissez un événement, vous êtes responsable de la gestion de cet événement.

- **Marquer comme résolu**

  Vous permet de changer l'état de l'événement en 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 (résolus par) pour les événements sélectionnés. Après avoir pris les mesures correctives nécessaires à l'événement, vous devez marquer l'événement comme résolu.

- **Ajouter alerte**

  Affiche la boîte de dialogue Ajouter une alerte qui vous permet d'ajouter une alerte pour l'événement sélectionné.

La section informations sur les événements s'affiche

La section informations sur les événements de la page Détails de l'événement vous permet d'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 sont pas applicables au type d'événement sont masqués. Vous pouvez afficher les détails de l'événement suivant :

- **Heure de déclenchement d'événement**

  Heure à laquelle l'événement a été généré.

- **État**

  État de l'événement : nouveau, validé, résolu ou Obsolète.

- **Cause obsolète**

  Les actions qui ont causé l'obsolescence de l'événement, par exemple, le problème a été corrigé.

- **Durée de l'événement**

  Pour les événements actifs (nouveaux et acquittés), il s'agit du temps entre la détection et l'heure où l'événement a été analysé pour la dernière fois. Pour les événements obsolètes, il s'agit du temps entre la détection et la résolution de l'événement.

  Ce champ est affiché pour tous les événements de performance et pour les autres types d'événements uniquement après leur résolution ou leur obsolescence.

- **Dernière vue**

  Date et heure auxquelles l'événement a été vu pour la dernière fois comme actif.

  Pour les événements de performances, 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 performances tant que l'événement est actif. Pour d'autres types d'événements, lorsque l'état Nouveau ou validé est défini sur non, ce contenu n'est pas mis à jour et le champ est donc masqué.

- **Gravité**

  Gravité de l'événement : critique ( ), erreur ( ), Avertissement ( ) et informations ( ).

- **Niveau d'impact**

  Niveau d'impact des événements : incident, risque, événement ou mise à niveau.

- **Zone d'impact**

  Domaine de l'impact de l'événement : disponibilité, capacité, performances, protection, configuration, Ou la sécurité.

- **Source**

  Nom de l'objet sur lequel l'événement s'est produit.

  Lorsque vous affichez les détails d'un événement de stratégie QoS partagé, ce champ contient jusqu'à trois des objets de charge de travail qui consomment le plus d'IOPS ou de Mo/sec.

  Vous pouvez cliquer sur le lien du nom de la source pour afficher la page d'informations de santé ou de performances de cet objet.

- **Annotations 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'état sur les clusters, les SVM et les volumes.

- **Groupes de sources**

  Affiche les noms de tous les groupes dont l'objet impacté est membre.

  Ce champ s'affiche uniquement pour les événements d'état sur les clusters, les SVM et les volumes.

- **Type de source**

  Type d'objet (par exemple SVM, Volume ou qtree) auquel l'événement est associé.

- **Sur Cluster**

  Nom du cluster sur lequel l'événement s'est produit.

  Vous pouvez cliquer sur le lien du nom du cluster pour afficher la page d'informations de santé ou de performances de ce cluster.

- **Nombre d'objets affectés**

Nombre d’objets affectés par l’événement.

Vous pouvez cliquer sur le lien 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**

  Nombre de volumes affectés par cet événement.

  Ce champ s’affiche uniquement pour les événements de performance sur des nœuds ou des agrégats.

- **Politique déclenchée**

  Nom de la police de seuil qui a émis l’événement.

  Vous pouvez placer le curseur sur le nom de la stratégie pour afficher les détails de la stratégie de seuil. Pour les règles de QoS adaptative, la règle définie, la taille de bloc et le type d’allocation (espace alloué ou espace utilisé) sont également affichés.

  Ce champ s’affiche uniquement pour les événements de performance.

- **ID règle**

  Pour les événements de la plate-forme 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.

- **Affecté à**

  Nom de la personne affectée au travail sur l’événement.

- **Paramètres d’alerte**

  Les informations suivantes concernant les alertes s’affichent :

  - Si aucune alerte n’est associée à l’événement sélectionné, un lien **Ajouter alerte** s’affiche.

    Vous pouvez ouvrir la boîte de dialogue Ajouter une alerte en cliquant sur le lien.

  - Si une alerte est 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.

  - Si plusieurs alertes sont associées à l’événement sélectionné, le nombre d’alertes s’affiche.

    Vous pouvez ouvrir la page 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**

  Date et heure auxquelles la dernière notification d'alerte a été envoyée.

- **Envoyer par**

  Mécanisme utilisé pour envoyer la notification d'alerte : e-mail ou interruption SNMP.

- **Exécution de script précédente**

  Nom du script exécuté lors de la génération de l'alerte.

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 propose quelques actions afin que vous puissiez tenter de résoudre l'événement par vous-même. Les actions suggérées sont personnalisées en fonction du type d'événement ou du type de seuil non atteint.

Cette zone s'affiche uniquement pour certains types d'événements.

Dans certains cas, il existe des liens **aide** 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, de ONTAP System Manager, d'OnCommand Workflow Automation, des commandes de l'interface de ligne de commande d'ONTAP ou une combinaison de ces outils.

Vous devez considérer les actions proposées ici comme une référence pour résoudre cet événement. L'action que vous prenez pour résoudre cet événement doit être basée sur le contexte de votre environnement.

Pour analyser l'objet et l'événement en détail, cliquez sur le bouton **analyser la charge de travail** pour afficher la page analyse de la charge de travail.

Unified Manager effectue un diagnostic approfondi et fournit une résolution unique. Lorsqu'elles sont disponibles, ces résolutions sont affichées avec un bouton **Fix it**. Cliquez sur ce bouton pour que Unified Manager corrige le problème à l'origine de l'événement.

Pour les événements relatifs à la plateforme Active IQ, cette section peut contenir un lien vers un article de la base de connaissances NetApp qui décrit le problème et les solutions 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 que la section diagnostic du système affiche

La section diagnostic du système de la page Détails de l'événement fournit des informations qui peuvent vous aider à diagnostiquer les problèmes qui pourraient être responsables de l'événement.

Cette zone s'affiche uniquement pour certains événements.

Certains événements de performances fournissent des graphiques pertinents à l'événement généré. Cela

inclut généralement le tableau IOPS ou Mbit/s et un graphique sur la latence pour les dix jours précédents. Lorsqu'elle est organisée, vous pouvez voir les composants de stockage qui affectent le plus la latence ou qui sont affectés par la latence lorsque l'événement est actif.

Pour les événements de performance dynamique, les graphiques suivants sont affichés :

- Latence de la charge de travail : affiche l'historique de latence des charges de travail les plus victimes, dominantes ou requins au niveau du composant lors des conflits.
- Charge de travail : affiche des détails sur l'utilisation des charges de travail du composant de cluster dans les conflits.
- Activité de ressource - affiche les statistiques de performances historiques du composant de cluster en conflit.

D'autres graphiques s'affichent lorsque certains composants du cluster présentent des conflits.

D'autres événements fournissent une brève description du type d'analyse exécuté sur l'objet de stockage par le système. Dans certains cas, il y aura une ou plusieurs lignes, un pour chaque composant analysé, pour des règles de performance 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 le cadre de 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 globale des événements.

Vous ne pouvez accéder à cette page que si vous avez le rôle Administrateur d'applications ou Administrateur de stockage.

Boutons de commande

Les boutons de commande 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 avez choisi de désactiver précédemment.

- **Règles de chargement**

  Lance la boîte de dialogue règles de chargement qui permet aux sites sans accès réseau externe de télécharger manuellement le fichier de règles Active IQ vers Unified Manager. Les règles sont exécutées autour de messages AutoSupport du cluster afin de générer des événements destinés à la configuration du système, au câblage, aux meilleures pratiques et à la disponibilité, tels que définis par la plateforme Active IQ.

- **Abonnez-vous à EMS Events**

Lance la boîte de dialogue s'abonner aux événements EMS, qui vous permet de vous abonner à la réception d'événements EMS spécifiques des clusters que vous surveillez. Le EMS collecte des informations sur les événements se produisant sur le cluster. Lorsqu'une notification est reçue pour un événement EMS auquel vous êtes abonné, un événement Unified Manager est généré avec le niveau de gravité approprié.

Vue liste

La vue liste affiche (sous forme de tableau) des informations sur les événements désactivés. Vous pouvez utiliser les filtres de colonne 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.

Désactiver la boîte de dialogue 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 spécifique ou pour un ensemble d'événements.

Vous devez avoir le rôle Administrateur d'applications ou 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**

  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 s'affiche également avec le nom de l'événement.

Boutons de commande

Les boutons de commande 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**

  Supprime les modifications et ferme la boîte de dialogue.

Gestion des alertes

Vous pouvez configurer des alertes pour qu'elles envoient automatiquement des notifications lorsque des événements ou événements spécifiques de certains types de sévérité se produisent. Vous pouvez également associer une alerte à un script exécuté lorsqu'une alerte est déclenchée.

Quelles sont les alertes

Les événements se produisent en permanence, mais 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 qu'un objet passe hors ligne. Vous pouvez également associer une alerte à un script exécuté lorsqu'une alerte est déclenchée.

Les critères de filtre incluent la classe d'objet, le nom ou la gravité de l'événement.

Les informations contenues dans un e-mail d'alerte

Dans les e-mails d'alerte Unified Manager, vous indiquez le type d'événement, la gravité de l'événement, le nom de la règle ou le seuil non respecté pour provoquer l'événement et la description de l'événement. L'e-mail fournit également un lien hypertexte pour chaque événement qui vous permet d'afficher la page de détails de l'événement dans l'interface utilisateur.

Les 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 a un changement important pendant une période de collecte, cela peut provoquer le déclenchement d'un événement critique et d'un événement d'avertissement en même temps pour la même stratégie de seuil. Dans ce cas, vous pouvez recevoir un e-mail pour l'événement d'avertissement et un autre pour l'événement critique. En effet, Unified Manager vous permet de vous abonner séparément pour recevoir des alertes en cas d'avertissement ou de franchissement de seuils critiques.

Voici un exemple d'e-mail d'alerte :

```
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
```

Ajout d’alertes

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

Ce dont vous aurez besoin

- Vous devez avoir configuré des 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 adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l’événement, vous devez l’avoir ajouté à Unified Manager à l’aide de la page scripts.
- Vous devez avoir le rôle Administrateur d’applications ou 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 de l’alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.

2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis 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 **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que 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 à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Evénements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel 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 affectez 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 qui a été précédemment sélectionné. En outre, 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 les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme 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 averti toutes les 15 minutes

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

1. Cliquez sur **Nom** et entrez **`HealthTest`** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
   a. Entrez **`abc`** dans le champ **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-la dans la zone Ressources sélectionnées.

c. Cliquez sur **exclure**, saisissez `xyz` dans le champ **Nom contient**, puis cliquez sur **Ajouter**.

3. Cliquez sur **Evénements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions**, puis saisissez `sample@domain.com` dans le champ alerte ces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Instructions d'ajout d'alertes

Vous pouvez ajouter des alertes en fonction d'une ressource, par exemple un cluster, un nœud, un agrégat ou un volume, ainsi que les événements d'un type de sévérité spécifique. Pour bénéficier de cette meilleure pratique, vous pouvez ajouter une alerte à l'un de vos objets stratégiques après avoir ajouté le cluster auquel cet objet appartient.

Vous pouvez utiliser les instructions et considérations suivantes pour créer des alertes afin de gérer efficacement vos systèmes :

- Description de l'alerte

  Vous devez fournir une description pour l'alerte afin qu'elle vous aide à suivre efficacement vos alertes.

- Ressources

  Vous devez décider quelle ressource physique ou logique requiert une alerte. Vous pouvez inclure et exclure des ressources, selon les 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 des alertes pour tous les objets de cette catégorie.

  > 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 pour tous les clusters, vous recevrez des alertes uniquement pour les événements critiques du cluster. Vous ne recevez pas d'alertes concernant 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, le cas échéant, quel type de gravité.

- Événements sélectionnés

  Si vous ajoutez une alerte en fonction du type d'événement généré, vous devez décider des événements qui nécessitent une alerte.

  Si vous sélectionnez une gravité d'événement, mais que vous ne sélectionnez aucun événement individuel (si vous laissez la colonne « Evénements sélectionnés » vide), vous recevrez alors 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 un trap 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 qu'elle envoie une notification répétée aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte. Si vous souhaitez que la notification d'événement soit répétée jusqu'à l'accusé de réception de l'événement, 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.

Ajout d'alertes en cas d'événements de performances

Vous pouvez configurer les alertes en cas d'événements de performance individuels comme n'importe quel autre événement reçu par Unified Manager. Par ailleurs, si vous souhaitez traiter tous les événements de performance comme si un e-mail est envoyé à la même personne, vous pouvez créer une seule alerte pour vous informer en cas de déclenchement d'événements de performance critiques ou d'avertissement.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

L'exemple ci-dessous montre comment créer un événement pour toutes les latence critique, les IOPS et les Mo/sec. Vous pouvez utiliser cette même méthodologie pour sélectionner des événements à partir de tous les compteurs de performances et pour tous les événements d'avertissement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Ne sélectionnez aucune ressource sur la page **Ressources**.

   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 **Evénements** et effectuez les opérations suivantes :
   a. Dans la liste gravité de l'événement, sélectionnez **critique**.
   b. Dans le champ Nom de l'événement contient, entrez `latency`, puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
   c. Dans le champ Nom de l'événement contient, entrez `iops`, puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
   d. Dans le champ Nom de l'événement contient, entrez `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 **Alert thavent Users**.
7. Configurez toutes les autres options de cette page pour l'émission des interruptions SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Test des alertes

Vous pouvez tester une alerte pour vérifier que vous l'avez correctement configurée. 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 à l'aide de l'alerte test.

Ce dont vous aurez besoin

- Vous devez avoir configuré des paramètres de notification tels que l'adresse électronique des destinataires, le serveur SMTP et le trap SNMP.

  Le serveur Unified Manager peut utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.

- Vous devez avoir affecté un script et configuré le script pour qu'il s'exécute lorsque l'alerte est générée.
- Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, sélectionnez l'alerte que vous souhaitez tester, puis cliquez sur **Test**.

   Un e-mail d'alerte de test est envoyé aux adresses e-mail que vous avez spécifiées lors de la création de l'alerte.

Activation et désactivation des alertes pour les événements résolus et Obsolète

Pour tous les événements que vous avez configurés pour envoyer des alertes, un message d'alerte est envoyé lorsque ces événements passent par tous les États disponibles : nouveau, validé, 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Par défaut, les alertes ne sont pas envoyées pour les événements lorsqu'elles passent à l'état résolu et Obsolète.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, effectuez l'une des actions suivantes en utilisant le curseur à côté de l'élément **alertes pour les événements résolus et Obsolète** :

Pour…	Procédez comme ça…
Arrêter l'envoi d'alertes car les événements sont résolus ou obsolètes	Déplacez le curseur vers la gauche
Démarrer l'envoi d'alertes lorsque les événements sont résolus ou obsolètes	Déplacez le curseur vers la droite

Exclusion de volumes de destination de reprise après incident de la génération des 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. Si vous avez configuré la reprise sur incident pour les SVM, toutefois, les volumes source et de destination ont le même nom, vous recevez des alertes pour les deux volumes.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez désactiver les alertes relatives aux volumes de destination de reprise sur incident en excluant les volumes qui ont le nom du SVM de destination. Ceci est possible car l'identifiant des événements de volume contient le nom du 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 exclut la génération de l'alerte sur un volume portant le même nom sur le SVM « vs1-dr ».

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

Étapes

1. Cliquez sur **Nom** et entrez 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 **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-la dans la zone **Ressources sélectionnées**.
3. Sélectionnez l'onglet **exclure**, sélectionnez **Volume**, entrez `vs1-dr` dans le champ **Nom contient**, puis

cliquez sur **Ajouter**.

Cela exclut la génération de l'alerte du volume « vol1 » sur la SVM « vs1-dr ».

4. Cliquez sur **Evénements** 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 **Alert thavent Users**.
6. Configurez toutes les autres options de cette page pour émettre des interruptions SNMP et exécuter un script, puis cliquez sur **Enregistrer**.

Affichage des 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 des alertes telles que la description de l'alerte, la méthode de notification et la fréquence, les événements qui déclenchent l'alerte, les destinataires des alertes et les ressources affectées, telles que les clusters, les agrégats et les volumes.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.

   La liste des alertes s'affiche dans la page Configuration des alertes.

Modification des 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, sélectionnez l'alerte que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier alerte**, modifiez le nom, les ressources, les événements et les actions, selon les besoins.

   Vous pouvez modifier ou supprimer le script associé à l'alerte.

4. Cliquez sur **Enregistrer**.

Suppression des alertes

Vous pouvez supprimer une alerte lorsqu'elle n'est plus requise. Par exemple, vous pouvez supprimer une alerte créée pour une ressource spécifique lorsque cette ressource n'est plus surveillée par Unified Manager.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Sur la page **Configuration des alertes**, sélectionnez les alertes que vous souhaitez supprimer, puis 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 les 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, l'état, la méthode de notification et la fréquence des notifications de l'alerte. Vous pouvez également ajouter, modifier, supprimer, activer ou désactiver des alertes à partir de cette page.

Vous devez avoir le rôle Administrateur d'applications ou 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 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 ajout ou modification.

- **Alertes pour les événements résolus et Obsolète**

  Permet d'activer ou de désactiver l'envoi d'alertes lorsque des événements sont déplacés vers les États résolu ou Obsolète. Cela peut aider les utilisateurs à recevoir des notifications inutiles.

Vue liste

La vue liste affiche, au format tabulaire, des informations sur les alertes créées. Vous pouvez utiliser les filtres de colonne pour personnaliser les données affichées. Vous pouvez également sélectionner une alerte pour afficher plus d'informations à ce sujet dans la zone de détails.

- **Statut**

  Indique 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 des interruptions 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 validé, résolu ou déplacé à l'état Obsolète.

Zone de détails

La zone de détails fournit des informations supplémentaires 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.

- **Inclut**

  Affiche le groupe de ressources pour lequel vous souhaitez déclencher l'alerte.

- **Exclusion**

  Affiche le groupe de ressources pour lequel 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 validé, résolu ou déplacé à 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 d'e-mails**

  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 informer lorsqu'un événement particulier est généré. Vous pouvez ainsi résoudre le problème rapidement et réduire ainsi l'impact sur votre environnement. Vous pouvez créer des alertes pour une seule ressource ou un ensemble de ressources, et pour les événements d'un type de gravité particulier. Vous pouvez également spécifier la méthode de notification et la fréquence des alertes.

Vous devez avoir le rôle Administrateur d'applications ou 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 de 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 pouvez inclure les ressources pour lesquelles vous souhaitez déclencher des alertes. Vous pouvez spécifier une chaîne de texte pour regrouper les ressources correspondant 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 des 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 à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure 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 les événements selon une gravité spécifique 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**

  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.

- **Avertir 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 qui a été précédemment sélectionné. En outre, 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 validé, résolu ou déplacé à 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 de temps spécifiée

- **Lancer le trap 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 à partir de **Storage Management** > **Feature Settings**.

Boutons de commande

- **Enregistrer**

  Crée une alerte et ferme la boîte de dialogue.

- **Annuler**

  Supprime les modifications et ferme la boîte de dialogue.

Boîte de dialogue Modifier l'alerte

Vous pouvez modifier les propriétés des alertes, telles que la ressource avec 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**

  Permet de modifier le nom de l'alerte.

- **Description de l'alerte**

  Vous permet de spécifier une description de 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 pouvez inclure les ressources pour lesquelles vous souhaitez déclencher des alertes. Vous pouvez spécifier une chaîne de texte pour regrouper les ressources correspondant 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 des 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 basés sur une gravité spécifique 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**

  Permet de sélectionner des événements dont le nom contient les caractères spécifiés.

Actions

Cette zone vous permet de spécifier la méthode de notification et la fréquence de notification.

- **Avertir 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**

  Permet de modifier la fréquence à laquelle le serveur de gestion envoie des notifications jusqu'à ce que

l'événement soit validé, résolu ou déplacé à 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 de temps spécifiée

- **Lancer le trap 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

- **Enregistrer**

  Enregistre les modifications et ferme la boîte de dialogue.

- **Annuler**

  Supprime les modifications et ferme la boîte de dialogue.

Gestion des 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 les scripts vers Unified Manager et de les exécuter est activée par défaut. Si votre entreprise ne souhaite pas autoriser cette fonctionnalité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité à partir de **Storage Management** > **Feature Settings**.

Informations connexes

"Activation et désactivation de la capacité à télécharger des scripts"

Fonctionnement des scripts avec les alertes

Vous pouvez associer une alerte à votre script afin que le script soit exécuté lorsqu'une alerte est générée pour un événement dans Unified Manager. Vous pouvez utiliser ces 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, des actions sont prises en fonction de votre script personnalisé pour ce type d'événement, et les actions **Fix it** ne sont pas disponibles par défaut sur la page actions de gestion ou 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 de vos scripts et recueillir des informations d'événement associées ou modifier des objets de stockage.

Exemple pour obtenir des 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 les valeurs de sortie suivantes s'affichent :

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Ajout de scripts

Vous pouvez ajouter des scripts dans Unified Manager et les associer aux alertes. Ces scripts sont exécutés automatiquement lorsqu'une alerte est générée. Ils vous permettent d'obtenir des informations sur les objets de stockage pour lesquels l'événement est généré.

Ce dont vous aurez besoin

- Vous devez avoir créé et enregistré les scripts que vous souhaitez ajouter au serveur Unified Manager.
- Les formats de fichier pris en charge pour les scripts sont Perl, Shell, PowerShell, Python et les `.bat` fichiers.

Plateforme sur laquelle Unified Manager est installé	Langues prises en charge
VMware	Scripts Perl et Shell
Linux	Scripts Perl, Python et Shell
Fenêtres	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 ne prennent en charge que 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 pas créés à un endroit quelconque du dossier d'installation d'Unified Manager.

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez télécharger des scripts personnalisés et collecter des informations détaillées sur 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 à partir de **Storage Management** > **Feature Settings**.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **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

"Activation et désactivation de la capacité à télécharger des scripts"

Suppression de scripts

Vous pouvez supprimer un script d'Unified Manager lorsque le script n'est plus nécessaire ou valide.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Le script ne doit pas être associé à une alerte.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **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 le script s'exécute correctement lorsqu'une alerte est générée pour un objet de stockage.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir téléchargé un script au format de fichier pris en charge vers Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **scripts**.
2. Dans la page **scripts**, ajoutez votre script de test.
3. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
4. Dans la page **Configuration des alertes**, effectuez l'une des opérations suivantes :

Pour…	Procédez comme ça…
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 **Test**.

   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 du stockage, vous pouvez utiliser les commandes de l'interface de ligne de commande pour effectuer des requêtes sur les objets de stockage (par exemple, sur les clusters, les agrégats, les volumes). Qtrees et LUN. Vous pouvez utiliser les commandes CLI pour interroger la base de données interne Unified Manager et la base de données ONTAP. Vous pouvez également utiliser les commandes de l'interface

de ligne de commandes dans des scripts exécutés au début ou à la fin d'une opération ou lorsqu'une alerte est déclenchée.

Toutes les commandes doivent être précédées de la commande `um cli login`, ainsi que d'un nom d'utilisateur et d'un mot de passe valides pour l'authentification.

> Pour exécuter la commande *um run*, assurez-vous que votre compte dispose de l'accès *console* application.

Commande CLI	Description	Sortie
`um cli login -u <username> [-p <password>]`	Se connecte à l'interface de ligne de commandes. En raison des implications de sécurité, vous devez entrer uniquement le nom d'utilisateur suivant l'option « -u ». Lorsqu'il est utilisé de cette manière, vous êtes invité à saisir le mot de passe et le mot de passe ne sera pas saisi dans la table historique ou processus. La session expire au bout de trois heures à compter de la date de connexion, après laquelle l'utilisateur doit se reconnecter.	Affiche le message correspondant.
`um cli logout`	Se déconnecte de l'interface de ligne de commandes.	Affiche le message correspondant.
`um help`	Affiche toutes les sous-commandes de premier niveau.	Affiche toutes les sous-commandes de premier niveau.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Le moyen le plus simple d'exécuter une commande sur un ou plusieurs hôtes. Principalement utilisé pour créer des scripts d'alerte afin d'obtenir ou d'effectuer une opération sur ONTAP. L'argument optionnel de délai définit une limite de temps maximale (en secondes) pour que la commande se termine 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 lues à partir de la base de données sont autorisées. Toutes les opérations de mise à jour, d'insertion ou de suppression ne sont pas prises en charge.	Les résultats sont affichés sous forme de tableau. Si un jeu vide est renvoyé, ou s'il y a une erreur de syntaxe ou une requête incorrecte, il affiche le message d'erreur approprié.

Commande CLI	Description	Sortie
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 effectuées. 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, alors les deux protocoles seront tentées 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 est tentée. Cette commande ne peut être exécutée que par l'administrateur du stockage.	Invite l'utilisateur à accepter le certificat et imprime le message correspondant.
um datasource list [<datasource-id>]	Affiche les sources de données des 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.
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 du 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.

Commande CLI	Description	Sortie
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Permet de définir une ou plusieurs options. La commande ne peut être exécutée que par l'administrateur du 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 un filtrage sur l'objet spécifié. -q est applicable 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 le objectType et "1" est l'objectId. La commande répertorie toutes les LUN du cluster ayant l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Répertorie les VM de stockage après filtrage sur l'objet spécifié. ObjectType peut être lun, qtree, cluster, volume, quota, ou svm. Par exemple : **`um svm list -cluster 1`** Dans cet exemple, "-cluster" est le objectType et "1" est l'objectId. La commande répertorie tous les VM de stockage du cluster dont l'ID est 1.	Affiche les valeurs suivantes sous forme de tableau : `Name and Cluster ID.`

Commande CLI	Description	Sortie
`um qtree list [-q] [ -ObjectType <object-id>]`	Le répertorie les qtrees après un filtrage sur l'objet spécifié. -q est applicable à toutes les commandes pour n'afficher aucun en-tête. ObjectType peut être lun, qtree, cluster, volume, quota, ou svm. Par exemple : **`um qtree list -cluster 1`** Dans cet exemple, "-cluster" est le objectType et "1" est l'objectId. La commande répertorie tous les qtrees du cluster dont l'ID est 1.	Affiche les valeurs suivantes sous forme de tableau : `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	Répertorie les disques après filtrage sur l'objet spécifié. ObjectType peut être un disque, un agrégat, un nœud ou un cluster. Par exemple : **`um disk list -cluster 1`** Dans cet exemple, "-cluster" est le 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.`
`um cluster list [-q] [-ObjectType <object-id>]`	Répertorie les clusters après le filtrage sur l'objet spécifié. ObjectType peut être disque, agrégat, nœud, cluster, lun, qtree, volume, quota ou svm. Par exemple : **`um cluster list -aggr 1`** Dans cet exemple, "-aggr" correspond à objectType et "1" à objectId. La commande répertorie le cluster auquel l'agrégat avec l'ID 1 appartient.	Affiche les valeurs suivantes sous forme de tableau : `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`

Commande CLI	Description	Sortie
`um cluster node list [-q] [-ObjectType <object-id>]`	Le répertorie les nœuds du cluster après un filtrage sur l'objet spécifié. ObjectType peut être un disque, un agrégat, un nœud ou un cluster. Par exemple : **`um cluster node list -cluster 1`** Dans cet exemple, "-cluster" est le 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`.
`um volume list [-q] [-ObjectType <object-id>]`	Répertorie les volumes après le filtrage sur l'objet spécifié. ObjectType peut être lun, qtree, cluster, volume, quota, svm ou agrégat. Par exemple : **`um volume list -cluster 1`** Dans cet exemple, "-cluster" est le objectType et "1" est l'objectId. La commande répertorie tous les volumes du cluster ayant l'ID 1.	Affiche les valeurs suivantes sous forme de tableau `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Répertorie les utilisateurs de quota après le filtrage sur l'objet spécifié. ObjectType peut être qtree, cluster, volume, quota ou svm. Par exemple : **`um quota user list -cluster 1`** Dans cet exemple, "-cluster" est le objectType et "1" est l'objectId. La commande répertorie tous les utilisateurs du quota au sein du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau `ID, Name, SID and Email`.

Commande CLI	Description	Sortie
um aggr list [-q] [-ObjectType <object-id>]	Répertorie les agrégats après un filtrage sur l'objet spécifié. ObjectType peut être un disque, un agrégat, un nœud, un cluster ou un volume. Par exemple : **um aggr list -cluster 1** Dans cet exemple, "-cluster" est le objectType et "1" est l'objectId. La commande répertorie tous les agrégats du cluster ayant l'ID 1.	Affiche les valeurs suivantes sous forme de tableau Aggr ID, and Aggr Name .
um event ack <event-ids>	Accepte 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>	Attribue 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 ID.	Affiche les valeurs suivantes sous forme de tableau Source, Source type, Name, Severity, State, User and Timestamp .
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.

La page scripts

La page scripts vous permet d'ajouter vos scripts personnalisés à Unified Manager. Vous pouvez associer ces scripts à des alertes pour activer la reconfiguration automatique des objets de stockage.

La page scripts vous permet d'ajouter ou de supprimer des scripts d'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 liste

La vue liste affiche, au format tabulaire, 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 avoir le rôle Administrateur d'applications ou Administrateur de stockage.

- **Sélectionnez fichier script**

  Vous permet de sélectionner un script pour l'alerte.

- **Description**

  Vous permet de spécifier une description pour le script.

Contrôle et gestion des performances du cluster

Présentation de la surveillance des performances Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) fournit des fonctions de contrôle des performances et d'analyse de la source des événements pour les systèmes exécutant le logiciel NetApp ONTAP.

Unified Manager vous aide à identifier les charges de travail qui surutilisent les composants du cluster et à réduire les performances des autres charges de travail sur le cluster. En définissant des règles de seuil de performances, vous pouvez également spécifier des valeurs maximales pour certains compteurs de performances afin que les événements soient générés lorsque le seuil est dépassé. Unified Manager vous alerte concernant ces événements de performance, afin de mettre en place des actions correctives et de rétablir les performances normales. Vous pouvez afficher et analyser les événements dans l'interface utilisateur Unified Manager.

Unified Manager surveille les performances de deux types de charges de travail :

- Les charges de travail définies par l'utilisateur

  Ces charges de travail sont constituées de volumes FlexVol et de volumes FlexGroup que vous avez créés dans votre cluster.

- Les charges de travail définies par le système

  Ces workloads sont constitués d'une activité système interne.

Fonctionnalités de contrôle des performances de Unified Manager

Unified Manager collecte et analyse les statistiques de performances à partir des systèmes exécutant le logiciel ONTAP. Il utilise des seuils de performances dynamiques et des seuils de performances définis par l'utilisateur pour surveiller un grand nombre de compteurs de performances sur de nombreux composants du cluster.

Un temps de réponse élevé (latence) indique que l'objet de stockage, par exemple un volume, fonctionne plus lentement qu'avec la normale. Ce problème indique également que les performances des applications client qui utilisent le volume ont diminué. Unified Manager identifie le composant de stockage qui se trouve à l'endroit où se trouve le problème de performance et fournit une liste des actions que vous pouvez entreprendre pour résoudre le problème de performance.

Unified Manager comprend les fonctionnalités suivantes :

- Surveille et analyse les statistiques de performances des workloads à partir d'un système exécutant le logiciel ONTAP.
- Suivi des compteurs de performances pour les clusters, les nœuds, les agrégats, les ports, les SVM, Volumes, LUN, espaces de noms NVMe et interfaces réseau (LIFS).
- Affiche des graphiques détaillés qui correspondent à l'activité des charges de travail dans le temps, y compris les IOPS (opérations), les Mo/s (débit), la latence (temps de réponse), l'utilisation la capacité de performance et le ratio cache.

- Vous permet de créer des règles de seuils de performances définies par l'utilisateur qui déclenchent des événements et envoient des alertes par e-mail lorsque les seuils sont atteints.
- Utilise des seuils définis par le système et des seuils de performances dynamiques qui sont des informations sur l'activité des workloads pour identifier et vous alerter des problèmes de performances.
- Identifie les règles de qualité de service (QoS) et les règles PSLs (Performance Service Level) appliquées à vos volumes et LUN.
- Identifie clairement le composant de cluster en conflit.
- Identifie les charges de travail qui surutilisent 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 disponibilité et de protection du stockage des données. Les deux interfaces utilisateur sont l'interface utilisateur Web de Unified Manager et la console de maintenance.

Si vous souhaitez utiliser les fonctions de protection dans Unified Manager, vous devez également installer et configurer OnCommand Workflow Automation (WFA).

Interface Web Unified Manager

L'interface utilisateur Web Unified Manager permet à un administrateur de surveiller et de résoudre les problèmes liés à la capacité de stockage, à la disponibilité et à la protection des données en cluster.

Ces sections décrivent les 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 Unified Manager.

Console de maintenance

La console de maintenance Unified Manager permet à un administrateur de surveiller, diagnostiquer et résoudre les problèmes liés au système d'exploitation, à la mise à niveau de la version, aux problèmes d'accès utilisateur et aux problèmes de réseau liés au serveur Unified Manager lui-même. Si l'interface utilisateur Web de 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 des données sur la configuration et les performances du cluster

L'intervalle de collecte des données de configuration *cluster* est de 15 minutes. Par exemple, une fois que vous avez ajouté un cluster, il faut 15 minutes pour afficher les informations relatives au cluster dans l'interface utilisateur Unified Manager. Cet intervalle s'applique lorsque vous apportez également des modifications à un cluster.

Par exemple, si vous ajoutez deux nouveaux volumes à un SVM dans un cluster, ces nouveaux objets

s’affichent dans l’interface utilisateur après l’intervalle d’interrogation suivant, qui peut prendre jusqu’à 15 minutes.

Unified Manager collecte les statistiques de performance 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 historiques de performances de cinq minutes et 180 jours de données historiques de performance d’une heure. Vous pouvez ainsi consulter des détails très précis sur les performances du mois en cours et les tendances générales de performances sur une période allant jusqu’à un an.

Les sondages sur la collecte des données sont compensés par quelques minutes pour que les données de chaque cluster ne soient pas envoyées simultanément, ce qui pourrait affecter les performances.

Le tableau suivant décrit les activités de collecte réalisées par Unified Manager :

Activité	Intervalle de temps	Description
Sondage sur les statistiques de performance	Toutes les 5 minutes	Collecte des données de performances en temps réel sur chaque cluster
Analyse statistique	Toutes les 5 minutes	Après chaque sondage de statistiques, Unified Manager compare les données collectées aux seuils dynamiques, définis par l’utilisateur et définis par le système. Si un seuil de performances a été dépassé, Unified Manager génère des événements et envoie des e-mails aux utilisateurs spécifiés s’il est configuré pour le faire.
Interrogation de configuration	Toutes les 15 minutes	Collecte d’informations d’inventaire détaillées par cluster afin d’identifier tous les objets de stockage (nœuds, SVM, volumes, etc.)
Récapitulatif	Toutes les heures	Le récapitule les 12 dernières collectes de données de performances 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 suppression des données	Tous les jours après minuit	Analyse les données d'un cluster afin d'établir des seuils dynamiques pour la latence du volume et les IOPS pendant les 24 prochaines heures. Supprime de la base de données toutes les données de performances de cinq minutes antérieures à 30 jours.
Suppression des données	Tous les jours après 2 heures du matin	Supprime de la base de données tous les événements de plus de 180 jours et les seuils dynamiques de plus de 180 jours.
Suppression des données	Tous les jours après 3:30	Supprime de la base de données toute donnée de performance d'une heure antérieure à 180 jours.

Qu'est-ce qu'un cycle de collecte de continuité des données

Un cycle de collecte de la continuité des données récupère les données de performances en dehors du cycle de collecte en temps réel des performances du cluster qui s'exécute, par défaut, toutes les cinq minutes. Les collections de continuité des données permettent à Unified Manager de combler les lacunes des données statistiques qui se produisent lorsqu'il n'est pas en mesure de collecter des données en temps réel.

Unified Manager effectue des sondages 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 d'historique des performances pendant les 15 jours précédents. Vous pouvez ainsi afficher deux semaines d'informations historiques sur les performances d'un cluster quelques heures après son ajout.

  En outre, 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 l'heure.

  Si le sondage 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 ces informations manquantes. Sans la collecte de continuité des données, la période de collecte suivante est ignorée.

- Unified Manager n'a pas été accessible depuis un certain temps, puis il est de nouveau en ligne, comme dans les cas suivants :
  - Il a été redémarré.

    - Elle a été arrêtée lors d'une mise à niveau du logiciel ou lors de la création d'un fichier de sauvegarde.
    - Une panne réseau est réparée.
- Un cluster a été inaccessible pendant une période et retourne en ligne, comme dans les situations suivantes :
    - Une panne réseau est réparée.
    - Une connexion réseau étendue lente a retardé la collecte normale des données de performances.

Un cycle de collecte de la continuité des données peut collecter un maximum de 24 heures de données historiques. Si Unified Manager est indisponible pendant plus de 24 heures, un écart s'affiche dans les données de performance dans les pages interface utilisateur.

Un cycle de collecte de continuité des données et un cycle de collecte des données en temps réel ne peuvent pas être exécutés en même temps. Le cycle de collecte de la continuité des données doit se terminer avant le début de la collecte des données de performance en temps réel. Lorsque la collecte de la continuité des données est nécessaire pour collecter plus d'une heure de données historiques, un message s'affiche en haut du volet Notifications.

Signification de l'horodatage dans les données et les événements collectées

L'horodatage qui apparaît dans les données d'état et de performance collectées, ou qui apparaît comme temps de détection d'un événement, est basé sur l'heure du cluster ONTAP, ajustée au fuseau horaire défini sur le navigateur Web.

Nous vous recommandons vivement 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 spécifique, vous pouvez vérifier que l'heure du cluster a été correctement définie.

Navigation dans les workflows de performances dans l'interface graphique d'Unified Manager

L'interface Unified Manager fournit de nombreuses pages pour la collecte et l'affichage des informations relatives aux performances. Le panneau de navigation de gauche vous permet de naviguer jusqu'aux pages de l'interface graphique et vous utilisez des onglets et des liens sur les pages pour afficher et configurer des informations.

Vous utilisez toutes les pages suivantes pour contrôler et dépanner les informations relatives aux performances du cluster :

- page de tableau de bord
- pages d'inventaire des objets réseau et de stockage
- pages de détails sur les objets de stockage (y compris l'explorateur de performances)
- pages de configuration et de configuration
- pages événements

Connexion à l'interface utilisateur

Vous pouvez vous connecter à l'interface utilisateur de Unified Manager à l'aide d'un navigateur Web pris en charge.

Ce dont vous aurez besoin

- Le navigateur Web doit respecter la configuration minimale requise.

  Consultez la matrice d'interopérabilité à l'adresse "mysupport.netapp.com/matrix" pour obtenir 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 de fonction**.

Étapes

1. Entrez l'URL dans votre navigateur Web, où l'URL correspond à l'adresse IP ou au 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, il se peut que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez accepter le risque de continuer l'accès ou installer un certificat numérique signé par l'autorité de certification pour l'authentification du serveur. . Sur l'écran de connexion, saisissez votre nom d'utilisateur et votre mot de passe.

Si vous vous connectez à l'interface utilisateur Unified Manager est protégé à l'aide de l'authentification SAML, vous entrez vos identifiants sur la page de connexion au fournisseur d'identités au lieu de la page de connexion de Unified Manager.

La page Tableau de bord s'affiche.

> Si le serveur Unified Manager n'est pas initialisé, une nouvelle fenêtre de navigateur affiche la première fenêtre de l'assistant d'expérience. Vous devez entrer un destinataire d'e-mail initial auquel les alertes par e-mail seront envoyées, le serveur SMTP qui traitera les communications par e-mail et si AutoSupport est activé pour envoyer les informations relatives à votre installation d'Unified Manager au support technique. L'interface de Unified Manager s'affiche une fois ces informations terminées.

Interface graphique et chemins de navigation

Unified Manager offre une grande flexibilité et vous permet d'effectuer plusieurs tâches de différentes manières. Il existe de nombreux chemins de navigation que vous découvrirez lorsque vous travaillez dans Unified Manager. Bien que toutes les combinaisons possibles de navigations ne puissent pas être affichées, vous devriez vous familiariser avec quelques-uns des scénarios les plus communs.

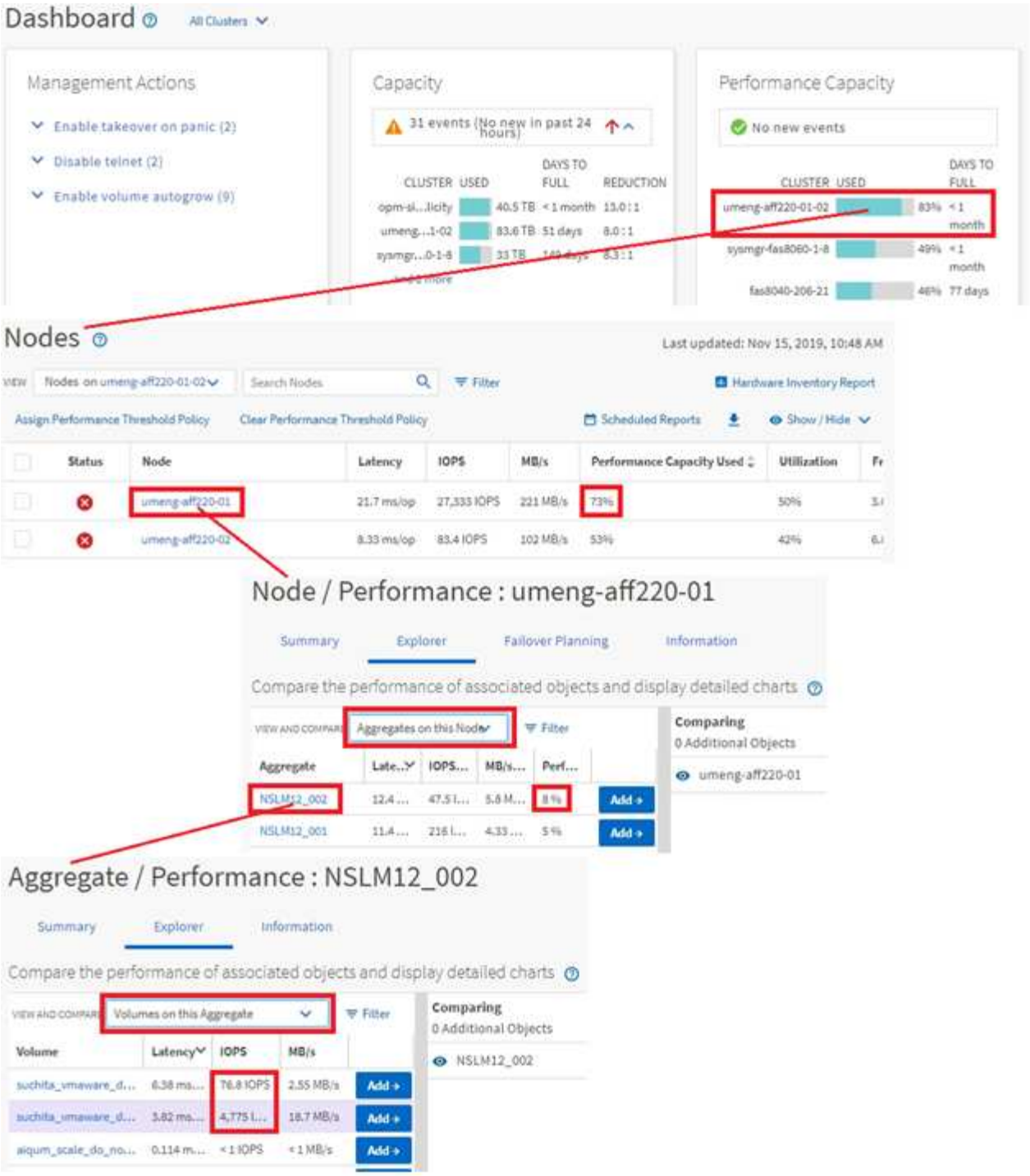
Contrôle de la navigation sur les objets du cluster

Vous pouvez contrôler les performances de tous les objets de tout cluster géré par Unified Manager. La surveillance des objets de stockage vous fournit des informations sur la performance du cluster et des objets, et inclut le contrôle des événements de performance. Vous pouvez afficher les performances et les événements de manière générale, ou étudier plus en détail les événements de performances et de performance des objets.

Voici un exemple de nombreuses navigations d'objets de cluster possibles :

1. Dans la page Tableau de bord, vérifiez les détails du volet capacité de performance pour identifier le cluster qui utilise la capacité la plus performante et cliquez sur le graphique à barres pour accéder à la liste des nœuds de ce cluster.
2. Identifiez le nœud dont la capacité en termes de performances est la plus élevée utilisée, puis cliquez sur ce nœud.
3. Sur la page Explorateur de nœuds/performances, cliquez sur **Aggregates sur ce noeud** dans le menu Afficher et Comparer.
4. Identifiez l'agrégat qui utilise la capacité de performances la plus élevée, puis cliquez sur cet agrégat.
5. Dans la page de l'explorateur de performances/d'agrégats, cliquez sur **volumes sur cet agrégat** dans le menu View and compare.
6. Identifiez les volumes qui utilisent le plus d'IOPS.

Vous devez étudier ces volumes afin de déterminer si vous devez appliquer une règle de QoS ou une règle de niveau de service de performances, ou modifier les paramètres des règles, de sorte que ces volumes n'utilisent pas un pourcentage aussi important d'IOPS sur le cluster.



Contrôle la navigation sur les performances du cluster

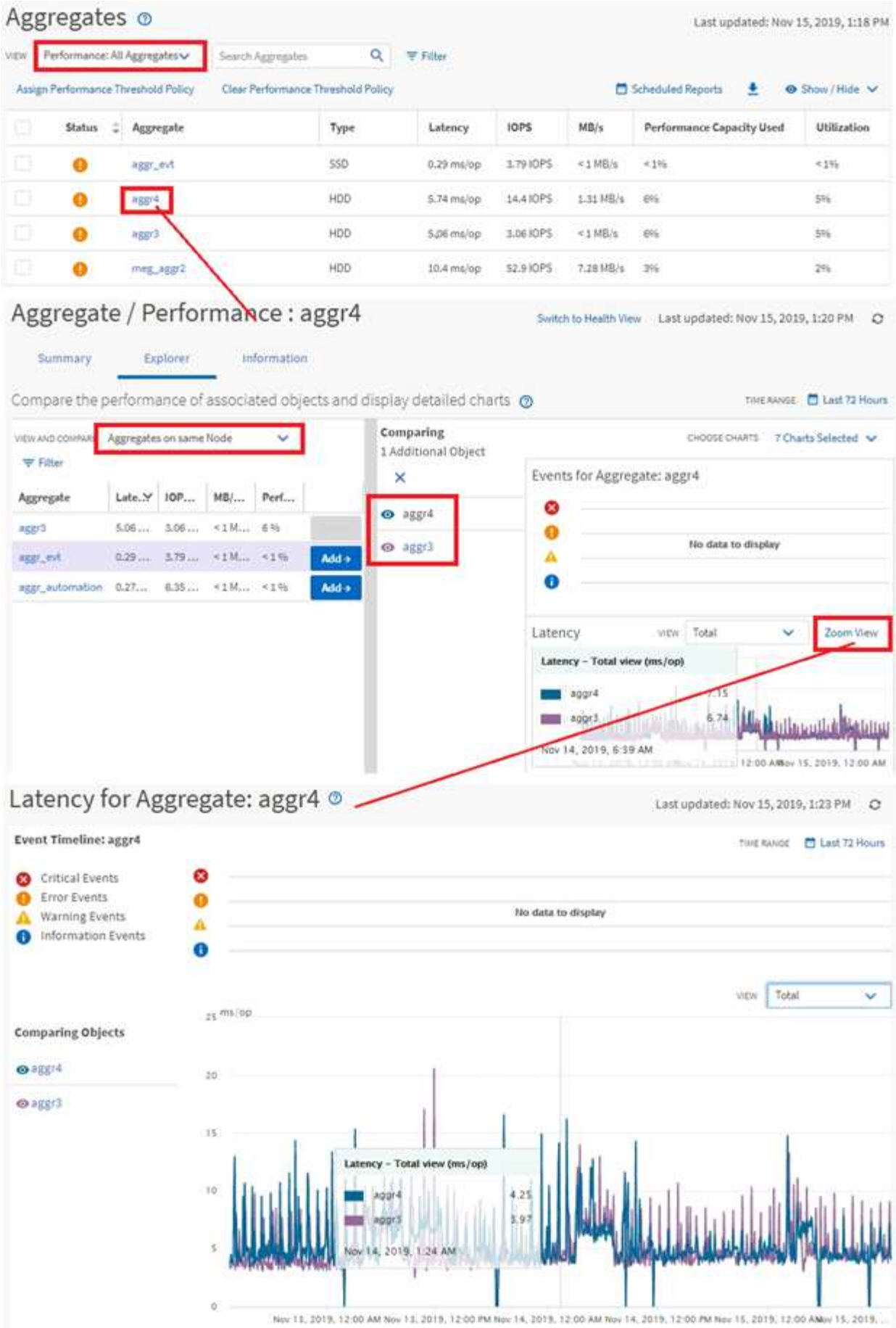
Vous pouvez contrôler les performances de tous les clusters gérés par Unified Manager. La surveillance des clusters offre une vue d'ensemble des performances du cluster et des objets, et inclut la surveillance des événements de performance. Vous pouvez afficher les performances et les événements de haut niveau. Vous pouvez également étudier plus en détail les événements de performance et de performance du cluster et des objets.

Voici un exemple de nombreux chemins de navigation de performances de cluster possibles :

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Pour afficher des informations sur les performances de ces agrégats, sélectionnez la vue performances : tous les agrégats.
3. Identifiez l'agrégat à examiner et cliquez sur son nom pour accéder à la page de l'explorateur de performances/agrégat.
4. Vous pouvez également sélectionner d'autres objets à comparer avec cet agrégat dans le menu Affichage et comparaison, puis ajouter un des objets au volet comparaison.

   Les statistiques des deux objets s'affichent dans les compteurs pour comparaison.

5. Dans le volet comparaison situé à droite de la page de l'Explorateur, cliquez sur **vue Zoom** dans l'un des diagrammes pour afficher des détails sur 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
Late...
IOP...
MB/...
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)
aggr4
7.15
aggr3
6.74
Nov 14, 2019, 6:39 AM
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
Information Events
No data to display
VIEW
Total
Comparing Objects
aggr4
aggr3
ms/op
25
20
15
10
5
0
Latency – Total view (ms/op)
aggr4
4.25
aggr3
3.97
Nov 14, 2019, 1:24 AM
Nov 13, 2019, 12:00 AM
Nov 13, 2019, 12:00 PM
Nov 14, 2019, 12:00 AM
Nov 14, 2019, 12:00 PM
Nov 15, 2019, 12:00 AM

Navigation dans l'investigation des événements

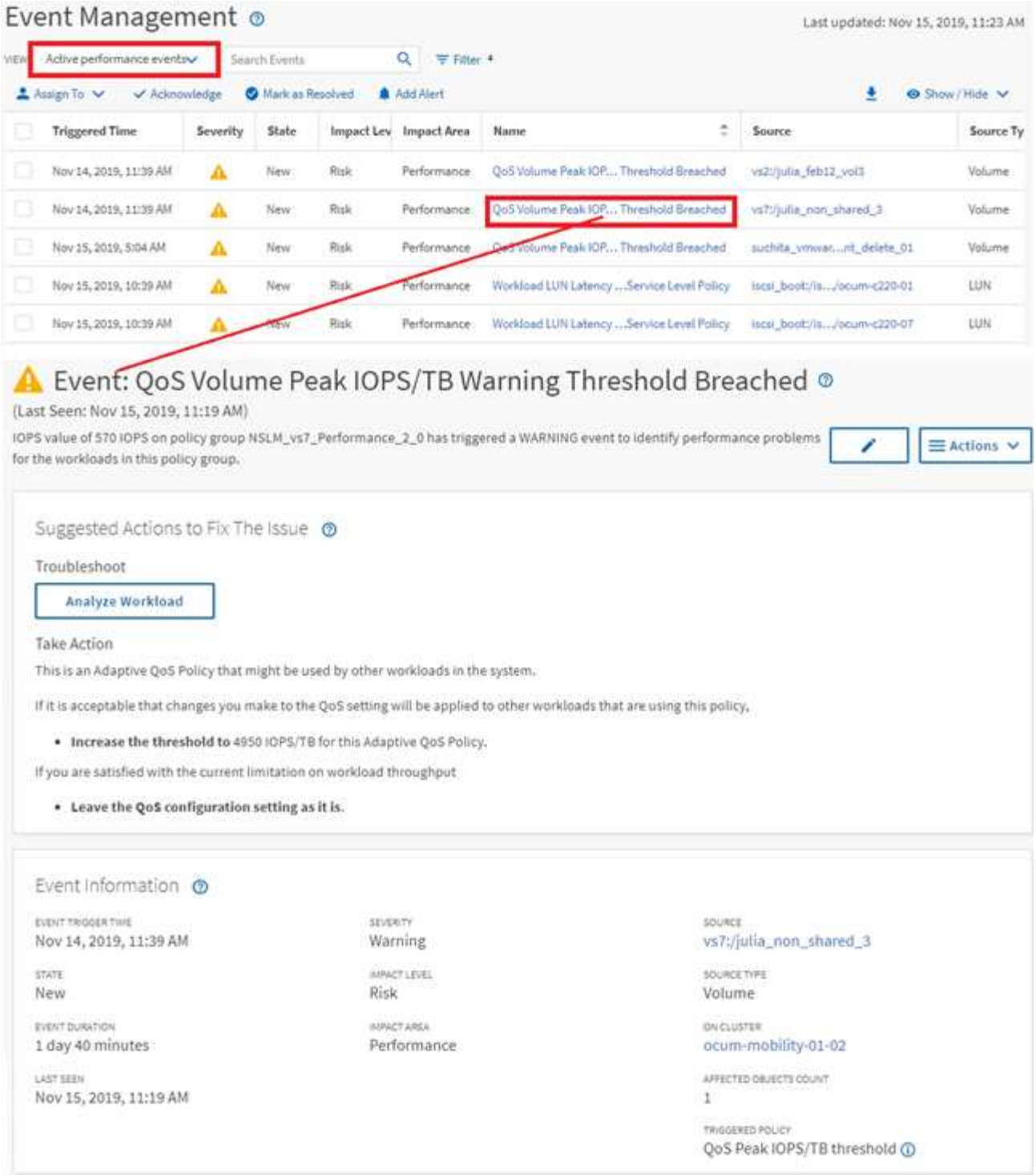
Les pages de détail des événements d'Unified Manager vous donnent une vue d'ensemble de tous les événements de performance. Cela peut être bénéfique lors de l'étude des événements de performance, du dépannage et de l'ajustement des performances du système.

En fonction du type d'événement de performance, vous pouvez voir l'un des deux types de pages détaillées d'événements :

- Page de détails des événements pour les événements de stratégie de seuil définis par l'utilisateur et par le système
- Page de détails des événements pour les événements de stratégie de seuil dynamique

C'est un exemple de navigation pour l'investigation d'événement.

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.
2. Dans le menu Affichage, cliquez sur **événements de performances actifs**.
3. Cliquez sur le nom de l'événement que vous souhaitez examiner et la page Détails de l'événement s'affiche.
4. Affichez la description de l'événement et examinez les actions suggérées (le cas échéant) pour afficher plus de détails sur l'événement qui peut vous aider à résoudre le problème. Vous pouvez cliquer sur le bouton **Analyze Workload** pour afficher des graphiques de performances détaillés afin de mieux analyser le problème.



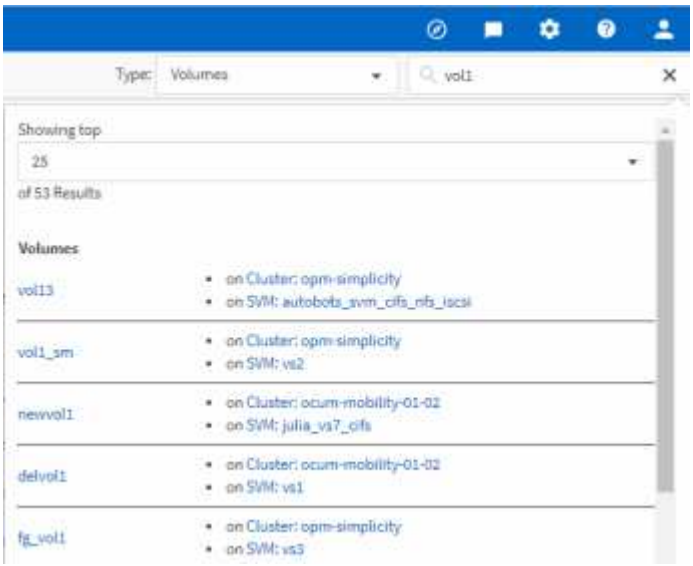
Recherche d’objets de stockage

Pour accéder rapidement à un objet spécifique, vous pouvez utiliser le champ **Rechercher tous les objets de stockage** en haut de la barre de menus. 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 classés par type d’objet de stockage et vous pouvez les filtrer dans le menu déroulant. Une recherche valide doit contenir au moins trois caractères.

La recherche globale affiche le nombre total de résultats, mais seuls les 25 meilleurs résultats sont accessibles. Pour cette raison, la fonction de recherche globale peut être considérée comme un outil de raccourci pour trouver des éléments spécifiques si vous connaissez les éléments que vous voulez rapidement localiser. 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 effectuer une recherche simultanée sur 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 cluster
- Nœuds : noms des nœuds
- Agrégats : noms des agrégats
- SVM : noms des SVM
- Volumes : noms des volumes
- LUN : chemins de LUN



Les LIFs et les ports ne sont pas interrogeables dans la barre de recherche globale.

Dans cet exemple, le type d'objet Volume est sélectionné dans la liste déroulante. La saisie de « vol » dans le champ **Rechercher tous les objets de stockage** affiche la 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 de l'explorateur de performances de cet objet. Pour la recherche d'événements, cliquez sur un élément dans le résultat de la recherche pour accéder à la page Détails de l'événement.

Filtrage du contenu de la page d'inventaire

Vous pouvez filtrer les données de page d'inventaire dans Unified Manager pour localiser rapidement des données en fonction de critères spécifiques. Vous pouvez utiliser le filtrage pour affiner le contenu des pages Unified Manager afin d'afficher uniquement les résultats qui vous intéressent. Ceci fournit une méthode très efficace pour n'afficher que

les données qui vous intéressent.

Utilisez **Filtering** pour personnaliser la vue de grille en fonction de vos préférences. Les options de filtre disponibles sont basées sur le type d'objet affiché 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**.
Numéro	Les opérateurs sont **supérieurs à**, **inférieurs à**, **dans le dernier** et **entre**.
Enum (texte)	Les opérateurs sont **is** et **n'est pas**.

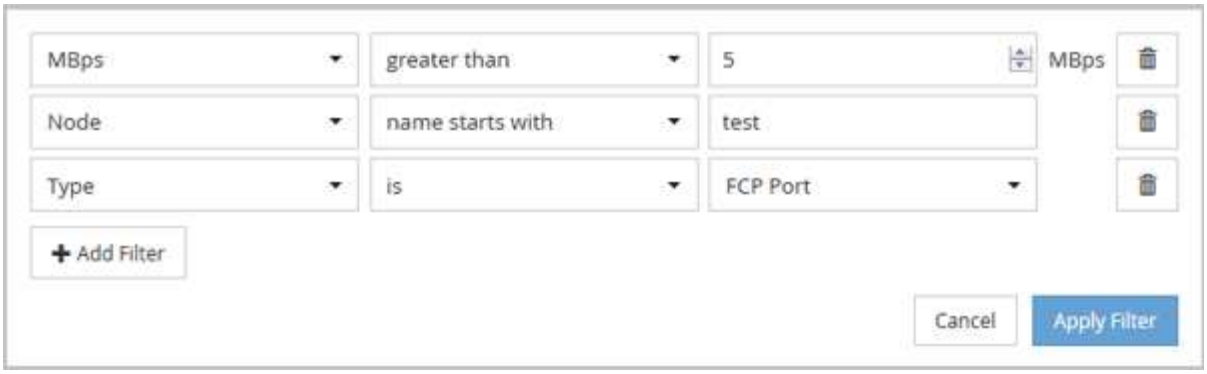
Les champs colonne, opérateur et valeur sont requis pour chaque filtre ; les filtres disponibles reflètent les colonnes filtrables de la page actuelle. Le nombre maximal de filtres que vous pouvez appliquer est de quatre. Les résultats filtrés sont basés sur des paramètres de filtre combinés. Les résultats 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 **Filter**. 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 entrez une valeur pour compléter le filtre de cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Ajouter filtre**. Un champ de filtre supplémentaire s'affiche. Effectuez ce filtre en suivant la procédure décrite dans les étapes précédentes. Notez que lors de l'ajout de votre quatrième filtre, le bouton **+Ajouter 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 s'affiche à droite du bouton filtre.
7. Utilisez le panneau filtrage pour supprimer des filtres individuels en cliquant sur l'icône de corbeille située 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 filtrage avec trois filtres. Le bouton **+Ajouter filtre** s'affiche lorsque vous avez moins de quatre filtres que le maximum.



Après avoir cliqué sur **appliquer le filtre**, le panneau filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Contrôle des performances du cluster depuis le tableau de bord

Le tableau de bord Unified Manager propose quelques panneaux indiquant l'état de performance générale de tous les clusters contrôlés par cette instance de Unified Manager. Il vous permet d'évaluer les performances globales des clusters gérés et de noter, localiser et attribuer rapidement la résolution de tout événement spécifique identifié.

Comprendre les panneaux de performances du tableau de bord

Le tableau de bord Unified Manager propose quelques panneaux présentant l'état de performance générale des clusters contrôlés dans votre environnement. Vous pouvez choisir d'afficher l'état de tous les clusters ou d'un cluster individuel.

En plus d'afficher les 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 dernières heures. Ces informations vous aident à déterminer les clusters que vous devrez analyser davantage pour résoudre les événements signalés. Un clic sur les événements affiche les quelques principaux événements et fournit un lien vers la page d'inventaire Event Management filtré pour afficher les événements de cette catégorie.

Les panneaux suivants fournissent l'état des performances.

- **Panneau capacité de performance**

  Lorsque vous affichez tous les clusters, ce panneau affiche la valeur de capacité des performances pour chaque cluster (moyenne sur l'heure précédente) et le nombre de jours jusqu'à ce que la capacité des performances atteigne la limite supérieure (basée sur le taux de croissance quotidien). Cliquez sur le graphique à barres pour accéder à la page d'inventaire des nœuds de 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.

  Lorsque vous affichez un seul cluster, ce volet affiche la capacité des performances du cluster, les IOPS totales et les valeurs de débit total.

- **Panneau d'IOPS de charge de travail**

  Lorsque la gestion active de la charge de travail est activée et que vous affichez un cluster unique, cette fenêtre affiche le nombre total de charges de travail actuellement exécutées dans une certaine plage d'IOPS.

- **Panneau performances 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 affectées à chaque niveau de service de performances défini. Cliquez sur un graphique à barres pour accéder aux charges de travail affectées à cette règle sur la page charges de travail.

- **Panneau vue d'ensemble de l'utilisation**

  Lorsque vous affichez tous les clusters, vous pouvez choisir d'afficher les clusters triés en fonction des IOPS ou du débit le plus élevés (Mbit/s).

  Lorsque vous affichez un seul cluster, vous avez la possibilité d'afficher les charges de travail présentes sur ce cluster, selon les critères les plus élevés en termes d'IOPS ou de débit (Mbit/s).

Messages de bannière et descriptions de performances

Unified Manager peut afficher des bannières sur la page Notifications (depuis le signal sonore de notification) pour vous alerter des problèmes liés à un cluster particulier.

Bannière message	Description	Solution
`No performance data is being collected from cluster` *`cluster_name`*`. Restart Unified Manager to correct this issue.`	Le service de collecte Unified Manager s'est arrêté et aucune donnée de performance n'est collectée depuis les clusters.	Redémarrez Unified Manager pour corriger ce problème. Si le problème persiste, contactez le support technique.
`More than x hour(s) of historical data is being collected from cluster` *`cluster_name`*`. Current data collections will start after all historical data is collected.`	Un cycle de collecte de la continuité des données est en cours d'exécution pour récupérer les données de performances en dehors du cycle de collecte en temps réel des performances du cluster.	Aucune action n'est requise. Les données actuelles sur le rendement seront recueillies une fois le cycle de collecte de la continuité des données terminé. Un cycle de collecte de continuité des données s'exécute lors de l'ajout d'un nouveau cluster ou lorsqu'Unified Manager n'a pas pu collecter de données de performance actuelles pour une raison ou une autre.

Modification de l'intervalle de collecte des statistiques de performances

L'intervalle de collecte par défaut des statistiques de performances est de 5 minutes.

Vous pouvez modifier cet intervalle à 10 ou 15 minutes si vous constatez que les collections des grands groupes ne se termine pas dans l'heure par défaut. Ce paramètre a un impact sur la collecte des statistiques de tous les clusters contrôlant cette instance de Unified Manager.

Ce dont vous aurez besoin

Vous devez disposer d'un ID utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

La question des collections de statistiques de performance qui ne se terminent pas à temps est indiquée par les messages de la bannière `Unable to consistently collect from cluster <cluster_name>` ou `Data collection is taking too long on cluster <cluster_name>`.

Vous devez modifier l'intervalle de collecte uniquement 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 défaut de 5 minutes peut affecter le nombre et la fréquence des événements de performances générés par Unified Manager. Par exemple, les seuils de performance définis par le système déclenchent des événements lorsque la règle est dépassée pendant 30 minutes. Lorsque vous utilisez des collections de 5 minutes, la police doit être dépassée pour six collections consécutives. Pour les collections de 15 minutes, la police doit être dépassée pour seulement deux périodes de collecte.

Un message en bas de la page Cluster Setup indique l'intervalle de collecte des données statistiques actuel.

Étapes

1. Connectez-vous en utilisant SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

   Les invites de la console de maintenance de Unified Manager s'affichent.

2. Saisissez le numéro de l'option de menu **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 utilisateur pour la maintenance.
4. Saisissez le numéro du nouvel intervalle d'interrogation que vous souhaitez définir, puis appuyez sur entrée.

Si vous avez modifié l'intervalle de collecte de Unified Manager à 10 ou 15 minutes et que vous disposez d'une connexion actuelle à un fournisseur de données externe (Graphite, par exemple), vous devez modifier l'intervalle de transmission du fournisseur de données de façon à ce qu'il soit supérieur ou égal à l'intervalle de collecte Unified Manager.

Dépannage des charges de travail à l'aide de l'analyseur de workloads

L'analyseur de charge de travail permet d'afficher des critères importants d'intégrité et de performance pour une charge de travail unique sur une seule page pour faciliter le dépannage. La visualisation des événements actuels et précédents d'une charge de travail vous permet de mieux comprendre pourquoi la charge de travail rencontre peut-être un problème de performances ou de capacité.

Cet outil vous aide également à déterminer si le stockage est la cause de tout problème de performance d'une application ou si le problème est causé par un problème de réseau ou autre.

Vous pouvez lancer cette fonctionnalité à partir de plusieurs endroits de l'interface utilisateur :

- Dans la sélection analyse de charge de travail du menu de navigation gauche
- Dans la page Détails de l'événement en cliquant sur le bouton **analyser la charge de travail**
- Depuis n'importe quelle page d'inventaire de workload (volume, LUN, workload, partage NFS ou partage SMB/CIFS), en cliquant sur l'icône plus ⋮, puis sur **Analyze Workload**
- Sur la page machines virtuelles, cliquez 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 toute 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 n'importe quelle page d'inventaire de la charge de travail ou de la machine virtuelle, le nom de la charge de travail est automatiquement renseigné et les données de la charge de travail sont présentées avec la plage de temps 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 automatiquement renseigné et les données de 10 jours s'affichent.

Données affichées par l'analyseur de flux de travail

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 le problème à l'origine de l'événement et des graphiques pour analyser les performances et l'historique des capacités.

En haut de la page, vous indiquez le nom de la charge de travail (volume ou LUN) à analyser, ainsi que le délai d'exécution des statistiques. Vous pouvez modifier le délai à tout moment si vous souhaitez afficher une période de temps plus courte ou plus longue.

Les autres zones de la page affichent les résultats de l'analyse et les graphiques de performances et de capacités.

> Les graphiques des charges de travail pour les LUN n'offrent pas le même niveau de statistiques que les graphiques des volumes. Vous remarquerez ainsi 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 survenus au cours de la période. Lorsqu'il existe des événements provenant de différentes zones d'impact (par exemple, performances et capacité), ces informations s'affichent pour vous permettre de sélectionner les détails du type d'événement qui vous intéresse. Cliquez sur le type d'événement pour afficher la liste des noms d'événement.

  S'il n'y a qu'un seul événement au cours de la période, une liste de recommandations pour résoudre le problème est indiquée pour certains événements.

- **Calendrier des événements**

  Affiche toutes les occurrences d'événements au cours de la période spécifiée. Placez le curseur sur

chaque événement pour afficher le nom de l'événement.

Si vous êtes arrivé sur cette page en cliquant sur le bouton **analyser charge de travail** de la page Détails de l'événement, l'icône de l'événement sélectionné apparaît plus grande pour vous permettre d'identifier l'événement.

- **Zone des graphiques de performance**

  Affiche les graphiques correspondant à la latence, au débit (IOPS et Mo/s) et à l'utilisation (pour le nœud et l'agrégat) en fonction du délai sélectionné. Vous pouvez cliquer sur le lien Afficher les détails des performances pour afficher la page de l'explorateur de performances pour la charge de travail si vous souhaitez 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**
    - **Latence de détail** (décomposée par lecture, écriture et autres processus)
    - **Cluster Components** latence (divisé par le composant de cluster)

Reportez-vous à la "Les composants du cluster et les conflits" pour obtenir une description des composants du cluster affichés ici. **Throughput affiche à la fois le débit en IOPS et en Mo/s pour la charge de travail sur la période sélectionnée. Le graphique comporte quatre vues qui vous permettent de voir : * débit total * débit ventilation (divisé par les lectures, écritures et autres processus)** * **débit du cloud** (les Mo/s utilisés pour écrire des données et les lire à partir du cloud; Pour les charges de travail qui Tiering de la capacité dans le cloud) *** IOPS avec prévision (prévision des valeurs de débit d'IOPS supérieures et inférieures attendues) ce graphique affiche également les paramètres de seuil de qualité de service (QoS) maximum et minimum, le cas échéant, Vous voyez ainsi où le système peut limiter le débit intentionnellement grâce aux règles de QoS. Utilisation** affiche l'utilisation à la fois pour l'agrégat et le nœud sur lequel la charge de travail s'exécute sur la période sélectionnée. Vous pouvez ici voir si votre agrégat ou nœud est sur-utilisé, ce qui peut entraîner une latence élevée. Lors de l'analyse des volumes FlexGroup, plusieurs nœuds et agrégats sont répertoriés dans les graphiques d'utilisation.

- **Zone de graphique de capacité**

  Affiche des graphiques correspondant à la capacité des données et à la capacité Snapshot du dernier mois pour la charge de travail.

  Pour les volumes, vous pouvez cliquer sur le lien Afficher les détails de capacité pour afficher la page Détails de l'intégrité de la charge de travail si vous souhaitez effectuer une analyse plus approfondie. Les LUN ne fournissent pas ce lien, car il n'y a pas de page Détails de l'état pour les LUN.

  - **Affichage de la capacité** affiche l'espace disponible total alloué à la charge de travail et à l'espace logique utilisé (après toutes les optimisations NetApp).
  - **Vue instantané** affiche l'espace total réservé pour les copies Snapshot et la quantité d'espace actuellement utilisée. Notez que les LUN ne fournissent pas de vue Snapshot.
  - **Cloud Tier View** affiche la capacité utilisée dans le Tier de performance local et la quantité utilisée dans le Tier cloud. Ces graphiques incluent une estimation du temps restant avant que la capacité soit saturée pour cette charge de travail. Ces informations sont basées sur l'historique d'utilisation 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 utiliser l'analyseur de charge de travail

Vous utilisez généralement l'analyseur de charge de travail pour résoudre un problème de latence signalé par un utilisateur, analyser plus précisément un événement ou une alerte signalé ou explorer une charge de travail qui fonctionne normalement.

Au cas où les utilisateurs vous ont contactés pour dire que l'application qu'ils utilisent s'exécute très lentement, vous pouvez consulter les diagrammes de latence, de débit et d'utilisation pour la charge de travail sur laquelle l'application est en cours d'exécution afin de déterminer si le stockage est à l'origine du problème de performances. Vous pouvez également utiliser le tableau de capacité pour vérifier si la capacité est faible, car un système ONTAP dont la capacité est supérieure à 85 % utilisée 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.

Si Unified Manager a généré un événement de performances et que vous souhaitez examiner plus en détail la cause du problème, vous pouvez lancer l'analyseur de charge de travail à partir de la page Détails de l'événement en cliquant sur le bouton **Analyze Workload** pour rechercher une partie de la latence, du débit, et les tendances de capacité pour la charge de travail.

Si vous remarquez un workload qui semble fonctionner de manière anormale lors de l'affichage d'une page d'inventaire de workload (volume, LUN, charge de travail, partage NFS ou partage SMB/CIFS), vous pouvez cliquer sur l'icône plus ⋮, puis sur **Analyze Workload** pour ouvrir la page Workload Analysis (analyse de charge de travail) afin d'examiner davantage le workload.

Utilisation de l'analyseur de flux de production

Il existe de nombreuses façons de démarrer l'analyseur de charge de travail à partir de l'interface utilisateur. Ici, nous décrivons le lancement de l'outil à partir du volet de navigation de gauche.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Workload Analysis**.

   La page analyse de la charge de travail s'affiche.

2. Si vous connaissez le nom du workload, entrez le nom. Si vous n'êtes pas sûr du nom complet, saisissez 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 pour une durée supérieure à la durée par défaut de 2 heures et cliquez sur **appliquer**.
4. Affichez la zone Résumé pour voir les événements survenus au cours de la période.
5. Affichez les graphiques de performances et de capacité pour vérifier si l'une des mesures est anormale et voir si des événements se alignent avec l'entrée anormale.

Contrôle des performances des clusters à partir de la page d'accueil Performance Cluster

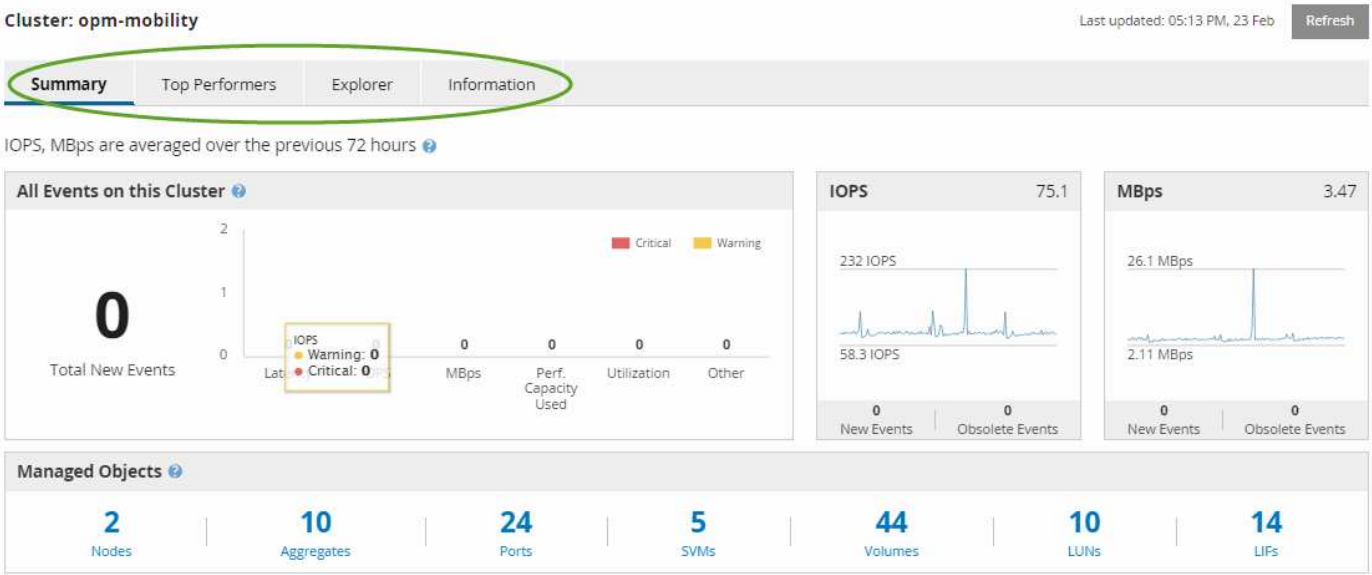
La page d'accueil Performance Cluster affiche l'état des performances générales d'un cluster sélectionné contrôlé par une instance de Unified Manager. Cette page vous permet d'évaluer les performances globales d'un cluster spécifique et de noter, localiser

ou attribuer rapidement la résolution de tout événement spécifique au cluster identifié.

Comprendre la page d'accueil de Performance Cluster

La page d'accueil Performance Cluster fournit une vue d'ensemble des performances de haut niveau d'un cluster sélectionné, en insistant sur l'état des performances des 10 objets les plus importants du cluster. Les problèmes de performances s'affichent en haut de la page, dans le panneau tous les événements de ce cluster.

La page d'accueil Performance Cluster offre une présentation générale de chaque cluster géré par une instance de Unified Manager. Cette page fournit des informations sur les événements et les performances. Elle vous permet également de contrôler et de dépanner les clusters. L'image suivante montre un exemple de la page d'accueil du cluster Performance Cluster pour le cluster appelé opm-Mobility :



Le nombre d'événements sur la page Cluster Summary peut ne pas correspondre au nombre d'événements sur la page Performance Event Inventory. En effet, la page Cluster Summary peut afficher un événement dans les barres latence et utilisation lorsque les règles de seuil de combinaison ont été enfreintes, alors que la page Performance Event Inventory n'affiche qu'un seul événement lorsqu'une règle de combinaison a été enfreinte.

> Si un cluster a été supprimé d'être géré par Unified Manager, l'état **supprimé** s'affiche à droite du nom du cluster en haut de la page.

Page d'accueil Performance Cluster

La page d'accueil Performance Cluster affiche l'état des performances de haut niveau d'un cluster sélectionné. Cette page vous permet d'accéder aux détails complets de chaque compteur de performances des objets de stockage du cluster sélectionné.

La page d'accueil Performance Cluster contient quatre onglets qui séparent les détails du cluster dans quatre zones d'information :

- Page récapitulative
  - Volet événements de cluster

    - Graphiques de performances en Mo/s et en IOPS
    - Volet objets gérés
- Haut de la page artistes interprètes ou exécutants
- Explorateur
- Page d'informations

Page Résumé du cluster de performances

La page Performance Cluster Summary récapitule les événements actifs, les performances IOPS et les performances MB/s d'un cluster. Cette page inclut également le nombre total d'objets de stockage dans le cluster.

Volet des événements de performance du cluster

Le volet événements de performance du cluster affiche les statistiques de performances et tous les événements actifs du cluster. Ceci est particulièrement utile pour le contrôle des clusters ainsi que de tous les événements et performances liés au cluster.

Tous les événements de ce volet Cluster

Le volet tous les événements de ce cluster affiche tous les événements de performance du cluster actifs pendant les 72 heures précédentes. Le total des événements actifs s'affiche à l'extrême gauche ; ce nombre représente le total de tous les événements nouveaux et acquittés 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 Active Events du cluster affiche le nombre total d'événements critiques et d'avertissement actifs :

- Latence (totale pour les nœuds, les agrégats, les SVM, les volumes, les LUN, et espaces de noms)
- IOPS (total pour les clusters, les nœuds, les agrégats, les SVM, les volumes, LUN et espaces de noms)
- Mo/s (total pour les clusters, les nœuds, les agrégats, les SVM, les volumes, LUNs, namespaces, ports et LIFs)
- Capacité de performance utilisée (totale pour les nœuds et les agrégats)
- Utilisation (total pour les nœuds, les agrégats et les ports)
- Autre (taux d'échec du cache pour les volumes)

Cette liste contient les événements de performances actifs déclenchés par les politiques de seuils définies par l'utilisateur, les règles de seuils définies par le système et les seuils dynamiques.

Les données graphiques (barres de compteur verticales) sont affichées en rouge ( ) pour les événements critiques et en jaune ( ) pour les événements d'avertissement. Positionnez le curseur sur chaque barre de compteur verticale pour afficher le type et le nombre réel 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 performance Total Active Events en cliquant sur les icônes **critique** et **Avertissement** de la légende. Si vous masquez certains types d'événements, les icônes de légende s'affichent en gris.

Panneaux de comptoir

Les panneaux de compteur affichent les événements d'activité et de performances du cluster pour les 72 heures précédentes et comprennent les compteurs suivants :

- **Panneau de compteur d'IOPS**

  Les IOPS indiquent la vitesse de fonctionnement du cluster en nombre d'opérations d'entrée/sortie par seconde. Ce panneau de compteurs offre une vue d'ensemble générale de l'état des IOPS du cluster pour la période précédente de 72 heures. Vous pouvez positionner le curseur de la souris sur la ligne de tendance du graphique pour afficher la valeur IOPS d'une heure précise.

- **Panneau de compteur MB/s**

  Mo/s indique la quantité de données transférées vers et depuis le cluster en mégaoctets par seconde. Ce panneau de compteurs offre une vue d'ensemble de haut niveau de l'état du Mo/s du cluster pour la période de 72 heures précédente. Vous pouvez positionner le curseur sur la ligne de tendance du graphique pour afficher la valeur MB/s pour une heure spécifique.

Le nombre en haut à droite du graphique dans la barre grise correspond à la valeur moyenne des 72 dernières heures. Les chiffres indiqués en bas et en haut du graphique de tendance sont les valeurs minimale et maximale pour la dernière période de 72 heures. La barre grise sous le tableau contient le nombre d'événements actifs (nouveaux et acquittés) et d'événements obsolètes de la dernière période de 72 heures.

Les panneaux du compteur 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'incident n'a pas été corrigé lui-même ou n'a pas été résolu. Le compteur de performances de l'objet de stockage reste au-dessus du seuil de performance.

- **Obsolète**

  Indique que l'incident n'est plus actif. Le problème à l'origine de l'incident s'est corrigé ou a été résolu. Le compteur de performance de l'objet de stockage n'est plus au-dessus du seuil de performance.

Pour **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 plus d'un événement, 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 une vue d'ensemble de haut niveau des types et nombres d'objets de stockage pour le cluster. Ce volet vous permet de suivre l'état des objets de chaque cluster.

Le nombre d'objets gérés est des données ponctuelles au cours de la dernière période de collecte. De nouveaux objets sont découverts toutes les 15 minutes.

Si vous cliquez sur le numéro lié d'un type d'objet, la page d'inventaire des performances de l'objet correspondant à ce type d'objet s'affiche. La page d'inventaire des objets est filtrée pour afficher uniquement

les objets de ce cluster.

Les objets gérés sont :

- **Nœuds**

  Système physique dans un cluster.

- **Agrégats**

  Un jeu de plusieurs groupes RAID (redundant array of Independent disks) qui peuvent être gérés comme une seule unité pour la protection et le provisionnement.

- **Ports**

  Point de connexion physique sur les nœuds utilisés pour se connecter à d'autres périphériques d'un réseau.

- **Machines virtuelles de stockage**

  Machine virtuelle fournissant un accès réseau via des adresses réseau uniques. Un SVM peut fournir des données dans un namespace distinct et peut être administré séparément du reste du cluster.

- **Volumes**

  Entité logique qui maintient les données utilisateur accessibles via un ou plusieurs protocoles d'accès pris en charge. Ce nombre inclut à la fois les volumes FlexVol et FlexGroup, mais pas les composants FlexGroup.

- **LUN**

  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 au sein d'un système d'exploitation informatique comme un périphérique.

- * Interfaces réseau*

  Interface réseau logique représentant un point d'accès réseau à un nœud. Le nombre inclut tous les types d'interface.

Haut de la page artistes interprètes ou exécutants

La page Top Performers affiche les objets de stockage dont les performances sont les plus élevées ou les performances les plus faibles, en fonction du compteur de performances sélectionné. Par exemple, dans la catégorie Storage VM, vous pouvez afficher les SVM qui possèdent les IOPS les plus élevées, ou la latence la plus élevée, ou les Mo/s. Cette page indique également si l'un des meilleurs collaborateurs a des événements de performance actifs (nouveaux ou reconnus).

La page exécutants supérieurs affiche un maximum de 10 de chaque objet. Notez que l'objet Volume inclut à la fois des volumes FlexVol et FlexGroup.

- **Plage de temps**

Vous pouvez sélectionner une plage horaire pour afficher les performances supérieures ; la plage horaire sélectionnée s'applique à tous les objets de stockage. Plages de temps disponibles :

- Dernière heure
- Dernières 24 heures
- Dernières 72 heures (par défaut)
- 7 derniers jours

- **Métrique**

  Cliquez sur le menu **Metric** 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 **latence**, **IOPS** et **Mo/s**. La modification du compteur recharge les données du panneau avec les performances supérieures en fonction du compteur sélectionné.

  Compteurs disponibles :

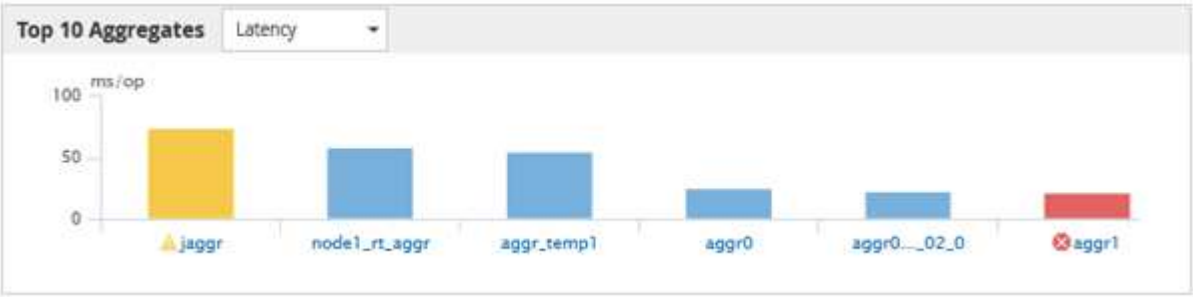
  - Latence
  - LES IOPS
  - Mo/s
  - Capacité de performance utilisée (pour les nœuds et les agrégats)
  - Utilisation (pour les nœuds et les agrégats)

- **Trier**

  Cliquez sur le menu **Trier** pour sélectionner un tri croissant ou décroissant pour l'objet et le compteur sélectionnés. Les options sont **les plus élevées à la plus basse** et **les plus basses à la plus élevée**. Ces options vous permettent d'afficher les objets avec les meilleures performances ou la plus faible performance.

- **Barre de compteur**

  La barre de compteurs du graphique affiche les statistiques de performances 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 performances, la barre de compteur s'affiche en bleu. Si une violation de seuil est active (un nouvel événement ou un événement acquitté), la barre est affichée en couleur pour l'événement : les événements d'avertissement sont affichés en jaune ( ) et les événements critiques sont affichés en rouge ( ). Les violations de seuil sont davantage indiquées par les icônes d'indicateurs d'événement de gravité pour les avertissements et les événements critiques.



Pour chaque graphique, l'axe X affiche les performances supérieures pour le type d'objet sélectionné. L'axe y affiche les unités applicables au compteur sélectionné. Cliquez sur le lien du nom d'objet sous chaque élément graphique à barres verticales pour accéder à la page d'arrivée des performances de

l'objet sélectionné.

- **Indicateur d'événement de gravité**

  L'icône de l'indicateur **Severity Event** s'affiche à gauche d'un nom d'objet pour les événements critiques () ou d'avertissement ( ) actifs dans les graphiques les plus performants. Cliquez sur l'icône de l'indicateur **événement de gravité** pour afficher :

  - **Un événement**

    Permet d'accéder à la page Détails de l'événement pour cet événement.

  - **Deux événements ou plus**

    Permet d'accéder à la page d'inventaire des événements, qui est filtrée pour afficher tous les événements pour l'objet sélectionné.

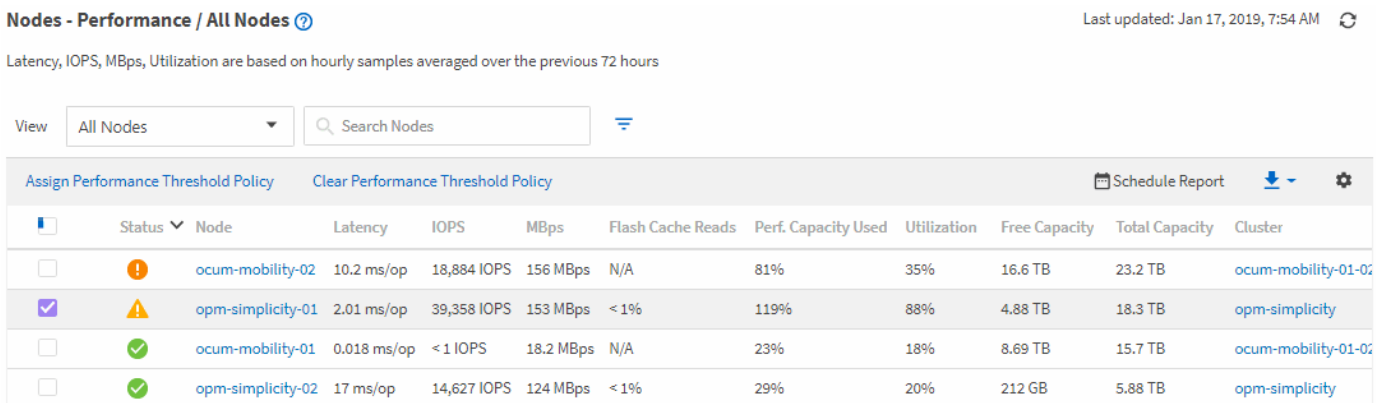
- **Bouton Exporter**

  Crée un `.csv` fichier contenant les données qui apparaissent dans la barre de compteur. Vous pouvez choisir de créer le fichier pour le cluster unique que vous visualisez ou pour tous les clusters du data Center.

Surveillance des performances à l'aide des pages d'inventaire des performances

Les pages de performances de l'inventaire des objets affichent des informations de performances, des événements de performance et l'état de santé de tous les objets d'une catégorie de type objet. Vous bénéficiez ainsi d'un aperçu complet de l'état de performance de chaque objet 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 général de l'état des objets, ce qui vous permet d'évaluer les performances globales de tous les objets et de comparer les données de performances de l'objet. Vous pouvez affiner le contenu des pages d'inventaire d'objets en effectuant des recherches, en triant et en filtrant. Cette fonction est avantageuse pour le contrôle et la gestion des performances des objets. Elle vous permet de localiser rapidement les objets présentant des problèmes de performance et de lancer le processus de dépannage.



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 lieu et les objets avec des événements d'avertissement sont répertoriés en second. Cela fournit une indication visuelle immédiate des problèmes à résoudre. Toutes les données de performance reposent sur une moyenne de 72 heures.

Vous pouvez facilement naviguer de la page performances de l'inventaire d'objets vers une page de détails d'objet en cliquant sur le nom de l'objet dans la colonne Nom de l'objet. Par exemple, sur la page d'inventaire performances/tous les nœuds, vous devez cliquer sur un objet noeud dans la colonne **nœuds**. La page de détails de l'objet fournit des informations détaillées et des détails sur l'objet sélectionné, y compris la comparaison côte à côte des événements actifs.

Affichage des pages d'inventaire des performances pour tous les objets de stockage

Les pages de l'inventaire des performances vous permettent d'obtenir un récapitulatif des informations sur les performances de chaque objet de stockage disponible, par exemple les clusters, les agrégats, les volumes, etc. Vous pouvez créer un lien vers les pages de détails de l'objet Performance pour afficher les informations détaillées d'un objet particulier.

Par défaut, les objets des pages de vue sont triés en fonction de la criticité de l'événement. 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 à résoudre.

Vous pouvez exporter des données de ces pages vers un (`.csv`fichier de valeurs séparées par des virgules), (.xlsx`un fichier Microsoft Excel ) ou un (`.pdf`document en utilisant le bouton **Rapports**, puis les données exportées pour générer des rapports. En outre, vous pouvez personnaliser la page, puis planifier la création et l'envoi d'un rapport par e-mail à intervalles réguliers en utilisant le bouton **Rapports programmés**.

Tous les champs de ces pages peuvent être utilisés dans les vues personnalisées et dans les rapports. Certains champs sont liés à des pages associées permettant une vue plus détaillée.

Performance : vue de tous les clusters

La vue Performance : tous les clusters affiche un aperçu des événements de performance, des données et des informations de configuration de chaque cluster surveillé par une instance de Unified Manager. Cette page vous permet de contrôler les performances des clusters et de résoudre les problèmes de performance et les événements seuils.

Vous pouvez affecter des stratégies de seuil de performances à ou effacer des stratégies de seuil à partir de n'importe quel objet sur les pages d'inventaire des objets à l'aide des boutons **affecter la stratégie de seuil de performances** et **Effacer la stratégie de seuil de performances**.

Les champs suivants sont importants dans la vue Performance : tous les clusters.

- FQDN du cluster : nom de domaine complet (FQDN) du cluster.
- IOPS : opérations d'entrée/sortie par seconde sur le cluster.
- Mo/s : débit sur le cluster, mesuré en MIB par seconde.
- Champs de capacité : capacité libre et totale en Gio.
- Nom d'hôte ou adresse IP : nom d'hôte ou adresse IP (IPv4 ou IPv6) du LIF de gestion du cluster.

- Version du système d'exploitation : version du logiciel ONTAP installé sur le cluster.

> Si différentes versions du logiciel ONTAP sont installées sur les nœuds du cluster, le numéro de version le plus faible est indiqué. Vous pouvez afficher la version de ONTAP installée sur chaque nœud depuis la vue Performance : tous les nœuds.

- Règle de seuil : règle de seuil de performance définie par l'utilisateur, ou règles 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 affectés. Les boutons attribuer une stratégie de seuil de performances et Effacer la stratégie de seuil de performances restent désactivés jusqu'à ce que vous sélectionniez un ou plusieurs objets en cliquant sur les cases à cocher situées à l'extrême gauche.

Performance : vue de tous les volumes

La vue performances : tous les volumes affiche un aperçu des événements de performance, des données des compteurs et des informations de configuration pour chaque volume FlexVol et volume FlexGroup contrôlé par une instance de Unified Manager. Vous pouvez ainsi surveiller rapidement les performances de vos volumes et résoudre les problèmes de performances et les seuils.

Si vous souhaitez analyser la latence et le débit d'un objet spécifique, cliquez sur le bouton plus d'options, puis sur **Analyze Workload**. Vous pouvez afficher les graphiques de performances et de capacité sur la page analyse des workloads. Vous pouvez afficher les détails sur System Manager étant donné que vous disposez d'identifiants valides pour System Manager.

> Pour les volumes DP (Data protection), seules les valeurs de compteur du trafic généré par les utilisateurs sont affichées. Les volumes racine ne sont pas affichés sur cette page.

Voici quelques champs importants dans la vue Performance : 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 le niveau de performances qu'une certaine capacité de stockage peut fournir.
- 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 de tous les volumes constitutifs.
- Mo/s : pour les volumes FlexVol, il s'agit du débit du volume, mesuré en mégaoctets par seconde. Pour les volumes FlexGroup, il s'agit de la somme des Mo/s pour tous les volumes constitutifs.
- Champs de capacité : capacité libre et totale en Gio.

Consultez les liens suivants pour plus d'informations :

- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"
- "Types de charges de travail surveillés par Unified Manager"
- "Affichage des paramètres de « policy group » QoS appliqués à des volumes ou LUN spécifiques"

- "Comprendre les recommandations d'Unified Manager concernant le Tiering des données dans le cloud"
- "Affichage des graphiques de performances pour comparer les volumes ou les LUN qui se trouvent dans le même groupe de règles de QoS"

Performance : vue de tous les agrégats

La vue Performance : tous les agrégats affiche un aperçu des événements de performances, des données et des informations de configuration de 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 seuils.

Voici quelques champs importants dans la vue Performance : tous les agrégats.

- Type : le type d'agrégat :
  - DISQUES DURS
  - Hybride. Combinaison de disques durs et de disques SSD, mais Flash Pool n'a pas été activé.
  - Hybride (Flash Pool). Combinaison de disques durs et de disques SSD et Flash Pool est activé.
  - SSD
  - Les disques SSD (FabricPool). Combinaison de SSD et d'un Tier cloud
  - Disque dur (FabricPool). Combinaison de disques durs et d'un Tier cloud
  - VMDisk (SDS). Disques virtuels au sein d'une machine virtuelle
  - Disque VMware (FabricPool). Combinaison de disques virtuels et d'un niveau cloud
  - LUN (FlexArray)
- Reporting des données inactives : si la fonctionnalité de reporting des données inactives est activée ou désactivée sur cet agrégat. Lorsque cette option est activée, les volumes de cet agrégat affichent la quantité de données inactives dans la vue Performance : tous les volumes. La valeur de ce champ est « N/A » lorsque la version de ONTAP ne prend pas en charge le reporting de données inactives.
- Règle de seuil : règle de seuil de performance définie par l'utilisateur, ou règles 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 affectés. Les boutons attribuer une stratégie de seuil de performances et Effacer la stratégie de seuil de performances 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 :
- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"

Performance : vue de tous les nœuds

La vue performances : tous les nœuds affiche un aperçu des événements de performance, des données et des informations de configuration pour chaque nœud contrôlé par une instance de Unified Manager. Vous pouvez ainsi surveiller rapidement les performances de vos nœuds et résoudre les problèmes de performances et les seuils.

> Les lectures Flash cache affichent le pourcentage d'opérations de lecture sur le nœud satisfait par le cache, au lieu d'être renvoyées à partir du disque. Les données de 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 du matériel** est disponible lorsque Unified Manager et les clusters qu'il gère sont installés sur un site sans connectivité réseau externe. Ce bouton génère un fichier .csv qui contient une liste complète des informations sur le cluster et le nœud, notamment les numéros de modèles matériels et de série, les types et nombres de disques, les licences installées. Cette fonctionnalité de reporting est utile pour le renouvellement de contrat dans des sites sécurisés qui ne sont pas connectés à la plateforme NetApp Active IQ. Vous pouvez affecter des stratégies de seuil de performances à ou effacer des stratégies de seuil à partir de n'importe quel objet sur les pages d'inventaire des objets à l'aide des boutons **affecter la stratégie de seuil de performances** et **Effacer la stratégie de seuil de performances**.

Consultez les liens suivants pour plus d'informations :

- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"
- "Génération d'un rapport d'inventaire du matériel pour le renouvellement du contrat"

Performances : vue de toutes les machines virtuelles de stockage

La vue performances : tous les VM de stockage affiche un aperçu des événements de performances, des données et des informations de configuration pour chaque SVM (Storage Virtual machine) contrôlé par une instance de Unified Manager. Vous pouvez ainsi surveiller rapidement les performances des SVM et résoudre les problèmes de performances et les seuils. 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 Data et Cluster. Unified Manager n'utilise ni n'affiche les SVM d'administration ou de nœuds.

Consultez les liens suivants pour plus d'informations :

- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"

Performances : vue de toutes les LUN

Performances : la vue de toutes les LUN affiche un aperçu des événements de performances, des données et des informations de configuration de chaque LUN surveillée par une instance de Unified Manager. Vous pouvez ainsi surveiller rapidement les performances des LUN et résoudre les problèmes de performances et les seuils.

Si vous souhaitez analyser la latence et le débit d'un objet spécifique, cliquez sur l'icône plus ⋮, puis sur **Analyze Workload** et vous pouvez afficher les graphiques de performances et de capacité sur la page **Workload Analysis**.

Consultez les liens suivants pour plus d'informations :

- "Contrôle des LUN dans une relation de groupe de cohérence"
- "Provisionner les LUN"
- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"
- "Affichage des volumes ou des LUN qui appartiennent au même groupe de règles de QoS".
- "Affichage des paramètres de « policy group » QoS appliqués à des volumes ou LUN spécifiques"

- "Provisionnement des LUN à l'aide d'API"

Performance : vue de tous les espaces de noms NVMe

La vue Performance : tous les espaces de noms NVMe présente les événements de performance, les données et les informations de configuration de chaque espace de nom NVMe surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances et l'intégrité de vos espaces de noms, et de résoudre les problèmes et les événements de seuils.

Les informations suivantes, entre autres, sont signalées : 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 est insuffisant.

Consultez les liens suivants pour plus d'informations :

- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"

Performance : vue de 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 de Unified Manager. Cette page vous permet de surveiller rapidement les performances de vos interfaces et de résoudre les problèmes de performances et les événements seuils. Les champs suivants sont importants dans la vue performances : toutes les interfaces réseau.

- IOPS : opérations d'entrée/sortie par seconde. IOPS ne s'applique pas aux LIF NFS et CIFS, et est affiché en tant que N/A pour ces types.
- Latence : temps de réponse moyen pour toutes les demandes d'E/S, exprimé en millisecondes par opération. La latence n'est pas applicable aux LIF NFS et CIFS, et elle est affichée sous la forme N/A pour ces types.
- Home Location : emplacement d'origine de l'interface, affiché sous la forme d'un nom de nœud et d'un nom de port, séparé 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 : emplacement actuel de l'interface, affiché sous la forme d'un nom de nœud et d'un nom de port, séparé 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 : rôle de l'interface : données, Cluster, Node Management ou intercluster.

> Les interfaces répertoriées sur cette page incluent les LIF Data, les LIFs Cluster, les LIFs Node Management et les LIF intercluster. Unified Manager n'utilise ni n'affiche les LIF de système.

Performance : vue de 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 contrôlé par une instance de Unified Manager. Vous pouvez ainsi surveiller rapidement les performances de vos ports et résoudre les problèmes de performances et les seuils. Pour un rôle de port, la fonction de port réseau est affichée, soit Data, soit Cluster. Les ports FCP ne peuvent pas avoir de rôle et le rôle est affiché en tant que N/A.

> Les valeurs des compteurs de performances sont affichées pour les ports physiques uniquement. Les valeurs de compteur ne s'affichent pas pour les VLAN ou les groupes d'interfaces.

Consultez les liens suivants pour plus d'informations :

- "Assignation de règles de seuil de performances aux objets de stockage"
- "Suppression des règles de seuil de performances des objets de stockage"

Performance : vue des groupes de règles de QoS

La vue QoS Policy Groups affiche les groupes de règles de QoS disponibles sur les clusters qui surveillent Unified Manager. Cela inclut les règles de QoS classiques, les règles de QoS adaptative et les règles de QoS attribuées à l'aide des niveaux de services de performance.

Voici quelques champs importants dans la vue performances : groupes de règles de QoS.

- QoS Policy Group : nom de la « policy group » QoS. Pour les règles 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 du SVM et d'autres informations qui ne sont pas dans le nom lorsque le niveau de service de performance a été défini dans NSLM. Par exemple, le nom « NSLM_vs6_Performance_2_0 » signifie qu'il s'agit de la règle PSL « Performance » définie par le système NSLM créée sur le SVM « vs6 » avec une latence attendue de « 2 ms/op ».
- SVM : la VM de stockage (SVM) à laquelle appartient le « QoS policy group ». Vous pouvez cliquer sur le nom de la VM de stockage pour accéder à la page détaillée de cette VM de stockage. Ce champ est vide si la politique de QoS a été créée sur la machine virtuelle de stockage Admin, car ce type de machine virtuelle de stockage représente le cluster.
- Débit min : débit minimal, en IOPS, garanti que le groupe de règles sera capable de fournir. Pour les règles adaptatives, il s'agit du minimum d'IOPS par To attendus alloués au volume ou à la LUN, en fonction de la taille allouée à l'objet de stockage.
- Débit max : débit, en IOPS et/ou en Mo/s que le groupe de règles ne doit pas dépasser. Lorsque ce champ est vide, cela signifie que la max dans l'ensemble défini dans ONTAP est infinie. Pour les règles adaptatives, il s'agit du maximum (pic) d'IOPS par To possibles alloués au volume ou au LUN, en fonction de la taille de l'objet de stockage alloué ou de la taille de l'objet de stockage utilisé.
- IOPS minimales absolues : pour les règles adaptatives, il s'agit de la valeur d'IOPS minimale absolue utilisée comme valeur prioritaire lorsque les IOPS attendues sont inférieures à cette valeur.
- Taille de bloc : taille de bloc spécifiée pour la règle adaptative de la qualité de service.
- Allocation min : indique si l'espace alloué ou l'espace utilisé est utilisé pour déterminer le débit maximal (pic) d'IOPS.
- Latence attendue : latence moyenne prévue pour les opérations d'entrée/sortie du stockage.
- Partagée : pour les règles de QoS classiques, que les valeurs de débit définies dans le groupe de règles soient partagées entre plusieurs objets.
- Objets associés : nombre de workloads affectés au groupe de règles QoS. Vous pouvez cliquer sur le bouton développer (⌄) en regard de QoS Policy Group Name pour afficher plus de détails sur la stratégie group.
- Capacité allouée : quantité d'espace utilisée par les objets du groupe de règles de QoS.
- Objets associés : nombre de charges de travail attribuées au groupe de règles de 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, reportez-vous aux rubriques sous "Gestion des performances à l'aide des informations de groupe de règles de QoS".

Raffinage du contenu de la page d'inventaire des performances

Les pages d'inventaire des objets de performances contiennent des outils qui vous aident à affiner le contenu des données d'inventaire des objets, ce qui vous permet de localiser rapidement et facilement des données spécifiques.

Les informations contenues dans les pages d'inventaire des objets Performance peuvent être étendues, souvent couvrant plusieurs pages. Ce type de données complètes est excellent pour la surveillance, le suivi et l'amélioration des performances. Cependant, la localisation de données spécifiques nécessite des outils pour vous permettre de localiser rapidement les données pour lesquelles vous recherchez. Par conséquent, les pages d'inventaire des objets Performance contiennent des fonctionnalités de recherche, de tri et de filtrage. En outre, la recherche et le filtrage peuvent travailler ensemble pour affiner davantage vos résultats.

Recherche sur les pages performances de l'inventaire des objets

Vous pouvez rechercher des chaînes dans les pages performances de l'inventaire des objets. Utilisez le champ **Search** 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 stratégie. Vous pouvez ainsi localiser rapidement des objets spécifiques et leurs données associées, ou consulter rapidement les règles et les données d'objets de stratégie associés.

Étape

1. Effectuez l'une des options suivantes en fonction de vos besoins de recherche :

Pour localiser ceci…	Tapez ceci…
Un objet spécifique	Le nom de l'objet dans le champ **Search**, puis cliquez sur **Search**. L'objet pour lequel vous avez recherché et ses données associées s'affiche.
Règle de seuil de performance définie par l'utilisateur	Tout ou partie du nom de la police dans le champ **Search**, puis cliquez sur **Search**. Les objets affectés à la stratégie pour laquelle vous avez recherché s'affichent.

Tri sur les pages performances de l'inventaire des objets

Vous pouvez trier toutes les données sur les pages performances de l'inventaire des objets par colonne dans l'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 début 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 la direction 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 **Status** (criticité de l'événement)

dans l'ordre décroissant, avec les événements de performance les plus critiques répertoriés en premier.

Étape

1. Vous pouvez cliquer sur un nom de colonne pour activer ou désactiver l'ordre de tri de la colonne dans l'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.

Filtrage des 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 restreindre le contenu des pages performances de l'inventaire des objets afin d'afficher uniquement les résultats que vous avez spécifiés. Cela constitue une méthode très efficace pour afficher uniquement les données de performance qui vous intéressent.

Vous pouvez utiliser le panneau filtrage pour personnaliser la vue de grille en fonction de vos préférences. Les options de filtre disponibles sont basées sur le type d'objet affiché 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**.
Numéro	Les opérateurs sont **supérieurs à**, **inférieurs à**, **dans le dernier** et **entre**.
Enum (texte)	Les opérateurs sont **is** et **n'est pas**.

Les champs colonne, opérateur et valeur sont requis pour chaque filtre ; les filtres disponibles reflètent les colonnes filtrables de la page actuelle. Le nombre maximal 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.

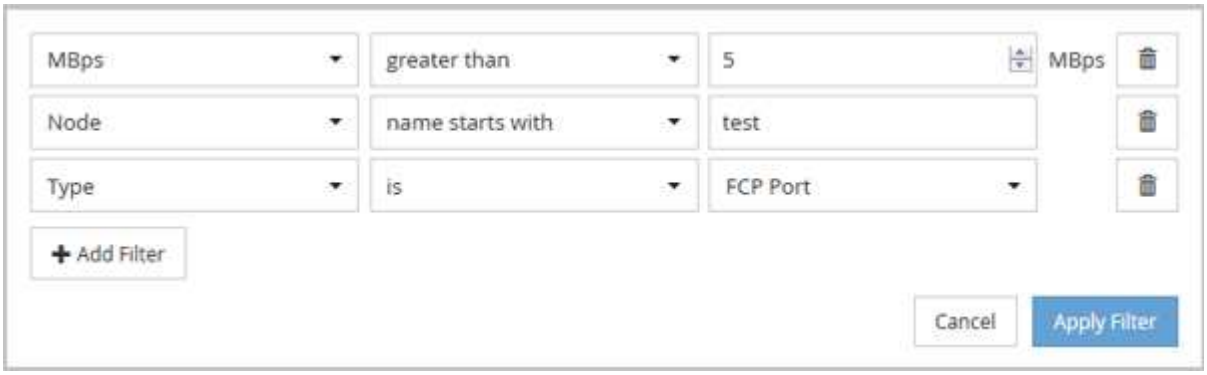
Vous pouvez ajouter des filtres à l'aide du panneau filtrage.

1. En haut de la page, cliquez sur le bouton **Filter**. 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 entrez une valeur pour compléter le filtre de cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Ajouter filtre**. Un champ de filtre supplémentaire s'affiche. Effectuez ce filtre en suivant la procédure décrite dans les étapes précédentes. Notez que lors de l'ajout de votre quatrième filtre, le bouton **+Ajouter 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 s'affiche à droite du bouton filtre.
7. Utilisez le panneau filtrage pour supprimer des filtres individuels en cliquant sur l'icône de corbeille située 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 filtrage avec trois filtres. Le bouton **+Ajouter filtre** s'affiche lorsque vous avez moins de quatre filtres que le maximum.



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 concernant le Tiering des données dans le cloud

La vue Performance : tous les volumes affiche des informations relatives à la taille des données utilisateur stockées sur le volume inactif (à froid). Unified Manager identifie certains volumes qui seraient bénéficient du Tiering des données inactives vers le Tier cloud (fournisseur cloud ou StorageGRID) d'un agrégat compatible FabricPool.

> FabricPool a été introduit dans ONTAP 9.2. Si vous utilisez une version du logiciel ONTAP antérieure à 9.2, les recommandations de Unified Manager pour hiérarchiser les données doivent donc mettre à niveau votre logiciel ONTAP. De plus, la `auto` règle de hiérarchisation a été introduite dans ONTAP 9.4 et la `all` règle de hiérarchisation a été introduite dans ONTAP 9.6. Par conséquent, si la recommandation est d'utiliser la règle de hiérarchisation automatique, vous devez effectuer une mise à niveau vers ONTAP 9.4 ou une version ultérieure.

Les trois champs suivants de la vue Performance : la vue tous les volumes fournit des informations permettant d'améliorer l'utilisation des disques du système de stockage et de gagner de l'espace sur le Tier de performance en déplaçant les données inactives vers le Tier cloud.

- **Politique de hiérarchisation**

  La règle de Tiering détermine si les données du volume restent dans le Tier de performance ou si certaines données sont déplacées depuis le Tier de performance vers le Tier cloud.

  La valeur de ce champ indique l'ensemble de règles de Tiering sur le volume, même si le volume ne réside pas actuellement sur un agrégat FabricPool. La règle de Tiering n'est appliquée que lorsque le volume se

trouve sur un agrégat FabricPool.

- **Données inactives**

  Les données inactives affichent la taille des données utilisateur stockées sur le volume inactif (à froid).

  Une valeur s'affiche ici uniquement lors de l'utilisation du logiciel ONTAP 9.4 ou supérieur car cela nécessite que l'agrégat sur lequel le volume est déployé ait la **`inactive data reporting parameter`** valeur **`enabled`**, et que le seuil minimum de jours de refroidissement ait été atteint (pour les volumes qui utilisent la **`snapshot-only`** règle de hiérarchisation ou **`auto`**). Autrement, la valeur est indiquée comme « N/A ».

- **Recommandation sur le cloud**

  Une fois suffisamment d'informations capturées concernant l'activité de données sur le volume, Unified Manager peut déterminer qu'aucune action n'est requise, ou que vous pouvez économiser de l'espace sur le Tier de performance en transférant les données inactives vers le Tier cloud.

> Le champ données inactives est mis à jour toutes les 15 minutes, mais le champ Cloud Recommendation est mis à jour tous les 7 jours lorsque l'analyse des données inactives est effectuée sur le volume. Par conséquent, la quantité exacte de données inactives peut différer d'un champ à l'autre. Le champ recommandations cloud affiche la date à laquelle l'analyse a été exécutée.

Lorsque l'option Rapport de données inactives est activée, le champ données inactives affiche la quantité exacte de données inactives. Sans la fonctionnalité de reporting des données inactives, Unified Manager utilise des statistiques de performance pour déterminer si les données sont inactives sur un volume. La quantité de données inactives ne s'affiche pas dans le champ données inactives dans ce cas, mais elle s'affiche lorsque vous passez le curseur sur le mot **Tier** pour afficher la recommandation de nuage.

Nos recommandations en matière de cloud sont les suivantes :

- **Apprentissage**. Des données insuffisantes ont été recueillies pour faire une recommandation.
- **Niveau**. L'analyse a déterminé que le volume contient des données inactives et que vous devez configurer le volume pour le déplacer vers le Tier cloud. Dans certains cas, vous devrez d'abord déplacer le volume vers un agrégat compatible FabricPool. Dans les autres cas où le volume se trouve déjà dans un agrégat FabricPool, il vous suffit de modifier la règle de Tiering.
- **Aucune action**. Soit le volume n'a que peu de données inactives, soit déjà défini sur la règle de hiérarchisation « automatique » d'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 règle de Tiering des volumes ou les paramètres de reporting des données inactives de l'agrégat, utilisez ONTAP System Manager, les commandes de l'interface de ligne de commande de ONTAP, ou une combinaison de ces outils.

Si vous êtes connecté à Unified Manager avec le rôle Administrateur d'applications ou Administrateur de stockage, le lien **configurer le volume** est disponible dans le cloud recommandé lorsque vous placez le curseur sur le mot **Tier**. Cliquez sur ce bouton pour ouvrir la page volumes dans System Manager afin d'effectuer la modification recommandée.

Contrôle des performances à l'aide des pages de l'explorateur de performances

Les pages de l'explorateur d'performances affichent des informations détaillées sur les performances de chaque objet d'un cluster. Cette page offre une vue détaillée des performances de tous les objets du cluster, ce qui vous permet de sélectionner et de comparer les données de performances d'objets spécifiques sur différentes périodes.

Vous pouvez également évaluer la performance globale de tous les objets et comparer les données de performances de l'objet dans un format côte à côte.

Présentation de l'objet racine

L'objet racine est la référence par rapport à laquelle d'autres comparaisons d'objets sont effectuées. Vous pouvez ainsi afficher et comparer les données d'autres objets avec l'objet racine, pour une analyse des données de performances permettant de résoudre et d'améliorer les performances de vos objets.

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 pas de 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 compteurs.

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 voulez comparer à un autre objet racine, vous devez cliquer sur le lien d'un objet et ouvrir sa page d'accueil.

Les événements et les seuils s'affichent uniquement pour les objets racine.

Appliquer le filtrage pour réduire la liste des objets corrélés dans la grille

Le filtrage vous permet d'afficher un sous-ensemble plus petit et plus bien défini d'objets 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 une latence supérieure à 1 ms/op.

Spécification d'une plage de temps pour les objets corrélés

Le sélecteur de plage horaire de la page Explorateur de performances vous permet de spécifier la plage horaire de la comparaison des données d'objet. La spécification d'une plage horaire permet de raffine le contenu des pages de l'Explorateur de performances pour n'afficher que les données d'objet dans la plage horaire spécifiée.

Le raffinage de la plage horaire permet de n'afficher que les données de performance 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.

Sélection d’une plage de temps prédéfinie

La sélection d’une plage de temps prédéfinie est un moyen rapide et efficace de personnaliser et de concentrer la sortie de données lors de l’affichage des données de performance d’objet du cluster. Lorsque vous sélectionnez une plage horaire prédéfinie, des données pouvant atteindre 13 mois sont disponibles.

Étapes

1. En haut à droite de la page **Performance Explorer**, cliquez sur **Time Range**.
2. Dans la partie droite du panneau **sélection plage de temps**, sélectionnez une plage de temps prédéfinie.
3. Cliquez sur **appliquer plage**.

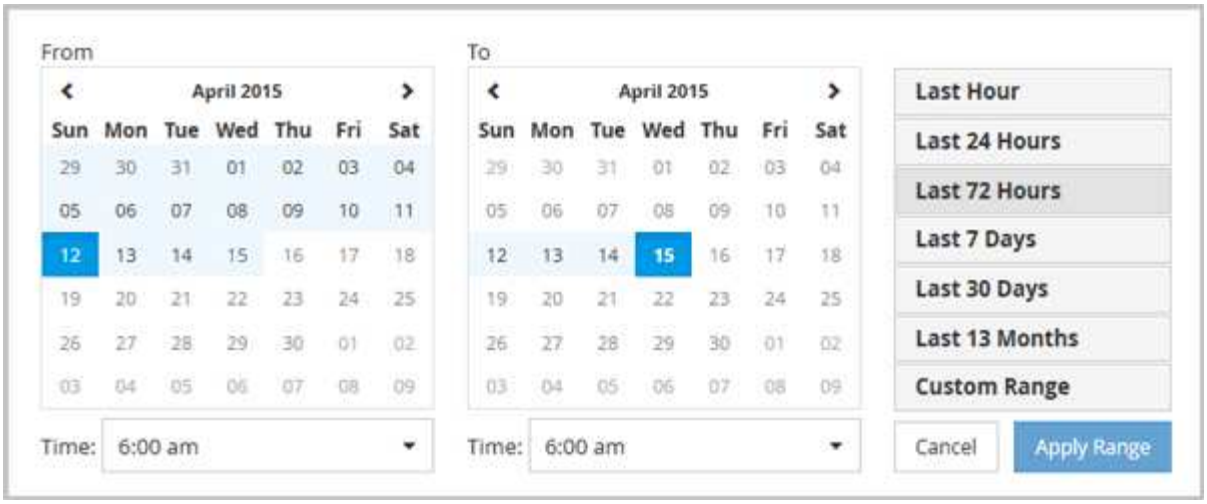
Spécification d’une plage horaire personnalisée

La page Explorateur de performances vous permet de spécifier la plage de date et d’heure de vos données de performances. La spécification d’une plage de temps personnalisée offre une plus grande flexibilité que l’utilisation de plages de temps prédéfinies lors du raffinage des données d’objet de cluster.

Vous pouvez sélectionner une plage horaire comprise entre une heure et 390 jours. 13 mois équivaut 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 d’effectuer un zoom avant sur des événements de performance ou une série d’événements spécifiques. La spécification d’une plage horaire facilite également le dépannage des problèmes de performances potentiels, car la spécification d’une plage de dates et d’heures permet d’afficher plus précisément les données entourant l’événement de performance. Utilisez la commande **Plage horaire** pour sélectionner des plages de date et d’heure prédéfinies, ou pour spécifier votre propre période et une plage de dates personnalisées pouvant aller jusqu’à 390 jours. Les boutons des plages de temps prédéfinies varient de la **dernière heure** à la **derniers 13 mois**.

Si vous sélectionnez l’option **derniers 13 mois** ou si vous spécifiez une plage de dates personnalisée supérieure à 30 jours, une boîte de dialogue vous avertissant que les données de performances affichées pour une période supérieure à 30 jours sont saisies en utilisant des moyennes horaires et pas une interrogation de données de 5 minutes. Par conséquent, une perte de la granularité visuelle de la chronologie peut se produire. Si vous cliquez sur l’option **ne plus afficher** dans la boîte de dialogue, le message ne s’affiche pas lorsque vous sélectionnez l’option **derniers 13 mois** ou que vous spécifiez une plage de dates personnalisée supérieure à 30 jours. Les données récapitulatives s’appliquent également à une période plus courte, si la plage horaire comprend une heure/date qui dépasse 30 jours à partir de la date d’aujourd’hui.

Lors de la sélection d’une plage horaire (personnalisée ou prédéfinie), les plages de temps 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 de temps prédéfinie, cliquez sur l'un des boutons **dernier…** à droite du panneau **Plage de temps**. Lorsque vous sélectionnez une plage horaire prédéfinie, des données pouvant atteindre 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 de temps.
3. Pour sélectionner une plage de dates personnalisée, cliquez sur la date de début dans le calendrier **from** à 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** à droite. Notez que la date de fin par défaut est aujourd'hui, sauf si vous spécifiez une autre date de fin. Le bouton **Plage personnalisée** situé 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 la commande **time** sous le calendrier **from** et sélectionnez l'heure de début. Pour spécifier l'heure de fin, cliquez sur la commande **time** sous le calendrier **to** à droite et sélectionnez l'heure de fin. Le bouton **Plage personnalisée** situé à droite du panneau Plage de temps est mis en surbrillance, indiquant que vous avez sélectionné une plage de temps personnalisée.
5. Vous pouvez également 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 évidence dans les calendriers, les heures de début et de fin spécifiées s'affichent dans les commandes **Time** et le bouton **Custom Range** est mis en surbrillance.
6. Après avoir sélectionné la plage de dates et d'heures, cliquez sur **appliquer la plage**. Les statistiques de performance de cette plage de temps s'affichent dans les graphiques et dans la chronologie des événements.

Définition de la liste des objets corrélés pour le graphique de comparaison

Vous pouvez définir une liste d'objets corrélés pour les données et les comparaisons de performances dans le volet Counter Chart. Par exemple, si votre ordinateur virtuel de stockage (SVM) rencontre un problème de performances, vous pouvez comparer tous les volumes du SVM afin d'identifier le volume à l'origine du problème.

Vous pouvez ajouter n'importe quel objet de la grille des objets corrélés aux volets Comparer et compteur graphique. Cela vous permet d'afficher et de comparer les données de plusieurs objets et avec l'objet racine. Vous pouvez ajouter et supprimer des objets dans et à partir de la grille d'objets corrélés ; cependant, 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 des objets, localisez l'objet que vous souhaitez ajouter, puis 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 des volets Counter Charts. La couleur de l'icône de l'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 pour les objets sélectionnés:

Pour cela…	Prendre cette action…
Cacher 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 de l'œil correspondant à cet objet devient grise.
Affiche un objet masqué	Cliquez sur l'icône en forme d'œil gris de l'objet sélectionné dans le volet comparaison. L'icône oeil revient à sa couleur d'origine et les données de l'objet sont réajoutées aux graphiques du volet compteurs.

3. **Facultatif:** supprimez les objets sélectionnés du volet **Comparer**:

Pour cela…	Prendre cette action…
Supprimer un objet sélectionné	Placez le pointeur de la souris sur le nom de l'objet sélectionné dans le volet de comparaison pour afficher le bouton Supprimer l'objet (**X**), puis cliquez sur le bouton. L'objet est supprimé du volet comparaison et ses données sont effacées des compteurs.
Supprime tous les objets sélectionnés	Cliquez sur le bouton Supprimer tout l'objet (**X**) en haut du volet de comparaison. Tous les objets sélectionnés et leurs données sont supprimés, ne laissant que l'objet racine.

Présentation des graphiques des compteurs

Les graphiques du volet compteurs permettent d'afficher et de comparer les données de performances de l'objet racine et des objets ajoutés à partir de la grille d'objets corrélés.

Cela peut vous aider à comprendre les tendances en matière de performances, ainsi qu'à isoler et résoudre les problèmes de performances.

Les graphiques de compteurs affichés par défaut sont les événements, latence, IOPS et Mbit/s. Vous pouvez choisir d'afficher des graphiques en option : utilisation, capacité utilisée pour les performances, IOPS disponibles, IOPS/To et taux de Miss cache. En outre, vous pouvez choisir d'afficher les valeurs totales ou la répartition par seconde pour les graphiques latence, IOPS, Mbit/s et capacité de performance utilisée.

L'Explorateur des performances affiche certains graphiques de compteurs par défaut, que l'objet de stockage les prenne en charge ou non. Lorsqu'un compteur n'est pas pris en charge, le compteur est vide et le message `Not applicable for <object>` s'affiche.

Les graphiques affichent les tendances de performances pour l'objet racine et pour tous les objets sélectionnés dans le volet comparaison. Les données de chaque graphique sont classées 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 uniques à l'objet sélectionné, ou les objets.

Les couleurs des lignes de tendance correspondent à la couleur du nom de l'objet telle qu'elle apparaît dans le volet de comparaison. Vous pouvez positionner le curseur sur un point sur n'importe quelle ligne de tendance pour afficher les détails de l'heure et de la valeur de ce point.

Si vous souhaitez étudier une période spécifique dans un graphique, vous pouvez utiliser l'une des méthodes suivantes :

- Utilisez le bouton **<** pour développer le volet compteurs afin de couvrir la largeur de la page.
- Utilisez le curseur (lorsqu'il passe à une loupe) pour sélectionner une partie de la période dans la carte pour la mise au point et l'agrandir. Vous pouvez cliquer sur Réinitialiser le zoom du graphique pour rétablir le temps par défaut du graphique.
- Utilisez le bouton **Zoom View** pour afficher un grand tableau de compteur unique contenant des détails étendus et des indicateurs de seuil.

> Parfois, les écarts dans les lignes de tendance s'affichent. Les écarts signifient qu'Unified Manager n'a pas pu collecter les données de performances du système de stockage ou qu'Unified Manager est peut-être en panne.

Types de graphiques de compteur de performances

Des graphiques de performances standard affichent les valeurs des compteurs de l'objet de stockage sélectionné. Chacun des tableaux de compteurs de décomposition affiche les valeurs totales séparées en lecture, écriture et autres catégories. De plus, certains graphiques de compteur de décomposition affichent des détails supplémentaires lorsque le graphique est affiché en vue Zoom.

Le tableau suivant affiche les graphiques de compteurs de performances disponibles.

Tableaux disponibles	Description du tableau
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 vue d'ensemble des raisons pour lesquelles les performances peuvent être affectées.
Latence - Total	Nombre de millisecondes nécessaires pour répondre aux demandes des applications. Notez que les valeurs moyennes de latence sont pondérées en E/S.
Latence : détail	Les mêmes informations sont affichées dans latence Total, mais avec les données de performances séparées en lecture, en écriture et autre latence. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, une 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 un composant du 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'elle est affichée pour un nœud, la sélection « Total » affiche les IOPS des données déplacées à travers ce nœud qui peuvent résider sur le nœud local ou distant et la sélection « Total (local) » affiche les IOPS pour les données qui résident uniquement sur le nœud actuel.

Tableaux disponibles	Description du tableau
IOPS : détail	Les mêmes informations sont affichées dans Total IOPS, mais avec les données de performances séparées en lecture, en écriture et autres IOPS. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, une LUN, ou un espace de noms. Lorsqu'il est affiché dans la vue Zoom, le graphique volumes affiche les valeurs de débit minimum et maximum de QoS, s'il est configuré dans ONTAP. Lorsqu'elle est affichée pour un nœud, la sélection « détail » affiche la répartition des IOPS pour les données qui se déplacent à travers ce nœud sur le nœud local ou distant, et la sélection « analyse (locale) » affiche la répartition des IOPS pour les données qui résident uniquement sur le nœud actuel.
IOPS - protocoles	Les mêmes informations s'affichent dans Total IOPS, mais les données de performance sont séparées dans des graphiques individuels pour le trafic des protocoles CIFS, NFS, FCP, NVMe et iSCSI. Cette option de tableau 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 des E/S, ce compteur mesure le niveau de performances qu'une quantité donnée de capacité de stockage peut fournir. Lorsqu'il est affiché dans la vue Zoom, le graphique des volumes affiche les valeurs de débit QoS attendues et de pic, si configuré dans ONTAP. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un volume.
Mo/s - Total	Nombre de mégaoctets de données transférées vers et depuis l'objet par seconde.

Tableaux disponibles	Description du tableau
MB/s - détail	Mêmes informations que ce graphique, mais avec des données de débit séparées en lectures de disque, des lectures Flash cache, des écritures et autres. Lorsqu'il est affiché dans la vue Zoom, le graphique volumes affiche les valeurs de débit maximum QoS, s'il est configuré dans ONTAP. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, une LUN, ou un espace de noms. Les données de Flash cache s'affichent uniquement pour les nœuds et uniquement lorsqu'un module Flash cache est installé sur le nœud.
Performance Capacity utilisée - Total	Pourcentage de capacité de performance consommé par le nœud ou l'agrégat.
Capacité utilisée – détail	Capacité de performance utilisait des données séparées en protocoles utilisateur et en arrière-plan du système. De plus, la capacité des performances libres est indiquée.
IOPS disponibles - Total	Nombre d'opérations d'entrée/sortie par seconde actuellement disponibles (libres) sur cet objet. Ce nombre est dû à l'soustraction des IOPS actuellement utilisées par rapport aux IOPS totales que Unified Manager calcule que l'objet peut exécuter. L'option de graphique s'applique uniquement lorsque l'objet sélectionné est un nœud ou un agrégat.
Utilisation : total	Pourcentage de ressources disponible de l'objet utilisé. L'utilisation indique l'utilisation des nœuds, l'utilisation des disques pour les agrégats et l'utilisation de la bande passante pour les ports. L'option de graphique s'applique uniquement lorsque l'objet sélectionné est un nœud, un agrégat ou un port.
Taux de Miss cache - Total	Pourcentage de demandes de lecture des applications client renvoyées à partir du disque au lieu d'être renvoyées à partir du 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 diagrammes de performance à afficher dans le volet compteurs. Vous pouvez ainsi afficher des données et des compteurs spécifiques en fonction de vos besoins de performances.

Étapes

1. Dans le volet **Counter Charts**, cliquez sur la liste déroulante **Choose charts**.
2. Ajouter ou supprimer des graphiques :

Pour…	Procédez comme ça…
Ajouter ou supprimer des graphiques individuels	Cliquez sur les cases à cocher en regard des graphiques que vous souhaitez afficher ou masquer
Ajouter tous les graphiques	Cliquez sur **Sélectionner tout**
Retirez tous les graphiques	Cliquez sur **désélectionner tout**

Vos sélections de graphiques s'affichent dans le volet compteurs. Notez que lorsque vous ajoutez des graphiques, les nouveaux graphiques sont insérés dans le volet compteurs afin de correspondre à l'ordre des graphiques répertoriés dans la liste déroulante choisir les graphiques. La sélection de graphiques supplémentaires peut nécessiter un défilement supplémentaire.

Développement du volet compteurs

Vous pouvez développer le volet diagrammes de compteur afin que les graphiques soient plus grands et plus lisibles.

Une fois que vous avez défini les objets de comparaison et la plage horaire des compteurs, vous pouvez afficher un volet compteur plus grand. Utilisez le bouton **<** au milieu de la fenêtre de l'explorateur de performances pour développer le volet.

Étape

1. Développez ou réduisez le volet **Counter Charts**.

Pour…	Procédez comme ça…
Développez le volet graphiques des compteurs pour qu'il s'adapte à la largeur de la page	Cliquez sur le bouton **<**
Réduisez le volet compteurs à la moitié droite de la page	Cliquez sur le bouton **>**

Modification de la mise au point des compteurs sur une période de temps plus courte

Vous pouvez utiliser la souris pour réduire la plage de temps pour vous concentrer sur une période spécifique dans le volet Tableau des compteurs ou dans la fenêtre vue Zoom des diagrammes des compteurs. Cela vous permet d'obtenir une vue plus granulaire et microscopique de n'importe quelle partie de la chronologie des données de performances, des événements et des seuils.

Ce dont vous aurez besoin

Le curseur doit avoir été remplacé par une loupe pour indiquer que cette fonctionnalité est active.

> Lors de l'utilisation de cette fonction, qui modifie la ligne de temps pour afficher des valeurs correspondant à l'affichage plus granulaire, la plage de temps et de dates du sélecteur **plage de temps** ne change pas des valeurs d'origine du graphique.

Étapes

1. Pour effectuer un zoom sur une période spécifique, cliquez à l'aide de la loupe et faites glisser la souris pour mettre en surbrillance la zone à afficher en détail.

   Les valeurs de compteur pour la période de temps que vous sélectionnez remplissent le compteur.

2. Pour revenir à la période d'origine définie dans le sélecteur **Time Range**, cliquez sur le bouton **Reset Chart Zoom**.

   Le compteur s'affiche dans son état d'origine.

Affichage des détails d'un événement dans la chronologie des événements

Vous pouvez afficher tous les événements et leurs détails dans le volet Calendrier des événements de l'Explorateur de performances. Cette méthode permet de visualiser rapidement et efficacement tous les événements d'état et de performances de l'objet racine dans une plage de temps spécifiée, ce qui peut être utile pour résoudre les problèmes de performances.

Le volet Event Timeline 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 son propre calendrier. Les événements uniques et multiples sont représentés par un point d'événement sur le calendrier. Vous pouvez positionner votre curseur sur un point d'événement pour afficher les détails de l'événement. Pour augmenter la granularité visuelle de plusieurs événements, vous pouvez réduire la plage de temps. Cela permet de propager plusieurs événements en un seul événement, ce qui vous permet d'afficher et d'étudier chaque événement séparément.

Chaque point d'événement de performance sur la chronologie des événements s'aligne verticalement avec un pic correspondant dans les lignes de tendance des diagrammes qui sont affichées sous la chronologie des événements. Cela permet une corrélation visuelle directe entre les événements et les performances globales. Les événements de santé sont également affichés dans le calendrier, mais ces types d'événements ne correspondent pas nécessairement à un pic dans un des graphiques de performances.

Étapes

1. Dans le volet **Event Timeline**, placez le curseur sur un point d'événement sur une chronologie pour afficher un résumé de l'événement ou des événements à ce point.

   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 d'un ou plusieurs événements :

Pour cela…	Cliquez sur ce bouton…
Afficher les détails d'un seul événement	**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. Cliquez sur un seul événement dans la boîte de dialogue événements multiples pour afficher la page Détails de l'événement appropriée.

Vue Zoom des diagrammes de compteur

Les diagrammes de compteur offrent une vue Zoom qui vous permet d'effectuer un zoom avant sur les détails de performance au cours de la période spécifiée. Vous pouvez ainsi consulter les informations de performances et les événements avec une granularité bien plus élevée, ce qui est avantageux lors du dépannage des problèmes de performances.

Lorsqu'elles sont affichées dans la vue Zoom, certaines des tableaux de répartition fournissent des informations supplémentaires par rapport à ce qui s'affiche lorsque le graphique n'est pas en vue Zoom. Par exemple, les pages d'affichage Zoom du graphique d'analyse en IOPS, en IOPS/To et en Mo/sec affichent les valeurs de la stratégie QoS pour les volumes et les LUN s'ils ont été définis dans ONTAP.

> Pour les politiques de seuils de performances définis par le système, seules les stratégies « surutilisées des ressources de nœud » et « dépassement de la limite de débit QoS » sont disponibles dans la liste **Policies**. Les autres règles de seuil définies par le système ne sont pas disponibles pour le moment.

Affichage de la vue Zoom des diagrammes de compteur

La vue Zoom des diagrammes de compteur fournit un niveau de détail plus fin pour le compteur sélectionné et son chronogramme associé. Cela amplifie les données du compteur, ce qui vous permet d'obtenir une vue plus précise des événements de performance et de leurs causes sous-jacentes.

Vous pouvez afficher la vue Zoom des diagrammes de compteur pour n'importe quel compteur.

Étapes

1. Cliquez sur **Zoom View** pour ouvrir le graphique sélectionné dans une nouvelle fenêtre de navigateur.

2. Si vous affichez un graphique détaillé, puis cliquez sur **Zoom View** le graphique détaillé est affiché en vue Zoom. Vous pouvez sélectionner **Total** en vue Zoom si vous souhaitez modifier l'option d'affichage.

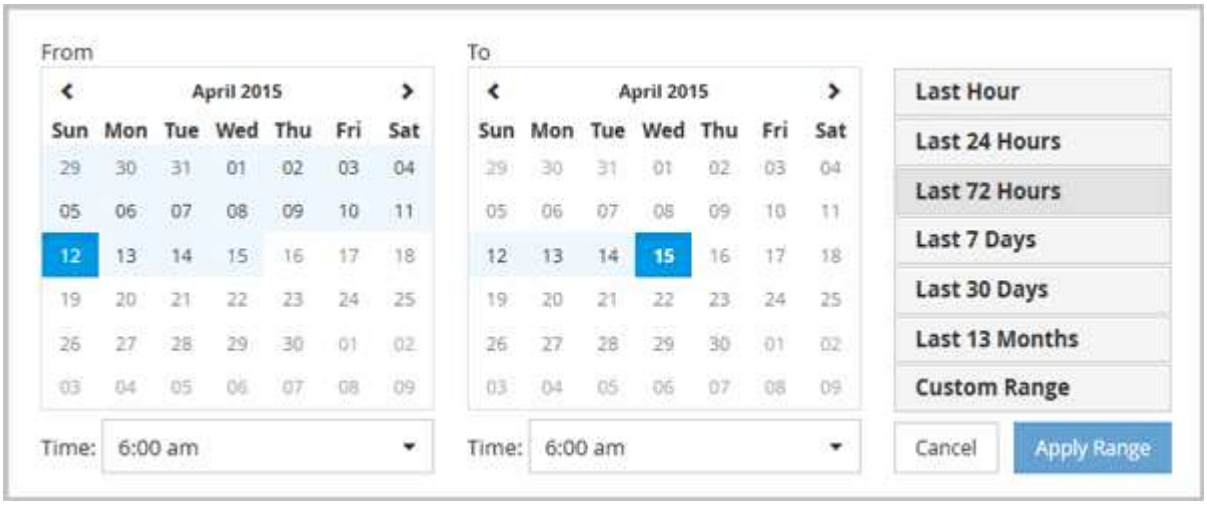
Spécification de la plage de temps dans la vue Zoom

La commande **Plage de temps** de la fenêtre Affichage du zoom des diagrammes de compteur vous permet de spécifier une plage de date et d'heure 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 équivaut 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 d'effectuer un zoom avant sur des événements de performance ou une série d'événements spécifiques. La spécification d'une plage horaire facilite également le dépannage des problèmes de performances potentiels, car la spécification d'une plage de dates et d'heures permet d'afficher plus précisément les données entourant l'événement de performance. Utilisez la commande **Plage horaire** pour sélectionner des plages de date et d'heure prédéfinies, ou pour spécifier votre propre période et une plage de dates personnalisées pouvant aller jusqu'à 390 jours. Les boutons des plages de temps prédéfinies varient de la **dernière heure** à la **derniers 13 mois**.

Si vous sélectionnez l'option **derniers 13 mois** ou si vous spécifiez une plage de dates personnalisée supérieure à 30 jours, une boîte de dialogue vous avertissant que les données de performances affichées pour une période supérieure à 30 jours sont saisies en utilisant des moyennes horaires et pas une interrogation de données de 5 minutes. Par conséquent, une perte de la granularité visuelle de la chronologie peut se produire. Si vous cliquez sur l'option **ne plus afficher** dans la boîte de dialogue, le message ne s'affiche pas lorsque vous sélectionnez l'option **derniers 13 mois** ou que vous spécifiez une plage de dates personnalisée supérieure à 30 jours. Les données récapitulatives s'appliquent également à une période plus courte, si la plage horaire comprend une heure/date qui dépasse 30 jours à partir de la date d'aujourd'hui.

Lors de la sélection d'une plage horaire (personnalisée ou prédéfinie), les plages de temps 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 de temps prédéfinie, cliquez sur l'un des boutons **dernier…** à droite du panneau **Plage de temps**. Lorsque vous sélectionnez une plage horaire prédéfinie, des données pouvant atteindre 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 de

temps.

3. Pour sélectionner une plage de dates personnalisée, cliquez sur la date de début dans le calendrier **from** à 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** à droite. Notez que la date de fin par défaut est aujourd'hui, sauf si vous spécifiez une autre date de fin. Le bouton **Plage personnalisée** situé 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 la commande **time** sous le calendrier **from** et sélectionnez l'heure de début. Pour spécifier l'heure de fin, cliquez sur la commande **time** sous le calendrier **to** à droite et sélectionnez l'heure de fin. Le bouton **Plage personnalisée** situé à droite du panneau Plage de temps est mis en surbrillance, indiquant que vous avez sélectionné une plage de temps personnalisée.
5. Vous pouvez également 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 évidence dans les calendriers, les heures de début et de fin spécifiées s'affichent dans les commandes **Time** et le bouton **Custom Range** est mis en surbrillance.
6. Après avoir sélectionné la plage de dates et d'heures, cliquez sur **appliquer la plage**. Les statistiques de performance de cette plage de temps s'affichent dans les graphiques et dans la chronologie des événements.

Sélection des seuils de performance dans la vue Zoom des diagrammes de compteur

Application de seuils dans la vue Zoom des diagrammes 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 tout en déterminant si le dépannage doit être votre prochaine étape.

La sélection de seuils dans la vue Zoom des diagrammes 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 **Policies** de la vue Zoom des diagrammes de compteur.

Une seule règle à la fois peut être appliquée à l'objet dans la vue Zoom des diagrammes de compteur.

Étape

1. Sélectionnez ou désélectionnez le qui est associé à une stratégie.

   Le seuil sélectionné est appliqué à la vue Zoom des diagrammes de compteur. Les seuils critiques sont affichés sous la forme d'une ligne rouge ; les seuils d'avertissement sont affichés sous la forme d'une ligne jaune.

Affichage de la latence de volume par composant du cluster

Vous pouvez afficher des informations détaillées sur la latence d'un volume à l'aide de la page Volume Performance Explorer. Le graphique compteur latence - Total affiche la latence totale sur le volume et le compteur latence - détail est utile pour déterminer l'impact de la latence de lecture et d'écriture sur le volume.

Par ailleurs, le tableau latence - composants du cluster affiche une comparaison détaillée de la latence de chaque composant du cluster afin de déterminer comment chaque composant contribue à la latence totale du

volume. Les composants de cluster suivants sont affichés :

- Le réseau
- Limite max. De QoS
- Limite minimale de QoS
- Traitement réseau
- Interconnexion de cluster
- Le traitement de données
- Opérations d'agrégats
- Activation de volume
- Ressources MetroCluster
- Latence cloud
- SnapMirror synchrone

Étapes

1. Dans la page **Volume Performance Explorer** pour le volume sélectionné, dans le graphique latence, sélectionnez **Cluster Components** dans le menu déroulant.

   Le tableau latence - composants du cluster est affiché.

2. Pour afficher une version plus grande de la carte, sélectionnez **vue Zoom**.

   Le tableau comparatif des composants du groupe d'instruments s'affiche. Vous pouvez restreindre la comparaison en désélectionnant ou en sélectionnant le qui est associé à chaque composant du cluster.

3. Pour afficher les valeurs spécifiques, déplacez le curseur dans la zone graphique pour afficher la fenêtre contextuelle.

Affichage du trafic des IOPS du SVM par protocole

Vous pouvez afficher des informations détaillées d'IOPS pour un SVM à partir de la page de l'explorateur des performances/SVM. Le graphique Op E/S par sec - total indique l'utilisation totale en IOPS sur la SVM, et le graphique compteurs d'IOPS - détail est utile pour déterminer l'impact des opérations de lecture, d'écriture et autres IOPS sur la SVM.

En outre, le tableau IOPS - protocoles affiche une comparaison détaillée du trafic d'IOPS pour chaque protocole utilisé sur la SVM. Les protocoles suivants sont disponibles :

- CIFS
- NFS
- FCP
- ISCSI
- FC-NVMe

Étapes

1. Dans la page **Performance/SVM Explorer** de votre SVM sélectionné, dans le tableau IOPS, sélectionnez

protocoles dans le menu déroulant.

Le tableau IOPS - protocoles s'affiche.

2. Pour afficher une version plus grande de la carte, sélectionnez **vue Zoom**.

   Le graphique comparatif du protocole avancé IOPS est affiché. Vous pouvez restreindre la comparaison en désélectionnant ou en sélectionnant le qui est associé à un protocole.

3. Pour afficher les valeurs spécifiques, déplacez le curseur dans la zone graphique de l'un des graphiques pour afficher la fenêtre contextuelle.

Affichage des graphiques de latence des volumes et des LUN pour vérifier la performance garantie

Vous pouvez afficher les volumes et les LUN que vous avez souscrits au programme « garantie de performances » pour vérifier que la latence n'a pas dépassé le niveau garanti.

La garantie de latence est une valeur inférieure à la milliseconde par opération, qui ne doit pas être dépassée. Elle est basée sur une moyenne horaire et non sur la période de collecte de performances de cinq minutes par défaut.

Étapes

1. Dans la vue **Performance : tous les volumes** ou **Performance : toutes les LUN**, sélectionnez le volume ou la LUN qui vous intéresse.
2. Dans la page **Performance Explorer** de votre volume ou LUN sélectionné, choisissez **moyenne horaire** dans le sélecteur **Afficher les statistiques dans**.

   La ligne horizontale du graphique latence affiche une ligne plus lisse lorsque les collections de cinq minutes sont remplacées par la moyenne horaire.

3. Si d'autres volumes sont présents sur le même agrégat et sont garantis par performances, vous pouvez ajouter ces volumes pour afficher leur valeur de latence sur le même graphique.

Affichage des performances de tous les clusters de baies SAN

Vous pouvez utiliser la vue performances : tous les clusters pour afficher l'état de performance de vos clusters de baies SAN.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez afficher les informations de présentation de tous les clusters de baies SAN dans la vue Performance : tous les clusters et les détails de la page Cluster / Performance Explorer.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.
2. Assurez-vous que la colonne « personnalité » est affichée dans la vue **Santé : tous les clusters** ou ajoutez-la à l'aide de la commande **Afficher/Masquer**.

Cette colonne affiche « toutes les baies SAN » pour tous les clusters de baies SAN.

3. Pour afficher des informations sur les performances de ces clusters, sélectionnez la vue **Performance : 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 **Explorer**.
6. Sur la page **Cluster / Performance Explorer**, sélectionnez **Nodes sur ce cluster** dans le menu **View and compare**.

   Vous pouvez comparer les statistiques de performances des deux nœuds de ce cluster pour vous assurer que la charge est quasiment identique sur les deux nœuds. En cas d'écarts importants entre les deux nœuds, vous pouvez ajouter le second nœud aux graphiques et comparer les valeurs sur une période plus longue afin d'identifier les problèmes de configuration.

Affichage des IOPS du nœud en fonction des workloads qui ne résident que sur le nœud local

Le tableau des compteurs d'IOPS du nœud peut indiquer où les opérations ne passent que par le nœud local à l'aide d'une LIF réseau pour effectuer des opérations de lecture/écriture sur des volumes d'un nœud distant. Les diagrammes IOPS - « Total (local) » et « panne (locale) » affichent les IOPS pour les données résidant dans des volumes locaux uniquement sur le nœud actuel.

Les versions « locales » de ces diagrammes de compteur sont similaires aux graphiques des nœuds pour la capacité de performance et l'utilisation, car ils affichent également uniquement les statistiques des données résidant sur des volumes locaux.

En comparant les versions « locales » de ces diagrammes de compteur aux versions totales régulières de ces diagrammes, vous pouvez voir s'il y a beaucoup de trafic passant par le noeud local pour accéder aux volumes sur le noeud distant. Ce cas peut entraîner des problèmes de performance, indiqué éventuellement par une utilisation élevée du nœud, si trop d'opérations passent par le nœud local pour atteindre un volume sur un nœud distant. Dans ce cas, vous pouvez déplacer un volume vers le nœud local ou créer une LIF sur le nœud distant où le trafic provenant des hôtes qui accèdent à ce volume peut être connecté.

Étapes

1. Dans la page **Performance/Node Explorer** de votre nœud sélectionné, dans le tableau 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. Dans 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. Affichez les deux graphiques les uns à côté des autres et identifiez les zones où les valeurs d'IOPS semblent être assez différentes.
6. Déplacez le curseur de la souris sur ces zones pour comparer les IOPS locales et totales d'un point dans le temps spécifique.

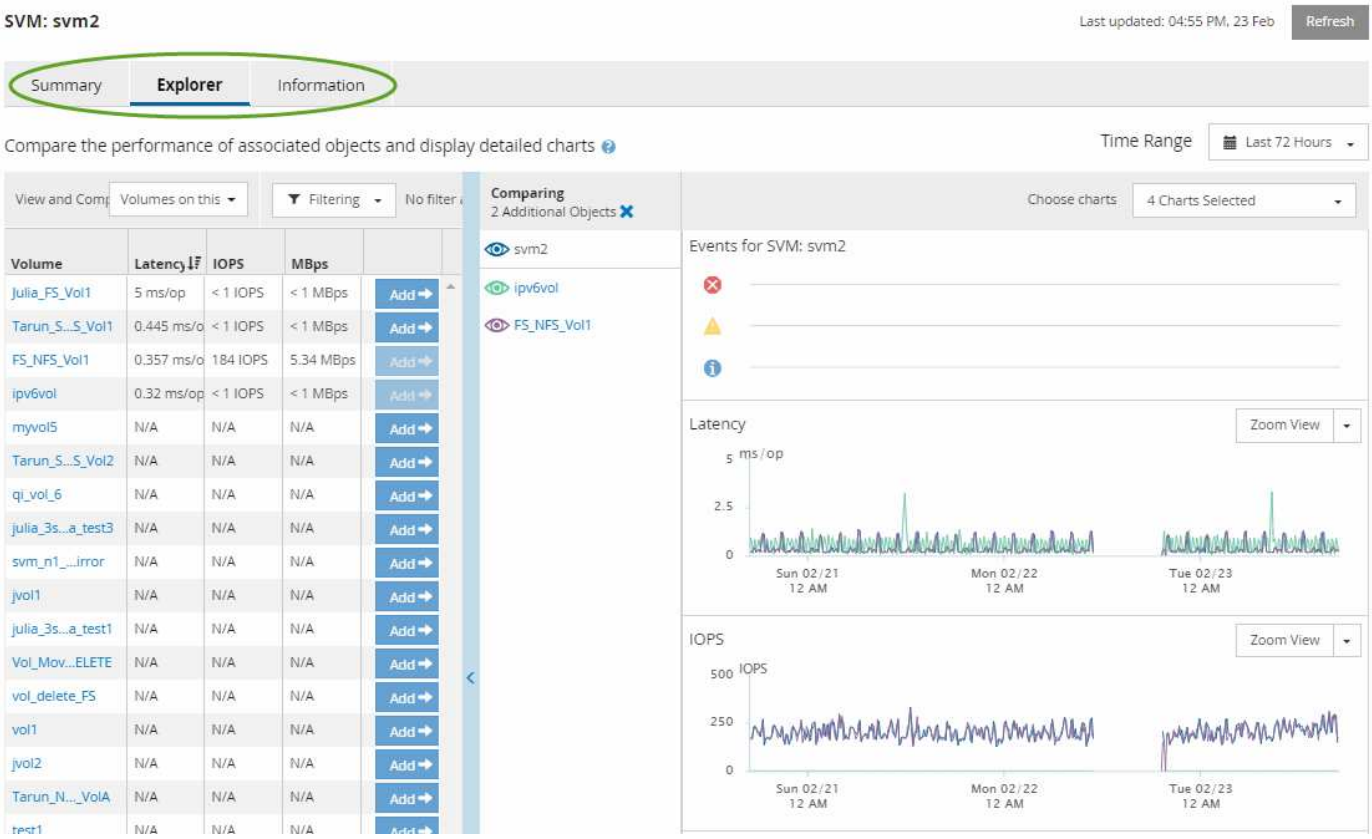
Composants des pages d'arrivée d'objet

Les pages d'arrivée d'objet fournissent des détails sur tous les événements critiques, d'avertissement et d'information. Elles offrent une vue détaillée des performances de tous les objets du cluster. Vous pouvez ainsi sélectionner et comparer des objets individuels sur différentes périodes.

Les pages de destination d'objet vous permettent d'examiner les performances globales de tous les objets et de comparer les données de performances d'objet dans un format côte à côte. Cela est bénéfique lors de l'évaluation des performances et du dépannage des événements.

> Les données affichées dans les panneaux récapitulatifs des compteurs et dans les 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 d'arrivée d'objet affichant les informations de l'Explorateur :



Selon l'objet de stockage affiché, la page d'accueil de l'objet peut disposer des onglets suivants qui fournissent des données de performances sur l'objet :

- Récapitulatif

  Affiche trois ou quatre graphiques de compteur contenant les événements et les performances par objet pour la période de 72 heures précédente, y compris une ligne de tendance indiquant les valeurs haute et basse pendant 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 liés. Cet onglet comprend jusqu'à onze diagrammes de compteur et un sélecteur de plage de temps, qui vous permettent d'effectuer diverses comparaisons.

- Informations

  Affiche les valeurs des attributs de configuration sans performances relatives à l'objet de stockage, y compris la version installée du logiciel ONTAP, le nom du partenaire haute disponibilité et le nombre de ports et de LIF.

- Les meilleurs collaborateurs

  Pour les clusters : affiche les objets de stockage qui présentent les meilleures performances ou les meilleures performances, en fonction du compteur de performances sélectionné.

- Planification des basculements

  Pour les nœuds : affiche l'estimation de l'impact sur la performance d'un nœud en cas de panne du partenaire de haute disponibilité du nœud.

- Détails

  Pour les volumes : affiche des statistiques de performances détaillées pour toutes les activités et opérations d'E/S de la charge de travail de volume sélectionnée. Cet onglet est disponible pour les volumes FlexVol, les volumes FlexGroup et les composants de FlexGroups.

Page récapitulative

La page Récapitulatif affiche les graphiques compteurs qui contiennent des informations détaillées sur les événements et les performances par objet pour la période de 72 heures précédente. Ces données ne sont pas automatiquement actualisées, mais sont en cours à compter du dernier chargement de page. Les graphiques de la page Résumé répondent à la question *dois-je regarder plus loin?*

Graphiques et statistiques des compteurs

Les tableaux récapitulatifs offrent un aperçu rapide et général de la dernière période de 72 heures et vous aident à identifier les problèmes possibles nécessitant une enquête plus approfondie.

Les statistiques des compteurs de la page récapitulative sont affichées sous forme de graphiques.

Vous pouvez positionner le curseur sur la ligne de tendance dans un graphique pour afficher les valeurs de compteur d'un point dans le temps particulier. Les tableaux récapitulatifs affichent également le nombre total d'événements critiques et d'avertissements 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.

- **MB/s**

  Débit moyen, exprimé en mégaoctets par seconde.

  Affiché pour tous les types d'objets.

- **Capacité de performance utilisée**

  Pourcentage de capacité de performance consommé par un nœud ou un agrégat.

  Affiché pour les nœuds et les agrégats uniquement.

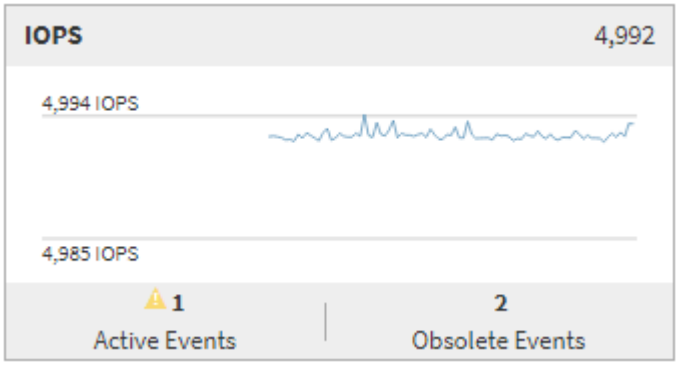
- **Utilisation**

  Pourcentage d'utilisation des objets pour les nœuds et les agrégats, ou utilisation de la bande passante pour les ports.

  Affiché pour les nœuds, les agrégats et les ports uniquement.

Le positionnement du curseur sur le nombre d'événements pour les événements actifs indique le type et le nombre d'événements. Les événements critiques sont affichés en rouge ( ) et les événements d'avertissement en jaune ( ).

Le nombre en haut à droite du graphique dans la barre grise correspond à la valeur moyenne des 72 dernières heures. Les chiffres indiqués en bas et en haut du graphique de tendance sont les valeurs minimale et maximale pour la dernière période de 72 heures. La barre grise sous le tableau contient le nombre d'événements actifs (nouveaux et acquittés) et d'événements obsolètes de la dernière période de 72 heures.



- **Diagramme de compteur de latence**

  Le graphique compteur de latence offre une vue d'ensemble générale de la latence de l'objet pour la période de 72 heures précédente. La valeur de latence correspond au temps de réponse moyen pour

toutes les demandes d'E/S ; exprimé en millisecondes par opération, temps de service, temps d'attente, ou les deux cas rencontrés par un paquet de données ou un bloc dans le composant de stockage du cluster à prendre en compte.

Haut (valeur de compteur) : le nombre dans l'en-tête affiche la moyenne pour la période de 72 heures précédente.

Moyen (graphique de performances) : le nombre au bas du graphique affiche la latence la plus faible, et le chiffre en haut du graphique affiche la latence la plus élevée pour la période de 72 heures précédente. Positionnez le curseur de votre souris sur la ligne de tendance du graphique pour afficher la valeur de latence d'une heure précise.

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.

- **Diagramme de compteur d'IOPS**

  Le tableau des compteurs d'IOPS fournit une présentation générale de l'état des IOPS de l'objet pour la période précédente de 72 heures. IOPS indique la vitesse du système de stockage en nombre d'opérations d'entrée/sortie par seconde.

  Haut (valeur de compteur) : le nombre dans l'en-tête affiche la moyenne pour la période de 72 heures précédente.

  Moyen (graphique de performances) : le nombre au 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. Positionnez le curseur de votre souris sur la ligne de tendance du graphique pour afficher la valeur IOPS d'une heure précise.

  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.

- **Compteur MB/s**

  Le diagramme de 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 compteur MB/s fournit une vue d'ensemble de haut niveau de la santé MB/s de l'objet pour la période de 72 heures précédente.

  Haut (valeur de compteur) : le nombre dans l'en-tête affiche le nombre moyen de Mo/s pour la période de 72 heures précédente.

  Moyen (graphique de performances) : la valeur au bas du graphique affiche le nombre le plus faible de MB/s, et la valeur au haut du graphique affiche le nombre le plus élevé de MB/s pour la période précédente de 72 heures. Placez le curseur sur la ligne de tendance du graphique pour afficher la valeur MB/s d'une heure spécifique.

  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 de compteur capacité de performance utilisée**

  Le tableau des compteurs capacité de performances utilisée affiche le pourcentage de capacité de performance consommé par l'objet.

Haut (valeur de compteur): le nombre dans l'en-tête affiche la capacité moyenne utilisée pour la période de 72 heures précédente.

Moyen (graphique de performances) : la valeur au bas du graphique affiche le pourcentage de capacité de performance le plus faible utilisé, et la valeur en haut du graphique affiche le pourcentage de capacité de performance le plus élevé pour la période de 72 heures précédente. Positionnez le curseur sur la ligne de tendance du graphique pour afficher la valeur de la capacité de performance utilisée pour une période donnée.

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.

- **Diagramme du compteur d'utilisation**

  Le graphique du compteur d'utilisation affiche le pourcentage d'utilisation de l'objet. Le graphique du compteur d'utilisation offre une vue d'ensemble détaillée du pourcentage d'utilisation de l'objet ou de la bande passante pour la période de 72 heures précédente.

  Haut (valeur de compteur) : le nombre dans l'en-tête affiche le pourcentage moyen d'utilisation pour la période de 72 heures précédente.

  Moyen (graphique de performances) : la valeur au bas du graphique affiche le pourcentage d'utilisation le plus faible, et la valeur en haut du graphique affiche le pourcentage d'utilisation le plus élevé pour la période de 72 heures précédente. Positionnez le curseur sur la ligne de tendance du graphique pour afficher la valeur d'utilisation d'une heure spécifique.

  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 Historique des événements, le cas échéant, répertorie les événements les plus récents survenus sur cet objet. Cliquez sur le nom de l'événement pour afficher les détails de l'événement sur la page Détails de l'événement.

Composants de la page Explorateur de performances

La page Performance Explorer vous permet de comparer les performances d'objets similaires dans un cluster, par exemple tous les volumes d'un cluster. Cette fonction est utile pour résoudre les problèmes de performances et ajuster les performances des objets. Vous pouvez également comparer des objets avec l'objet racine, qui est la référence par rapport à laquelle d'autres comparaisons d'objets sont effectuées.

Vous pouvez cliquer sur le bouton **basculer vers l'affichage de l'état de santé** pour afficher la page Détails de l'état de santé de cet objet. Dans certains cas, vous apprendrez des informations importantes sur les paramètres de configuration du stockage de cet objet qui peuvent vous aider à résoudre un problème.

La page de l'explorateur de performances affiche la liste des objets du cluster et leurs données de performance. Cette page affiche tous les objets de cluster du même type (par exemple, les volumes et leurs statistiques de performance spécifiques aux objets) dans un format tabulaire. Cette vue fournit une vue d'ensemble efficace des performances des objets du cluster.

Si « N/A » apparaît dans une cellule de la table, cela signifie qu'une valeur pour ce compteur n'est pas disponible parce qu'il n'y a pas d'E/S sur cet objet à l'heure actuelle.

La page Explorateur de performances contient les composants suivants :

- **Plage de temps**

  Permet de sélectionner une plage horaire pour les données d'objet.

  Vous pouvez choisir une plage prédéfinie ou spécifier votre propre plage horaire personnalisée.

- **Afficher et Comparer**

  Permet de sélectionner le type d'objet corrélé qui est affiché dans la grille.

  Les options disponibles dépendent du type d'objet racine et des 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.

- **Filtrage**

  Permet de réduire la quantité de données reçues en fonction de vos préférences.

  Vous pouvez créer des filtres qui s'appliquent aux données d'objet (par exemple, IOPS supérieures à 4). Vous pouvez ajouter jusqu'à quatre filtres simultanés.

- * Comparaison*

  Affiche la liste des objets que vous avez sélectionnés pour la comparaison avec l'objet racine.

  Les données des objets du volet comparaison sont affichées dans les compteurs.

- **Afficher les statistiques dans**

  Pour les volumes et les LUN, vous permet de sélectionner si les statistiques s'affichent après chaque cycle de collecte (5 minutes par défaut) ou si les statistiques sont affichées sous forme de moyenne horaire. Cette fonctionnalité vous permet de consulter l'graphique de latence en prise en charge du programme NetApp de garantie de la performance.

- **Diagrammes de compteur**

  Affiche les données représentées sous forme graphique pour chaque catégorie de performance d'objet.

  En général, 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.

- **Calendrier des événements**

  Affiche les événements de performance et d'intégrité qui se produisent sur la chronologie que vous avez sélectionnée dans le composant intervalle de temps.

Gestion des performances à l'aide des informations de groupe de règles de QoS

Unified Manager vous permet d'afficher les groupes de règles de qualité de service disponibles sur tous les clusters que vous surveillez. Ces règles peuvent avoir été définies à l'aide du logiciel ONTAP (System Manager ou de l'interface de ligne de commandes ONTAP) ou de règles de niveau de service Performance de Unified Manager. Unified Manager affiche également quels volumes et LUN ont un groupe de règles de QoS attribué.

Pour plus d'informations sur le réglage des paramètres QoS, reportez-vous à la section "Présentation de la gestion des performances"

Comment la QoS du stockage peut contrôler le débit des workloads

Vous pouvez créer un groupe de règles de qualité de services (QoS) pour contrôler la limite des E/S par seconde (IOPS) ou du débit (Mbit/s) pour les workloads qu'il contient. Si les charges de travail font partie d'un groupe de règles sans limite définie, telles que le groupe de règles par défaut ou la limite définie ne répond pas à vos besoins, vous pouvez augmenter la limite ou déplacer les charges de travail vers un nouveau groupe de règles ou un groupe existant présentant la limite souhaitée.

Il est possible d'affecter des groupes de règles de QoS « classiques » à des charges de travail individuelles, par exemple un seul volume ou une LUN. Dans ce cas, le workload peut utiliser la limite de débit complète. Les groupes de règles de qualité de service peuvent également être affectés à plusieurs charges de travail, dans ce cas la limite de débit est « rouge » au sein des charges de travail. Par exemple, une limite de 9,000 000 IOPS attribuée à trois charges de travail permettrait de limiter les IOPS combinées au-delà de 9,000 000 IOPS.

Il est également possible d'attribuer des groupes de règles de QoS « évolutifs » à des charges de travail individuelles ou à plusieurs charges de travail. Cependant, même lorsqu'il est attribué à plusieurs charges de travail, le débit de chaque charge de travail est limité au lieu de partager la valeur du débit avec d'autres charges. De plus, les règles de QoS adaptative ajustent automatiquement le débit en fonction de la taille du volume et par charge de travail, ainsi le rapport IOPS/téraoctets selon la taille du volume modifié. Par exemple, si le pic est défini sur 5,000 IOPS/To dans une règle de QoS adaptative, un volume de 10 To a un débit maximal de 50,000 IOPS. Si le volume a été redimensionné de façon ultérieure à 20 To, la QoS adaptative ajuste le nombre maximal de 100,000 000 IOPS.

À partir de la version ONTAP 9.5, vous pouvez inclure la taille de bloc lors de la définition d'une règle de QoS adaptative. Cette configuration est ainsi convertie en seuil IOPS/To en Mo/s en nombre maximal de blocs dans les cas où les charges de travail utilisent des tailles de blocs très importantes, dont le débit est ensuite élevé.

Pour les règles de QoS des groupes partagés, lorsque les IOPS ou les Mo/s de tous les workloads d'un groupe de règles dépassent la limite définie, le groupe de règles accélère les workloads pour limiter leur activité, ce qui peut diminuer la performance de tous les workloads du groupe de règles. Si un événement de performance dynamique est généré par la limitation de groupe de règles, la description de l'événement affiche le nom du groupe de règles concerné.

Dans le vue Performance: All 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 peut avoir contribué à l'évènement. Sur la page de l'explorateur de volumes/performances, vous pouvez sélectionner d'autres volumes ou LUN sur le volume pour

comparer les IOPS du workload affecté ou l'utilisation du débit Mbit/s.

En attribuant les charges de travail sur lesquelles les ressources de nœud sont surutilisées à un paramètre de groupe de règles plus restrictif, le groupe de règles accélère les charges de travail en vue de limiter leur activité, ce qui permet de réduire l'utilisation des ressources de ce nœud. Toutefois, si vous souhaitez que la charge de travail puisse utiliser davantage de ressources de nœud, vous pouvez augmenter la valeur du groupe de règles.

Vous pouvez utiliser System Manager, les commandes ONTAP ou les niveaux de service de performance de Unified Manager pour gérer les groupes de règles, notamment les tâches suivantes :

- Création d'une « policy group »
- Ajout ou suppression de charges de travail dans un « policy group »
- Déplacement d'une charge de travail entre des groupes de règles
- Modification de la limite de débit d'un groupe de règles
- Déplacement d'une charge de travail vers un autre agrégat et/ou nœud

Affichage de tous les groupes de règles de QoS disponibles sur tous les clusters

Vous pouvez afficher la liste de tous les groupes de règles de QoS disponibles sur les clusters qui surveillent Unified Manager. Cela inclut les règles de QoS classiques, les règles de QoS adaptatives et les règles de qualité de service gérées par les règles de niveau de services de performance de Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **QoS Policy Groups**.

   Les performances : l'affichage classique des groupes de règles de QoS sont affichées par défaut.

2. Affichez les paramètres de configuration détaillés pour chaque groupe de règles de QoS traditionnel disponible.
3. Cliquez sur le bouton développer (⌄) en regard du nom du groupe de stratégies QoS pour afficher plus de détails sur le groupe de règles.
4. Dans le menu Affichage, sélectionnez l'une des options supplémentaires pour afficher tous les groupes de règles de QoS adaptatifs ou pour afficher tous les groupes de règles de QoS créés à l'aide des niveaux de service Performance Unified Manager.

Affichage des volumes ou des LUN qui appartiennent au même groupe de règles de QoS

Vous pouvez afficher la liste des volumes et des LUN qui ont été attribués au même groupe de règles de QoS.

Dans le cas des groupes de règles de QoS traditionnels qui sont « rouges » entre plusieurs volumes, il peut être utile de vérifier si certains volumes utilisent le débit défini pour le groupe de règles. Il vous aide également à décider si vous pouvez ajouter d'autres volumes au groupe de règles sans affecter les autres volumes.

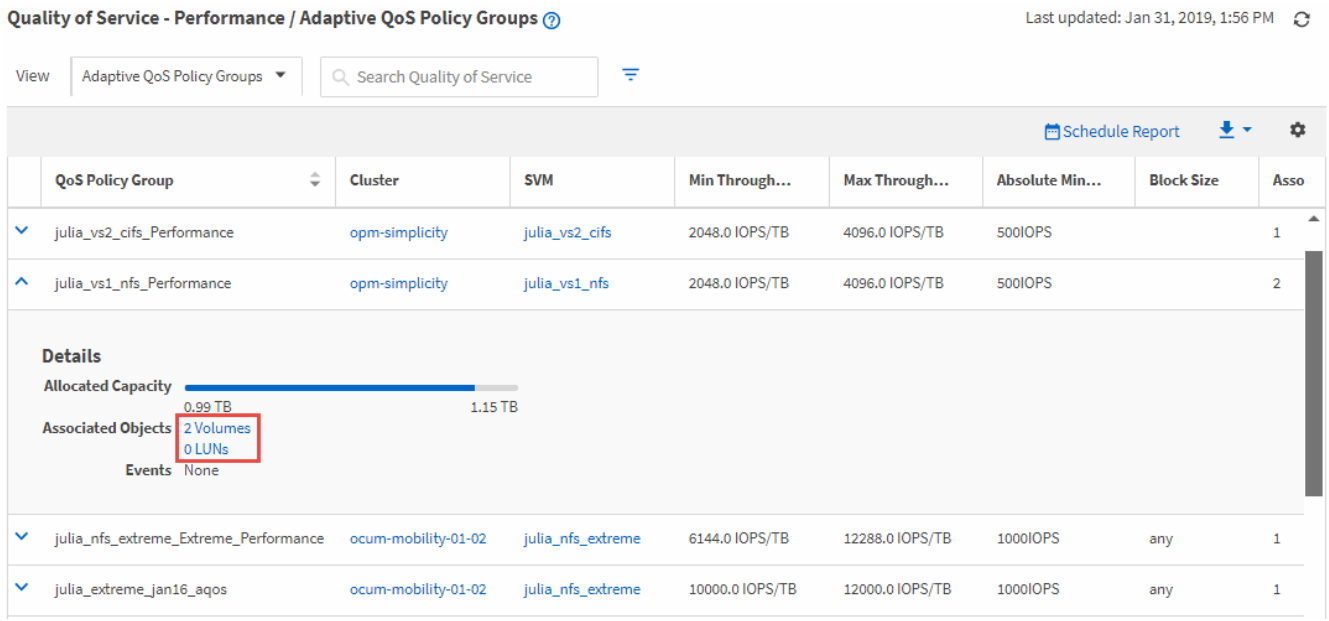
Dans le cas des règles de QoS adaptative et des règles de niveaux de service de performance Unified Manager, Cela peut être utile pour afficher tous les volumes ou LUN qui utilisent une « policy group » afin de voir les objets qui seraient affectés si vous avez modifié les paramètres de configuration de la règle de QoS.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **QoS Policy Groups**.

   Les performances : l'affichage classique des groupes de règles de QoS sont affichées par défaut.

2. Si vous êtes intéressé par le groupe de polices traditionnelles, restez sur cette page. Sinon, sélectionnez l'une des options d'affichage supplémentaires pour afficher tous les groupes de règles de QoS adaptatifs ou tous les groupes de règles de QoS créés par les niveaux de service Performance Unified Manager.
3. Dans la stratégie QoS qui vous intéresse, cliquez sur le bouton développer ( ) en regard du nom du groupe de règles QoS pour en savoir
   plus.



4. Cliquez sur le lien volumes ou LUN pour afficher les objets qui utilisent cette politique de QoS.

   La page d'inventaire des performances des volumes ou des LUN s'affiche avec la liste triée des objets qui utilisent la politique de QoS.

Affichage des paramètres de « policy group » QoS appliqués à des volumes ou LUN spécifiques

Vous pouvez afficher les groupes de règles de QoS appliqués à vos volumes et LUN et afficher les paramètres de configuration détaillés de chaque règle de QoS pour accéder à la vue des groupes de règles de QoS.

Les étapes pour afficher la politique de QoS appliquée à un volume sont indiquées ci-dessous. Les étapes permettant d'afficher ces informations concernant une LUN sont similaires.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.

   La vue Santé : tous les volumes s'affiche par défaut.

2. Dans le menu Affichage, sélectionnez **Performance: Volumes dans QoS Policy Group**.
3. Recherchez le volume que vous souhaitez consulter et faites défiler vers la droite jusqu'à ce que la

colonne **QoS Policy Group** s'affiche.

4. Cliquez sur le nom du groupe de stratégies QoS.

   La page QoS correspondante s'affiche selon qu'il s'agit d'une règle de QoS classique, d'une règle de QoS adaptative ou d'une règle de QoS créée à l'aide des niveaux de service Performance Unified Manager.

5. Afficher les paramètres de configuration détaillés de la « policy group » de QoS
6. Cliquez sur le bouton développer ( ) en regard du nom du groupe de stratégies QoS pour afficher plus de détails sur le groupe de règles.

Affichage des graphiques de performances pour comparer les volumes ou les LUN qui se trouvent dans le même groupe de règles de QoS

Vous pouvez afficher les volumes et les LUN qui se trouvent dans les mêmes groupes de règles de QoS, puis comparer les performances d'un seul graphique Op E/S par sec, B./s ou Op E/S par sec ou par sec pour identifier tout problème.

Les étapes de comparaison des performances des volumes d'un même groupe de règles de QoS sont présentées ci-dessous. Les étapes permettant d'afficher ces informations concernant une LUN sont similaires.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.

   La vue Santé : tous les volumes s'affiche par défaut.

2. Dans le menu Affichage, sélectionnez **Performance: Volumes dans QoS Policy Group**.
3. Cliquez sur le nom du volume que vous souhaitez consulter.

   La page Explorateur de performances s'affiche pour le volume.

4. Dans le menu Affichage et comparaison, sélectionnez **volumes dans le même groupe de règles QoS**.

   Les autres volumes qui partagent la même politique de 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 compteurs d'IOPS, de Mo/s, d'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 des intervalles différents autres que la valeur par défaut de 72 heures.

Affichage des différents types de règles de QoS dans les graphiques de débit

Vous pouvez afficher les paramètres de règles de qualité de service (QoS) définis par ONTAP et appliqués à un volume ou à une LUN dans les tableaux de bord Performance Explorer et Workload Analysis Op E/S par sec, IOPS/To et MB/s. Les informations affichées dans les graphiques diffèrent selon le type de règle de 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, limitant ainsi l'impact sur les charges de travail concurrentes pour les ressources système. Un paramètre de

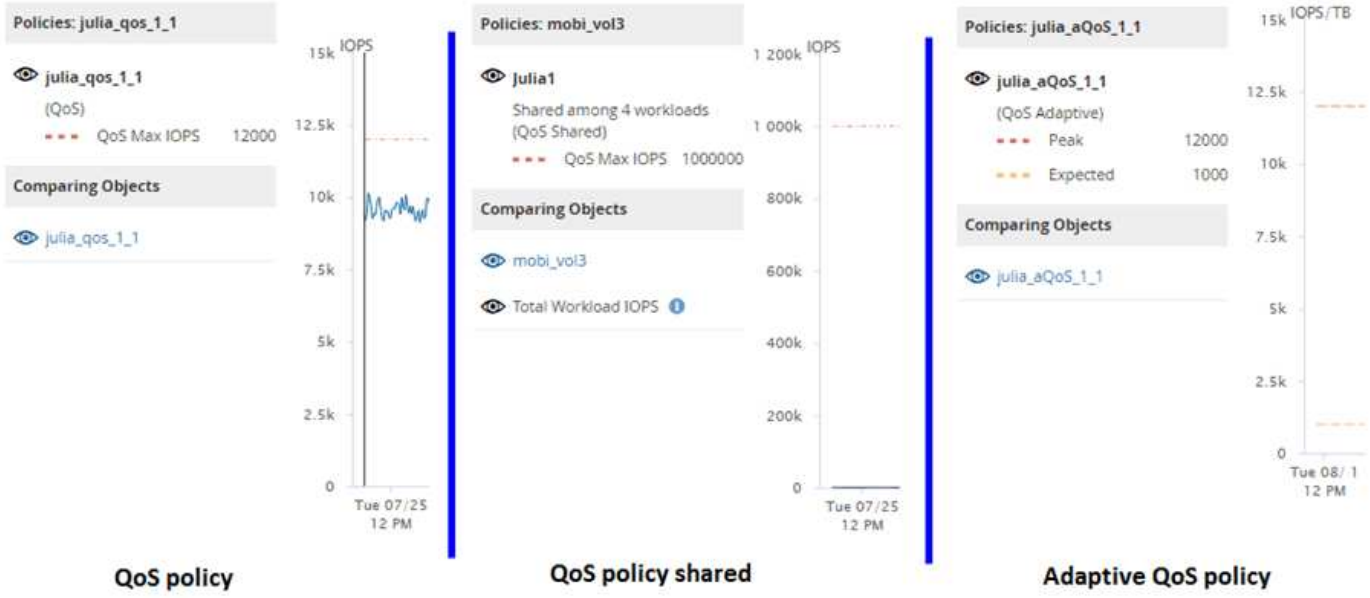
débit minimal (ou « attendu ») définit le débit minimal à disposition de la charge de travail afin qu'une charge de travail critique réponde aux objectifs de débit minimaux, indépendamment de la demande des charges de travail concurrentes.

Les politiques de QoS partagées et non partagées pour les IOPS et les MB/s utilisent les termes "minimum" et "maimum" pour définir le sol et le plafond. Les politiques de QoS adaptative pour l'IOPS/To, qui ont été introduites à ONTAP 9.3, utilisent les termes « attendus » et « pic » pour définir le sol et le plafond.

Bien que ONTAP vous permet de créer ces deux types de règles de QoS, selon la méthode d'application des workloads, il existe trois manières que la règle de QoS s'affiche dans les graphiques de performances.

Type de règle	Fonctionnalité	Indicateur dans l'interface Unified Manager
Politique partagée de la qualité de service attribuée à une charge de travail unique ou règle de qualité de service non partagée attribuée à une seule charge de travail ou à plusieurs charges de travail	Chaque workload peut consommer le paramètre de débit spécifié	Affiche « `(QoS)` »
Règle partagée de qualité de service attribuée à plusieurs charges de travail	Toutes les charges de travail partagent le paramètre de débit spécifié	Affiche «»(QoS partagée)»
Règle de QoS adaptative attribuée à une ou plusieurs charges de travail	Chaque workload peut consommer le paramètre de débit spécifié	Affiche « `(QoS Adaptive)` »

La figure suivante montre un exemple de l'affichage des trois options dans les tableaux des compteurs.



Lorsqu'une politique de QoS normale a été définie dans IOPS apparaît dans le graphique IOPS/To pour une charge de travail, ONTAP convertit la valeur d'IOPS en valeur d'IOPS/To, et Unified Manager affiche cette règle dans le graphique IOPS/To avec le texte « QoS, définie en IOPS ».

Lorsqu'une règle de QoS adaptative qui a été définie en IOPS/To apparaît dans le graphique IOPS pour une charge de travail, ONTAP convertit la valeur IOPS/To en valeur IOPS, et Unified Manager affiche cette règle dans le graphique IOPS avec le texte « QoS Adaptive - utilisée » Définies en IOPS/To« (IOPS/To) » ou « QoS adaptative - allouée, définie en IOPS/To » selon la configuration du paramètre d'allocation d'IOPS maximal. Lorsque le paramètre d'allocation est défini sur « espace alloué », les IOPS maximales sont calculées en fonction de la taille du volume. Lorsque le paramètre d'allocation est défini sur « espace utilisé », les IOPS maximales sont calculées en fonction de la quantité de données stockées sur le volume, en tenant compte des gains d'efficacité du stockage.

> Le tableau 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 tableau lorsque la capacité utilisée tombe en dessous de 128 Go au cours de la période sélectionnée.

Affichage des paramètres minimal et maximal de QoS des charges de travail dans l'explorateur de performances

Vous pouvez afficher les paramètres de règles de qualité de service (QoS) définies par ONTAP sur un volume ou une LUN dans les graphiques de l'explorateur de performances. La définition maximale du débit limite l'impact des workloads concurrents sur les ressources système. La valeur minimale du débit permet de s'assurer qu'une charge de travail critique satisfait aux objectifs de débit minimaux, indépendamment de la demande des charges de travail concurrentes.

Le débit de QoS « minimum » et « maimum » en IOPS et en Mo/s ne sont affichés dans les diagrammes de compteur que s'ils ont été configurés dans ONTAP. Les paramètres de débit minimal sont uniquement disponibles sur les systèmes qui exécutent le logiciel ONTAP 9.2 ou version ultérieure, uniquement sur les systèmes AFF. Ils peuvent être définis uniquement pour la valeur d'IOPS pour le moment.

Les règles de QoS adaptative sont disponibles à partir de ONTAP 9.3 et sont exprimées en IOPS/To au lieu des IOPS. Ces règles ajustent automatiquement la valeur de la règle de qualité de services en fonction de la taille du volume, par charge de travail, ainsi le rapport IOPS/téraoctets selon la taille du volume modifié. Vous pouvez appliquer un « policy group » de QoS adaptative aux volumes uniquement. La terminologie de la qualité de service « attendue » et « pic » est utilisée pour les politiques de QoS adaptatives plutôt que de minimum et maximum.

Unified Manager génère des événements d'avertissement pour les violations de règles de QoS lorsque le débit de la charge de travail a dépassé le paramètre maximal de règle de QoS défini pour chaque période de collecte de performances pour l'heure précédente. Le débit de la charge de travail peut dépasser le seuil de qualité de service pendant une courte période seulement au cours de chaque période de collecte, mais Unified Manager affiche le débit « moyen » pendant la période de collecte sur le graphique. Vous pouvez donc voir des événements QoS alors que le débit d'une charge de travail n'a pas dépassé le seuil des règles affiché dans le tableau.

Étapes

1. Dans la page **Performance Explorer** pour le volume ou le LUN sélectionné, effectuez les opérations suivantes pour afficher les paramètres de plafond et de sol de la QoS :

Les fonctions que vous recherchez…	Procédez comme ça…
Afficher le plafond des IOPS (QoS max)	Dans le graphique Total ou décomposition en IOPS, cliquez sur **vue Zoom**.
Afficher le plafond MB/s (QoS max)	Dans le graphique MB/s Total ou décomposition, cliquez sur **Zoom View**.
Voir au sol des IOPS (QoS min)	Dans le graphique Total ou décomposition en IOPS, cliquez sur **vue Zoom**.
Afficher le plafond IOPS/To (pic de QoS)	Pour les volumes, dans le graphique IOPS/To, cliquez sur **vue Zoom**.
Afficher les paramètres IOPS/To (QoS attendue)	Pour les volumes, dans le graphique IOPS/To, cliquez sur **vue Zoom**.

La ligne horizontale en pointillés correspond à la valeur de débit minimale ou maximale définie dans ONTAP. Vous pouvez également voir les modifications apportées aux valeurs de QoS.

2. Pour afficher les valeurs en IOPS et en Mo/s spécifiques par rapport au paramètre QoS, déplacez le curseur dans la zone graphique pour afficher la fenêtre contextuelle.

Si vous remarquez que certains volumes ou LUN ont des IOPS ou des Mo/s très élevés et que certains stress les ressources système, vous pouvez utiliser System Manager ou l'interface de ligne de commande de ONTAP pour ajuster les paramètres de 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, reportez-vous à la section "Présentation de la gestion des performances"

Gestion des performances grâce à la capacité en termes de performances et aux informations d'IOPS disponibles

Performance Capacity indique le débit que vous pouvez obtenir d'une ressource sans dépasser les performances utiles de cette ressource. Lorsqu'il est utilisé des compteurs de performances existants, la capacité de performances est le point où l'utilisation maximale est atteint depuis un nœud ou un agrégat avant que la latence ne devienne un problème.

Unified Manager collecte les statistiques de capacité des performances à partir des nœuds et des agrégats de chaque cluster. *Performance Capacity used* représente le pourcentage de capacité de performance actuellement utilisée et *performance free* représente le pourcentage de capacité de performance qui est toujours disponible.

Tandis que la fonction libération de la capacité qui constitue un pourcentage de ressource encore disponible, *Available IOPS* représente le nombre d'IOPS pouvant être ajoutés à la ressource avant d'atteindre la capacité de performance maximale. Cette mesure vous permet d'ajouter des charges de travail d'un nombre prédéterminé d'IOPS à une ressource.

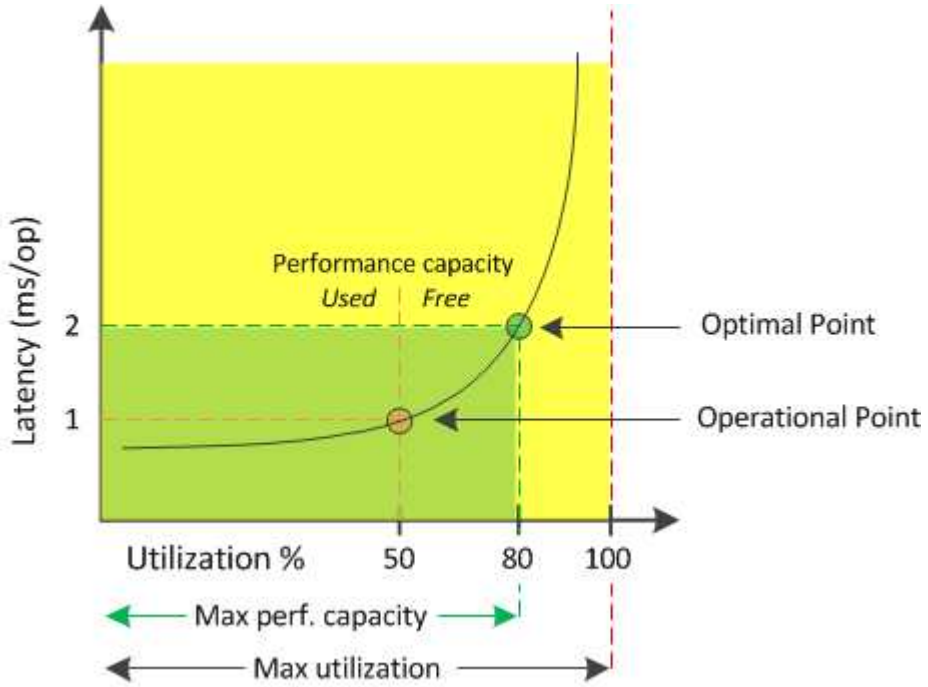
Le contrôle des informations sur la capacité en matière de performances présente les avantages suivants :

- Aide au provisionnement et à l'équilibrage des flux de travail.
- Vous aide à éviter de surcharger un nœud ou de repousser ses ressources au-delà du point optimal, réduisant ainsi la nécessité de résoudre le problème.
- Elle vous permet de déterminer avec plus de précision les endroits où un équipement de stockage supplémentaire peut être nécessaire.

Quelle est la capacité des performances utilisée

Le compteur de performances utilisé vous permet de déterminer si les performances d'un nœud ou d'un agrégat atteignent un point où les performances peuvent se dégrader si les charges de travail augmentent. Il peut également vous indiquer si un nœud ou un agrégat est actuellement utilisé pendant des périodes spécifiques. Les performances utilisées sont similaires aux taux d'utilisation, mais la première fournit des informations supplémentaires sur les capacités de performances disponibles dans une ressource physique pour une charge de travail spécifique.

La capacité à performances optimales utilisées est au point de permettre à un nœud ou un agrégat d'optimiser l'utilisation et la latence (temps de réponse) et d'être utilisé de manière efficace. Un exemple de latence par rapport à une courbe d'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. En se basant sur les statistiques collectées par l'agrégat, Unified Manager détermine que des performances supplémentaires sont disponibles pour cet agrégat. Dans cet exemple, le *optimal point* est identifié comme le point où l'agrégat est à 80% d'utilisation avec une latence de 2.0 ms/op. Vous pouvez donc ajouter davantage de volumes et de LUN à cet agrégat, afin que vos systèmes soient utilisés plus efficacement.

Le compteur de capacités de performances utilisé devrait être un nombre supérieur au compteur de « utilisation », car des capacités de performances augmentent l'impact sur la latence. Par exemple, si un nœud

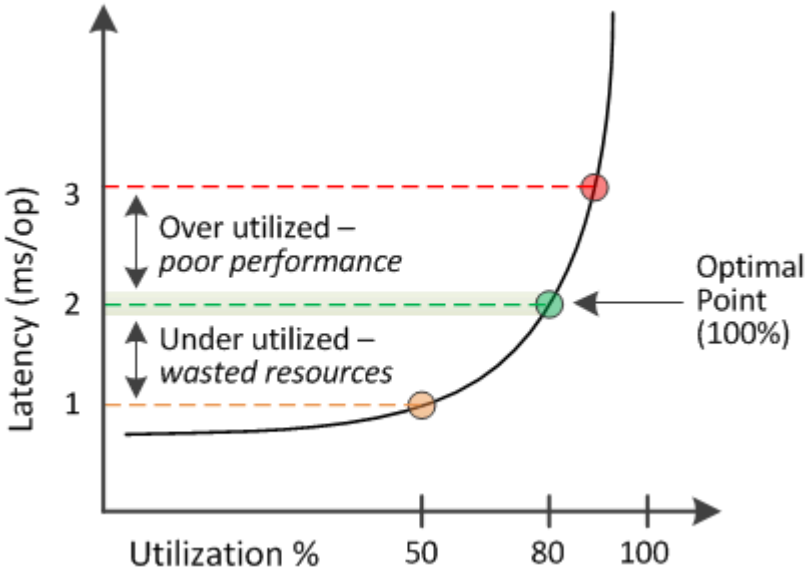
ou un agrégat est utilisé à 70 %, la valeur de la capacité de performances peut se situe dans la plage de 80 à 100 %, selon la valeur de latence.

Dans certains cas, le compteur d'utilisation peut cependant être plus élevé sur la page Tableau de bord. Cet aspect est normal car le tableau de bord actualise les valeurs de compteur actuelles à chaque période de collecte. Il n'affiche pas les moyennes sur un certain temps, comme les autres pages de l'interface utilisateur Unified Manager. Le compteur de performances utilisé est le mieux utilisé comme indicateur de performance moyenne sur une période de temps, alors que le compteur d'utilisation est le mieux utilisé pour déterminer l'utilisation instantanée d'une ressource.

Signification de la capacité en termes de performances utilisée

La valeur de performance utilisée permet d'identifier les nœuds et les agrégats actuellement sur-utilisés ou sous-utilisés. Vous pouvez ainsi redistribuer les charges de travail afin d'améliorer l'efficacité de vos ressources de stockage.

La figure suivante montre la courbe de latence par rapport à l'utilisation d'une ressource et identifie, avec des points de couleur, trois zones où le point opérationnel actuel peut être localisé.



- Un pourcentage de capacité de performances utilisé égal à 100 est au point optimal.

  À ce stade, les ressources sont utilisées efficacement.

- Un pourcentage de capacité de performances utilisé supérieur à 100 indique que le nœud ou l'agrégat est sur-exploité et que les charges de travail bénéficient de performances sous-optimales.

  Aucune nouvelle charge de travail ne doit être ajoutée à la ressource et la redistribution des charges de travail existantes peut s'avérer nécessaire.

- Un pourcentage de capacité de performances utilisé inférieur à 100 indique que le nœud ou l'agrégat est sous-utilisé, et que les ressources ne sont pas utilisées efficacement.

  Il est possible d'ajouter davantage de charges de travail à une ressource.

Contrairement à l'utilisation, le pourcentage de capacité haute performance utilisé peut être supérieur à 100 %. Il n'y a pas de pourcentage maximal, mais les ressources sont généralement comprises entre 110 et 140 % lorsqu'elles sont sur-exploitées. Des pourcentages plus élevés indiquerait une ressource avec des problèmes graves.

Les IOPS disponibles

Le compteur IOPS disponibles identifie le nombre restant d'IOPS pouvant être ajouté à un nœud ou à un agrégat avant que la ressource n'atteigne sa limite.

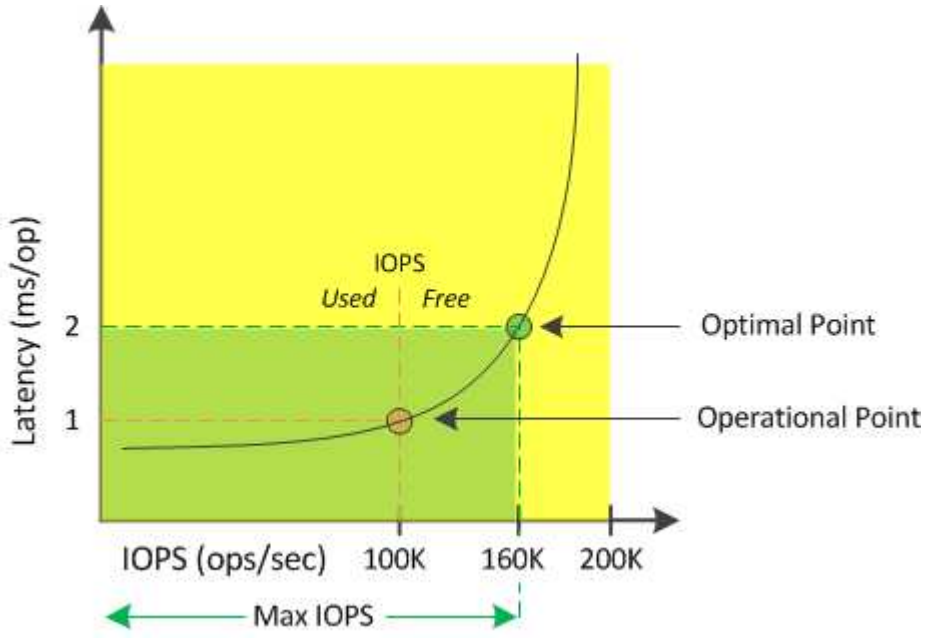
Le nombre total d'IOPS qu'un nœud peut fournir est basé sur les caractéristiques physiques du nœud—par exemple, le nombre de processeurs, la vitesse du processeur et la quantité de RAM. Le nombre total d'opérations d'E/S par seconde qu'un agrégat peut fournir dépend des propriétés physiques des disques, par exemple un disque SATA, SAS ou SSD.

Il se peut que les IOPS totales de tous les volumes d'un agrégat ne correspondent pas au nombre total d'IOPS de l'agrégat. Cet article est abordé dans l'article suivant de la base de connaissance : KB "Pourquoi la somme de toutes les IOPS du volume d'un agrégat ne correspond-elle pas aux IOPS de l'agrégat ?"

Le compteur de performances disponible affiche le pourcentage de ressource qui reste disponible, mais le compteur IOPS disponible indique le nombre exact d'IOPS (charges de travail) à ajouter 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 sans capacité en termes de performances de 30 % indique que vous bénéficiez de capacité de performances gratuites. Toutefois, cette valeur n'apporte aucune visibilité sur le nombre de charges de travail que vous pouvez déployer sur ces nœuds. Le compteur IOPS disponible peut indiquer que vous disposez de 500 000 IOPS disponibles sur le système FAS8060, mais que seuls 100 000 IOPS sont disponibles sur le système FAS2520.

La figure suivante présente un exemple de latence par rapport aux courbes IOPS pour un nœud.



Le nombre maximal d'IOPS qu'une ressource peut fournir est le nombre d'IOPS lorsque la capacité de performance utilisée compteur est de 100 % (le point optimal). Le point opérationnel identifie que le nœud

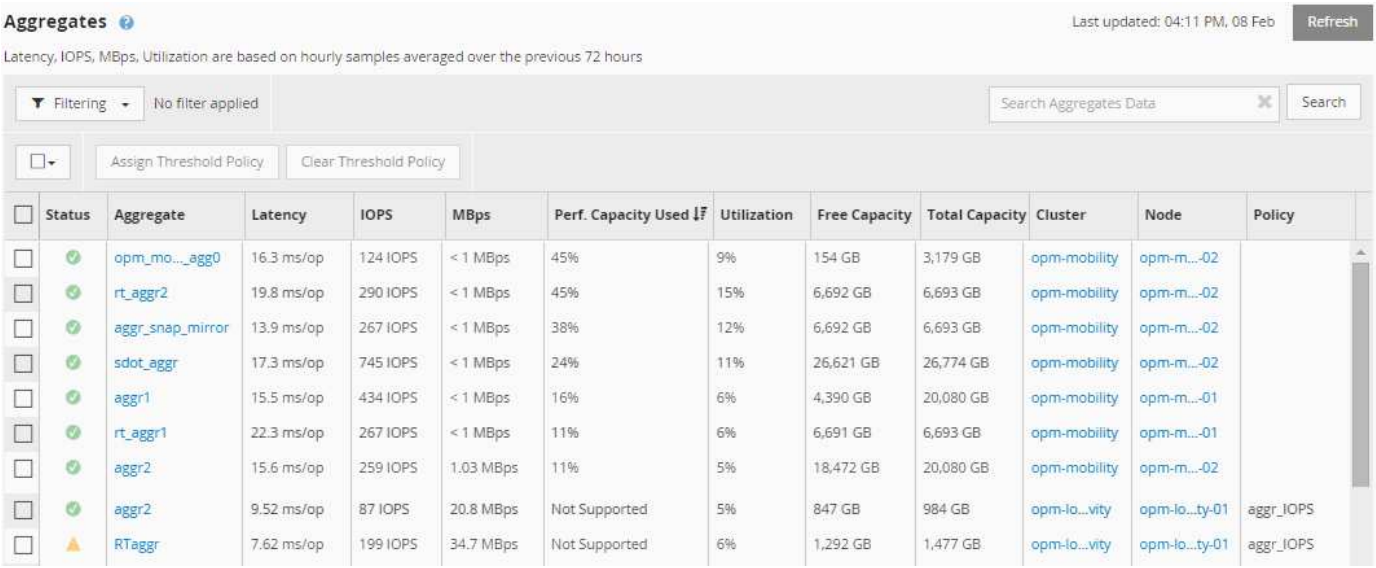
fonctionne actuellement à 100 000 IOPS avec une latence de 1.0 ms/op. En fonction des statistiques collectées à partir du nœud, Unified Manager détermine que les IOPS maximales du nœud sont de 160 000, ce qui signifie que 60 000 IOPS sont disponibles ou libres. Vous pouvez donc ajouter des workloads à ce nœud afin que vos systèmes soient utilisés plus efficacement.

> Lorsque l'activité de la ressource est minimale, la valeur des IOPS disponibles est calculée en supposant qu'une charge de travail générique s'appuie sur environ 4,500 000 IOPS par cœur de processeur. En effet, Unified Manager n'a pas de données pour estimer avec précision les caractéristiques de la charge de travail traitée.

Affichage des valeurs de capacité des nœuds et des performances des agrégats utilisées

Vous pouvez contrôler les valeurs de performance de la capacité utilisée pour tous les nœuds ou pour tous les agrégats d'un cluster, ou afficher les détails d'un nœud ou agrégat unique.

Les valeurs utilisées relatives à la capacité de performance apparaissent dans le tableau de bord, les pages Inventaire des performances, la page collaborateurs les plus performants, la page Créer une stratégie de seuil, les pages Explorateur de performances et les graphiques détaillés. Par exemple, la page performances : tous les agrégats fournit une colonne capacité de performance utilisée pour afficher la valeur de performance utilisée pour tous les agrégats.



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 contrôle du compteur de performances utilisé vous permet d'identifier ce qui suit :

- Que les nœuds ou les agrégats de n'importe quel cluster disposent d'une capacité haute performance utilisée
- Que des nœuds ou des agrégats de tous les clusters disposent d'événements de capacité de performances active
- Les nœuds et les agrégats qui présentent la capacité de performance la plus élevée et la plus faible au sein d'un cluster
- Les valeurs des compteurs de latence et d'utilisation associées à des nœuds ou des agrégats qui possèdent des valeurs de capacité haute performance utilisée
- L'impact des valeurs de performance utilisées pour les nœuds d'une paire haute disponibilité sera affecté

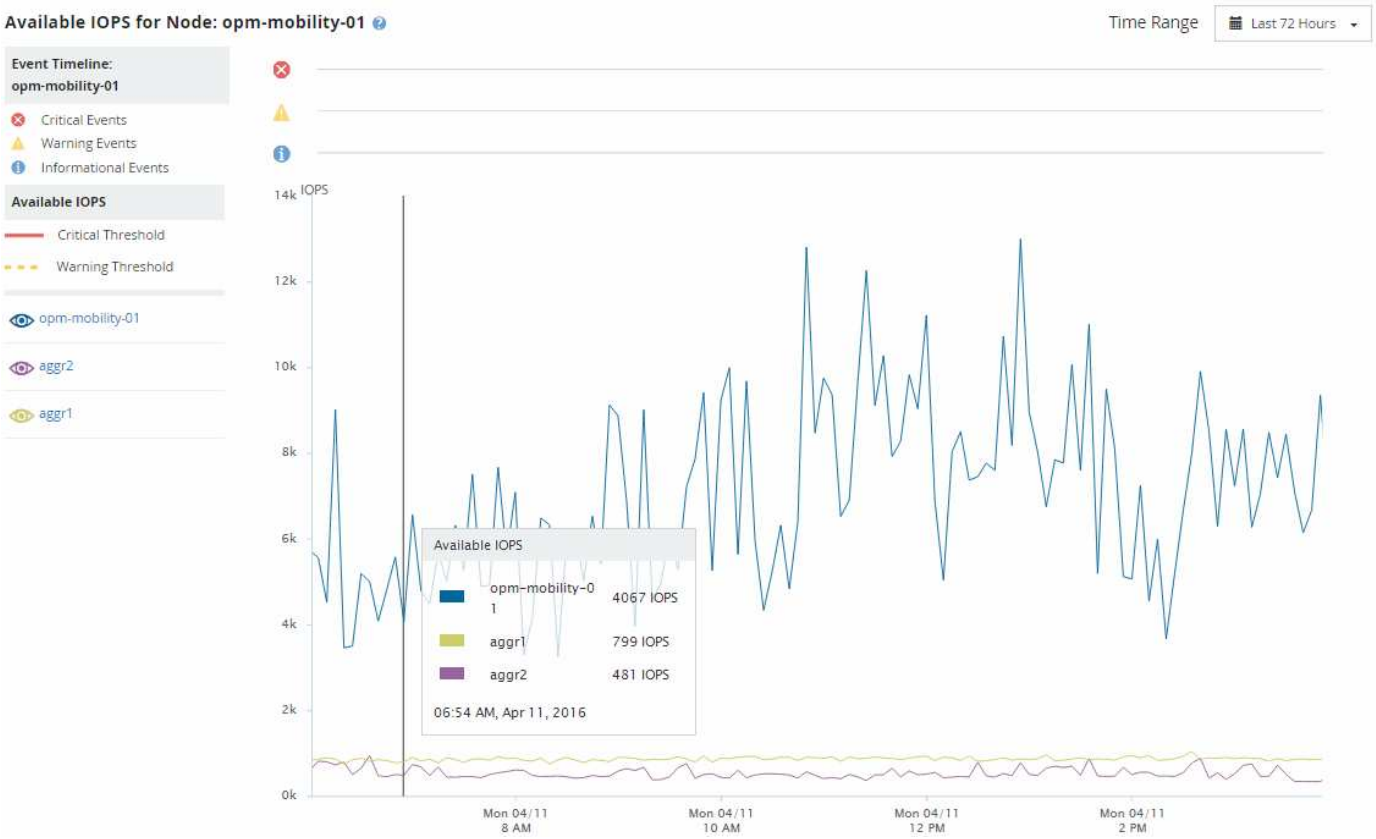
en cas de panne de l'un des nœuds

- Les volumes et les LUN les plus sollicités d'un agrégat dont les capacités de performances sont élevées

Affichage des valeurs d'IOPS disponibles du nœud et de l'agrégat

Vous pouvez contrôler les valeurs d'IOPS disponibles pour tous les nœuds ou pour tous les agrégats d'un cluster, ou afficher les détails d'un seul nœud ou agrégat.

Les valeurs d'IOPS disponibles apparaissent sur les pages Performance Inventory et dans les graphiques de la page Performance Explorer pour les nœuds et les agrégats. Par exemple, lorsque vous affichez un nœud dans la page Explorateur de nœuds/performances, vous pouvez sélectionner le compteur « IOPS disponibles » dans la liste afin de pouvoir comparer les valeurs d'IOPS disponibles pour le nœud et plusieurs agrégats sur ce nœud.



La surveillance du compteur IOPS disponible vous permet d'identifier :

- Les nœuds ou les agrégats qui disposent des valeurs d'IOPS les plus élevées pour déterminer l'emplacement où les futurs workloads peuvent être déployés.
- Pour identifier les ressources dont vous devez contrôler les problèmes de performance futurs, les nœuds ou les agrégats disposant des valeurs d'IOPS les plus faibles.
- Les volumes et les LUN les plus sollicités d'un agrégat qui dispose d'une faible valeur des IOPS disponibles.

Affichage des graphiques des compteurs de capacité de performances pour identifier les problèmes

Vous pouvez consulter les diagrammes de capacité des performances utilisés pour les

nœuds et les agrégats sur la page de l'explorateur de performances. Vous pouvez ainsi consulter des données détaillées sur la capacité de performances pour les nœuds et les agrégats sélectionnés pendant un délai spécifique.

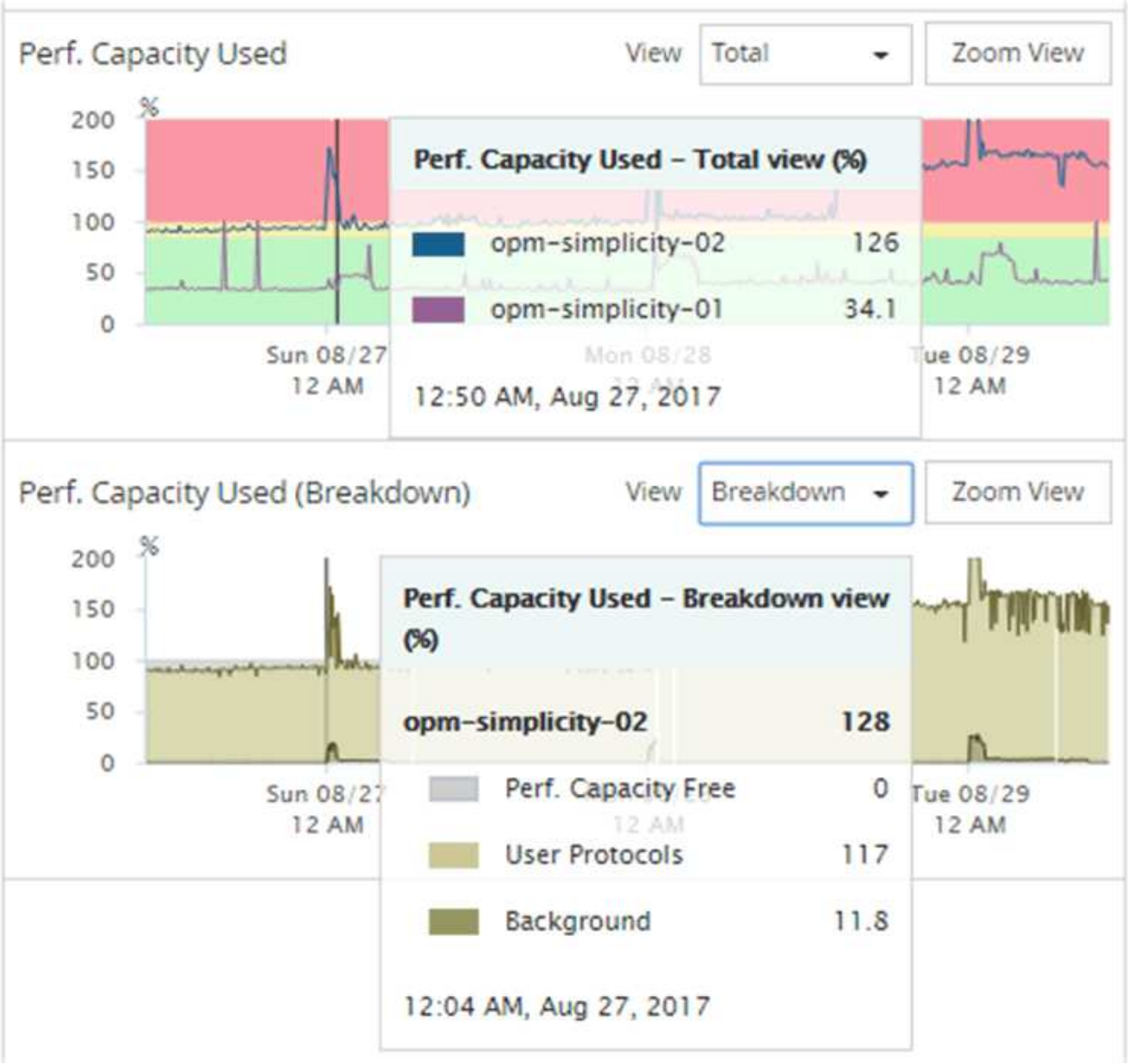
Le tableau des compteurs standard affiche les valeurs de capacité de performances utilisées pour les nœuds ou agrégats sélectionnés. Le tableau des compteurs d'analyse affiche les valeurs de capacité de performance totale pour l'objet racine, séparées en utilisation en fonction des protocoles utilisateur par rapport aux processus du système en arrière-plan. En outre, la capacité des performances libres est également indiquée.

> Comme 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 paraître artificiellement élevé lors de l'exécution de ces processus. Ces processus s'exécutent généralement autour de minuit lorsque le niveau d'utilisation du cluster est bas. Si vous voyez un pic d'activité du protocole utilisateur vers minuit, vérifiez si les tâches de sauvegarde du 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'une page de noeud ou d'agrégat **Landing**.
2. Dans le volet **compteur graphiques**, cliquez sur **choisir les graphiques**, puis sélectionnez **Perf. Tableau capacité utilisée**.
3. Faites défiler vers le bas jusqu'à ce que vous puissiez afficher la carte.

   Les couleurs du graphique standard indiquent lorsque l'objet se trouve dans la plage optimale (jaune), lorsque l'objet est sous-utilisé (vert) et lorsque l'objet est surutilisé (rouge). Le tableau décomposition affiche des détails détaillés sur la capacité de performances pour l'objet racine uniquement.



4. Si vous souhaitez afficher l'un ou l'autre des graphiques en format plein format, cliquez sur **vue Zoom**.

   Vous pouvez ainsi ouvrir plusieurs diagrammes dans une fenêtre distincte afin de comparer les valeurs de capacité utilisée avec les valeurs d'IOPS ou de Mo/sec sur la même période.

Conditions du seuil de performance utilisé par la capacité de performance

Vous pouvez créer des règles de seuils de performances définies par l'utilisateur, de sorte que les événements se déclenchent lorsque la capacité de performance utilisée pour un nœud ou un agrégat dépasse le seuil de capacité de performance défini défini.

En outre, les nœuds peuvent être configurés avec une règle de seuil « prise en charge de la capacité de performances utilisée ». Cette règle de seuil total les statistiques de performance utilisées pour les deux nœuds d'une paire HA afin de déterminer si la capacité de l'un des nœuds serait insuffisante si l'autre nœud tombe en panne. 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 dans la règle de basculement

peut être appliquée aux deux nœuds.

> Cette équivalence des performances utilisée est généralement vrai entre les nœuds. Cependant, en cas de trafic croisé sur 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 aux autres nœuds partenaires peut légèrement différente en fonction du nœud défaillant.

Les conditions de performance utilisées peuvent également être utilisées comme paramètres de seuil de performance secondaire pour créer une règle de seuil de combinaison lors de la définition de seuils pour les LUN et les volumes. La condition de performance utilisée est appliquée à l'agrégat ou au nœud sur lequel réside le volume ou la LUN. Par exemple, vous pouvez créer une stratégie de seuil de combinaison à l'aide des critères suivants :

Objet de stockage	Compteur de performances	Seuil d'avertissement	Seuil critique	Durée
Volumétrie	Latence	15 ms/op	25 ms/op	20 minutes
Agrégat	Capacité utilisée	80%	95%	

Les stratégies de seuil de combinaison n'entraînent la génération d'un événement que lorsque les deux conditions sont enfreintes pendant toute la durée.

Utilisation du compteur de performances utilisé pour gérer les performances

Généralement, les entreprises souhaitent profiter d'une capacité de performance utilisée inférieure à 100 et pouvoir utiliser les ressources de manière efficace tout en réservant une capacité de performance supplémentaire pour supporter les pics de demande. Vous pouvez utiliser des règles de seuil pour personnaliser l'envoi d'alertes pour des valeurs de capacité haute performance utilisée.

Vous pouvez établir des objectifs spécifiques en fonction de vos exigences de performances. Par exemple, les entreprises de services financiers pourraient réserver davantage de capacité de rendement pour garantir l'exécution opportune des opérations. Ces entreprises peuvent vouloir définir des seuils de capacité pour les performances utilisés dans une plage de 70-80 %. Dans ce secteur, les entreprises de fabrication dont les marges sont plus faibles pourraient choisir de réserver une capacité moins performante si elles risquent de mieux gérer les coûts IT. Ces entreprises peuvent définir des seuils de capacité pour les performances utilisés dans les plages de 85-95 %.

Lorsque la valeur de performance capacité utilisée dépasse le pourcentage défini dans une règle de seuil définie par l'utilisateur, Unified Manager envoie un e-mail d'alerte et l'ajoute à la page Event Inventory. Les problèmes potentiels sont ainsi gérés avant qu'ils n'affectent les performances. Ces événements peuvent également servir d'indicateurs pour déplacer et modifier les charges de travail au sein de vos nœuds et agrégats.

Présentation et utilisation de la page planification du basculement de nœud

La page planification du basculement de nœud/performances estime l'impact sur les

performances d'un nœud en cas de défaillance du nœud partenaire haute disponibilité. Unified Manager établit les estimations sur les performances historiques des nœuds de la paire HA.

L'estimation de l'impact d'un basculement sur les performances vous permet de planifier dans les scénarios suivants :

- Si un basculement entraîne une dégradation constante des performances estimées du nœud de basculement, il est possible d'envisager de prendre des mesures correctives pour réduire l'impact sur les performances dû à un basculement.
- Avant de lancer un basculement manuel afin d'effectuer des tâches de maintenance matérielle, vous pouvez évaluer l'impact du basculement sur les performances du nœud de basculement afin de déterminer le meilleur moment pour effectuer cette tâche.

Utilisation de la page planification de basculement de nœud pour déterminer les actions correctives

En fonction des informations affichées sur la page Performance/Node Failover Planning, vous pouvez effectuer des actions pour vérifier qu'un basculement ne provoque pas de chute des performances d'une paire haute disponibilité 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 haute disponibilité vers d'autres nœuds du cluster. Vous êtes ainsi assuré que le nœud principal peut continuer à fournir des performances acceptables après un basculement.

Composants de la page planification de basculement de nœud

Les composants de la page Performance/Node Failover Planning s'affichent dans une grille et dans le volet de comparaison. Vous pouvez ainsi évaluer l'impact d'un basculement de nœud sur les performances du nœud qui Takeover.

Grille des statistiques de performances

La page Performance/Node Failover Planning affiche une grille contenant des statistiques de latence, d'IOPS, d'utilisation et de capacité de performances utilisées.

> Les valeurs de latence et d'IOPS affichées sur cette page et dans la page de l'explorateur des performances/des nœuds peuvent ne pas correspondre car des compteurs de performances différents sont utilisés pour calculer les valeurs permettant de prévoir le basculement des nœuds.

Dans la grille, chaque nœud est associé à l'un des rôles suivants :

- Primaire

  Nœud qui prend le relais du partenaire de haute disponibilité lorsque le partenaire tombe en panne. L'objet racine est toujours le nœud principal.

- En tant que partenaire

Le nœud qui échoue dans le scénario de basculement.

- Basculement estimé

  Identique au nœud principal. Les statistiques de performances affichées pour ce nœud affichent les performances du nœud de basculement après le basculement du partenaire en panne.

> Bien que le workload du nœud de basculement soit équivalent aux workloads combinés des deux nœuds après un basculement, les statistiques du nœud de basculement estimé ne correspondent pas à 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 que la latence du nœud partenaire est de 3 ms/op, le nœud de basculement 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 que la page Explorateur de performances/nœuds est affichée, vous pouvez cliquer sur l'onglet **planification de basculement** pour voir comment les performances changent dans ce scénario de défaillance de nœud. Par exemple, si le nœud 1 est le nœud principal et que le nœud 2 est le nœud partenaire, vous pouvez cliquer sur Node2 pour en faire le nœud principal. De cette manière, vous pouvez voir comment les modifications estimées s'matière à la performance en fonction de la panne de chaque nœud.

Panneau de comparaison

La liste ci-dessous décrit les composants affichés dans le volet comparaison par défaut :

- **Graphiques d'événements**

  Elles s'affichent au même format que celles de la page Performance Explorer des nœuds/performances. Ils sont applicables uniquement au nœud principal.

- **Diagrammes de compteur**

  Ils affichent les statistiques historiques du compteur de performances affiché dans la grille. Sur chaque graphique, le graphique du nœud de basculement estimé affiche les performances estimées en cas de basculement.

  Supposons par exemple que le graphique utilisation affiche 73 % pour le nœud de basculement estimé à 11 h, le 8 février. En cas de basculement, l'utilisation du nœud de basculement se serait alors révélée à 73 %.

  Les statistiques historiques vous aident à trouver le temps optimal pour initier un basculement, réduisant ainsi le risque de surcharge du nœud de reprise. Vous pouvez planifier un basculement uniquement à des moments où les performances prévues du nœud de basculement 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/nœuds, cette page n'affiche pas le bouton **Ajouter** pour vous permettre d'ajouter des objets pour la comparaison des statistiques.

Vous pouvez personnaliser le volet de comparaison de la même manière que dans la page Explorateur de performances/nœuds. La liste suivante fournit des exemples de personnalisation des graphiques :

- Cliquez sur le nom d'un nœud pour afficher ou masquer les statistiques du nœud dans les compteurs.
- Cliquez sur **Zoom View** pour afficher un graphique détaillé pour un compteur particulier dans une nouvelle

fenêtre.

Utilisation d’une stratégie de seuil avec la page planification du basculement de nœud

Vous pouvez créer une règle de seuil de nœud afin d’être averti dans la page Performance/Node Failover Planning lorsqu’un basculement potentiel dégrade les performances du nœud de basculement.

La règle de seuil de performances définie par le système intitulée « paire HA de nœud sur-utilisée » 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 performance combinée des nœuds d’une paire haute disponibilité dépasse 200 %.

En cas de règle du seuil défini par le système, un basculement risque d’entraîner une augmentation de la latence du nœud de basculement à un niveau inacceptable. Lorsque vous voyez un événement généré par cette règle pour un nœud particulier, vous pouvez accéder à la page Performance/Node Failover Planning de ce nœud pour afficher la valeur de latence prévue due à un basculement.

Outre l’utilisation de cette politique de seuils définie par le système, vous pouvez créer des règles de seuil en utilisant le compteur « capacité de performance utilisée - basculement », puis appliquer la règle aux nœuds sélectionnés. Si vous spécifiez un seuil inférieur à 200 %, vous pouvez recevoir un événement avant que le seuil de la règle définie par le système ne soit atteint. Vous pouvez également spécifier la période minimale pendant laquelle le seuil est dépassé à moins de 30 minutes si vous souhaitez être notifié avant la génération de l’événement de règle défini par le système.

Par exemple, vous pouvez définir une règle de seuil pour générer un événement d’avertissement si la capacité de performance combinée des nœuds d’une paire haute disponibilité dépasse 175 % pendant plus de 10 minutes. Vous pouvez appliquer cette politique au Node1 et Node2, qui forment une paire HA. Après avoir reçu une notification d’événement d’avertissement pour le nœud 1 ou le nœud 2, vous pouvez afficher la page Performance/Node Failover Planning de ce nœud afin d’évaluer l’impact estimé des performances sur le nœud de basculement. Vous pouvez prendre des actions correctives afin d’éviter de surcharger le nœud de basculement en cas de basculement. Si vous prenez des mesures lorsque la capacité de performance combinée des nœuds est inférieure à 200 %, la latence du nœud de basculement n’atteint pas un niveau inacceptable, même en cas de basculement pendant ce temps.

Utilisation du tableau d’analyse de la capacité sur les performances utilisée pour la planification du basculement

Le graphique détaillé capacité en performances utilisée - détail indique la capacité en performances utilisée pour le nœud principal et le nœud partenaire. Il affiche également la capacité de performances disponibles sur le nœud de basculement estimé. Ces informations vous permettent de déterminer si vous rencontrez un problème de performances en cas de panne du nœud partenaire.

Outre l’affichage de la capacité de performance totale utilisée pour les nœuds, le graphique décomposition décompose les valeurs de chaque nœud en protocoles utilisateur et en processus d’arrière-plan.

- Les protocoles utilisateur correspondent aux opérations d’E/S depuis et vers les applications utilisateur du cluster.
- Les processus d’arrière-plan sont les processus système internes impliqués dans l’efficacité du stockage, la réplication des données et l’intégrité du système.

Ce niveau de détail supplémentaire vous permet de déterminer si un problème de performance est causé par l'activité de l'application utilisateur ou par les processus du système en arrière-plan, tels que la déduplication, la reconstruction RAID, le nettoyage des disques et les copies SnapMirror.

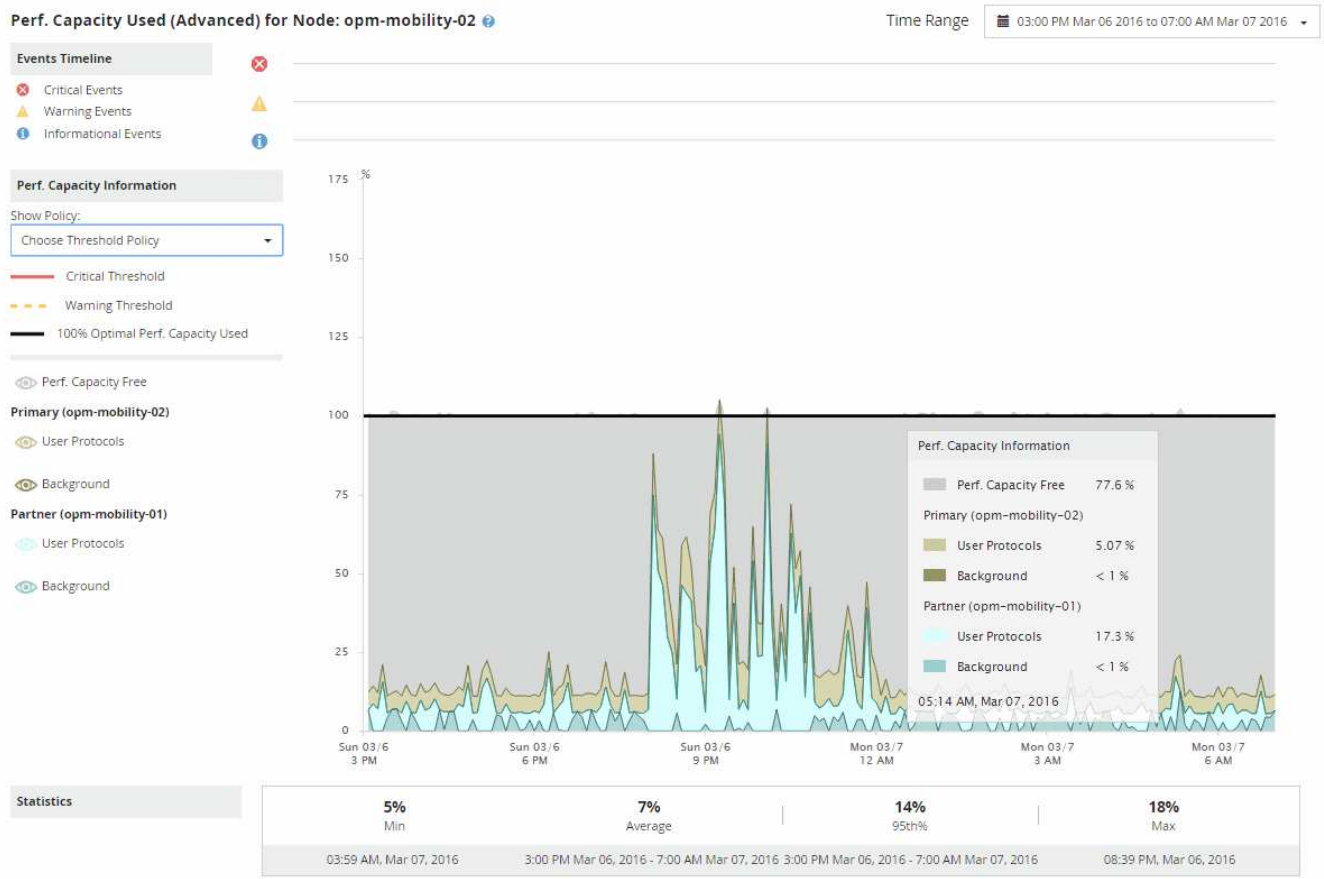
Étapes

1. Accédez à la page **Performance/Node Failover Planning** du nœud qui servira de nœud de basculement estimé.
2. Dans le sélecteur **Time Range**, choisissez la période pour laquelle les statistiques historiques sont affichées dans la grille des compteurs et dans les diagrammes.

   Les graphiques des compteurs correspondant aux statistiques du nœud principal, du nœud partenaire et du nœud de basculement estimé sont affichés.

3. Dans la liste **choisir les graphiques**, sélectionnez **Perf. Capacité utilisée**.
4. Dans le **Perf. Graphique capacité utilisée**, sélectionnez **détail** et cliquez sur **vue Zoom**.

   Le tableau détaillé de Perf. La capacité utilisée s'affiche.



5. Déplacez le curseur sur le tableau détaillé pour afficher les informations relatives à la capacité de performance utilisée dans la fenêtre contextuelle.

   La Perf. Le pourcentage libre de capacité correspond à la capacité de performances disponible sur le nœud de basculement estimé. Elle indique le niveau de performances restant sur le nœud de basculement après un basculement. Si elle est de 0 %, un basculement entraîne une augmentation de la latence à un niveau inacceptable sur le nœud de basculement.

6. Envisagez de mettre en œuvre des actions correctives pour éviter une faible part de la capacité disponible.

Si vous prévoyez de lancer un basculement pour la maintenance du nœud, sélectionnez un moment pour faire échouer le nœud partenaire lorsque le pourcentage de capacité libre de performance n'est pas égal à 0.

Collecte des données et contrôle des performances des workloads

Unified Manager collecte et analyse les activités des charges de travail toutes les 5 minutes afin d'identifier les événements de performances et détecte les changements de configuration toutes les 15 minutes. Il conserve jusqu'à 30 jours de données d'historique des performances et des événements de 5 minutes. Ces données permettent d'établir les prévisions de latence pour toutes les charges de travail surveillées.

Unified Manager doit collecter au moins 3 jours d'activité de la charge de travail avant de pouvoir lancer son analyse. Pour ce faire, il est possible d'afficher la prévision de latence pour le temps de réponse E/S sur la page analyse des charges de travail et sur la page Détails des événements. Lors de la collecte de cette activité, la prévision de latence n'affiche pas toutes les modifications effectuées à partir de l'activité de la charge de travail. Après avoir collecté 3 jours d'activité, Unified Manager ajuste la latence prévue toutes les 24 heures à 12 h 00, pour prendre en compte les modifications de l'activité des charges de travail et établir un seuil de performance dynamique plus précis.

Au cours des 4 premiers jours qui suivent la surveillance d'une charge de travail par Unified Manager, si plus de 24 heures se sont écoulées depuis la dernière collecte de données, les graphiques de latence n'affichent pas les prévisions de latence pour cette charge de travail. Les événements détectés avant la dernière collection sont toujours disponibles.

> L'heure d'été change l'heure système, ce qui modifie la prévision 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 cette période, vous pouvez continuer à utiliser Unified Manager, mais, puisque Unified Manager utilise les prévisions de latence pour détecter des événements dynamiques, certains événements peuvent ne pas être précis. Les événements détectés avant le changement de temps ne sont pas affectés.

Types de charges de travail surveillés par Unified Manager

Unified Manager permet de surveiller les performances de deux types de charges de travail : définies par l'utilisateur et défini par le système.

- ***charges de travail définies par l'utilisateur***

  Débit d'E/S des applications vers le cluster. Ce sont des processus impliqués dans les requêtes de lecture et d'écriture. Un volume, une LUN, un partage NFS, un partage SMB/CIFS et un workload sont une charge de travail définie par l'utilisateur.

  > Unified Manager surveille uniquement l'activité des workloads sur le cluster. Il ne surveille pas les applications, les clients ou les chemins d'accès entre les applications et le cluster.

  Si un ou plusieurs des éléments suivants sont vrais pour une charge de travail, il ne peut pas être surveillé 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 les utilisateurs.)
- 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 impliquées dans l'efficacité du stockage, la réplication des données et l'état du système, notamment :

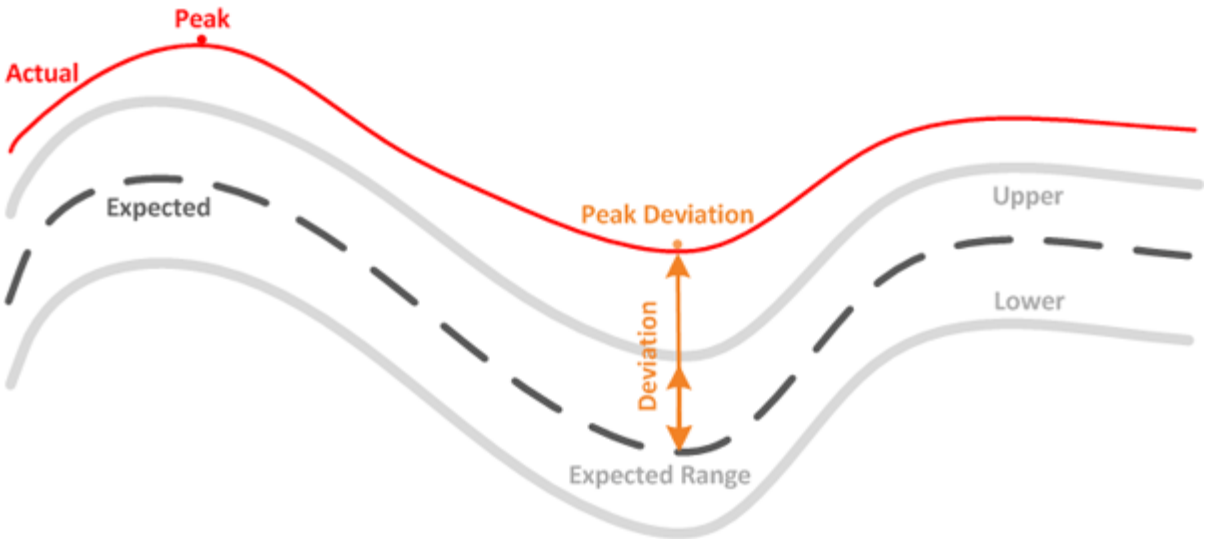
  - Efficacité du stockage, comme la déduplication
  - État de santé du disque, qui inclut la reconstruction RAID, le nettoyage du disque, etc
  - Réplication des données, notamment les copies SnapMirror
  - Activités de gestion
  - État de santé du système de fichiers, qui inclut les diverses activités WAFL
  - Les scanners de système de fichiers, tels que la numérisation WAFL
  - Allègement de la charge des copies, comme les opérations d'efficacité du stockage déchargées depuis les hôtes VMware
  - État du système, comme les déplacements de volume, la compression des données, etc
  - Volumes non surveillés

Les données de performance des charges de travail définies par le système s'affichent dans l'interface graphique uniquement lorsque le composant de cluster utilisé par ces charges de travail conflits. Par exemple, vous ne pouvez pas rechercher le nom d'une charge de travail définie par le système pour afficher les données de performance dans l'interface graphique.

Valeurs de mesure des performances des charges 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 workloads. Il compare les valeurs statistiques réelles de la charge de travail à la prévision de latence pour déterminer si les performances de la charge de travail sont trop élevées ou trop faibles. Un workload qui n'exécute pas comme prévu entraîne un événement de performance dynamique à vous notifier.

Dans l'illustration suivante, la valeur réelle, en rouge, représente les statistiques de performance 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 de crête indique le changement le plus important entre les valeurs attendues et les valeurs réelles.



Le tableau suivant répertorie les valeurs de mesure des performances des workloads.

Mesure	Description
Activité	Pourcentage de la limite de qualité de service utilisée par les workloads dans le groupe de règles. Si Unified Manager détecte une modification au groupe de règles, par exemple l'ajout ou la suppression d'un volume ou la modification de la limite de QoS, les valeurs réelles et attendues peuvent dépasser 100 % de la limite définie. Si une valeur dépasse 100 % de la limite définie, elle s'affiche sous la forme de > 100 %. Si une valeur est inférieure à 1 % de la limite définie, elle s'affiche sous la forme <1 %.
Réel	La valeur des performances mesurée à un moment spécifique pour une charge de travail donnée.
Déviation	Changement 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. Une valeur de déviation négative indique que la performance de la charge de travail est inférieure à la valeur attendue, tandis qu'une valeur de déviation positive indique que la performance de la charge de travail est supérieure à la valeur attendue.

Mesure	Description
Attendu	Les valeurs attendues sont basées sur l'analyse des données historiques de performances pour une charge de travail donnée. Unified Manager analyse ces valeurs statistiques afin de déterminer la plage attendue (prévision de latence) de valeurs.
Prévision de latence (plage prévue)	La prévision de latence est une prévision des valeurs de performance supérieure et inférieure attendues. Pour la latence des workloads, les valeurs supérieures constituent le seuil de performance. Lorsque la valeur réelle franchit le seuil de performances, Unified Manager déclenche un événement de performance dynamique.
Pic	Valeur maximale mesurée sur une période de temps.
Déviation de crête	Valeur de déviation maximale mesurée sur une période de temps.
Profondeur de la file d'attente	Nombre de demandes d'E/S en attente du composant d'interconnexion.
Du stockage	Pour les composants de traitement de réseau, de traitement de données et d'agrégat, le pourcentage de temps d'activité requis pour mener à bien les opérations de la charge de travail sur une période donnée. Par exemple, le pourcentage de temps alloué aux composants de traitement réseau ou de traitement de données pour traiter une demande d'E/S ou à un agrégat pour répondre à une demande de lecture ou d'écriture.
Débit d'écriture	Débit en écriture, en mégaoctets par seconde (Mo/s), allant des charges de travail sur un cluster local au cluster partenaire dans une configuration MetroCluster.

Parmi les performances attendues

La prévision de latence est une prévision des valeurs de performance supérieure et inférieure attendues. Pour la latence des workloads, les valeurs supérieures constituent le seuil de performance. Lorsque la valeur réelle franchit le seuil de performances, Unified Manager déclenche un événement de performance dynamique.

Par exemple, pendant les heures de bureau normales entre 9:00 et 5:00, la plupart des employés peuvent vérifier leurs e-mails entre 9:00 et 10:30. L'augmentation de la demande sur les serveurs de messagerie entraîne une augmentation de l'activité de la charge de travail sur le stockage interne pendant cette période. Les employés risquent de remarquer le ralentissement des temps de réponse de la part de leurs clients de

messagerie.

Pendant l'heure du déjeuner entre 12 h 00 et 13 h 00 et à la fin de la journée de travail après 5 h 00, la plupart des employés sont probablement loin de leurs ordinateurs. La demande sur les serveurs de messagerie diminue généralement, tout en diminuant la demande sur le stockage interne. Il est également possible de planifier des opérations de charge de travail, telles que les sauvegardes de stockage ou les analyses antivirus, qui démarrent après 5 h 00 et augmentent l'activité sur le stockage interne.

Sur plusieurs jours, l'augmentation et la diminution de l'activité de la charge de travail déterminent la plage d'activité attendue (prévision de latence), avec des limites supérieure et inférieure pour une charge de travail. Lorsque l'activité de workload réelle d'un objet se trouve en dehors des limites supérieure ou inférieure et reste en dehors des limites pendant un certain temps, il peut indiquer que l'objet est sur-utilisé ou sous-utilisé.

Mode de création de la prévision de latence

Unified Manager doit collecter au moins 3 jours d'activité de la charge de travail avant de commencer son analyse. Il est alors possible avant que la prévision de latence pour le temps de réponse d'E/S ne soit affichée dans l'interface graphique. La collecte de données minimale requise ne tient pas compte de toutes les modifications apportées à l'activité de la charge de travail. Après avoir collecté les 3 premiers jours d'activité, Unified Manager ajuste la prévision de latence toutes les 24 heures à 12:00 pour refléter l'évolution de l'activité des charges de travail et établir un seuil de performance dynamique plus précis.

> L'heure d'été change l'heure système, ce qui modifie la prévision 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 cette période, vous pouvez continuer à utiliser Unified Manager, mais, puisque Unified Manager utilise les prévisions de latence pour détecter des événements dynamiques, certains événements peuvent ne pas être précis. Les événements détectés avant le changement de temps ne sont pas affectés.

Mode d'utilisation de la prévision de latence dans l'analyse des performances

Unified Manager utilise les prévisions de latence pour représenter l'activité d'E/S type (temps de réponse) typique de vos charges de travail surveillées. Il vous alerte lorsque la latence réelle d'une charge de travail se situe au-dessus des limites supérieures de la prévision de latence, ce qui déclenche un événement de performance dynamique. Vous pouvez ainsi analyser le problème de performance et prendre des mesures correctives pour le résoudre.

La prévision de latence définit la base de performances pour la charge de travail. Il apprend des mesures de performance passées dont il a besoin pour prévoir les niveaux de performance 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 le modèle de base pour déterminer quand la latence réelle est au-dessus ou en dessous d'un seuil ou en dehors des limites de la plage prévue. La comparaison entre les valeurs réelles et attendues crée un profil de performances pour la charge de travail.

Lorsque la latence réelle d'une charge de travail dépasse le seuil de performance dynamique, en raison d'un conflit au niveau d'un composant du cluster, la latence est élevée et la charge de travail fonctionne plus lentement que prévu. Les performances des autres charges de travail qui partagent les mêmes composants du cluster peuvent également être plus lentes que prévu.

Unified Manager analyse l'événement seuil à atteindre et détermine si l'activité est un événement de performances. Si l'activité de la charge de travail élevée reste cohérente pendant une longue période,

notamment plusieurs heures, Unified Manager considère que l'activité est normale et ajuste de manière dynamique les prévisions de latence afin de constituer le nouveau seuil de performance dynamique.

Certaines charges de travail peuvent avoir une activité faible et cohérente, où la latence prévue n'est pas fortement modifiée dans le 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, en gris, de 3.5 millisecondes par opération (ms/op) à sa plus faible et de 5.5 ms/opération à sa plus élevée. Si la latence réelle, en bleu, augmente soudainement à 10 ms/interruption, en raison d'un pic intermittent du trafic réseau ou d'un conflit sur un composant du cluster, il est alors au-dessus des prévisions de latence et a dépassé le seuil de performance dynamique.

Lorsque le trafic réseau a diminué ou que le composant de cluster n'est plus conflit, la latence est renvoyée dans la prévision de latence. Si la latence reste supérieure ou égale à 10 ms/opération sur une longue période, vous pouvez être contraint d'effectuer une action corrective pour résoudre le problème.

Comment Unified Manager utilise une latence de charge de travail pour identifier les problèmes de performance

La latence (temps de réponse) correspond au temps nécessaire pour qu'un volume d'un cluster réponde aux demandes d'E/S des applications client. Unified Manager utilise la latence pour détecter les événements de performance et vous alerter.

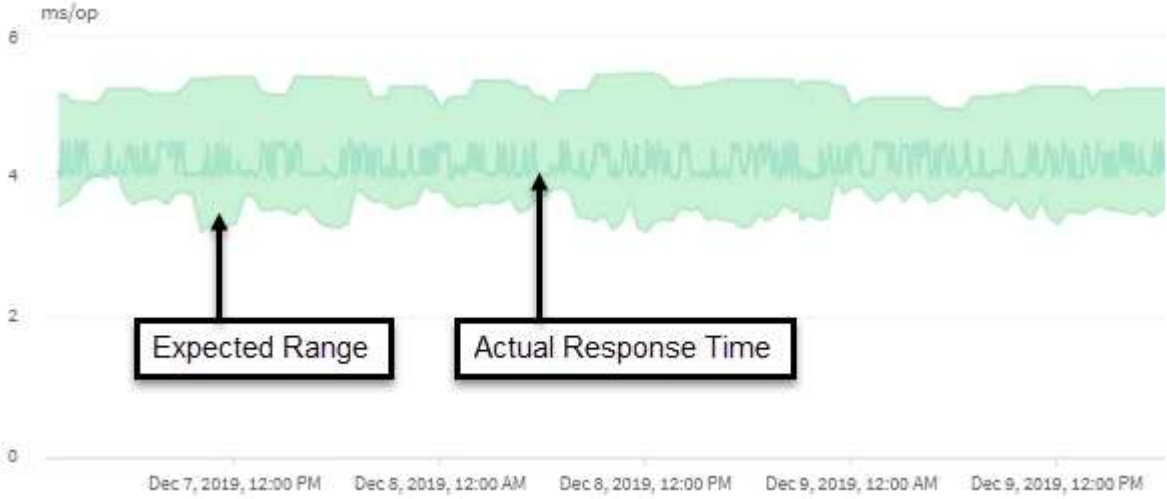
Une latence élevée signifie que les demandes provenant des applications vers un volume d'un cluster prennent plus de temps que d'habitude. La cause de la latence élevée peut se trouver sur le cluster lui-même, en raison d'un conflit sur un ou plusieurs composants du cluster. Une latence élevée peut également être provoquée par des problèmes en dehors du cluster, tels que des goulets d'étranglement du réseau, des problèmes avec le client qui héberge les applications ou des problèmes avec ces mêmes applications.

> Unified Manager surveille uniquement l'activité des workloads sur le cluster. Il ne surveille pas les applications, les clients ou les chemins d'accès entre les applications et le cluster.

Les opérations sur le cluster, comme effectuer des sauvegardes ou exécuter une déduplication, qui augmentent les besoins des composants de cluster partagés par d'autres charges de travail peuvent également contribuer à la latence élevée. Si la latence réelle dépasse le seuil de performances dynamiques de la plage attendue (latence prévue), Unified Manager analyse l'événement afin de déterminer s'il s'agit d'un événement de performances que vous devrez résoudre. La latence est mesurée en millisecondes par

opération (ms/op).

Dans le graphique Total de latence de la page analyse de charge de travail, vous pouvez visualiser une analyse des statistiques de latence afin de voir comment l'activité de processus individuels, tels que les requêtes de lecture et d'écriture, est comparé aux statistiques de latence globale. La comparaison vous permet de déterminer quelles opérations ont l'activité la plus élevée ou si des opérations spécifiques ont une activité anormale qui affecte 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 provoqué par un problème sur le cluster. Vous pouvez également identifier les activités spécifiques à la charge de travail ou les composants de cluster impliqués dans l'événement.



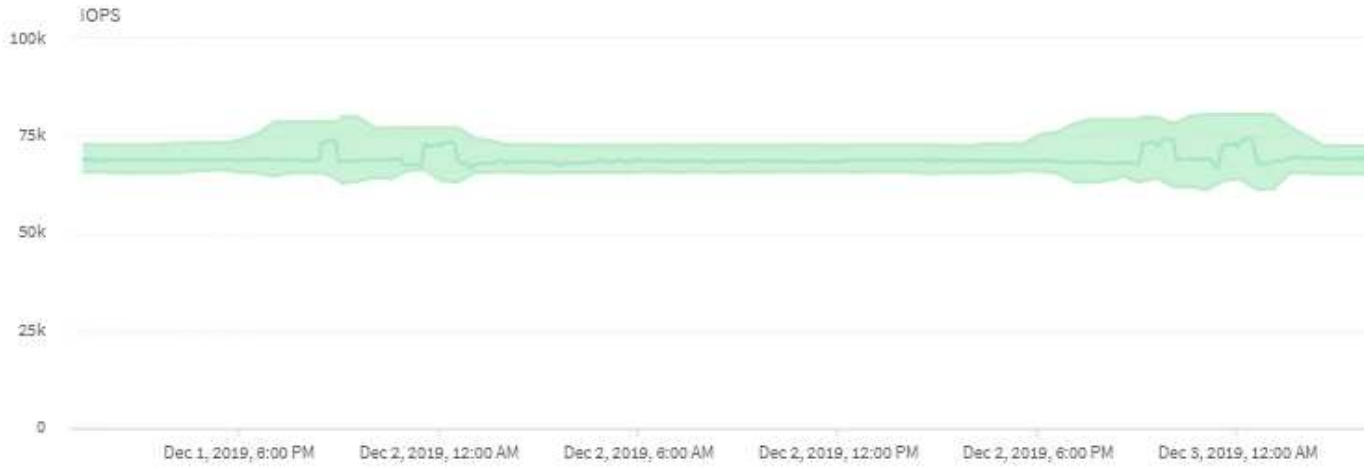
Cet exemple montre le graphique latence . L'activité du temps de réponse réel (latence) est une ligne bleue et la prévision de latence (plage prévue) est verte.

> Il peut y avoir des lacunes dans la ligne bleue si Unified Manager n'a pas pu collecter des données. Cela peut se produire du fait que le cluster ou le volume était inaccessible, Unified Manager a été désactivé pendant cette période ou que la collecte a pris plus de 5 minutes.

Comment les opérations d'un cluster peuvent affecter la latence des charges de travail

Les opérations (IOPS) représentent l'activité de tous les workloads définis par le système et l'utilisateur sur un cluster. Les statistiques Op E/S par sec vous aident à déterminer si les processus du cluster, tels que réaliser des sauvegardes ou exécuter la déduplication, ont un impact sur la latence (temps de réponse) d'une charge de travail ou s'ils ont pu être responsables d'un événement de performances.

Lors de l'analyse des événements de performances, vous pouvez utiliser les statistiques relatives aux IOPS pour déterminer si un événement de performances a été provoqué par un problème sur le cluster. Vous pouvez identifier les activités spécifiques à chaque charge de travail qui peuvent être les principales sources d'événements de performances. Les IOPS sont mesurées en opérations par seconde (OPS/s).



L'exemple montre le graphique IOPS. Les statistiques d'opérations réelles sont une ligne bleue et la prévision des statistiques d'opérations d'E/S par seconde est verte.

> Dans certains cas de surcharge d'un cluster, Unified Manager peut afficher le message `Data collection is taking too long on Cluster` *`cluster_name`*. Cela signifie que les statistiques à analyser sont insuffisantes pour Unified Manager. Vous devez réduire les ressources utilisées par le cluster afin de collecter les statistiques.

Contrôle des performances des configurations MetroCluster

Unified Manager vous permet de contrôler le débit d'écriture entre les clusters d'une configuration MetroCluster afin d'identifier les workloads dont le débit d'écriture est élevé.

Si ces charges de travail hautes performances provoquent d'autres volumes du cluster local des temps de réponse d'E/S élevés, Unified Manager déclenche des événements de performance qui vous avertissent.

> Unified Manager traite les clusters dans une configuration MetroCluster comme des clusters individuels. Il ne fait aucune distinction entre les clusters qui sont des partenaires ou établit un lien entre le débit d'écriture de chaque cluster.

Lorsqu'un cluster local d'une configuration MetroCluster met en miroir ses données vers son cluster partenaire, les données sont écrites sur la mémoire NVRAM, puis transférées sur les liens ISL vers les agrégats distants. Unified Manager analyse la mémoire NVRAM pour identifier les charges de travail dont le débit d'écriture élevé utilise la mémoire NVRAM, ce qui engendre des conflits.

Les charges de travail dont la déviation 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, entraînant la contention, sont appelées *bullies*. Seules les demandes d'écriture sont mises en miroir vers le cluster partenaire, Unified Manager n'analyse pas le débit de lecture.

Vous pouvez afficher le débit de tous les clusters d'une configuration MetroCluster en analysant les charges de travail des LUN et volumes correspondants à partir des écrans suivants. Vous pouvez filtrer les résultats par cluster. Dans le volet de navigation de gauche :

- **Stockage > clusters > Performance : vue tous les clusters**. Voir
- **Stockage > volumes > performances : vue tous les volumes**.

- **Stockage > LUN > performances : vue toutes 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 performances pour une configuration MetroCluster"

"Rôles des charges de travail impliquées dans un événement de performance"

"L'identification des charges de travail victimes impliquées dans la mise en œuvre d'un événement de performance"

"L'identification des workloads dominants impliqués dans un événement de performance"

"L'identification des charges de travail Shark impliquées dans un événement de performance"

Présentation des événements de performances et des alertes

Les événements de performance sont des incidents liés aux performances des charges de travail sur un cluster. Ils vous aident à identifier les workloads avec des temps de réponse lents. Avec les événements de santé qui se sont produits en même temps, vous pouvez déterminer les problèmes qui pourraient avoir causé, ou contribué à, les 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 performance de certains types de gravité se produisent.

Sources des événements de performance

Les événements de performance sont des problèmes liés aux performances des charges de travail sur un cluster. Ils vous aident à identifier les objets de stockage avec des temps de réponse lents, également appelés « latence élevée ». Avec d'autres événements de santé qui se sont produits en même temps, vous pouvez déterminer les problèmes qui pourraient avoir causé, ou contribué à, les délais de réponse lents.

Unified Manager reçoit des événements de performance des sources suivantes :

- **Événements de politique de seuil de performances définis par l'utilisateur**

  Problèmes de performances basés sur des valeurs de seuil personnalisées que vous avez définies. Vous configurez des règles de seuil de performances pour les objets de stockage, par exemple des agrégats et des volumes, de sorte que les événements soient générés lorsqu'une valeur de seuil pour un compteur de performances a été atteinte.

Vous devez définir une règle de seuil de performances et l'affecter à un objet de stockage pour recevoir ces événements.

- **Événements de politique de seuil de performances définis par le système**

  Problèmes de performances basés sur des valeurs seuils définies par le système. Ces règles de seuil sont incluses dans l'installation de Unified Manager afin de couvrir les problèmes de performance les plus courants.

  Ces règles de seuil sont activées par défaut et vous pouvez afficher des événements peu après l'ajout d'un cluster.

- **Événements seuil de performances dynamiques**

  Problèmes de performance dus à des défaillances ou à des erreurs dans une infrastructure IT, ou à la sur-utilisation des ressources du cluster par les charges de travail. La cause de ces événements peut être un simple problème qui se corrige au cours d'un certain temps ou qui peut être résolu par une réparation ou un changement de configuration. Un événement à seuil dynamique indique que les workloads d'un système ONTAP sont lents en raison d'autres workloads dont l'utilisation des composants du cluster partagé est élevée.

  Ces seuils sont activés par défaut et vous pouvez afficher des événements après trois jours de collecte des données d'un nouveau cluster.

Types de sévérité des événements de performance

Chaque événement de performance est associé à un type de gravité pour vous aider à hiérarchiser les événements nécessitant une action corrective immédiate.

- **Critique**

  Un événement sur les performances peut entraîner une interruption des services si des actions correctives ne sont pas prises immédiatement.

  Les événements critiques sont envoyés à partir de seuils définis par l'utilisateur uniquement.

- **Avertissement**

  Un compteur de performances pour un objet de cluster est hors de la plage normale et doit être surveillé pour vérifier qu'il n'atteint pas la gravité critique. Les événements de ce niveau de gravité n'entraînent pas d'interruption des services, mais une action corrective immédiate peut ne pas être 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 exécutée. Par exemple, lorsqu'un objet de stockage est supprimé ou en cas de modification de la configuration, l'événement contenant des informations de type de gravité est généré.

  Les événements d'informations sont envoyés directement depuis ONTAP lorsqu'il détecte une modification de configuration.

Pour plus d'informations, consultez les liens suivants :

- "Que se passe-t-il lorsqu'un événement est reçu"
- "Les informations contenues dans un e-mail d'alerte"
- "Ajout d'alertes"
- "Ajout d'alertes en cas d'événements de performances"

Modifications de configuration détectées par Unified Manager

Unified Manager surveille vos clusters pour modifier la configuration, ce qui vous permet de déterminer si une modification a pu être causée ou contribué 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 auxquelles la modification a été détectée.

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 affecté les performances de l'objet de cluster sélectionné. Si la modification a été détectée en même temps qu'un événement de performance ou à peu près, la modification peut avoir contribué au problème, qui a déclenché l'alerte d'événement.

Unified Manager peut détecter les événements de modification suivants, classés dans la catégorie « événements d'information » :

- Un volume est déplacé entre agrégats.

  Unified Manager peut détecter lorsque le déplacement est en cours, terminé ou échoué. Lorsqu'Unified Manager est inactif pendant le déplacement d'un volume, lors de sa sauvegarde, il détecte le déplacement de volume et affiche un événement de modification pour celui-ci.

- Le débit (Mbit/s ou IOPS) d'un groupe de règles de QoS contenant un ou plusieurs changements de charge de travail surveillés.

  La modification de la limite d'un groupe de règles peut entraîner des pics intermittents de latence (temps de réponse), qui peuvent également déclencher des événements pour le groupe de règles. La latence revient progressivement à la normale et tous les événements provoqués par les pics deviennent obsolètes.

- Un nœud d'une paire haute disponibilité prend le relais ou renvoie le stockage de son nœud partenaire.

  Unified Manager peut détecter la fin de l'opération de basculement, de basculement partiel ou de rétablissement. Si le basculement est causé par un nœud paniqué, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de restauration de ONTAP a été effectuée correctement.

  La version précédente et la nouvelle version sont affichées.

Types de règles de seuils de performance définies par le système

Unified Manager fournit des règles de seuil standard qui contrôlent les performances du cluster et génèrent automatiquement des événements. Ces règles sont activées par

défaut et génèrent des événements d'avertissement ou d'information lorsque les seuils de performances surveillés sont enfreintes.

> Les règles de seuil de performance 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 règles de seuils de performance définies par le système, vous pouvez désactiver les événements de règles individuelles à partir de la page de configuration des événements.

Règles de seuil du cluster

Les règles de seuil des performances du cluster définies par le système sont attribuées, par défaut, à chaque cluster contrôlé par Unified Manager :

- **Déséquilibre de charge du groupe**

  Identifie les situations où un nœud fonctionne à une charge bien plus élevée que les autres nœuds du cluster et peut donc affecter les latences des charges de travail.

  Pour ce faire, il compare la valeur de capacité en termes de performances utilisée pour tous les nœuds d'un cluster afin de voir si un nœud a dépassé la valeur seuil de 30 % pendant plus de 24 heures. Il s'agit d'un incident d'avertissement.

- **Déséquilibre de capacité du groupe**

  Identifie les situations où la capacité utilisée d'un agrégat est bien plus élevée que celle des autres agrégats du cluster et affecte donc potentiellement l'espace requis pour les opérations.

  Pour ce faire, elle compare la valeur de capacité utilisée de tous les agrégats du cluster afin de voir si la différence entre 70 % d'un agrégat. Il s'agit d'un incident d'avertissement.

Règles de seuil des nœuds

Les règles de seuil de performance des nœuds définies par le système sont attribuées par défaut à chaque nœud des clusters contrôlé par Unified Manager :

- **Seuil de capacité utilisée de performances dépassé**

  Identifie les situations dans lesquelles un nœud fonctionne au-delà des limites de son efficacité opérationnelle et risque par conséquent d'affecter la latence des charges de travail.

  Pour ce faire, il recherche des nœuds qui utilisent plus de 100 % de leur capacité en performance pendant plus de 12 heures. Il s'agit d'un incident d'avertissement.

- **Surutilisation de la paire HA de nœuds**

  Identifie les situations dans lesquelles les nœuds d'une paire haute disponibilité fonctionnent au-dessus des limites de l'efficacité opérationnelle de la paire haute disponibilité.

  Pour ce faire, le système étudie la valeur de la capacité en termes de performances utilisée pour les deux nœuds de la paire haute disponibilité. Si la capacité de performance combinée des deux nœuds dépasse 200 % pendant plus de 12 heures, un basculement de contrôleur affecte les latences des charges de travail. Il s'agit d'un événement informatif.

- **Fragmentation de disque de nœud**

  Identifie les situations où un ou plusieurs disques d'un agrégat sont fragmentés, ralentissant les principaux services système et potentiellement affecter les latences des charges de travail sur un nœud.

  Pour ce faire, il s'agit de certains ratios d'opération de lecture et d'écriture sur tous les agrégats d'un nœud. Cette règle peut également être déclenchée lors de la resynchronisation SyncMirror ou lorsque des erreurs sont détectées lors des opérations de nettoyage du disque. Il s'agit d'un incident d'avertissement.

  > La règle de « fragmentation des disques des nœuds » analyse les agrégats uniquement composés de disques durs ; les agrégats Flash Pool, SSD et FabricPool ne sont pas analysés.

Règles de seuil agrégées

La règle de seuil de performance des agrégats définis par le système est attribuée par défaut à chaque agrégat des clusters contrôlé par Unified Manager :

- **Disques agrégés sur-utilisés**

  Identifie les situations dans lesquelles un agrégat fonctionne au-delà des limites de son efficacité opérationnelle et peut ainsi affecter le latence des charges de travail. Ce cas est identifié par la recherche d'agrégats où les disques de l'agrégat sont utilisés à plus de 95 % pendant plus de 30 minutes. Cette règle multicondition effectue alors l'analyse suivante pour déterminer la cause du problème :

  - Un disque de l'agrégat est-il actuellement en cours d'opération de maintenance en arrière-plan ?

    Certaines activités de maintenance en arrière-plan qu'un disque peut être en cours de reconstruction sont : disque, nettoyage de disque, resynchronisation SyncMirror et reparité.

  - Existe-t-il un goulet d'étranglement au niveau des communications dans l'interconnexion Fibre Channel du tiroir disque ?
  - L'agrégat dispose-t-il trop peu d'espace libre ? Un événement d'avertissement est émis pour cette politique uniquement si une ou plusieurs des trois politiques subordonnées sont également considérées comme enfreintes. Un événement de performances n'est pas déclenché si seuls les disques de l'agrégat sont utilisés à plus de 95 %.

  > La politique « d'agrégation de disques sur-utilisés » analyse les agrégats de disques durs uniquement et les agrégats Flash Pool (hybrides) ; les agrégats SSD et FabricPool ne sont pas analysés.

Règles de seuil de latence des workloads

Les règles de seuil de latence de la charge de travail définies par le système sont attribuées à toute charge de travail dont la règle de niveau de service de performance est configurée et dont la valeur de « latence attendue » est définie :

- **Seuil de latence de volume de charge de travail/LUN dépassé tel que défini par le niveau de service de performances**

  Identifie les volumes (partages de fichiers) et les LUN qui ont dépassé leur limite de « latence attendue » et qui ont un impact sur les performances des charges de travail. Il s'agit d'un incident d'avertissement.

Pour ce faire, il recherche des charges de travail qui ont dépassé la valeur de latence prévue pour 30 % de l'heure précédente.

Règles de seuil de QoS

Les règles de seuil de performances de QoS définies par le système sont attribuées à toute charge de travail dont la règle de débit maximal est la QoS ONTAP configurée (IOPS, IOPS/To ou Mo/s). Unified Manager déclenche un événement lorsque la valeur du débit des workloads est inférieure de 15 % à la valeur de la QoS configurée :

- **QoS Max IOPS ou seuil MB/s**

  Identifie les volumes et les LUN qui ont dépassé leur limite maximale en termes d'IOPS ou de débit en Mo/s de qualité de service, et qui affectent la latence des charges de travail. Il s'agit d'un incident d'avertissement.

  Lorsqu'une seule charge de travail est attribuée à un groupe de règles, elle recherche les charges de travail qui ont dépassé le seuil de débit maximal défini dans le groupe de règles QoS attribué au cours de chaque période de collecte pendant l'heure précédente.

  Lorsque plusieurs charges de travail partagent une seule règle de QoS, celle-ci est ajoutée en ajoutant les IOPS ou les Mo/s de tous les workloads de la règle et en vérifiant le total dans la limite.

- **QoS Peak IOPS/To ou IOPS/To avec seuil de taille de bloc**

  Identifie les volumes qui ont dépassé la limite de débit en IOPS/To adaptative pour la qualité de service (ou IOPS/To avec limite de taille de bloc), tout en affectant la latence de la charge de travail. Il s'agit d'un incident d'avertissement.

  Pour ce faire, la conversion du seuil maximal d'IOPS/To défini dans la règle de QoS adaptative en une valeur maximale d'IOPS basée sur la taille de chaque volume. Elle recherche les volumes qui ont dépassé la limite d'IOPS maximale de QoS au cours de chaque période de collecte de performances pendant l'heure précédente.

  > Cette règle s'applique aux volumes uniquement lorsque le cluster est installé avec ONTAP 9.3 et les versions ultérieures.

  Lorsque l'élément « taille de bloc » a été défini dans la règle de QoS adaptative, le seuil est converti en valeur MB/s maximale basée sur la taille de chaque volume. Ensuite, il recherche les volumes qui ont dépassé la limite de qualité de service en Mo/s au cours de chaque période de collecte des performances pour l'heure précédente.

  > Cette règle s'applique aux volumes uniquement lorsque le cluster est installé avec ONTAP 9.5 et les versions ultérieures.

Analyse et notification des événements de performance

Les événements de performance vous signalent les problèmes de performances d'E/S concernant une charge de travail générée par des conflits sur un composant de cluster. Unified Manager analyse l'événement pour identifier toutes les charges de travail impliquées, le composant dans les conflits et si l'événement reste un problème à résoudre.

Unified Manager surveille la latence (temps de réponse) et les IOPS (opérations) des volumes d'un cluster. Lorsque d'autres charges de travail surfont un composant de cluster, par exemple, les conflits sont possibles et le composant ne peut pas fonctionner à un niveau optimal pour répondre aux demandes de charge de travail. Les performances des autres charges de travail qui utilisent le même composant peuvent être affectées, ce qui entraîne une augmentation des latences. Si la latence franchit le seuil de performance dynamique, Unified Manager déclenche un événement de performance afin de vous en avertir.

Analyse des événements

Unified Manager effectue les analyses suivantes, en s'appuyant sur les statistiques de performance des 15 derniers jours, pour identifier les workloads victime, les workloads dominants 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 des 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 représentent plus de 10 opérations par seconde (OPS/s).
  - Pour les volumes situés sur des agrégats 100 % 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 plus de 100 OPS/s.
- Identifie le composant de cluster dans les conflits.

> Si la latence des charges de travail victimes au niveau de l'interconnexion de cluster est supérieure à 1 ms, Unified Manager le traite comme important et déclenche un événement pour l'interconnexion de cluster.

- Identifie les charges de travail dominantes qui font l'objet d'une surutilisation du composant de cluster et qui l'entraînent des conflits.
- Classe les charges de travail impliquées, en fonction de leur déviation de l'utilisation ou de l'activité d'un composant du cluster, afin de déterminer les principaux changements d'utilisation du composant du cluster et les victimes les plus affectées.

Un événement peut se produire brièvement et se corriger après le composant qu'il utilise n'est plus en conflit. Un événement continu est un événement qui se produit de nouveau pour le même composant de cluster au cours d'un intervalle de cinq minutes et qui reste à l'état actif. Pour les événements continus, Unified Manager déclenche une alerte après avoir détecté le même événement à deux intervalles d'analyse consécutifs.

Lorsqu'un événement est résolu, il reste disponible dans Unified Manager dans le cadre de l'enregistrement des anciens problèmes de performances d'un volume. Chaque événement possède un ID unique qui identifie le type d'événement et les volumes, le cluster et les composants de cluster impliqués.

> Un seul volume peut être impliqué dans plusieurs événements simultanément.

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'incident n'a pas été corrigé lui-même ou n'a pas été résolu. Le compteur de performances de

l'objet de stockage reste au-dessus du seuil de performance.

- **Obsolète**

  Indique que l'incident n'est plus actif. Le problème à l'origine de l'incident s'est corrigé ou a été résolu. Le compteur de performance de l'objet de stockage n'est plus au-dessus du seuil de performance.

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 à des adresses e-mail spécifiées. Vous pouvez afficher des informations d'analyse détaillées sur un événement et obtenir des suggestions de résolution de cet événement sur la page Détails de l'événement et sur la page analyse des charges de travail.

Interaction d'événement

Sur la page Détails de l'événement et sur la page analyse de la charge de travail, vous pouvez interagir avec les événements de la manière suivante :

- Le déplacement de la souris sur un événement affiche un message indiquant la date et l'heure de détection de l'événement.

  S'il y a plusieurs événements pour la même période, le message indique le nombre d'événements.

- Lorsque vous cliquez sur un seul événement, une boîte de dialogue affiche des informations plus détaillées sur l'événement, notamment les composants de cluster impliqués.

  Le composant en conflit est entouré et mis en évidence 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 des détails sur les trois événements les plus récents. Vous pouvez cliquer sur un événement pour afficher l'analyse des événements 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, de l'utilisation d'un composant 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 d'une charge de travail. Ces informations déterminent le rôle de chaque charge de travail dans l'événement et leur classement 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 valeurs analysées pour la dernière fois et la plage de valeurs attendue identifie les workloads pour lesquels les performances ont le plus été affectées par l'événement.

Supposons par exemple qu'un cluster contient 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 5-10 millisecondes par opération (ms/op) et sa latence réelle est généralement d'environ 7 ms. La prévision de latence pour la charge de travail B est de 10-20 ms/op et sa latence réelle est généralement d'environ 15 ms/op. La latence prévue pour les deux charges de travail est très bonne. En raison de conflits sur le cluster, la latence des deux charges de travail augmente à 40 ms/opération, franchissement du seuil de performance dynamique, qui correspond aux limites supérieures

des prévisions de latence et au déclenchement d'événements. L'écart de latence, entre les valeurs attendues et les valeurs supérieures au seuil de performances, 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/activité, mais la charge de travail A avait l'impact le plus important sur les performances, car elle avait l'écart de latence le plus élevé à 33 ms/opération.

Sur la page Détails de l'événement, dans la section diagnostic système, vous pouvez trier les charges de travail par variation de l'activité, de l'utilisation ou du débit d'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 en termes d'activité, d'utilisation, de débit ou de latence depuis que l'événement a été détecté à partir des valeurs attendues pour déterminer l'ordre de tri de la charge de travail. Pour la latence, les points rouges (🔴) indiquent un seuil de performance traversant une charge de travail victime, et l'impact suivant sur la latence. Chaque point rouge indique un niveau d'écart plus élevé de latence, ce qui vous aide à identifier les workloads victimes dont la latence a le plus été affectée par un événement.

Les composants du cluster et les conflits

Vous pouvez identifier les problèmes de performance du cluster lorsqu'un composant du cluster entre en conflit. Les performances des charges de travail qui utilisent le ralentissement du composant et leur temps de réponse (latence) augmente pour les requêtes client, ce qui déclenche un événement dans Unified Manager.

Un composant en conflit ne peut pas se faire à un niveau optimal. Ses performances ont diminué, et la performance des autres composants et charges de travail du cluster, appelés *victimes*, peut avoir augmenté la latence. Pour mettre un composant à l'extérieur des conflits, vous devez réduire sa charge de travail ou augmenter sa capacité à gérer davantage de travail, de sorte que les performances puissent revenir à des niveaux normaux. Unified Manager collecte et analyse les performances des charges de travail toutes les cinq minutes. En effet, il ne détecte que lorsqu'un composant du cluster est constamment sur-utilisé. Les pics transitoires de surutilisation qui durent pendant une courte durée dans l'intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être soumis à des conflits car une ou plusieurs charges de travail y sont en concurrence pour que leurs demandes d'E/S soient traitées. Des charges de travail peuvent être affectées sur l'agrégat, ce qui entraîne une baisse des performances. Pour réduire la quantité d'activité sur l'agrégat, différentes étapes sont possibles : déplacer une ou plusieurs charges de travail vers un agrégat ou un nœud moins occupé, par exemple, afin de réduire les besoins globaux de la charge de travail sur l'agrégat en cours. Pour un groupe de règles de qualité de service, vous pouvez ajuster la limite de débit ou déplacer les workloads vers un autre groupe de règles, de sorte que les charges de travail ne soient plus restreintes.

Unified Manager contrôle les composants de cluster suivants pour vous alerter en cas de 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 la fin des transactions « de transfert prêt » avant que le cluster puisse répondre à une demande d'E/S. Si le composant réseau constitue un 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 de plusieurs charges de travail.

- **Traitement réseau**

  Composant logiciel dans le cluster impliqué dans le traitement des E/S entre la couche de protocole et le cluster. Le traitement du réseau de traitement des nœuds a peut-être changé depuis la détection de l'événement. Si le composant de traitement de réseau est en conflit, son utilisation élevée au niveau du

nœud de traitement réseau a un impact sur la latence d'une ou de plusieurs charges de travail.

Lors de l'utilisation d'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 de qualité de service max**

  Représente le paramètre de débit maximal (crête) du groupe de règles de qualité de service (QoS) de stockage affecté à la charge de travail. Si le composant de groupe de règles conflits, cela signifie que toutes les charges de travail du groupe de règles sont restreintes par la limite de débit définie, qui a un impact sur la latence d'une ou plusieurs de ces charges de travail.

- **Limite de qualité de service min**

  Représente la latence pour une charge de travail générée par le paramètre de débit de QoS minimal (attendu) attribué à d'autres workloads. Si, pour certaines charges de travail, la qualité de service minimale est définie sur la majorité de la bande passante pour garantir le débit promis, d'autres charges de travail sont restreintes et affichent une latence plus élevée.

- * Interconnexion de cluster*

  La représente les câbles et adaptateurs avec lesquels les nœuds en cluster sont physiquement connectés. Si le composant d'interconnexion de cluster est en conflit, cela signifie un temps d'attente élevé pour les demandes d'E/S au niveau de l'interconnexion de cluster se répercute sur la latence d'une ou de plusieurs charges de travail.

- **Traitement de données**

  Composant logiciel dans le cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient la charge de travail. Le traitement des données de traitement du nœud peut avoir changé depuis la détection de l'événement. Si le composant de traitement des données conflit, une utilisation élevée au niveau du nœud de traitement des données affecte la latence d'un ou de plusieurs workloads.

- **Activation du volume**

  Processus permettant de suivre l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1000 volumes sont actifs, ce processus surveille en même temps le nombre de volumes stratégiques devant accéder aux ressources par le biais du nœud. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques subissent une latence telle qu'elle est identifiée ici.

- **Ressources MetroCluster**

  La représente les ressources MetroCluster, y compris la NVRAM et les liens ISL, utilisés pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster rencontre des conflits, il s'agit d'un débit d'écriture élevé avec les charges de travail sur le cluster local ou d'un problème d'état de santé de la liaison ayant un impact sur la latence d'une ou de plusieurs charges de travail sur le cluster local. Si le cluster ne se trouve pas dans une configuration MetroCluster, cette icône n'est pas affichée.

- **Agrégat ou agrégat SSD**

  Agrégat de stockage sur lequel les charges de travail s'exécutent. Si le composant de l'agrégat est en conflit, une utilisation élevée de l'agrégat a un impact sur la latence d'une ou de plusieurs charges de

travail. Un agrégat se compose de tous les disques durs, ou d'un mélange de disques durs et de disques SSD (un agrégat Flash Pool), ou d'une combinaison de disques durs et d'un niveau de cloud (un agrégat FabricPool). Un « agrégat SD » se compose de tous les SSD (un agrégat 100 % Flash), ou d'une combinaison de SSD et d'un niveau cloud (un agrégat FabricPool).

- * Latence 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 dans le cloud conflits, une grande quantité de lectures sur les volumes hébergés sur le Tier cloud ont une incidence sur la latence d'un ou de plusieurs workloads.

- **SnapMirror de synchronisation**

  Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur depuis le volume primaire vers le volume secondaire dans une relation SnapMirror synchrone. Si le composant SnapMirror synchrone entre en conflit, l'activité des opérations SnapMirror synchrone a un impact sur la latence d'un ou de plusieurs workloads.

Rôles des charges de travail impliquées dans un événement de performance

Unified Manager utilise des rôles pour identifier la participation d'une charge de travail en cas de performance. Les rôles sont les victimes, les taureaux et les requins. Une charge de travail définie par l'utilisateur peut être une victime, un tyran et un requin en même temps.

Rôle	Description
Victime	Charge de travail définie par l'utilisateur dont les performances ont diminué en raison des autres charges de travail, appelées « bullies », qui sont sur-utilisées lors de l'utilisation d'un composant du cluster. Seules les charges de travail définies par l'utilisateur sont identifiées comme victimes. Unified Manager identifie les charges de travail victimes en fonction de leur écart de latence, où la latence réelle, pendant un événement, a été considérablement améliorée par rapport à sa prévision de latence (plage prévue).
Intimider	Une charge de travail définie par l'utilisateur ou définie par le système dont l'utilisation excessive d'un composant de cluster a entraîné une diminution des performances d'autres charges de travail, appelées « victimes ». Unified Manager identifie les workloads dominants en fonction de leur déviation par l'utilisation d'un composant de cluster, où l'utilisation réelle, au cours d'un événement, a considérablement augmenté à partir de sa plage d'utilisation prévue.

Rôle	Description
Requin	Charge de travail définie par l'utilisateur, avec l'utilisation la plus élevée d'un composant de cluster, et non pas toutes les charges de travail impliquées dans un événement. Unified Manager identifie les charges de travail Shark en fonction de leur utilisation d'un composant de cluster pendant un événement.

Les charges de travail d'un cluster peuvent partager la plupart des composants du cluster, tels que les agrégats et la CPU pour le traitement du réseau et des données. Lorsqu'une charge de travail, par exemple un volume, augmente l'utilisation d'un composant de cluster au point que le composant ne peut pas répondre efficacement aux exigences de la charge de travail, le composant engendre des conflits. La charge de travail sur-utilisation d'un composant de cluster est un phénomène tyran. Les autres charges de travail qui partagent ces composants, et dont la performance est impactée par le tyran, sont les victimes. L'activité provenant des charges de travail définies par le système, telles que la déduplication ou les copies Snapshot, peut également créer des « brimades ».

Lorsqu'Unified Manager détecte un événement, il identifie tous les workloads et composants de cluster impliqués, notamment les workloads dominants qui ont causé l'événement, le composant de cluster en conflit et les workloads victimes dont les performances ont diminué en raison de l'augmentation de l'activité des workloads dominants.

> Si Unified Manager ne peut pas identifier les charges de travail dominantes, cette alerte s'applique uniquement aux charges de travail victimes et au composant de cluster concerné.

Unified Manager est capable d'identifier les charges de travail victimes de charges de travail dominantes. Il peut également y avoir une identification lorsque ces mêmes charges de travail deviennent des charges de travail dominantes. Un workload peut être un tyran à lui-même. Par exemple, une charge de travail élevée au ralenti par une limite de groupe de règles entraîne le restriction de toutes les charges de travail du groupe de règles, y compris de celles-ci. Une charge de travail dominante ou victime dans un événement de performance continu peut changer son rôle ou ne plus y participer.

Gestion des seuils de performances

Les règles de seuil de performances vous permettent de déterminer le point à partir duquel Unified Manager génère un événement afin d'informer les administrateurs système des problèmes qui pourraient affecter la performance des charges de travail. Ces stratégies de seuil sont appelées seuils de performance définis par l'utilisateur.

Cette version prend en charge les seuils de performance dynamiques, définis par l'utilisateur et définis par le système. Avec des seuils de performance dynamiques et définis par le système, Unified Manager analyse l'activité des charges de travail pour déterminer la valeur seuil appropriée. Grâce aux 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 performance définis par le système et les seuils de performance dynamiques sont définis par Unified Manager et ne peuvent pas être configurés. Si vous recevez des événements inutiles des règles de seuils de performance définies par le système, vous pouvez désactiver chacune des règles à partir de la page de configuration des événements.

Fonctionnement des règles de seuil de performances définies par l’utilisateur

Vous définissez des règles de seuil de performances sur les objets de stockage (sur les agrégats et les volumes, par exemple). Un événement peut ainsi être envoyé à l’administrateur du stockage pour informer l’administrateur que le cluster rencontre un problème de performances.

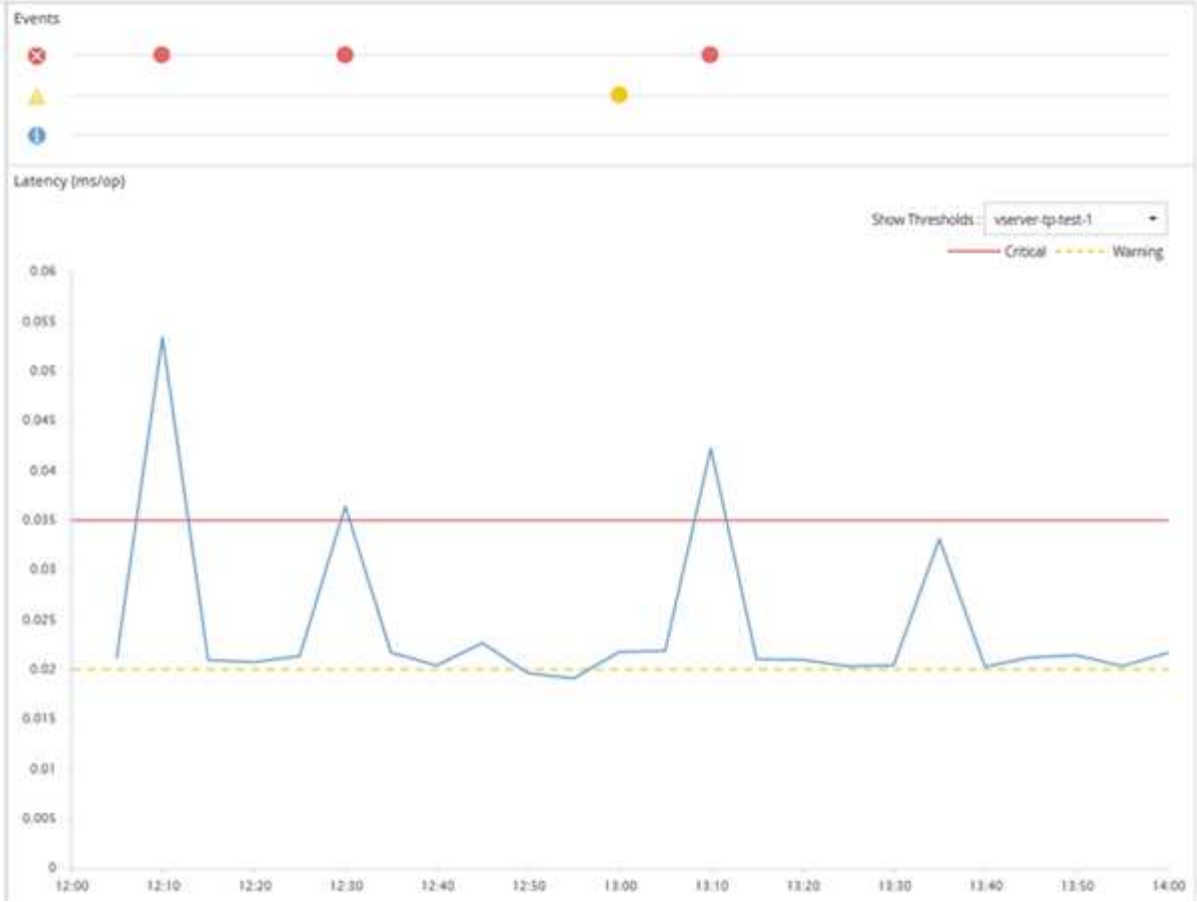
Vous créez une règle de seuil de performances pour un objet de stockage en :

- Sélection d’un objet de stockage
- Sélection d’un compteur de performances associé à cet objet
- Spécification de valeurs définissant les limites supérieures du compteur de performances considérées comme des situations d’avertissement et critiques
- Spécification d’une période qui définit la durée du compteur devant dépasser la limite supérieure

Par exemple, vous pouvez définir une règle de seuil de performance sur un volume afin de recevoir une notification d’événements critiques 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 illustré ici, indiquant qu’un seuil d’avertissement (icône jaune) a été dépassé à 1:00 et qu’un seuil critique (icône rouge) a été dépassé à 12:10, 12:30 et 1:10 :



Une violation de seuil doit se produire en continu pendant la durée spécifiée. Si le seuil passe 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 règle de seuils de combinaison qui requiert deux compteurs de performances pour dépasser leurs limites maximales avant qu'un événement ne soit généré. Par exemple, vous pouvez créer une stratégie de seuil à l'aide des critères suivants :

Objet cluster	Compteur de performances	Seuil d'avertissement	Seuil critique	Durée
Volumétrie	Latence	10 millisecondes	20 millisecondes	15 minutes
Agrégat	Du stockage	65%	85%	

Les règles de seuil qui utilisent deux objets de cluster provoquent la génération d'un événement uniquement lorsque les deux conditions sont remplies. Par exemple, en utilisant la règle de seuil définie dans le tableau :

Si la latence du volume est moyenne…	Et l'utilisation des disques de l'agrégat est…	Alors…
15 millisecondes	50%	Aucun événement n'est signalé.

Si la latence du volume est moyenne…	Et l'utilisation des disques de l'agrégat est…	Alors…
15 millisecondes	75%	Un incident d'avertissement est signalé.
25 millisecondes	75%	Un incident d'avertissement est signalé.
25 millisecondes	90%	Un événement critique est signalé.

Que se passe-t-il lorsqu'une règle de seuil de performances est enfreinte

Lorsqu'une valeur de compteur dépasse sa valeur de seuil de performances définie pour la durée spécifiée, 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 Performance Cluster Summary, la page Events et la page Performance Inventory spécifique à l'objet.
- (Facultatif) une alerte par e-mail concernant l'événement peut être envoyée à un ou plusieurs destinataires d'e-mail et une interruption SNMP peut être envoyée à un destinataire 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 règle d'avertissement ou de seuil critique est enfreinte.

Après une violation de la règle de seuil de performances sur un objet de stockage, aucun autre événement n'est généré pour cette règle jusqu'à ce que la valeur de compteur atteigne la valeur seuil inférieure à laquelle la durée est réinitialisée pour cette limite. Même si le seuil reste dépassé, l'heure de fin de l'événement est mise à jour en permanence pour indiquer que cet événement est en cours.

Un événement de seuil capture ou gèle les informations relatives à la gravité et à la définition de stratégie de sorte que les informations de seuil uniques s'affichent avec l'événement, même si la stratégie de seuil est modifiée ultérieurement.

Quels compteurs de performances peuvent être suivis à l'aide de seuils

Certains compteurs de performances courants, tels que les IOPS et les Mo/s, peuvent comporter des seuils pour tous les objets de stockage. D'autres compteurs peuvent avoir des seuils définis pour certains objets de stockage uniquement.

Compteurs de performances disponibles

Objet de stockage	Compteur de performances	Description
Cluster	LES IOPS	Nombre moyen d’opérations d’entrée/sortie que le cluster traite par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférées à et depuis ce cluster par seconde.	Nœud
LES IOPS	Nombre moyen d’opérations d’entrée/sortie que le nœud traite par seconde.	Mo/s
Nombre moyen de mégaoctets de données transférées vers et depuis ce nœud par seconde.	Latence	Nombre moyen de millisecondes nécessaires pour répondre aux demandes des applications par le nœud.
Du stockage	Pourcentage moyen du processeur et de la mémoire vive du nœud utilisé.	Performance capacité utilisée
Pourcentage moyen de capacité de performance consommée par le nœud	Performance capacité utilisée - basculement	Pourcentage moyen de capacité de performance consommée par le nœud, plus la capacité de performance de son nœud partenaire.
Agrégat	LES IOPS	Nombre moyen d’opérations d’entrée/sortie les processus agrégés par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférées à et depuis cet agrégat par seconde.	Latence
Nombre moyen de millisecondes nécessaires à l’agrégat pour répondre aux demandes des applications.	Du stockage	Pourcentage moyen des disques de l’agrégat utilisés
Performance capacité utilisée	Pourcentage moyen de capacité de performance consommée par l’agrégat	VM de stockage
LES IOPS	Nombre moyen d’opérations d’entrée/sortie que la SVM traite par seconde.	Mo/s

Objet de stockage	Compteur de performances	Description
Nombre moyen de mégaoctets de données transférées à et à partir de cette SVM par seconde.	Latence	Nombre moyen de millisecondes nécessaires pour répondre aux demandes des applications par la SVM.
Volumétrie	LES IOPS	Nombre moyen d'opérations d'entrée/sortie les processus de volume par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférées vers et depuis ce volume par seconde.	Latence
Nombre moyen de millisecondes nécessaires pour répondre aux demandes de l'application par le volume	Taux de manque du cache	Pourcentage moyen de demandes de lecture des applications client renvoyées à partir du volume plutôt que d'être renvoyées à partir du cache.
LUN	LES IOPS	Nombre moyen d'opérations d'entrée/sortie que la LUN traite par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférées à et à partir de cette LUN par seconde.	Latence
Nombre moyen de millisecondes nécessaires pour répondre aux demandes des applications par la LUN.	Espace de noms	LES IOPS
Nombre moyen d'opérations d'entrée/sortie les processus d'espace de noms par seconde.	Mo/s	Nombre moyen de mégaoctets de données transférées à et depuis ce namespace par seconde.
Latence	Nombre moyen de millisecondes nécessaires pour répondre aux demandes de l'application par l'espace de noms	Port
Utilisation de la bande passante	Pourcentage moyen de la bande passante disponible du port utilisée.	Mo/s

Objet de stockage	Compteur de performances	Description
Nombre moyen de mégaoctets de données transférées vers et depuis ce port par seconde.	Interface réseau (LIF)	Mo/s

Quels objets et compteurs peuvent être utilisés dans les stratégies de seuils de combinaison

Seuls certains compteurs de performances peuvent être utilisés ensemble dans le cadre de stratégies mixtes. Lorsque des compteurs de performances primaires et secondaires sont spécifiés, les deux compteurs de performances doivent dépasser leurs limites maximales avant la génération d'un événement.

Objet et compteur de stockage primaire	Compteur et objet de stockage secondaire
Latence du volume	IOPS du volume
Volume en Mo/s	Utilisation des agrégats
Capacité de performance des agrégats utilisée	Utilisation des nœuds
Capacité de performance du nœud utilisée	Capacité du nœud utilisée – basculement
Latence de la LUN	IOPS DE LA LUN
Mo/s de LUN	Utilisation des agrégats
Capacité de performance des agrégats utilisée	Utilisation des nœuds
Capacité de performance du nœud utilisée	Capacité du nœud utilisée – basculement

Lorsqu'une règle de combinaison de volumes est appliquée à un volume FlexGroup au lieu d'être sur un volume FlexVol, seuls les attributs « IOPS de volume » et « Mo/s de volume » peuvent être sélectionnés comme compteur secondaire. Si la règle de seuil contient l'un des attributs de nœud ou d'agrégat, elle ne sera pas appliquée au volume FlexGroup et un message d'erreur décrivant ce cas s'affiche. En effet, les volumes FlexGroup peuvent exister sur plusieurs nœuds ou agrégats.

Création de règles de seuils de performance définies par l'utilisateur

Vous créez des règles de seuil de performances pour les objets de stockage, de sorte 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Vous créez des stratégies de seuil de performances en entrant les valeurs de seuil sur la page Créer une stratégie de seuil de performances. Vous pouvez créer de nouvelles stratégies en définissant toutes les valeurs de la stratégie dans cette page, ou vous pouvez faire une copie d'une stratégie existante et modifier les valeurs dans la copie (appelée *clonage*).

Les valeurs de seuil valides sont de 0.001 à 10,000,000 pour les nombres, de 0.001-100 pour les pourcentages et de 0.001-200 pour les pourcentages de capacité utilisée pour les performances.

> 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'événements** > **performances**.

   La page seuils de performance s'affiche.

2. Cliquez sur le bouton approprié selon que vous souhaitez créer une nouvelle stratégie ou si vous souhaitez cloner une règle similaire et modifier la version clonée.

Pour…	Cliquez sur…
Création d'une nouvelle règle	**Créer**
Cloner une règle existante	Sélectionnez une stratégie existante et cliquez sur **Clone**

   La page Créer une stratégie de seuil de performances ou Cloner la stratégie de seuil de performances s'affiche.

3. Définissez la règle de seuil en spécifiant les valeurs de seuil des compteurs 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 règle.

   b. Sélectionnez le compteur de performances à suivre et spécifiez les valeurs limites qui définissent les événements Avertissement et critique.

      Vous devez définir au moins un avertissement ou une limite critique. Il n'est pas nécessaire de définir les deux types de limites.

   c. Sélectionnez un compteur de performances secondaire, si nécessaire, et spécifiez les valeurs limites pour les événements Avertissement et critique.

      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 soit signalé. Seuls certains objets et compteurs peuvent être configurés à l'aide d'une règle de combinaison.

   d. Sélectionnez la durée pendant laquelle les valeurs limites doivent être enfreintes pour un événement à envoyer.

   Lors du clonage d'une règle existante, vous devez entrer un nouveau nom pour cette règle.

4. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

   Vous êtes renvoyé à la page seuils de performances. Un message de réussite en haut de la page confirme la création de la règle de seuil et fournit un lien vers la page Inventaire pour ce type d'objet afin d'appliquer la nouvelle règle aux objets de stockage immédiatement.

Si vous souhaitez appliquer la nouvelle stratégie de seuil aux objets de stockage à ce moment-là, vous pouvez cliquer sur le lien **accéder à Object_type Now** pour accéder à la page Inventaire.

Assignation de règles de seuil de performances aux objets de stockage

Vous affectez une règle de seuil de performances définie par l'utilisateur à un objet de stockage. Unified Manager signale ainsi un événement si la valeur du compteur de performances dépasse le paramètre de règle.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

La ou les règles de seuil de performances que vous souhaitez appliquer à l'objet doivent exister.

Vous ne pouvez appliquer qu'une seule règle de performances à la fois à un objet ou à un groupe d'objets.

Vous pouvez attribuer un maximum de trois règles de seuil à chaque objet de stockage. Lors de l'affectation de règles à plusieurs objets, si le nombre maximal de règles est déjà attribué à l'un des objets, Unified Manager effectue les actions suivantes :

- Applique la stratégie à tous les objets sélectionnés qui n'ont pas atteint leur maximum
- Ignore les objets qui ont atteint le nombre maximal de règles
- Affiche un message indiquant que la stratégie n'a pas été attribuée à tous les objets

Étapes

1. Dans la page d'inventaire des performances d'un objet de stockage, sélectionnez l'objet ou les objets vers lesquels vous souhaitez attribuer une règle de seuil :

Pour affecter des seuils à…	Cliquez sur…
Un seul objet	La case à cocher située à gauche de cet objet.
Objets multiples	La case à cocher à gauche de chaque objet.
Tous les objets de la page	La liste déroulante et choisissez **Sélectionner tous les objets de cette page**.
Tous les objets du même type	La 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 stratégies de seuil à de nombreux objets.

2. Faites votre sélection, puis cliquez sur **attribuer une stratégie de seuil de performances**.

   La page attribuer une stratégie de seuil de performances s'affiche et affiche la liste des stratégies de seuil qui existent pour ce type spécifique d'objet de stockage.

3. Cliquez sur chaque stratégie pour afficher les détails des paramètres de seuil de performances afin de vérifier que vous avez sélectionné la stratégie de seuil correcte.
4. Après avoir sélectionné la stratégie de seuil appropriée, cliquez sur **affecter stratégie**.

   Un message de réussite en haut de la page confirme que la règle de seuil a été attribuée à l'objet ou aux objets et fournit un lien vers la page d'alerte pour vous permettre de configurer les paramètres d'alerte de cet objet et de cette règle.

Si vous souhaitez que des alertes soient envoyées par e-mail, ou en tant que trap SNMP, pour vous informer qu'un événement de performance particulier a été généré, vous devez configurer les paramètres d'alerte dans la page Configuration de l'alerte.

Affichage des règles de seuils de performances

Vous pouvez afficher toutes les règles de seuils de performance actuellement définies à partir de la page seuils de performance.

La liste des stratégies de seuils est triée par ordre alphabétique par nom de la règle et comprend les stratégies de tous les types d'objets de stockage. Vous pouvez cliquer sur un en-tête de colonne pour trier les polices d'après cette colonne. Si vous recherchez une stratégie spécifique, utilisez les mécanismes de filtre et de recherche pour affiner la liste des stratégies de seuils qui s'affichent dans la liste de stocks.

Vous pouvez placer le curseur sur le nom de la stratégie et le nom de la condition pour afficher les détails de configuration de la stratégie. En outre, 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'événements** > **performances**.

   La page seuils de performance s'affiche.

Modification des règles de seuils de performances définies par l'utilisateur

Vous pouvez modifier les paramètres de seuil des règles de seuils de performances existantes. Cela peut être utile si vous constatez que vous recevez trop ou trop peu d'alertes pour certaines conditions de seuil.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Vous ne pouvez pas modifier le nom de la règle ou le type d'objet de stockage actuellement contrôlé pour les règles de seuils existantes.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **seuils d'événements** > **performances**.

La page seuils de performance s'affiche.

2. Sélectionnez la stratégie de seuil à modifier et cliquez sur **Modifier**.

   La page Modifier la stratégie de seuil de performances s'affiche.

3. Apportez vos modifications à la stratégie de seuil et cliquez sur **Enregistrer**.

   Vous êtes renvoyé à la page seuils de performances.

Une fois qu'elles ont été enregistrées, les modifications sont immédiatement mises à jour sur tous les objets de stockage qui utilisent la règle.

En fonction du type de modifications apportées à la règle, vous pouvez consulter les paramètres d'alerte configurés pour les objets qui utilisent la règle dans la page Configuration des alertes.

Suppression des règles de seuil de performances des objets de stockage

Vous pouvez supprimer une règle de seuil de performance définie par l'utilisateur d'un objet de stockage lorsque vous ne souhaitez plus que Unified Manager contrôle la valeur du compteur de performances.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Vous ne pouvez supprimer qu'une seule stratégie à la fois d'un objet sélectionné.

Vous pouvez supprimer une règle de seuil de plusieurs objets de stockage en sélectionnant plusieurs objets dans la liste.

Étapes

1. Dans la page **Inventory** d'un objet de stockage, sélectionnez un ou plusieurs objets dont au moins une règle de seuil de performances est appliquée.

Pour effacer les seuils de…	Procédez comme ça…
Un seul objet	Cochez la case située à gauche de cet objet.
Objets multiples	Cochez la case à gauche de chaque objet.
Tous les objets de la page	Cliquez sur ☐▾ dans l'en-tête de colonne.

2. Cliquez sur **Effacer la stratégie de seuil de performances**.

   La page Effacer la stratégie de seuil s'affiche et affiche la liste des stratégies de seuil actuellement affectées aux objets de stockage.

3. Sélectionnez la stratégie de seuil à supprimer des objets et cliquez sur **Effacer la stratégie**.

   Lorsque vous sélectionnez une stratégie de seuil, les détails de la stratégie s'affichent pour vous permettre de confirmer que vous avez sélectionné la stratégie appropriée.

Que se passe-t-il lorsqu'une règle de seuil de performances est modifiée

Si vous ajustez la valeur de compteur ou la durée d'une règle de seuil de performances existante, la modification de règle s'applique à tous les objets de stockage qui utilisent la règle. Le nouveau paramètre a lieu immédiatement et Unified Manager commence à comparer les valeurs des compteurs de performances avec les nouveaux paramètres seuils pour toutes les données de performance nouvellement collectées.

Si des événements actifs existent pour des objets qui utilisent la règle de seuil modifiée, les événements sont marqués comme obsolètes et la règle de seuil commence à surveiller le compteur comme une nouvelle règle de seuil définie.

Lorsque vous affichez le compteur sur lequel le seuil a été appliqué dans la vue détaillée des compteurs, 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 affichez les données historiques lorsque l'ancien paramètre de seuil était en vigueur.

> Comme les anciens paramètres de seuil n'apparaissent pas dans la vue détaillée des compteurs, il est possible que les événements historiques apparaissent sous les lignes de seuil actuelles.

Que se passe-t-il aux règles de seuils de performances lorsqu'un objet est déplacé

Étant donné que des règles de seuils de performances sont attribuées aux objets de stockage, si vous déplacez un objet, toutes les règles de seuil attribuées restent liées à l'objet une fois le déplacement terminé. Par exemple, si vous déplacez un volume ou une LUN vers un autre agrégat, les règles de seuil sont toujours actives pour le volume ou la LUN du nouvel agrégat.

Il existe une condition de compteur secondaire pour la politique de seuils (une règle 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 au nœud sur lequel le volume ou la LUN a été déplacé.

S'il existe de nouveaux événements actifs pour les objets qui utilisent la règle de seuil modifiée, les événements sont marqués comme obsolètes et la règle de seuil commence à surveiller le compteur comme une nouvelle règle de seuil définie.

Lors d'une opération de déplacement de volume, ONTAP envoie un événement de modification d'information. Une icône d'événement de changement apparaît dans la chronologie des événements sur la page de l'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 règle de seuil définie par l'utilisateur est supprimée de l'objet. Si nécessaire, vous devez affecter une stratégie de seuil à l'objet une fois l'opération de déplacement terminée. Des règles de seuils dynamiques et définies par le système sont cependant appliquées automatiquement à un objet après son déplacement vers un nouveau cluster.

Fonctionnalité de seuil de règle lors du basculement et du rétablissement haute disponibilité

Lorsqu'une opération de basculement ou de rétablissement se produit dans une configuration haute

disponibilité, les objets déplacés d'un nœud vers un autre nœud conservent leur règle de seuil de la même manière que dans les opérations de déplacement manuel. Unified Manager vérifie que la configuration du cluster change toutes les 15 minutes. L'impact du basculement vers le nouveau nœud n'est donc pas identifié avant l'interrogation suivante de la configuration du cluster.

> Si une opération de basculement et de rétablissement se produit au cours de la période de collecte des modifications de configuration de 15 minutes, le déplacement des statistiques de performance d'un nœud vers un autre nœud risque de ne pas être visible.

Fonctionnalité de règle de seuil pendant le transfert d'agrégats

Si vous déplacez un agrégat d'un nœud vers un autre à l'aide de la `aggregate relocation start` commande, les règles de seuil uniques et combinées sont conservées sur tous les objets, et la partie nœud de la règle de seuil est appliquée au nouveau nœud.

Fonctionnalité de règle de seuil lors du basculement de MetroCluster

Les objets qui se déplacent d'un cluster vers un autre cluster d'une configuration MetroCluster ne conservent pas leurs paramètres de règle de seuil définis par l'utilisateur. Si nécessaire, vous pouvez appliquer des politiques de seuil aux volumes et aux LUN qui ont été déplacés vers le cluster partenaire. Une fois qu'un objet est replacé dans son cluster d'origine, la règle de seuil définie par l'utilisateur est réappliquée automatiquement.

Pour plus d'informations, voir "Comportement des volumes lors du basculement et du rétablissement".

Analyse des événements de performances

Vous pouvez analyser les événements de performances afin d'identifier quand ils ont été détectés, qu'ils soient actifs (nouveaux ou confirmés) ou obsolètes, les charges de travail et les composants du cluster impliqués, ainsi que les options de résolution des événements par vos propres moyens.

Affichage des informations relatives aux événements de performances

Vous pouvez utiliser la page d'inventaire de la gestion des événements pour afficher la liste de tous les événements de performance sur les clusters contrôlés par Unified Manager. Ces informations vous permettent de déterminer les événements les plus critiques, puis d'accéder à des informations détaillées afin de déterminer la cause de l'événement.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

La liste des événements est triée par heure détectée, avec les événements les plus récents 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 les événements par colonne État pour afficher les événements par gravité. Si vous recherchez un événement spécifique ou un type d'événement spécifique, vous pouvez utiliser le filtre et les mécanismes de recherche pour affiner la liste des événements qui apparaissent dans la liste.

Les événements de toutes les sources s'affichent sur cette page :

- Règle de seuil de performance définie par l'utilisateur
- Règle seuil de performance défini par le système
- Seuil de performances dynamiques

La colonne Type d'événement répertorie la source de l'événement. Vous pouvez sélectionner un événement pour afficher les détails de l'événement sur la page Détails de l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.
2. Dans le menu Affichage, sélectionnez **événements de performances actifs**.

   La page affiche tous les événements nouveaux et performances acquittées qui ont été générés au cours des 7 derniers jours.

3. Recherchez un événement à analyser et cliquez sur son nom.

   La page de 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 dans la page de l'explorateur de performances et dans un e-mail d'alerte.

Analyse des événements à partir de seuils de performances 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 règle. Cela indique que l'objet du cluster rencontre un problème de performances.

La page Détails des événements vous permet d'analyser l'événement de performance et de prendre des mesures correctives, le cas échéant, pour rétablir les performances normales.

Réponse aux événements seuil de performance définis par l'utilisateur

Vous pouvez utiliser Unified Manager pour analyser les événements de performance provoqués par un compteur de performances qui franchissement d'un seuil critique ou d'avertissement défini par l'utilisateur. Vous pouvez également utiliser Unified Manager pour vérifier l'état de santé du composant de cluster afin de déterminer si les événements d'état récemment détectés sur le composant ont contribué à l'événement de performances.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- En effet, il doit y avoir de nouveaux événements ou des événements de performances 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 causé l'événement.

   Par exemple, le message « la valeur de latence de 456 ms/op a déclenché un événement D'AVERTISSEMENT basé sur le réglage de seuil de 400 ms/op » indique qu'un événement d'avertissement de latence s'est produit pour l'objet.

3. Passez le curseur de la souris sur le nom de la stratégie pour afficher des détails sur la stratégie de seuil à l'origine de l'événement.

   Cela inclut le nom de la règle, le compteur de performances évalué, la valeur de compteur qui doit être dépassée pour être considérée comme un événement critique ou d'avertissement, et la durée à laquelle le compteur doit dépasser la valeur.

4. Notez le **Event Trigger Time** afin de pouvoir déterminer si d'autres événements pourraient avoir eu lieu en même temps et qui auraient pu contribuer à cet événement.
5. Suivez l'une des options ci-dessous pour approfondir l'analyse de l'événement, afin de déterminer si vous devez effectuer des actions pour résoudre le problème de performances :

Option	Actions d'investigation possibles
Cliquez sur le nom de l'objet source pour afficher la page Explorateur de cet objet.	Cette page vous permet d'afficher les détails de l'objet et de les comparer à d'autres objets de stockage similaires pour déterminer si d'autres objets de stockage présentent un problème de performance similaire en même temps. Par exemple, pour vérifier si les autres volumes du même agrégat présentent également un problème de performances.
Cliquez sur le nom du cluster pour afficher la page Cluster Summary.	Cette page vous permet d'afficher les détails du cluster sur lequel réside cet objet afin de vérifier si d'autres problèmes de performance se sont produits en même temps.

Analyse des événements à partir de seuils de performances définis par le système

Les événements générés à partir des seuils de performance définis par le système indiquent qu'un compteur de performances ou un ensemble de compteurs de performances pour un objet de stockage a dépassé le seuil d'une règle définie par le système. Cela indique que l'objet de stockage, par exemple un agrégat ou un nœud, rencontre un problème de performances.

La page Détails des événements vous permet d'analyser l'événement de performance et de prendre des mesures correctives, le cas échéant, pour rétablir les performances normales.

> Les règles de seuil définies par le système ne sont pas activées sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Réponse aux événements seuil de performance définis par le système

Vous pouvez utiliser Unified Manager pour analyser les événements de performance provoqués par un compteur de performances qui franchissement d'un seuil d'avertissement défini par le système. Vous pouvez également utiliser Unified Manager pour vérifier l'état de santé du composant de cluster afin de déterminer si les événements récents détectés sur le composant ont contribué à l'événement de performance.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- En effet, il doit y avoir de nouveaux événements ou des événements de performances 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 causé l'événement.

   Par exemple, le message « la valeur d'utilisation du nœud de 90 % a déclenché un événement D'AVERTISSEMENT basé sur un seuil de 85 % » indique qu'un événement d'avertissement d'utilisation du nœud s'est produit pour l'objet cluster.

3. Notez le **Event Trigger Time** afin de pouvoir déterminer si d'autres événements pourraient avoir eu lieu en même temps et qui auraient pu contribuer à cet événement.
4. Sous **diagnostic du système**, consultez la brève description du type d'analyse que la règle définie par le système exécute sur l'objet 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 d'autres types de graphiques d'événements définis par le système, les performances de l'objet s'affichent.

5. Sous **actions suggérées**, cliquez sur le lien **Aidez-moi à faire ceci** pour afficher les actions suggérées que vous pouvez effectuer afin d'essayer et de résoudre l'événement de performance par vous-même.

Réponse aux événements de performance du groupe de règles de QoS

Unified Manager génère des événements d'avertissement de stratégie de qualité de service lorsque le débit de la charge de travail (IOPS, IOPS/To ou Mbit/s) a dépassé le paramètre de règle de qualité de service ONTAP défini et que la latence des workloads est en train de devenir affectée. Ces événements définis par le système permettent de corriger les problèmes de performance potentiels avant que de nombreuses charges de travail ne soient affectées par la latence.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Il doit y avoir des événements de performances nouveaux, acquittés ou obsolètes.

Unified Manager génère des événements d'avertissement pour les violations de règles de qualité de service lorsque le débit de la charge de travail a dépassé le paramètre de règle de QoS défini pour chaque période de collecte des performances pendant l'heure précédente. Le débit de la charge de travail peut dépasser le seuil de qualité de service pendant une courte période seulement au cours de chaque période de collecte, mais

Unified Manager affiche uniquement le débit « moyen » pendant la période de collecte sur le graphique. Vous pouvez donc recevoir des événements de qualité de service alors que le débit d'une charge de travail n'a pas dépassé le seuil des règles affiché dans le tableau.

Vous pouvez utiliser System Manager ou les commandes ONTAP pour gérer les « policy Groups », notamment les tâches suivantes :

- Création d'un nouveau groupe de règles pour la charge de travail
- Ajout ou suppression de charges de travail dans un « policy group »
- Déplacement d'une charge de travail entre des groupes de règles
- Modification de la limite de débit d'un groupe de règles
- Déplacement d'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 causé l'événement.

   Par exemple, le message « 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 en savoir plus sur le moment où l'événement s'est produit et la durée pendant laquelle l'événement a été actif.

   En outre, pour les volumes ou les LUN qui partagent le débit d'une règle de QoS, vous pouvez voir les noms des trois principales charges de travail qui consomment le plus d'IOPS ou de Mo/sec.

4. Dans la section **diagnostic du système**, examinez les deux graphiques : un pour le nombre total d'IOPS ou de Mo/s moyens (selon l'événement) et un pour la latence. Cette approche vous permet de déterminer les composants du cluster qui affectent le plus la latence lorsque la charge de travail approche la limite maximale de QoS.

   Pour un événement de politique de QoS partagée, les trois principaux workloads sont présentés dans le tableau de débit. Si plus de trois charges de travail partagent la politique de QoS, des charges de travail supplémentaires sont ajoutées dans la catégorie « autres charges de travail ». En outre, le graphique latence affiche la latence moyenne sur tous les workloads faisant partie de la politique de QoS.

   Notez que pour les événements de la politique adaptative de QoS, les graphiques IOPS et Mbit/s affichent des valeurs d'IOPS ou de Mo/s converties par ONTAP à partir de la règle 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 que vous devez effectuer afin d'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 tenter de résoudre l'événement de performance.

Présentation des événements des règles de QoS adaptative qui ont une taille de bloc définie

Les groupes de règles de QoS adaptative ajustent automatiquement un plafond ou un sol de débit en fonction de la taille du volume. Ainsi, ils maintiennent le rapport IOPS/To en fonction de la taille du volume. Depuis la version ONTAP 9.5, vous pouvez spécifier la

taille de bloc dans la règle de QoS afin d'appliquer efficacement un seuil Mo/s en même temps.

L'assignation d'un seuil IOPS dans une règle de QoS adaptative impose une limite uniquement au nombre d'opérations qui se produisent dans chaque workload. En fonction de la taille de bloc définie sur le client qui génère les workloads, certains IOPS incluent beaucoup plus de données et, par conséquent, alourdit considérablement la charge de travail sur les nœuds qui traitent les opérations.

La valeur MB/s d'une charge de travail est générée à l'aide de la formule suivante :

```
MB/s = (IOPS * Block Size) / 1000
```

Si une charge de travail moyenne est de 3,000 000 IOPS et que la taille de bloc sur le client est définie sur 32 Ko, la valeur réelle en Mo/s pour cette charge de travail est de 96. Si cette même charge de travail moyenne est de 3,000 000 IOPS et que la taille de bloc du client est définie sur 48 Ko, la capacité effective en Mo/s de cette charge de travail est de 144. Vous pouvez constater que le nœud traite 50 % de données en plus lorsque la taille de bloc est supérieure.

Examinons la règle de QoS adaptative suivante avec une taille de bloc définie et le mode de déclenchement des événements en fonction de la taille de bloc définie sur le client.

Créez une règle et définissez le débit maximal sur 2,500 IOPS/To avec une taille de bloc de 32 Ko. Cette configuration définit ainsi le seuil en Mo/s à 80 Mo/s ((2500 IOPS * 32 Ko) / 1000) pour un volume dont la capacité utilisée est de 1 To. Notez que Unified Manager génère un événement 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 …**	
	LES IOPS	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 et que les IOPS sont de 4,000 et que la taille de bloc de QoS est définie sur 32 Ko pour le client, le débit en Mo/s est de 128 Mo/s ((4,000 IOPS * 32 Ko) / 1000). Aucun événement n'est généré dans ce scénario car 4,000 IOPS et 128 Mo/s sont tous les deux inférieurs au seuil d'un volume utilisant 2 To d'espace.

Si le volume utilise 2 To d'espace disponible et que le nombre d'IOPS est de 4,000 et que la taille de bloc de QoS est définie sur 64 Ko sur le client, le débit de Mo/s est de 256 Mo/s ((4,000 IOPS * 64 Ko) / 1000). Dans ce cas, les 4,000 IOPS ne génèrent pas d'événement, mais la valeur MB/s de 256 MB/s est au-dessus du seuil de 144 MB/s et un évènement est généré.

Par conséquent, lorsqu'un événement est déclenché en fonction d'une violation MB/s pour une stratégie QoS adaptative qui inclut la taille du bloc, un graphique MB/s s'affiche dans la section diagnostic système de la page Détails de l'événement. Si l'événement est déclenché en fonction d'une violation des IOPS de la règle de QoS adaptative, un graphique Op E/S par sec s'affiche dans la section diagnostic système. Si une violation se produit à la fois pour les IOPS et les Mo/s, vous recevrez deux événements.

Pour plus d'informations sur le réglage des paramètres QoS, reportez-vous àla section "Présentation de la gestion des performances".

Réponse aux événements de performance surexploités relatifs aux ressources des nœuds

Unified Manager génère des événements d'avertissement surexploités lorsqu'un nœud se trouve au-dessus des limites de son efficacité opérationnelle, et risque par conséquent d'affecter la latence des charges de travail. Ces événements définis par le système permettent de corriger les problèmes de performance potentiels avant que de nombreuses charges de travail ne soient affectées par la latence.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- En effet, il doit y avoir de nouveaux événements ou des événements de performances obsolètes.

Unified Manager génère des événements d'avertissement pour les violations de règles mises en excès de 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 System Manager ou les commandes ONTAP pour corriger ce type de problème de performance, notamment les tâches suivantes :

- Création et application d'une politique de QoS à tous les volumes ou LUN sur-utilisant les ressources système
- Réduction de la limite de débit maximal de QoS d'un groupe de règles auquel des workloads ont été appliqués
- Déplacement d'une charge de travail vers un autre agrégat ou nœud
- Augmentation de la capacité par l'ajout de disques au nœud ou par mise à niveau vers un nœud avec un processeur plus rapide et 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 causé l'événement.

   Par exemple, le message « Perf. La valeur utilisée de la capacité de 139 % sur la simplicité-02 a déclenché un événement D'AVERTISSEMENT pour identifier les problèmes de performances potentiels dans l'unité de traitement des données.» indique que la capacité de performances sur la simplicité du nœud 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 principales charges de travail et un pour la latence sur les principales charges de travail. Lorsqu'elle est organisée, vous pouvez voir les workloads à l'origine de la latence sur le nœud.

   Vous pouvez afficher les charges de travail appliquées aux règles de QoS et celles qui ne le sont pas en déplaçant le curseur sur le graphique des IOPS.

4. Dans la section **actions suggérées**, examinez les suggestions et déterminez les actions que vous devez effectuer afin d'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 tenter de résoudre l'événement de performance.

Répondre aux événements de performances du déséquilibre des clusters

Unified Manager génère un avertissement de déséquilibre de cluster lorsqu'un nœud d'un cluster fonctionne à une charge bien plus élevée que les autres nœuds et peut donc affecter la latence des charges de travail. Ces événements définis par le système permettent de corriger les problèmes de performance potentiels avant que de nombreuses charges de travail ne soient affectées par la latence.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Unified Manager génère des événements d'avertissement concernant le non-respect des règles de seuil de déséquilibre du cluster en comparant la valeur de capacité utilisée pour tous les nœuds du cluster et vérifier s'il existe une différence de charge de 30 % entre tous les nœuds.

Cette procédure vous permet d'identifier les ressources suivantes afin de déplacer des charges de travail hautes performances vers un nœud inférieur :

- Les nœuds du même cluster sont moins utilisés
- Les agrégats du nouveau nœud les moins utilisés
- Les volumes les plus performants du nœud actuel

Étapes

1. Affichez la page **Event** details pour afficher des informations sur l'événement.
2. Consultez la **Description**, qui décrit la violation de seuil qui a causé l'événement.

   Par exemple, le message « le compteur de capacité de performances utilisé 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 de l'un des nœuds est sur-utilisée et affecte les performances du nœud.

3. Consultez le texte de la **actions suggérées** pour déplacer un volume hautes performances du nœud avec la valeur de capacité haute performance utilisée vers un nœud dont la capacité de performance est la plus faible.
4. Identifiez les nœuds dont la capacité de performance utilisée est 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 **Cluster / Performance Summary**, cliquez sur **Nodes** dans la zone **Managed Objects**.
   c. Dans la page d'inventaire **Nodes**, triez les nœuds en fonction de la colonne **capacité de performance utilisée**.
   d. Identifiez les nœuds dont la capacité utilisée est la plus élevée et la plus faible en termes de performance, et notez ces noms.
5. Identifiez le volume en utilisant les IOPS les plus élevées sur le nœud présentant la capacité de performance la plus élevée utilisée :
   a. Cliquez sur le nœud présentant la valeur la plus élevée en termes de capacité de performance utilisée.

b. Dans la page **Node / Performance Explorer**, sélectionnez **Aggregates sur ce noeud** dans le menu **View and compare**.

c. Cliquez sur l'agrégat dont la capacité utilisée est la plus élevée.

d. Dans la page **Aggregate / Performance Explorer**, sélectionnez **volumes sur cet agrégat** dans le menu **View and compare**.

e. Triez les volumes selon la colonne **IOPS** et notez le nom du volume en utilisant les IOPS les plus élevées, ainsi que le nom de l'agrégat où réside le volume.

6. Identifier l'agrégat avec le taux d'utilisation le plus faible sur le nœud présentant la capacité de performances la plus faible au taux d'utilisation :

   a. Cliquez sur **Storage** > **Aggregates** pour afficher la page d'inventaire **Aggregates**.

   b. Sélectionnez la vue **Performance : tous les agrégats**.

   c. Cliquez sur le bouton **Filter** et ajoutez un filtre où ""Node"" est égal au nom du nœud dont la capacité de performance utilisée est la plus faible que vous avez indiquée à l'étape 4.

   d. Écrire le nom de l'agrégat qui présente la valeur de capacité de performances la plus faible utilisée.

7. Déplacez le volume du nœud surchargé vers l'agrégat identifié comme présentant un faible taux d'utilisation sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement en utilisant ONTAP System Manager, OnCommand Workflow Automation et les commandes ONTAP ou une combinaison de ces outils.

Au bout de quelques jours, vérifiez si vous recevez le même problème de déséquilibre de groupe d'instruments.

Analyse des événements à partir de seuils de performances dynamiques

Les événements générés à partir de seuils dynamiques indiquent que le temps de réponse réel d'une charge de travail est trop élevé ou trop faible par rapport à la plage de temps de réponse prévue. La page Détails des événements vous permet d'analyser l'événement de performance et de prendre des mesures correctives, le cas échéant, pour rétablir les performances normales.

> Les seuils de performance dynamiques ne sont pas activés sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Identification des charges de travail victimes impliquées dans la mise en œuvre d'un processus dynamique de performances

Unified Manager vous permet d'identifier les charges de travail de volume qui présentent l'écart le plus important en termes de temps de réponse (latence) causé par un composant de stockage en conflit. L'identification de ces charges de travail vous permet de comprendre pourquoi les applications client qui y accèdent ont été plus lentes que d'habitude.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

- Il doit y avoir des événements de performances dynamiques nouveaux, acquittés ou obsolètes.

La page Détails de l'événement affiche une liste des charges de travail définies par l'utilisateur et par le système, classées par la déviation la plus élevée de l'activité ou de l'utilisation sur le composant ou le plus touché par l'événement. Les valeurs sont basées sur les pics identifiés par Unified Manager lors de sa 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 victimes**.
3. Passez le curseur de la souris 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.

Identification des workloads dominants impliqués dans un événement de performance dynamique

Dans Unified Manager, vous pouvez identifier les workloads qui présentent la déviation la plus élevée de l'utilisation d'un composant de cluster en conflit. L'identification de ces workloads vous permet de comprendre pourquoi certains volumes du cluster ont des temps de réponse lents (latence).

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Il doit y avoir des événements de performances dynamiques nouveaux, acquittés ou obsolètes.

La page des détails de l'événement affiche la liste des workloads définis par l'utilisateur et par le système classés selon l'utilisation la plus élevée du composant ou la plus affectée par l'événement. Les valeurs sont basées sur les pics identifiés par Unified Manager lors de sa 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 importantes**.
3. Placez le curseur de la souris sur les graphiques pour afficher les principaux workloads dominants définis par l'utilisateur qui affectent le composant.

Identification des charges de travail Shark impliquées dans un événement de performance dynamique

Dans Unified Manager, vous pouvez identifier les charges de travail présentant la déviation la plus élevée d'utilisation pour un composant de stockage en conflit. L'identification de ces charges de travail vous permet de déterminer si ces charges de travail doivent être déplacées vers un cluster moins utilisé.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Il existe de nouveaux événements dynamiques de performances, confirmés ou obsolètes.

La page des détails de l'événement affiche la liste des workloads définis par l'utilisateur et par le système classés selon l'utilisation la plus élevée du composant ou la plus affectée par l'événement. Les valeurs sont basées sur les pics identifiés par Unified Manager lors de sa 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 le curseur de la souris 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 Shark.

Analyse des événements de performances 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 proposées pour les résoudre.

Des événements de performance MetroCluster peuvent être dus à des charges de travail *dominantes* qui surutilisent les liaisons intercommutateurs (ISL) entre les clusters ou à des problèmes d'intégrité de la liaison. Unified Manager surveille chaque cluster dans une configuration MetroCluster de manière indépendante, sans tenir compte des événements de performance qui se produisent sur un cluster partenaire.

Les événements de performance des deux clusters de la configuration MetroCluster sont également affichés sur la page du tableau de bord de Unified Manager. Vous pouvez également afficher les pages Santé de Unified Manager pour vérifier l'état de santé de chaque cluster et pour afficher leur relation.

Analyse d'un événement de performances dynamiques sur un cluster dans une configuration MetroCluster

Vous pouvez utiliser Unified Manager pour analyser le cluster dans une configuration MetroCluster sur laquelle un événement de performances a été détecté. Vous pouvez identifier le nom du cluster, le temps de détection des événements et les charges de travail *tyran* et *victime* impliquées.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Dans une configuration MetroCluster, il doit y avoir de nouveaux événements de performances, confirmés ou obsolètes.
- Les deux clusters de la configuration MetroCluster doivent être surveillés par la même instance de Unified Manager.

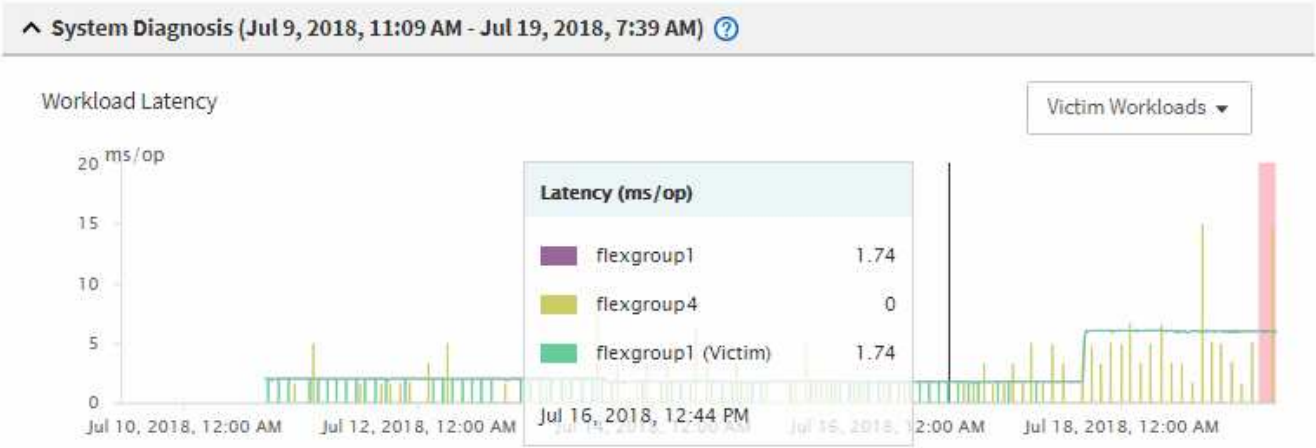
Étapes

1. Affichez la page **Détails de l'événement** pour afficher des informations sur l'événement.
2. Consultez la description de l'événement pour connaître 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 placez le curseur sur l'icône pour afficher une description de l'icône.

3. Notez le nom du cluster et l'heure de détection des événements. Ces informations peuvent être utilisées pour analyser les événements de performances sur le cluster partenaire.
4. Dans les graphiques, examinez les charges de travail *victime* pour vérifier que leurs temps de réponse sont supérieurs au seuil de performance.

   Dans cet exemple, la charge de travail victime est affichée dans le texte du curseur de la souris. Les graphiques latence affichent, à un modèle de latence cohérent et général, pour les charges de travail victimes impliquées. Bien que la latence anormale des charges de travail victimes ait déclenché l'événement, un modèle de latence cohérent peut indiquer que les workloads 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 y envoie une quantité importante d'E/S, vous envisagez peut-être d'augmenter la latence. Si la latence des charges de travail renvoie dans la plage attendue, l'état d'événement devient obsolète et reste dans cet état pendant plus de 30 minutes, vous pouvez sans doute ignorer la situation. Si l'événement est en cours et reste dans le nouvel état, vous pouvez l'étudier davantage pour déterminer si d'autres problèmes ont causé l'événement.

5. Dans le graphique débit des charges de travail, sélectionnez **charges de travail bulles** pour afficher les charges de travail dominantes.

   La présence de charges de travail dominantes indique que l'événement peut avoir été causé par un ou plusieurs workloads sur le cluster local qui utilisent les ressources MetroCluster. Les workloads dominants ont un débit d'écriture élevé en exemple (Mbit/s).

   Ce graphique présente le modèle de débit d'écriture (Mbit/s) élevé des charges de travail. Vous pouvez examiner le modèle de Mo/s d'écriture pour identifier un débit anormal, ce qui peut indiquer qu'une charge de travail surutilise les ressources MetroCluster.

   Si aucune charge de travail dominante n'est impliquée dans l'événement, l'événement peut avoir été provoqué par un problème de santé lié à la liaison entre les clusters ou à un problème de performance sur le cluster partenaire. Vous pouvez utiliser Unified Manager pour vérifier l'état de santé des deux clusters

dans une configuration MetroCluster. Vous pouvez également utiliser Unified Manager pour vérifier et analyser les événements de performance sur le cluster partenaire.

Analyse d'un événement de performances dynamiques 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 permet de déterminer si un événement sur le cluster distant a provoqué un événement sur son cluster partenaire.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Vous devez avoir analysé un événement de performance sur un cluster local dans une configuration MetroCluster et obtenu le temps de détection de l'événement.
- Vous devez avoir vérifié l'état de santé du cluster local et de son groupe de partenaires impliqué dans l'événement de performance et avoir obtenu le nom du groupe de partenaires.

Étapes

1. Connectez-vous à l'instance Unified Manager qui contrôle le cluster partenaire.
2. Dans le volet de navigation de gauche, cliquez sur **Evénements** pour afficher la liste des événements.
3. Dans le sélecteur **Time Range**, sélectionnez **Last Hour**, puis cliquez sur **Apply Range**.
4. Dans le sélecteur **Filtering**, sélectionnez **Cluster** dans le menu déroulant de gauche, saisissez le nom du groupe de partenaires dans le champ de texte, puis cliquez sur **appliquer le filtre**.

   Si aucun événement n'est enregistré pour le cluster sélectionné au cours de la dernière heure, cela signifie que le cluster n'a rencontré aucun problème de performance au cours du moment où l'événement a été détecté sur son partenaire.

5. Si des événements sont détectés sur le cluster sélectionné au cours de la dernière heure, comparez le temps de détection de l'événement à celui de l'événement sur le cluster local.

   Si ces événements impliquent des charges de travail dominantes entraînant des conflits au niveau du composant de traitement des données, un ou plusieurs de ces composants peuvent avoir généré l'événement sur le cluster local. Vous pouvez cliquer sur l'événement pour l'analyser et passer en revue les actions suggérées pour le résoudre sur la page Détails de l'événement.

   Si ces événements n'impliquent pas de charges de travail dominantes, ils n'ont pas provoqué l'événement de performance sur le cluster local.

Réponse à un événement de performance dynamique causé par l'accélération du groupe de règles de QoS

Vous pouvez utiliser Unified Manager pour rechercher un événement de performance provoqué par un groupe de règles de qualité de service (QoS) qui restreint le débit du workload (Mbit/s). Cette accélération a permis d'augmenter les temps de réponse (latence) des workloads de volumes dans le groupe de règles. Vous pouvez utiliser les informations d'événement pour déterminer si de nouvelles limites des groupes de règles sont nécessaires pour arrêter la restriction.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Il doit y avoir des événements de performances nouveaux, acquittés 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 affectées par la restriction.

   > La description peut afficher la même charge de travail pour la victime et le tyran, car la restriction en fait la charge de travail victime de lui-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 retrouver ultérieurement.

4. Dans les graphiques latence de la charge de travail et utilisation de la charge de travail, sélectionnez **charges de travail importantes**.
5. Passez le curseur de la souris sur les graphiques pour afficher les principales charges de travail définies par l'utilisateur qui affectent le groupe de règles.

   La charge de travail en haut de la liste a la plus grande déviation et a provoqué la restriction. L'activité correspond au pourcentage de la limite de groupe de règles utilisée 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 supérieure.
7. Sur 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 l'analyse.

   Les graphiques détaillés sont affichés sous le tableau latence et le graphique Op E/S par sec.

8. Comparez les limites de qualité de service dans le graphique **latence** pour voir quelle quantité d'accélération a affecté la latence au moment de l'événement.

   Le groupe de règles de QoS possède un débit maximal de 1,000 opérations par seconde (op/s), que les workloads IT ne peuvent pas dépasser collectivement. Au moment de l'événement, le débit combiné des charges de travail du groupe de règles était de plus de 1,200 opérations/s, ce qui a poussé le groupe de règles à ralentir son activité à 1,000 opérations/s.

9. Comparez les valeurs **reads/écrit latence** aux valeurs **reads/writes/Other**.

   Les deux graphiques présentent un nombre élevé de demandes de lecture avec une latence élevée, mais le nombre de requêtes et la latence pour les demandes d'écriture sont faibles. Ces valeurs vous permettent de déterminer la présence d'un haut débit ou d'un grand nombre d'opérations ayant augmenté la latence. Vous pouvez utiliser ces valeurs pour décider de mettre une limite de groupe de règles sur le débit ou les opérations.

10. Utilisez ONTAP System Manager pour augmenter la limite actuelle du groupe de règles à 1,300 op/s.
11. Après une journée, revenez à Unified Manager et entrez la charge de travail que vous avez enregistrée à l'étape 3 dans la page **analyse de la charge de travail**.
12. Sélectionnez le tableau décomposition du débit.

Le graphique lit/écrit/autre s'affiche.

13. En haut de la page, pointez votre curseur sur l'icône de changement d'événement ( ) pour la modification de la limite du groupe de règles.
14. Comparez le graphique **reads/writes/Other** avec le graphique **latence**.

    Les requêtes de lecture et d'écriture sont identiques, mais l'accélération a cessé et la latence a diminué.

Réponse à un événement de performance dynamique provoqué par une panne de disque

Vous pouvez utiliser Unified Manager pour analyser un événement de performances provoqué par l'utilisation excessive d'un agrégat par des charges de travail. Vous pouvez également utiliser Unified Manager pour vérifier l'état de santé de l'agrégat et vérifier si les événements récemment détectés sur l'agrégat ont contribué à ce qui se passe.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Il doit y avoir des événements de performances nouveaux, acquittés 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.

   Plusieurs volumes victime sont affectés par des conflits entre le composant du cluster. L'agrégat, qui se trouve au milieu d'une reconstruction RAID pour remplacer le disque défectueux par un disque de spare, est le composant du cluster en conflit. Sous composant en conflit, l'icône d'agrégat est mise en surbrillance rouge et le nom de l'agrégat est affiché entre parenthèses.

3. Dans le graphique utilisation des charges de travail, sélectionnez **charges de travail vitales**.
4. Placez le curseur de la souris sur le graphique pour afficher les principales charges de travail dominantes qui affectent le composant.

   Les charges de travail les plus exigeantes avec une utilisation maximale depuis la détection de l'événement sont affichées en haut du graphique. L'un des workloads les plus importants est le système de stockage sur disque défini par le système, qui indique une reconstruction RAID. La reconstruction est le processus interne impliqué dans la reconstruction de l'agrégat sur le disque de spare. La charge de travail Disk Health, associée à d'autres charges de travail de l'agrégat, a probablement provoqué un conflit 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 que Unified Manager analyse l'événement et détecte si l'agrégat est toujours en conflit.
6. Actualiser les **Détails de l'événement**.

   Une fois la reconstruction RAID terminée, vérifiez que l'état est obsolète, ce qui indique que l'événement est résolu.

7. Dans le graphique utilisation des charges de travail, sélectionnez **charges de travail vitales** pour afficher les charges de travail de l'agrégat en fonction du pic d'utilisation.

8. Dans la zone **actions suggérées**, cliquez sur le bouton **analyser la charge de travail** pour la charge de travail supérieure.
9. Dans la page **Workload Analysis**, définissez la plage horaire pour afficher les 24 dernières heures (1 jour) de données pour le volume sélectionné.

   Dans la chronologie des événements, un point rouge (●) indique quand l'événement de panne de disque s'est produit.

10. Dans le graphique utilisation des nœuds et de l'agrégat, masquez la ligne des statistiques de nœud afin que la ligne d'agrégat soit toujours la seule.
11. Comparez les données de ce tableau aux données au moment de l'événement dans le graphique **latence**.

    Au moment de l'événement, l'utilisation de l'agrégat affiche une quantité élevée d'activités de lecture et d'écriture, causée par les processus de reconstruction RAID, qui a augmenté la latence du volume sélectionné. Quelques heures après l'événement s'est produit, les lectures, les écritures et la latence ont diminué, confirmant que l'agrégat n'est plus en conflit.

Réponse à un événement de performances dynamiques provoqué par un basculement haute disponibilité

Vous pouvez utiliser Unified Manager pour analyser un événement lié aux performances, causé par le traitement de données élevé sur un nœud de cluster dans une paire haute disponibilité. Vous pouvez également utiliser Unified Manager pour vérifier l'état de santé des nœuds afin de déterminer si des événements d'état récemment détectés sur les nœuds ont contribué à la réalisation de ces événements.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Il doit y avoir des événements de performances nouveaux, acquittés 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.

   Un volume victime a été affecté par le composant du cluster dans le cadre de conflits. Le nœud de traitement des données, qui a repris tous les workloads depuis son nœud partenaire, est le composant de cluster en conflit. Sous composant en conflit, l'icône traitement des données est surlignée en rouge et le nom du nœud qui traitait le traitement des données au moment de l'événement est affiché entre parenthèses.

3. Dans **Description**, cliquez sur le nom du volume.

   La page Explorateur de volumes de performances s'affiche. En haut de la page, dans la ligne heure des événements, l'icône d'événement de changement (●) indique l'heure à laquelle Unified Manager a détecté le début du basculement haute disponibilité.

4. Pointez votre curseur sur l'icône d'événement de modification pour le basculement haute disponibilité et des informations détaillées sur le basculement haute disponibilité s'affichent dans le texte du curseur de la souris.

Dans le graphique latence, un événement indique que le volume sélectionné a dépassé le seuil de performances défini en raison d'une latence élevée tout au long du même temps que le basculement haute disponibilité.

5. Cliquez sur **Zoom View** pour afficher le graphique latence sur une nouvelle page.
6. Dans le menu Affichage, sélectionnez **composants de cluster** pour afficher la latence totale par composant de cluster.
7. Placez le curseur de la souris sur l'icône d'événement de modification correspondant au début de la prise de contrôle haute disponibilité et comparez la latence pour le traitement des données à la latence totale.

   Au moment du basculement haute disponibilité, le traitement des données a connu un pic d'activité suite à l'augmentation de la demande de charge de travail sur le nœud de traitement des données. La meilleure utilisation du CPU a déclenché la latence et a déclenché l'événement.

8. Une fois le nœud défaillant résolu, utilisez ONTAP System Manager pour effectuer un retour HA, qui déplace les workloads du nœud partenaire vers le nœud fixe.
9. Une fois le retour haute disponibilité terminé, après la prochaine découverte de configuration dans Unified Manager (environ 15 minutes), recherchez l'événement et la charge de travail déclenchés par le basculement haute disponibilité dans la page d'inventaire **Event Management**.

   L'événement déclenché par le basculement HA dispose désormais d'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 réduit la latence totale. Le nœud utilisé par le volume sélectionné pour le traitement des données a résolu l'événement.

Résoudre les événements de performances

Vous pouvez utiliser les actions suggérées pour essayer et résoudre par vous-même les événements de performances. Les trois premières suggestions sont toujours affichées et les actions de la quatrième suggestion sont spécifiques au type d'événement affiché.

Les liens **Help Me Do this** 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, de ONTAP System Manager, d'OnCommand Workflow Automation, des commandes de l'interface de ligne de commande d'ONTAP ou une combinaison de ces outils.

Confirmation que la latence se trouve dans la plage prévue

Lorsqu'un composant de cluster conflit, des workloads de volume qui l'utilisent peuvent avoir réduit le temps de réponse (latence). Vous pouvez examiner la latence de chaque charge de travail victime dans le composant en conflit pour confirmer que sa latence réelle se situe dans la plage prévue. Vous pouvez également cliquer sur le nom d'un volume pour afficher les données historiques du volume.

Si l'événement de performances est dans un état obsolète, la latence de chaque victime impliquée dans l'événement peut avoir été retournée dans la plage prévue.

Examinez l’impact des modifications de configuration sur les performances des charges de travail

Les modifications de configuration sur le cluster, telles qu’une défaillance de disque, un basculement haute disponibilité ou un volume déplacé, peuvent avoir un impact négatif sur la performance 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 récente de la configuration s’est produite et la comparer aux opérations et à la latence (temps de réponse) afin de voir s’il y a eu un changement d’activité pour la charge de travail du volume sélectionnée.

Les pages de performances de Unified Manager ne peuvent détecter qu’un nombre limité d’événements de modification. Les pages d’intégrité fournissent des alertes pour d’autres événements provoqués par des modifications de configuration. Vous pouvez rechercher le volume dans Unified Manager pour afficher l’historique des événements.

Possibilité d’améliorer les performances des charges de travail côté client

Vous pouvez vérifier les charges de travail de vos clients, par exemple les applications ou les bases de données, qui envoient des E/S aux volumes concernés par un événement de performances afin de 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 plus fort pour répondre à la demande. Si vous savez quels clients disposent d’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 réduisant la quantité d’E/S vers ce volume. Vous pouvez aussi appliquer ou augmenter une limite au groupe de règles de QoS dont le volume est membre.

Vous pouvez analyser les clients et leurs applications pour déterminer si les clients envoient plus d’E/S qu’à d’autres fins, ce qui peut provoquer des conflits sur un composant du cluster. Sur la page Détails de l’événement, la section diagnostic du système affiche les charges de travail du volume supérieur utilisant le composant en conflit. Si vous savez quel client accède à un volume particulier, vous pouvez vous rendre sur le client pour déterminer si le matériel client ou une application ne fonctionne pas comme prévu ou fait plus de travail que d’habitude.

Dans une configuration MetroCluster, les demandes d’écriture vers un volume situé sur un cluster local sont mises en miroir sur un volume du cluster distant. En effet, le volume source du cluster local étant synchronisé avec le volume de destination du 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 effectuent moins d’opérations de synchronisation, ce qui réduit l’impact sur les performances des autres workloads.

Vérifiez si le client ou le réseau ne présentent pas de problème

Lorsque les clients connectés aux volumes d’un cluster augmentent leurs demandes d’E/S, le cluster doit travailler plus fort pour répondre à la demande. La demande accrue sur le cluster peut créer des conflits entre les composants, 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 du système affiche les charges de travail du volume supérieur utilisant le composant en conflit. Si vous savez quel client accède à un volume particulier, vous

pouvez vous rendre sur le client pour déterminer si le matériel client ou une application ne fonctionne pas comme prévu ou fait 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 goulets d'étranglement ou des charges de travail concurrentes qui peuvent avoir entraîné des demandes d'E/S entre le cluster et des clients connectés à fonctionner plus lentement que prévu. Vous devrez peut-être contacter votre administrateur réseau pour obtenir de l'aide.

Vérifier si les autres volumes du groupe de règles de QoS ont une activité particulièrement élevée

Examinez les charges de travail du groupe de règles de qualité de service (QoS) avec le changement d'activité le plus important pour déterminer si plusieurs charges de travail ont été à l'origine de l'événement. Vous savez également si d'autres charges de travail dépassent la limite de débit définie ou si elles restent dans la plage d'activité attendue.

Sur la page Détails de l'événement, dans la section diagnostic du système, vous pouvez trier les charges de travail par déviation maximale de l'activité pour afficher les charges de travail avec le changement d'activité le plus important en haut du tableau. Ces charges de travail peuvent être les « mensonges » dont l'activité a dépassé la limite définie et qui ont pu provoquer l'événement.

Vous pouvez accéder à la page d'analyse des charges de travail pour chaque charge de travail de volume pour examiner son activité IOPS. Si la charge de travail a des périodes d'activité très élevées, elle a peut-être contribué à l'événement. Vous pouvez modifier les paramètres du groupe de règles pour la charge de travail ou déplacer la charge de travail vers un autre groupe de règles.

Pour gérer les groupes de règles, vous pouvez utiliser ONTAP System Manager ou les commandes de l'interface de ligne de commandes ONTAP :

- Création d'une « policy group ».
- Ajout ou suppression de charges de travail dans un « policy group »
- Déplacez une charge de travail entre les groupes de règles.
- Modifier la limite de débit d'un groupe de règles.

Déplacement des interfaces logiques

Le transfert des interfaces logiques (LIF) vers un port moins occupé peut aider à améliorer l'équilibrage de la charge, à faciliter les opérations de maintenance et l'ajustement des performances, et à réduire l'accès indirect.

L'accès indirect peut diminuer l'efficacité du système. Elle survient lorsqu'un workload 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 le déplacement des LIF afin d'utiliser le même nœud pour le traitement réseau et le traitement des données. Vous pouvez configurer l'équilibrage de charge pour que ONTAP déplace automatiquement les LIF occupées vers un autre port ou vous pouvez déplacer une LIF manuellement.

* Avantages*	Considérations
• Améliorer l'équilibrage des charges. • Réduire les accès indirects.	Lors du déplacement d'une LIF connectée à des partages CIFS, les clients qui accèdent aux partages CIFS sont déconnectés. Toute demande de lecture ou d'écriture vers les partages CIFS est perturbée.

Vous utilisez les commandes ONTAP pour configurer l'équilibrage de charge. Pour plus d'informations, consultez la documentation relative à la mise en réseau de ONTAP.

Vous utilisez ONTAP System Manager et les commandes de l'interface de ligne de commande ONTAP pour déplacer les LIF manuellement.

Exécutez les opérations d'efficacité du stockage à un moment moins occupé

Vous pouvez modifier la règle ou la planification qui gère les opérations d'efficacité du stockage pour s'exécuter lorsque les charges de travail des volumes concernés sont moins occupées.

Les opérations d'efficacité du stockage peuvent utiliser un nombre élevé de ressources CPU du cluster et devenir un tyran pour les volumes sur lesquels les opérations sont exécutées. Si les volumes victimes ont une activité élevée en même temps que lorsque 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 règles QoS par déviation de pic d'activité pour identifier les charges de travail dominantes. Si la mention « efficacité de stockage » s'affiche en haut du tableau, ces opérations intimident les charges de travail victimes. En modifiant la règle d'efficacité ou la planification de l'exécution lorsque ces charges de travail sont moins occupées, vous pouvez empêcher les opérations d'efficacité du stockage d'provoquer des conflits sur un cluster.

ONTAP System Manager peut être utilisé pour gérer les règles d'efficacité. Vous pouvez utiliser les commandes ONTAP pour gérer les règles d'efficacité et les planifications.

Définition de l'efficacité du stockage

L'efficacité du stockage vous permet de stocker le maximum de données pour un coût minimum et de gérer la croissance rapide des données tout en consommant moins d'espace. La stratégie NetApp d'efficacité du stockage repose sur la base intégrée de la virtualisation du stockage et du stockage unifié fournies par son système d'exploitation ONTAP principal et son système de fichiers WAFL (Write Anywhere File Layout).

L'efficacité du stockage inclut l'utilisation de technologies telles que le provisionnement fin, la copie Snapshot, la déduplication, la compression des données, FlexClone, Réplication fine avec SnapVault et SnapMirror volume, RAID-DP, Flash cache, l'agrégat Flash Pool et les agrégats compatibles FabricPool, qui permettent d'augmenter l'utilisation du stockage et de réduire les coûts de stockage.

L'architecture de stockage unifié vous permet de consolider efficacement un réseau de stockage (SAN), un stockage NAS et un stockage secondaire sur une seule plateforme.

Les disques haute densité, comme les disques SATA (Serial Advanced Technology Attachment) configurés dans des agrégats Flash Pool ou avec la technologie Flash cache et RAID-DP, améliorent l'efficacité sans nuire aux performances et à la résilience.

Un agrégat compatible FabricPool comprend un agrégat SSD ou HDD (à partir de ONTAP 9.8) comme Tier de performance local et un magasin d'objets que vous spécifiez comme Tier cloud. La configuration d'FabricPool vous aide à gérer les données du Tier de stockage (le Tier local ou le Tier cloud) à stocker selon que la fréquence d'accès aux données est élevée.

Les technologies telles que le provisionnement fin, la copie Snapshot, la déduplication, la compression des données, la réplication fine avec SnapVault et SnapMirror volume, et FlexClone, permettent de réaliser des économies plus importantes. Ces technologies peuvent être utilisées séparément ou ensemble pour optimiser l'efficacité du stockage.

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 l'ajout de disques, vous constaterez une amélioration des performances de lecture uniquement après avoir rélocalisé les données sur les disques que vous avez ajoutés.

Ces instructions peuvent être utilisées lorsqu'Unified Manager a reçu des événements d'agrégat déclenchés par des seuils de performance dynamiques ou définis par le système :

- Lorsque vous avez reçu un événement de seuil dynamique, l'icône du composant de cluster représentant l'agrégat dans un conflit s'affiche en rouge sur la page des détails d'événements.

  Sous l'icône, entre parenthèses, est 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 présente 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, vous devrez peut-être contacter votre administrateur ou acheter plus de disques. 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 des agrégats HDD et Flash Pool uniquement. Ne pas réaffecter de données sur des agrégats SSD ou FabricPool.

Comment l'activation de Flash cache sur un nœud peut améliorer les performances des charges de travail

Vous pouvez améliorer les performances des charges de travail en activant la mise en cache intelligente des données Flash cache™ sur chaque nœud du cluster.

Un module Flash cache, ou module d'accélération des performances module de mémoire PCIe, optimise les performances des charges de travail exigeant une capacité de lecture aléatoire maximale en fonctionnant comme un cache de lecture externe intelligent. Ce matériel fonctionne en tandem avec le composant logiciel

WAFL External cache de ONTAP.

Dans Unified Manager, l'icône de composant de cluster qui représente l'agrégat dans les conflits est mise en surbrillance rouge sur la page des détails d'événements. Sous l'icône, entre parenthèses, est 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 vérifier si Flash cache est installé ou activé et 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 sur la configuration requise pour l'utiliser, consultez le rapport technique suivant :

"Rapport technique 3832 : guide des meilleures pratiques de Flash cache"

Comment l'activation de Flash Pool sur un agrégat de stockage peut améliorer les performances des charges de travail

Vous pouvez améliorer la performance des charges de travail en activant la fonction Flash Pool sur un agrégat. Un Flash Pool est un agrégat qui regroupe des disques durs et des disques SSD. Les disques durs sont utilisés pour le stockage primaire et les disques SSD fournissent un cache d'écriture et de lecture haute performance qui optimise les performances de l'agrégat.

Dans Unified Manager, la page Détails des événements affiche le nom de l'agrégat en conflit. Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour vérifier si Flash Pool est activé pour un agrégat. Si vous avez installé des disques SSD, vous pouvez utiliser l'interface de ligne de commandes pour l'activer. Si des disques SSD sont installés, vous pouvez exécuter la commande suivante sur l'agrégat pour vérifier 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, par exemple l'agrégat en conflit.

Pour plus d'informations sur Flash Pool et sur les conditions requises pour son utilisation, consultez le *Guide de gestion du stockage physique clustered Data ONTAP*.

Vérification de l'état de la configuration MetroCluster

Vous pouvez utiliser Unified Manager pour vérifier l'état des clusters d'une configuration MetroCluster sur IP ou FC. L'état et les événements vous aident à déterminer s'il existe des problèmes matériels ou logiciels qui peuvent affecter les performances de vos charges de travail.

Si vous configurez Unified Manager pour envoyer des alertes par e-mail, vous pouvez vérifier dans votre courrier électronique s'il existe des problèmes d'intégrité sur le cluster local ou distant qui pourraient avoir contribué à un événement de performances. Dans l'interface graphique Unified Manager, vous pouvez sélectionner **gestion des événements** pour afficher une liste des événements en cours, puis utiliser les filtres pour afficher uniquement les événements de configuration MetroCluster.

Pour plus d'informations, voir "Vérification de l'état de santé des clusters dans une configuration MetroCluster"

Vérification de la configuration MetroCluster

Vous pouvez éviter les problèmes de performances des charges de travail en miroir dans des configurations MetroCluster sur FC et IP en vous assurant que la configuration MetroCluster est correctement configurée. Vous pouvez également améliorer les performances des charges de travail en modifiant la configuration ou en mettant à niveau des composants logiciels ou matériels.

Reportez-vous au "Documentation MetroCluster" pour obtenir les instructions de configuration des clusters dans la configuration MetroCluster, y compris les commutateurs Fibre Channel (FC), les câbles et les liens ISL (Inter-switch Links). Il permet également de configurer le logiciel MetroCluster de sorte que les clusters locaux et distants puissent communiquer avec les données de volume en miroir. Pour obtenir des informations spécifiques à votre configuration MetroCluster sur IP, reportez-vous àla section "Installez une configuration MetroCluster IP".

Vous pouvez comparer votre configuration MetroCluster aux exigences du "Documentation MetroCluster" afin de déterminer si une modification ou une mise à niveau des composants de votre configuration MetroCluster peut améliorer les performances des workloads. Cet comparatif peut vous aider à répondre aux questions suivantes :

- Les contrôleurs sont-ils adaptés à vos charges de travail ?
- Devez-vous mettre à niveau vos bundles ISL vers une bande passante plus importante pour gérer davantage de débit ?
- Pouvez-vous régler les crédits tampon à tampon (BBC) de vos commutateurs pour augmenter la bande passante ?
- Si vos charges de travail disposent d'un débit d'écriture élevé vers le stockage SSD, devez-vous mettre à niveau vos ponts FC-SAS pour prendre en charge le débit ?

Informations connexes

- Pour plus d'informations sur le remplacement ou la mise à niveau des composants MetroCluster, reportez-vous au "Documentation MetroCluster" .
- Pour plus d'informations sur la mise à niveau des contrôleurs, reportez-vous aux sections "Mise à niveau des contrôleurs d'une configuration FC MetroCluster à l'aide du basculement et du rétablissement" et "Mise à niveau des contrôleurs d'une configuration IP MetroCluster à l'aide du basculement et du rétablissement"

Déplacement des charges de travail vers un autre agrégat

Unified Manager vous permet d'identifier un agrégat moins occupé que l'agrégat dans lequel résident vos charges de travail, puis de déplacer les volumes ou les LUN sélectionnés vers cet agrégat. Le déplacement de charges de travail hautes performances vers un agrégat moins occupé, ou un agrégat sur lequel le stockage Flash est activé, permet à la charge de travail de réaliser davantage d'efficacité.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Vous devez avoir enregistré le nom de l'agrégat actuellement ayant 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 performances.

Cette procédure vous permet d'identifier les ressources suivantes afin de déplacer des charges de travail hautes performances vers un agrégat inférieur :

- Agrégats du même cluster moins utilisés
- Les volumes les plus performants de l'agrégat actuel

Étapes

1. Identifier l'agrégat du cluster le moins utilisé :
   a. Dans la page de détails **Event**, cliquez sur le nom du cluster sur lequel réside l'agrégat.

      Les détails du cluster s'affichent sur la page d'accueil Performance/Cluster.

   b. Sur la page **Résumé**, cliquez sur **Aggregates** dans le volet **objets gérés**.

      La liste des agrégats sur ce cluster s'affiche.

   c. Cliquez sur la colonne **utilisation** pour trier les agrégats par le moins utilisés.

      Vous pouvez également identifier les agrégats ayant la capacité **libre** la plus élevée. Ainsi, vous disposez d'une liste d'agrégats potentiels vers lesquels vous pouvez déplacer des charges de travail.

   d. Écrire le nom de l'agrégat dans lequel vous souhaitez déplacer les charges de travail.
2. Identifiez les volumes les plus performants de l'agrégat ayant reçu l'événement :
   a. Cliquez sur l'agrégat qui présente le problème de performances.

      Les détails de l'agrégat sont affichés sur la page de l'explorateur des performances/agrégats.

   b. Dans le sélecteur **Time Range**, sélectionnez **30 derniers jours**, puis cliquez sur **Apply Range**.

      Vous pouvez ainsi afficher une période d'historique de performance plus longue que celle des 72 heures par défaut. Vous souhaitez déplacer un volume qui utilise de nombreuses ressources de façon cohérente, pas seulement au cours des 72 dernières heures.

   c. Dans le contrôle **View and compare**, sélectionnez **volumes sur cet agrégat**.

      Une liste des volumes FlexVol et des volumes composant FlexGroup sur cet agrégat est affichée.

   d. Pour afficher les volumes les plus performants, triez par Mo/s, puis par IOPS les plus élevées.
   e. Notez les noms des volumes que vous souhaitez déplacer vers un autre agrégat.
3. Déplacez les volumes hautes performances vers l'agrégat que vous avez identifié comme présentant un faible taux d'utilisation.

   Vous pouvez effectuer l'opération de déplacement en utilisant ONTAP System Manager, OnCommand Workflow Automation et les commandes ONTAP ou une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacement des workloads vers un nœud différent

Grâce à Unified Manager, vous pouvez identifier un agrégat sur un autre nœud moins occupé que le nœud sur lequel vos charges de travail sont en cours d'exécution, puis déplacer les volumes sélectionnés vers cet agrégat. Le déplacement de charges de travail hautes performances vers un agrégat sur un nœud moins occupé permet aux workloads sur les deux nœuds de gagner en efficacité.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou 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 performances pendant un mois ou plus.

Cette procédure vous aide à identifier les ressources suivantes afin de déplacer des charges de travail hautes performances vers un nœud le plus faible utilisé :

- Les nœuds du même cluster présentent la plus grande capacité de performances disponible
- Les agrégats du nouveau nœud ayant la capacité de performances la plus élevée
- Les volumes les plus performants du nœud actuel

Étapes

1. Identifiez un nœud dans le cluster qui présente la capacité de performances disponible la plus élevée :
   a. Sur la page **Détails de l'événement**, cliquez sur le nom du cluster sur lequel réside le nœud.

      Les détails du cluster s'affichent sur la page d'accueil Performance/Cluster.

   b. Dans l'onglet **Résumé**, cliquez sur **noeuds** dans le volet **objets gérés**.

      La liste des nœuds de ce cluster s'affiche.

   c. Cliquez sur la colonne **capacité de performance utilisée** pour trier les nœuds par le pourcentage le moins utilisé.

      Vous trouverez ainsi une liste de nœuds potentiels vers lesquels vous pouvez déplacer des charges de travail.

   d. Notez le nom du nœud vers lequel vous souhaitez déplacer les charges de travail.
2. Identifier un agrégat sur le nouveau nœud le moins utilisé :
   a. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates** et sélectionnez **Performance** > **tous les agrégats** dans le menu Affichage.

      La vue Performance : tous les agrégats s'affiche.

   b. Cliquez sur **Filtering**, sélectionnez **Node** dans le menu déroulant de gauche, saisissez le nom du noeud dans le champ de texte, puis cliquez sur **appliquer le filtre**.

      La vue Performance : tous les agrégats sont de nouveau affichés avec la liste des agrégats disponibles sur ce nœud.

c. Cliquez sur la colonne **capacité de performance utilisée** pour trier les agrégats par le moins utilisé.

   Ainsi, vous disposez d'une liste d'agrégats potentiels vers lesquels vous pouvez déplacer des charges de travail.

d. Écrire le nom de l'agrégat dans lequel vous souhaitez déplacer les charges de travail.

3. Identifiez les charges de travail hautes performances du nœud ayant reçu l'événement :
   a. Revenez à la page **Détails de l'événement** pour l'événement.
   b. Dans le champ **volumes affectés**, cliquez sur le lien correspondant au nombre de volumes.

      La vue Performance : tous les volumes s'affiche avec une liste filtrée des volumes de ce nœud.

   c. Cliquez sur la colonne **capacité totale** pour trier les volumes selon le plus grand espace alloué.

      Ceci fournit une liste de volumes potentiels que vous pouvez déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que le nom des agrégats actuels où ils résident.
4. Déplacez les volumes vers les agrégats que vous avez identifiés comme présentant la meilleure capacité de performances disponible sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement en utilisant ONTAP System Manager, OnCommand Workflow Automation et les commandes ONTAP ou une combinaison de ces outils.

Après quelques jours, vous pouvez vérifier si vous recevez le même type d'événements du même nœud ou de l'agrégat.

Déplacement des charges de travail vers un agrégat sur un autre nœud

Grâce à Unified Manager, vous pouvez identifier un agrégat sur un autre nœud moins occupé que le nœud sur lequel vos charges de travail sont en cours d'exécution, puis déplacer les volumes sélectionnés vers cet agrégat. Le déplacement de charges de travail hautes performances vers un agrégat sur un nœud moins occupé permet aux charges de travail des deux nœuds de gagner en efficacité.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou 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 performances.

Cette procédure vous permet d'identifier les ressources suivantes afin de déplacer des charges de travail hautes performances vers un nœud inférieur :

- Les nœuds du même cluster sont moins utilisés
- Les agrégats du nouveau nœud les moins utilisés
- Les volumes les plus performants du nœud actuel

Étapes

1. Identifier un nœud du cluster le moins utilisé :
   a. Dans la page **Event** details, cliquez sur le nom du cluster sur lequel réside le nœud.

      Les détails du cluster s'affichent sur la page d'accueil Performance/Cluster.

   b. Sur la page **Résumé**, cliquez sur **noeuds** dans le volet **objets gérés**.

      La liste des nœuds de ce cluster s'affiche.

   c. Cliquez sur la colonne **utilisation** pour trier les nœuds par le moins utilisé.

      Vous pouvez également identifier les nœuds qui ont la plus grande **capacité libre**. Vous trouverez ainsi une liste de nœuds potentiels vers lesquels vous pouvez déplacer des charges de travail.

   d. Notez le nom du nœud vers lequel vous souhaitez déplacer les charges de travail.
2. Identifier un agrégat sur le nouveau nœud le moins utilisé :
   a. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates** et sélectionnez **Performance** > **tous les agrégats** dans le menu Affichage.

      La vue Performance : tous les agrégats s'affiche.

   b. Cliquez sur **Filtering**, sélectionnez **Node** dans le menu déroulant de gauche, saisissez le nom du noeud dans le champ de texte, puis cliquez sur **appliquer le filtre**.

      La vue Performance : tous les agrégats sont de nouveau affichés avec la liste des agrégats disponibles sur ce nœud.

   c. Cliquez sur la colonne **utilisation** pour trier les agrégats par le moins utilisés.

      Vous pouvez également identifier les agrégats ayant la capacité **libre** la plus élevée. Ainsi, vous disposez d'une liste d'agrégats potentiels vers lesquels vous pouvez déplacer des charges de travail.

   d. Écrire le nom de l'agrégat dans lequel vous souhaitez déplacer les charges de travail.
3. Identifiez les charges de travail hautes performances du nœud ayant reçu l'événement :
   a. Revenez à la page **Event** details de l'événement.
   b. Dans le champ **volumes affectés**, cliquez sur le lien correspondant au nombre de volumes.

      La vue Performance : tous les volumes s'affiche avec une liste filtrée des volumes de ce nœud.

   c. Cliquez sur la colonne **capacité totale** pour trier les volumes selon le plus grand espace alloué.

      Ceci fournit une liste de volumes potentiels que vous pouvez déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que le nom des agrégats actuels où 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 en utilisant ONTAP System Manager, OnCommand Workflow Automation et les commandes ONTAP ou une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacement des workloads vers un nœud dans une autre paire haute disponibilité

Unified Manager permet d'identifier un agrégat sur un nœud d'une autre paire haute disponibilité avec plus de capacité de performances que la paire haute disponibilité sur laquelle sont actuellement exécutées vos charges de travail. Vous pouvez ensuite déplacer les volumes sélectionnés vers des agrégats sur la nouvelle paire haute disponibilité.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Votre cluster doit comprendre au moins deux paires haute disponibilité

  Ce processus de résolution des problèmes ne peut pas être utilisé si le cluster ne compte qu'une seule paire haute disponibilité.

- Vous devez avoir enregistré les noms des deux nœuds de la paire haute disponibilité qui présentent 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 performances pendant un mois ou plus.

Le déplacement de charges de travail hautes performances vers un agrégat d'un nœud présentant une capacité plus élevée en termes de performances permet aux charges de travail des deux nœuds d'être plus efficaces. Cette procédure vous permet d'identifier les ressources suivantes pour déplacer les charges de travail haute performance vers un nœud qui dispose de plus de capacité de performances disponible sur une autre paire haute disponibilité :

- Les nœuds d'une paire haute disponibilité différente sur le même cluster qui présentent la plus grande capacité de performances libres
- Les agrégats des nouveaux nœuds qui offrent la meilleure capacité de performances disponible
- Les volumes les plus performants sur les nœuds actuels

Étapes

1. Identifiez les nœuds qui font partie d'une autre paire haute disponibilité sur le même cluster :
   a. Sur la page **Détails de l'événement**, cliquez sur le nom du cluster sur lequel se trouvent les nœuds.

      Les détails du cluster s'affichent sur la page d'accueil Performance/Cluster.

   b. Sur la page **Résumé**, cliquez sur **noeuds** dans le volet **objets gérés**.

      La liste des nœuds de ce cluster est affichée dans la vue performances : tous les nœuds.

   c. Écrire les noms des nœuds qui se trouvent dans différentes paires haute disponibilité de la paire haute disponibilité actuellement ayant un problème de performances.
2. Identifiez un nœud dans la nouvelle paire haute disponibilité qui présente la capacité de performances la plus élevée :
   a. Dans la vue **Performance : tous les nœuds**, cliquez sur la colonne **Performance Capacity utilisé** pour trier les nœuds par le pourcentage le moins utilisé.

Vous trouverez ainsi une liste de nœuds potentiels vers lesquels vous pouvez déplacer des charges de travail.

b. Écrire 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 présente la capacité de performances la plus élevée :

   a. Dans la vue **Performance : tous les nœuds**, cliquez sur le nœud.

      Les détails des nœuds s'affichent sur la page Performance/Node Explorer.

   b. Dans le menu **View and compare**, sélectionnez **Aggregates sur ce noeud**.

      Les agrégats de ce nœud s'affichent dans la grille.

   c. Cliquez sur la colonne **capacité de performance utilisée** pour trier les agrégats par le moins utilisé.

      Ainsi, vous disposez d'une liste d'agrégats potentiels vers lesquels vous pouvez déplacer des charges de travail.

   d. Écrire le nom de l'agrégat dans lequel vous souhaitez déplacer les charges de travail.

4. Identifiez les charges de travail haute performance issues des nœuds qui ont reçu l'événement :

   a. Revenez à la page **Event** details de l'événement.

   b. Dans le champ **volumes affectés**, cliquez sur le lien correspondant au nombre de volumes du premier nœud.

      La vue Performance : tous les volumes s'affiche avec une liste filtrée des volumes de ce nœud.

   c. Cliquez sur la colonne **capacité totale** pour trier les volumes selon le plus grand espace alloué.

      Cela fournit une liste de volumes potentiels que vous pouvez déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que le nom des agrégats actuels où ils résident.

   e. Exécutez les étapes 4c et 4d pour le second nœud qui faisait partie de cet événement pour identifier les volumes que vous souhaitez également déplacer à partir de ce nœud.

5. Déplacez les volumes vers les agrégats que vous avez identifiés comme présentant la meilleure capacité de performances disponible sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement en utilisant ONTAP System Manager, OnCommand Workflow Automation et les commandes ONTAP ou une combinaison de ces outils.

Après quelques jours, vous pouvez vérifier si vous recevez le même type d'événements du même nœud ou de l'agrégat.

Déplacement des workloads vers un autre nœud dans une paire haute disponibilité différente

Grâce à Unified Manager, vous pouvez identifier un agrégat sur un nœud d'une autre paire haute disponibilité moins occupée que la paire haute disponibilité sur laquelle vos charges de travail sont actuellement exécutées. Vous pouvez ensuite déplacer les

volumes sélectionnés vers des agrégats sur la nouvelle paire haute disponibilité. Le déplacement de charges de travail hautes performances vers un agrégat sur un nœud moins occupé permet aux charges de travail des deux nœuds de gagner en efficacité.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Le cluster doit comprendre au moins deux paires haute disponibilité ; ce processus de correction n'est pas possible si votre cluster ne compte qu'une seule paire haute disponibilité.
- Vous devez avoir enregistré les noms des deux nœuds de la paire haute disponibilité qui présentent 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 performances.

Cette procédure vous permet d'identifier les ressources suivantes afin de déplacer des charges de travail haute performance vers un nœud le plus faible utilisé sur une autre paire haute disponibilité :

- Les nœuds d'une paire haute disponibilité différente sur le même cluster qui sont moins utilisés
- Les agrégats sur les nouveaux nœuds les moins utilisés
- Les volumes les plus performants sur les nœuds actuels

Étapes

1. Identifiez les nœuds qui font partie d'une autre paire haute disponibilité sur le même cluster :
   a. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters** et sélectionnez **Performance** > **tous les clusters** dans le menu Affichage.

      La vue Performance : tous les clusters est affichée.

   b. Cliquez sur le numéro dans le champ **nombre de nœuds** pour le cluster actuel.

      La vue Performance : tous les nœuds est affichée.

   c. Écrire les noms des nœuds qui se trouvent dans différentes paires haute disponibilité de la paire haute disponibilité actuellement ayant le problème de performances.
2. Identifier un nœud dans la nouvelle paire HA la moins utilisée :
   a. Cliquez sur la colonne **utilisation** pour trier les nœuds par le moins utilisé.

      Vous pouvez également identifier les nœuds qui ont la plus grande **capacité libre**. Vous trouverez ainsi une liste de nœuds potentiels vers lesquels vous pouvez déplacer des charges de travail.

   b. Notez le nom du nœud vers lequel vous souhaitez déplacer les charges de travail.
3. Identifier un agrégat sur le nouveau nœud le moins utilisé :
   a. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates** et sélectionnez **Performance** > **tous les agrégats** dans le menu Affichage.

      La vue Performance : tous les agrégats s'affiche.

   b. Cliquez sur **Filtering**, sélectionnez **Node** dans le menu déroulant de gauche, saisissez le nom du noeud dans le champ de texte, puis cliquez sur **appliquer le filtre**.

La vue Performance : tous les agrégats sont de nouveau affichés avec la liste des agrégats disponibles sur ce nœud.

c. Cliquez sur la colonne **utilisation** pour trier les agrégats par le moins utilisés.

   Vous pouvez également identifier les agrégats ayant la capacité **libre** la plus élevée. Ainsi, vous disposez d'une liste d'agrégats potentiels vers lesquels vous pouvez déplacer des charges de travail.

d. Écrire le nom de l'agrégat dans lequel vous souhaitez déplacer les charges de travail.

4. Identifiez les charges de travail haute performance issues des nœuds qui ont reçu l'événement :
   a. Revenez à la page **Event** details de l'événement.
   b. Dans le champ **volumes affectés**, cliquez sur le lien correspondant au nombre de volumes du premier nœud.

      La vue Performance : tous les volumes s'affiche avec une liste filtrée des volumes de ce nœud.

   c. Cliquez sur la colonne **capacité totale** pour trier les volumes selon le plus grand espace alloué.

      Cela fournit une liste de volumes potentiels que vous pouvez déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que le nom des agrégats actuels où ils résident.
   e. Exécutez les étapes 4c et 4d pour le second nœud qui faisait partie de cet événement pour identifier les volumes 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 en utilisant ONTAP System Manager, OnCommand Workflow Automation et les commandes ONTAP ou 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 règles de QoS pour hiérarchiser le travail sur ce nœud

Vous pouvez définir une limite au groupe de règles de QoS pour contrôler la limite d'E/S par seconde (IOPS) ou de débit en Mbit/s pour les workloads qu'il contient. Si des charges de travail se trouvent dans un groupe de règles sans limite définie, telles que le groupe de règles par défaut ou la limite définie ne répond pas à vos besoins, vous pouvez augmenter la limite définie ou déplacer les charges de travail vers un nouveau groupe de règles ou un groupe existant présentant la limite souhaitée.

Si un événement de performance d'un nœud est causé par des charges de travail qui utilisent trop les ressources du nœud, la description de l'événement sur la page Détails de l'événement affiche un lien vers la liste des volumes concernés. Sur la page Performance/volumes, vous pouvez trier les volumes affectés par IOPS et Mo/sec pour voir quelles charges de travail ont le plus d'utilisation qui pourrait avoir contribué à cet événement.

En attribuant les volumes sur lesquels les ressources de nœud sont surutilisées à un paramètre de groupe de règles plus restrictif, le groupe de règles accélère les workloads afin de limiter leur activité, ce qui permet de réduire l'utilisation des ressources de ce nœud.

Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour gérer les « policy Groups », notamment les tâches suivantes :

- Création d'une « policy group »
- Ajout ou suppression de charges de travail dans un « policy group »
- Déplacement d'une charge de travail entre des groupes de règles
- Modification de la limite de débit d'un groupe de règles

Supprimez les volumes et les LUN inactifs

Une fois l'espace libre de l'agrégat identifié comme un problème, vous pouvez rechercher les volumes et les LUN inutilisés et les supprimer de l'agrégat. Cela peut aider à réduire le problème de peu d'espace disque.

Si un événement de performance d'un agrégat est provoqué par un manque d'espace disque, quelques méthodes vous permettent 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 Performance : tous les volumes. De là, vous pouvez trier les volumes affectés par **IOPS** pour voir quels volumes n'ont pas été actifs.

Pour identifier les LUN non utilisées :

1. Dans 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 **Storage** > **LUNs** et sélectionnez **Performance** > **toutes les LUN** dans le menu Affichage.
3. Cliquez sur **Filtering**, sélectionnez **Aggregate** 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 des LUN affectées par **IOPS** pour afficher les LUN qui ne sont pas actives.

Une fois les volumes et LUN inutilisés, vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour supprimer ces objets.

Ajout de disques et reconstruction des agrégats

Vous pouvez ajouter des disques à un agrégat pour augmenter la capacité de stockage et les performances de cet agrégat. Après l'ajout de disques, vous constatez uniquement une amélioration des performances 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, vous devrez peut-être contacter votre administrateur ou acheter plus de disques. 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"

Configuration d'une connexion entre un serveur Unified Manager et un fournisseur de données externe

La connexion entre un serveur Unified Manager et un fournisseur de données externe vous permet d'envoyer les données de performance du cluster à un serveur externe de sorte que les gestionnaires du stockage puissent diagramme des 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 externes » dans la console de maintenance.

Données de performances qui peuvent être envoyées à un serveur externe

Unified Manager collecte de nombreuses données de performances dans tous les clusters qu'il surveille. Vous pouvez envoyer des groupes de données spécifiques à un serveur externe.

En fonction des données de performances que vous voulez saisir, vous pouvez choisir d'envoyer l'un des groupes de statistiques suivants :

Groupe de statistiques	Données incluses	Détails
Contrôle des performances	Statistiques de performances générales pour les objets suivants : • LUN • Volumes	Ce groupe fournit une latence totale ou des IOPS 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 • 64 bits	Ce groupe fournit des statistiques d'utilisation du nœud et regroupe les ressources physiques dans tous les clusters surveillés. Il fournit également les statistiques collectées dans le groupe moniteur de performances.

Groupe de statistiques	Données incluses	Détails
Accédez à des informations détaillées	Statistiques de lecture/écriture de niveau inférieur et statistiques par protocole pour tous les objets suivis : • Nœuds • 64 bits • LUN • Volumes • Disques • LIF • Ports/NIC	Ce groupe fournit des ventilations 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 cluster, est modifié sur le système de stockage, l'ancien et le nouveau objets contiennent des données de performances sur le serveur externe (appelé « chemin_métrique »). Les deux objets ne sont pas corrélés au même objet. Par exemple, si vous modifiez le nom d'un volume de « Volume 1_acct » à « acct_vol1 », vous verrez d'anciennes données de performances de l'ancien volume et de nouvelles données de performances du nouveau volume.

Consultez l'article 30096 de la base de connaissances pour obtenir la liste de tous les compteurs de performances pouvant être envoyés à un fournisseur de données externe.

"Compteurs de performances Unified Manager pouvant être exportés vers un fournisseur de données externe"

Configuration de Graphite pour recevoir les données de performances par Unified Manager

Le graphite est un outil logiciel ouvert permettant de rassembler et de représenter les données de performances des systèmes informatiques. Votre serveur et votre logiciel Graphite doivent être configurés correctement pour recevoir des données statistiques de Unified Manager.

NetApp ne vérifie pas les versions spécifiques de Graphite ou d'autres outils tiers.

Le serveur Graphite ne reçoit pas les données de performances des volumes d'Unified Manager.

Une fois Graphite installé, d'après les instructions d'installation, vous devez apporter les modifications suivantes pour prendre en charge le transfert de données statistiques à partir de Unified Manager :

- Dans le `/opt/graphite/conf/carbon.conf` fichier, le nombre maximal 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 envoyer, des milliers de nouveaux fichiers peuvent être créés au départ. Avec 200 fichiers par minute, la création initiale de tous les fichiers de mesure peut prendre 15 minutes ou plus. Une fois que tous les

fichiers de mesures uniques ont été 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` fichier doit être remplacée par « 0.0.0.0 » par «»:»» (**`LINE_RECEIVER_INTERFACE = ::`**)
- Dans le `/opt/graphite/conf/storage-schemas.conf` fichier, le `retentions` paramètre doit être utilisé pour définir la fréquence sur 5 minutes et la période de conservation sur le nombre de jours correspondant à votre environnement.

  La durée de conservation peut être aussi longue que celle de votre environnement, mais la valeur de fréquence doit être définie sur 5 minutes pour au moins un paramètre de rétention. Dans l'exemple suivant, une section est définie pour Unified Manager à l'aide du `pattern` paramètre, et les valeurs définissent la fréquence initiale sur 5 minutes et la période de conservation sur 100 jours : **`[OPM]`**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  > Si le tag fournisseur par défaut passe de « NetApp-performance » à quelque chose de différent, ce changement doit également être reflété dans le `pattern` paramètre.

> 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 les données collectées ne sont pas conservées.

Configuration d'une connexion à partir d'un serveur Unified Manager vers un fournisseur de données externe

Unified Manager peut envoyer les données relatives aux performances du cluster à un serveur externe. Vous pouvez spécifier le type de données statistiques envoyées et l'intervalle d'envoi des données.

Ce dont vous aurez besoin

- Un ID utilisateur doit être 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 le port par défaut n'est pas utilisé 2003)
- Vous devez avoir configuré le serveur distant et le logiciel tiers pour qu'il puisse recevoir des données statistiques du serveur Unified Manager.
- Vous devez savoir quel groupe de statistiques vous voulez envoyer :
  - PERFORMANCE_INDICATEUR : statistiques du moniteur de performances
  - RESOURCE_UTILISATION : statistiques de contrôle des performances et de l'utilisation des ressources
  - DRILL_DOWN : toutes les statistiques
- Vous devez connaître l'intervalle de temps auquel vous souhaitez transmettre des 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 pendant chaque transmission est deux (ou trois) fois plus grande que lors de l'utilisation de l'intervalle de 5 minutes par défaut.

> Si vous définissez l'intervalle de collecte des performances d'Unified Manager sur 10 ou 15 minutes, vous devez modifier l'intervalle de transmission de sorte 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 de Unified Manager s'affichent.

2. Dans la console de maintenance, saisissez le numéro de l'option de menu **External Data Provider**.

   Le menu connexion au serveur externe s'affiche.

3. Saisissez le numéro de l'option de menu **Ajouter/Modifier connexion serveur**.

   Les informations de connexion actuelles du serveur s'affichent.

4. Lorsque vous y êtes invité, tapez `y` pour continuer.
5. Lorsque vous y êtes invité, entrez l'adresse IP ou le nom du serveur de destination et les informations relatives au port du serveur (si elles sont différentes du port par défaut 2003).
6. Lorsque vous y êtes invité, tapez `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. Saisissez le numéro de l'option de menu **Modify Server Configuration**.

   Les informations de configuration actuelles du serveur s'affichent.

9. Lorsque vous y êtes invité, tapez `y` pour continuer.
10. Lorsque vous y êtes invité, entrez 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 de groupe de statistiques	`0` - INDICATEUR_PERFORMANCES (par défaut) `1` - UTILISATION_DES_RESSOURCES `2` - FORER_DOWN

Pour..	Entrer…
Étiquette du fournisseur	Nom descriptif du dossier dans lequel les statistiques seront stockées sur le serveur externe. « netapp-performance » est le nom par défaut, mais vous pouvez entrer une autre valeur. En utilisant la notation en pointillés, vous pouvez définir une structure hiérarchique de dossiers. Par exemple, en entrant **`stats.performance.netapp`** les statistiques se trouvent dans **stats** > **performance** > **NetApp**.
Intervalle de transmission	**`5`** (par défaut), **`10`**, ou **`15`** minutes
Activer/désactiver	**`0`** - Désactiver **`1`** - Activer (par défaut)

11. Lorsque vous y êtes invité, tapez **`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. Tapez **`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 spécifié. L'affichage des mesures dans l'outil externe prend quelques minutes. Vous devrez peut-être actualiser votre navigateur pour afficher les nouvelles mesures dans la hiérarchie des mesures.

Contrôlez et gérez l'état du cluster

Présentation de 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 de serveur Unified Manager offre évolutivité, compatibilité et fonctionnalités avancées de contrôle et de notification.

Il offre de nombreuses fonctionnalités : surveillance, alerte, gestion de la disponibilité et de la capacité des clusters, gestion des fonctionnalités de protection et regroupement des données de diagnostic et envoi au support technique.

Vous pouvez utiliser Unified Manager pour surveiller vos clusters. Lorsqu'un problème se produit au sein du cluster, Unified Manager vous informe des détails de ces problèmes par le biais d'événements. Certains événements vous fournissent également une action corrective que vous pouvez effectuer pour corriger ces problèmes. Vous pouvez configurer les alertes pour les événements afin que lorsque des problèmes se produisent, vous être averti par e-mail et des interruptions SNMP.

Unified Manager vous permet de gérer les objets de stockage de votre environnement en les associant à des annotations. Vous pouvez créer des annotations personnalisées et associer de façon dynamique des clusters, des machines virtuelles de stockage 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 santé et de capacité pour l'objet de cluster respectif.

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 désigne les blocs physiques utilisés dans le volume. La capacité physique utilisée est généralement inférieure à la capacité logique utilisée en raison de la réduction des données provenant des fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression).
- Capacité logique : espace logique désigne l'espace utilisable (blocs logiques) dans un volume. L'espace logique désigne la manière dont l'espace théorique peut être utilisé, sans tenir compte des résultats obtenus grâce à la déduplication ou à la compression. L'espace logique utilisé est 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 semble souvent plus importante que la capacité physique utilisée, car elle ne reflète pas la compression des données et d'autres réductions de l'espace physique. La capacité logique totale peut donc être supérieure à l'espace provisionné.

Unités de mesure de la capacité

Unified Manager calcule la capacité de stockage en fonction des unités binaires de 1024 (2^{10}) octets. Dans ONTAP 9.10.0 et versions antérieures, ces unités étaient affichées sous la forme Ko, Mo, Go, To et PB. À partir de ONTAP 9.10.1, ces objets sont affichés dans Unified Manager comme Kio, Mio, Gio, Tio et Pio.

Les unités utilisées pour le débit continuent d'être de kilo-octets par seconde (Kbit/s), mégaoctets par seconde (Mbit/s), gigaoctets par seconde (Gbit/s) ou téraoctets par seconde (Tbit/s), 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	Kio	1024	1024 octets
MO	Mio	1024 * 1024	1 048 576 octets
GO	Gio	1024 * 1024 * 1024	1 073 741 824 octets
TO	Tio	1024 * 1024 * 1024 * 1024	1 099 511 627 776 octets

Fonctionnalités de contrôle de l'état de santé de Unified Manager

Unified Manager repose sur une infrastructure de serveurs qui offre évolutivité, compatibilité et fonctionnalités avancées de surveillance et de notification. 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, tiroirs disques, paires SFO, ports, Et Flash cache
  - Objets logiques : clusters, serveurs virtuels de stockage (SVM), agrégats, volumes, LUN, namespaces, Qtrees, LIF, copies Snapshot, chemins de jonction, partages NFS, Partages SMB, quotas d'utilisateur et de groupe, groupes de règles de QoS et groupes 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 (synchrones et asynchrones) et relations SnapVault
- Affichage de la détection et du contrôle du cluster
- Configurations MetroCluster sur FC et IP : affichage et contrôle de la configuration, des problèmes et de l'état de connectivité des composants du cluster. Commutateurs et ponts MetroCluster pour les configurations MetroCluster over FC
- Alertes améliorées, événements et infrastructure de seuils
- Prise en charge des utilisateurs locaux, de LDAP, LDAPS, de l'authentification SAML
- RBAC (pour un ensemble de rôles prédéfinis)
- AutoSupport et bundle de support
- Tableau de bord amélioré pour afficher la capacité, la disponibilité, la protection et l'état des performances

de l'environnement

- Interopérabilité du déplacement de volumes, historique des déplacements de volumes et historique des modifications apportées au chemin de jonction
- Étendue de la zone d'impact qui affiche sous forme graphique les ressources affectées par des événements tels que des disques défaillants, la mise en miroir des agrégats MetroCluster dégradés et les disques de rechange MetroCluster laissés derrière des événements
- Zone d'effet possible affichant l'impact des événements MetroCluster
- Actions correctives suggérées : affiche les actions nécessaires pour gérer des événements tels que des disques défaillants, la mise en miroir de l'agrégat MetroCluster dégradé et les disques de rechange MetroCluster laissés en retard
- Ressources susceptibles d'être affectées zone affichant les ressources susceptibles d'être affectées pour des événements tels que l'événement Volume hors ligne, Volume restreint et l'événement Volume à provisionnement fin en cas de risque
- Prise en charge des SVM avec des volumes FlexVol ou FlexGroup
- Prise en charge de la surveillance des volumes racines des nœuds
- Contrôle amélioré des copies Snapshot, y compris le calcul de l'espace récupérable et la suppression des copies Snapshot
- Annotations pour les objets de stockage
- La création et la gestion de rapports sur les informations d'objet 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 les flux de travail

  Le site Storage Automation Store comprend des packs de flux de travail de stockage automatisés certifiés NetApp conçus pour être utilisés avec OnCommand Workflow Automation (WFA). Vous pouvez télécharger les packs, puis les importer dans WFA pour les exécuter. Les workflows automatisés sont disponibles ici :

  "Le Storage Automation Store"

Les 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 disponibilité et de protection du stockage des données. Les deux interfaces utilisateur sont l'interface utilisateur Web de Unified Manager et la console de maintenance.

Si vous souhaitez utiliser les fonctions de protection dans Unified Manager, vous devez également installer et configurer OnCommand Workflow Automation (WFA).

Interface Web Unified Manager

L'interface utilisateur Web Unified Manager permet à un administrateur de surveiller et de résoudre les problèmes liés à la capacité de stockage, à la disponibilité et à la protection des données en cluster.

Ces sections décrivent les 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 Unified Manager.

Console de maintenance

La console de maintenance Unified Manager permet à un administrateur de surveiller, diagnostiquer et résoudre les problèmes liés au système d'exploitation, à la mise à niveau de la version, aux problèmes d'accès utilisateur et aux problèmes de réseau liés au serveur Unified Manager lui-même. Si l'interface utilisateur Web de 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 contrôle de l'état des clusters et des objets du cluster

Unified Manager utilise des requêtes d'API périodiques et un moteur de collecte des données pour collecter les données à partir des clusters. En ajoutant des clusters à la base de données Unified Manager, vous pouvez contrôler et gérer ces clusters pour détecter les risques de disponibilité et de capacité.

Présentation du contrôle des clusters

Vous pouvez ajouter des clusters à la base de données Unified Manager afin de surveiller la disponibilité, la capacité et d'autres informations, notamment sur l'utilisation du CPU, les statistiques d'interface, l'espace disque libre, l'utilisation des qtrees et l'environnement du châssis.

Les événements sont générés si l'état est anormal ou lorsqu'un seuil prédéfini est atteint. S'il est configuré pour ce faire, Unified Manager envoie une notification à un destinataire spécifié lorsqu'un événement déclenche une alerte.

Présentation des volumes root du nœud

Vous pouvez surveiller le volume racine du nœud à l'aide de Unified Manager. Il est recommandé que la capacité du volume racine du nœud soit suffisante pour éviter que le nœud ne cesse 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 volume racine du nœud presque plein est généré. Vous pouvez configurer une alerte pour l'événement afin d'obtenir une notification. Vous pouvez prendre les mesures appropriées pour éviter la panne du nœud à l'aide de ONTAP System Manager ou de l'interface de ligne de commande de ONTAP.

> La fonctionnalité de surveillance des volumes root de nœud n'est pas disponible si les clusters exécutent ONTAP 9.14.1 ou une version ultérieure.

Présentation des événements et des seuils pour les agrégats racine du nœud

Vous pouvez contrôler l'agrégat racine du nœud à l'aide de Unified Manager. Il est recommandé de provisionner de façon épaisse le volume racine dans l'agrégat racine afin d'empêcher l'arrêt du nœud.

Par défaut, les événements de capacité et de performance ne sont pas générés pour les agrégats racine. En outre, les valeurs de seuil utilisées par Unified Manager ne s'appliquent pas aux agrégats racine du nœud. Seul un représentant du support technique peut modifier les paramètres de ces événements. 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 des mesures appropriées pour empêcher l'arrêt du nœud en utilisant ONTAP System Manager ou l'interface de ligne de commande de ONTAP.

> La fonctionnalité de surveillance des agrégats racines de nœuds n'est pas disponible si les clusters exécutent ONTAP 9.14.1 ou une version ultérieure.

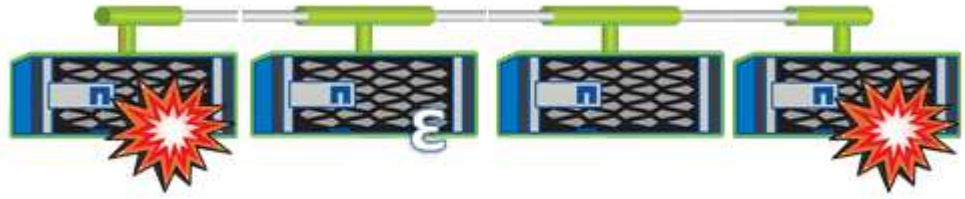
Présentation du quorum et de l'epsilon

Le quorum et l'epsilon sont des mesures importantes de l'état de santé du cluster et des fonctions qui indiquent ensemble que les clusters répondent aux problèmes potentiels de communication et de connectivité.

Quorum est une condition préalable à un cluster pleinement opérationnel. Lorsqu'un cluster est au quorum, une simple majorité de nœuds sont en bon état et peuvent communiquer entre eux. En cas de perte du quorum, le cluster n'a plus la possibilité d'effectuer des opérations normales sur le cluster. Un seul ensemble de nœuds peut avoir le quorum à la fois car tous les nœuds partagent collectivement une vue unique des données. Par conséquent, si deux nœuds qui ne communiquent pas sont autorisés à modifier les données de manière divergentes, il n'est plus possible de réconcilier les données en une seule vue de données.

Chaque nœud du cluster participe à un protocole de vote qui élit un maître de nœud ; chaque nœud restant est un deuxième nœud. Le nœud maître est chargé de synchroniser les informations sur le cluster. Lorsque le quorum est formé, il est maintenu par vote continu. Si le nœud maître se met hors ligne et que le cluster est encore au quorum, un nouveau maître est élu par les nœuds qui restent en ligne.

Étant donné qu'il y a la possibilité d'une TIE dans un cluster qui a un nombre pair de nœuds, un nœud a un poids fractionnaire supplémentaire appelé epsilon. Si la connectivité entre deux portions égales d'un grand cluster tombe en panne, le groupe de nœuds contenant epsilon maintient le quorum, en supposant que tous les nœuds sont en bon état. Par exemple, l'illustration suivante montre un cluster à quatre nœuds où deux des nœuds ont échoué. Cependant, comme l'un des noeuds survivants contient epsilon, le cluster reste dans le quorum même s'il n'y a pas une simple majorité de noeuds sains.



Epsilon est automatiquement affecté au premier nœud lors de la création du cluster. Si le nœud qui contient epsilon devient défectueux, prend le relais de son partenaire haute disponibilité ou est repris par son partenaire haute disponibilité, puis il est automatiquement réaffecté à un nœud saine dans une paire haute disponibilité différente.

La mise hors ligne d'un nœud peut affecter la capacité du cluster à rester dans le quorum. Par conséquent, ONTAP émet un message d'avertissement si vous tentez une opération qui détiendra le cluster du quorum ou qui le mettra hors service de la perte du quorum. Vous pouvez désactiver les messages d'avertissement de quorum en utilisant la commande cluster quorum-service options modify au niveau des privilèges avancés.

De manière générale, en supposant une connectivité fiable entre les nœuds du cluster, un cluster plus grand est plus stable qu'un cluster plus petit. Le quorum nécessaire à une simple majorité de 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 le maintien du quorum. Les clusters à deux nœuds utilisent la haute disponibilité du cluster dans lequel aucun nœud ne contient epsilon ; les deux nœuds sont plutôt interrogés en continu afin de garantir que si un nœud tombe en panne, l'autre dispose d'un accès en lecture/écriture complet aux données, ainsi que de l'accès aux interfaces logiques et aux fonctions de gestion.

Affichage de la liste et des détails des clusters

Vous pouvez utiliser la vue Santé : tous les clusters pour afficher votre inventaire des clusters. Le vue capacité : tous les clusters permet d'afficher des informations résumées sur la capacité de stockage et l'utilisation de tous les clusters.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez également afficher les détails des clusters individuels, tels que leur état, leur capacité, leur configuration, les LIF, les nœuds, Et disques dans ce cluster à l'aide de la page des détails du cluster / intégrité.

Les détails de la vue Santé : tous les clusters, capacité : tous les clusters et la page des détails Cluster / Santé vous aident à planifier votre stockage. Par exemple, avant de provisionner un nouvel agrégat, vous pouvez sélectionner un cluster spécifique dans l'onglet Santé : tous les clusters et obtenir les détails de capacité pour déterminer si le cluster dispose de l'espace requis.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **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 des 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 **Cluster / Health** details.

Informations connexes

- "Page Cluster / Health Details"
- "Performance : vue de tous les clusters"
- "Contrôle des configurations MetroCluster"
- "Affichage de l'état de sécurité pour les clusters et les VM de stockage"
- "Quels sont les critères de sécurité évalués"

Vérification de l'état de santé des clusters dans une configuration MetroCluster

Vous pouvez utiliser Active IQ Unified Manager (Unified Manager) pour vérifier l'état de fonctionnement des clusters et de leurs composants dans les configurations MetroCluster over FC et MetroCluster over IP. Si les clusters étaient impliqués dans un événement de performances détecté par Unified Manager, l'état de santé peut vous aider à déterminer

si un problème matériel ou logiciel a contribué à l'événement.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Vous devez avoir analysé un événement de performance pour une configuration MetroCluster et obtenu le nom du cluster concerné.
- Les deux clusters de la configuration MetroCluster sur FC et IP doivent être surveillés par la même instance de Unified Manager.

Détermination de l'état du cluster dans la configuration MetroCluster sur FC

Procédez comme suit pour déterminer l'intégrité du cluster dans une configuration MetroCluster sur FC.

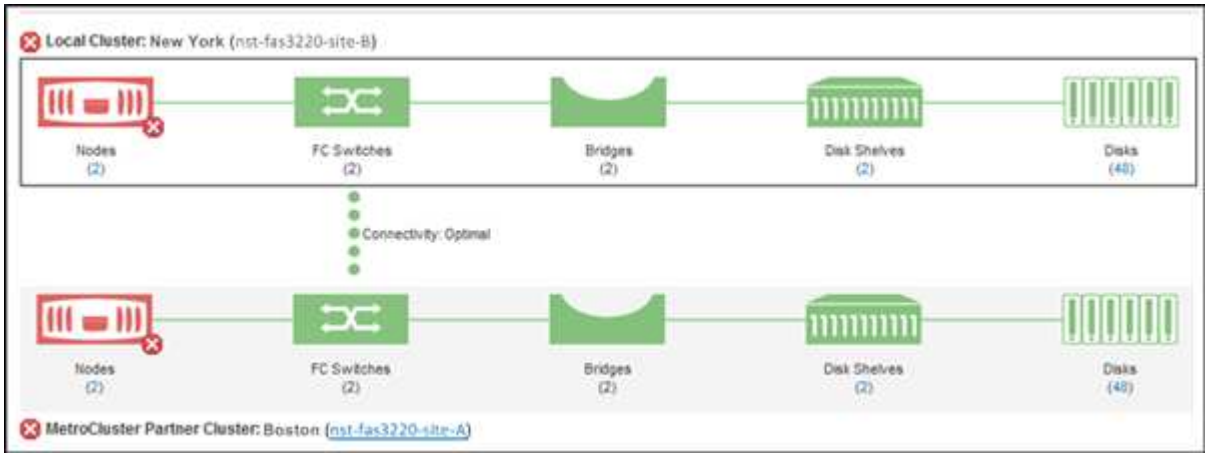
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management** pour afficher la liste des événements.
2. Dans le panneau filtre, sélectionnez tous les filtres MetroCluster dans la catégorie **Type de source**. Tous les événements soulevés dans votre environnement pour toutes les configurations MetroCluster.
3. Cliquez sur le nom du cluster en regard d'un événement MetroCluster.

   > 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 over FC.

   La vue Santé : tous les clusters s'affiche avec des informations détaillées sur l'événement.

4. Sélectionnez l'onglet **connectivité MetroCluster** pour afficher l'intégrité de la connexion entre le cluster sélectionné et son cluster partenaire.

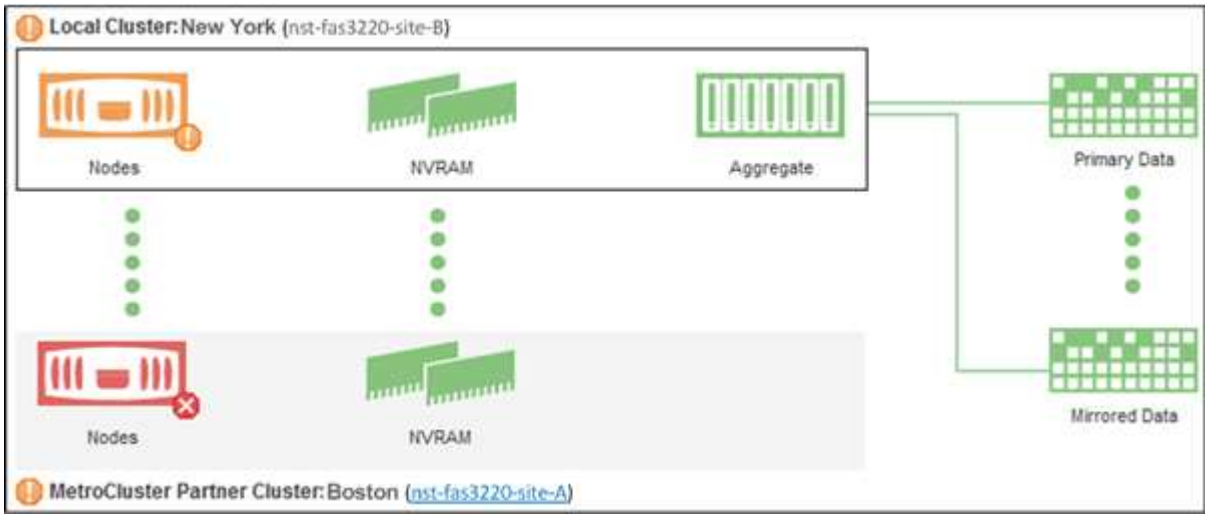


   Dans cet exemple, les noms et les composants du cluster local et de son cluster partenaire sont affichés. Une icône jaune ou rouge indique un événement de santé pour le composant mis en surbrillance. L'icône connectivité représente le lien entre les clusters. Vous pouvez pointer le curseur de la souris sur une icône pour afficher les informations sur les événements ou cliquer sur l'icône pour afficher les événements. Un problème de santé peut avoir contribué à l'événement de performance sur l'un ou l'autre des clusters.

   Unified Manager surveille le composant NVRAM de la liaison entre les clusters. Si l'icône des commutateurs FC sur le cluster local ou partenaire ou l'icône de connectivité est rouge, un problème de

santé de la liaison peut avoir causé l'événement de performances.

5. Sélectionnez l'onglet **réplication MetroCluster**.



Dans cet exemple, si l'icône NVRAM du cluster local ou partenaire est jaune ou rouge, un problème de santé lié à la mémoire NVRAM peut avoir provoqué l'événement de performances. Si aucune icône rouge ou jaune n'est affichée sur la page, un problème de performances peut avoir été causé par l'événement de performances du cluster partenaire.

Détermination de l'état du cluster dans la configuration MetroCluster sur IP

Procédez comme suit pour déterminer l'intégrité du cluster dans une configuration MetroCluster sur IP.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management** pour afficher la liste des événements.
2. Dans le panneau de filtre, sous la catégorie **Type de source**, sélectionnez le `MetroCluster Relationship` filtre. Tous les événements soulevés dans votre environnement pour toutes les configurations MetroCluster.

> Si vous ne voyez pas les événements MetroCluster signalés, vous pouvez utiliser la barre de recherche pour effectuer une recherche par le nom du cluster concerné dans l'événement lié à votre configuration MetroCluster sur IP.

3. Cliquez sur le nom du cluster, en regard de l'événement MetroCluster qui vous concerne. La page clusters s'affiche avec les détails de ce cluster. Pour plus d'informations sur la détermination des problèmes de santé, reportez-vous à "Surveiller les problèmes de connectivité dans la configuration MetroCluster over IP"la section .

Affichage de l'état de santé et de capacité de tous les clusters de baies SAN

Vous pouvez utiliser les pages Cluster Inventory pour afficher l'état d'intégrité et de capacité de tous les clusters SAN Array.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez afficher les informations de présentation de tous les clusters de baies SAN dans la vue Santé : tous les clusters et capacité : tous les clusters. De plus, vous pouvez afficher les détails sur la page Cluster / Health Details.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.
2. Assurez-vous que la colonne « personnalité » est affichée dans la vue **Santé : tous les clusters** ou ajoutez-la à l'aide de la commande **Afficher/Masquer**.

   Cette colonne affiche « toutes les baies SAN » pour tous les clusters de 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 de santé et la capacité de stockage dans ces clusters, cliquez sur le nom d'un cluster All SAN Array.

   Consultez les détails de l'onglet Santé, capacité et nœuds de la page Détails du cluster/intégrité

Affichage de la liste des nœuds et des détails

Vous pouvez utiliser la vue Santé : tous les nœuds pour afficher la liste des nœuds des clusters. Vous pouvez utiliser la page de détails Cluster / Health pour afficher des informations détaillées sur les nœuds faisant partie du cluster surveillé.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez afficher des informations détaillées, telles que l'état des nœuds, le cluster qui contient le nœud, les informations détaillées sur la capacité des agrégats (utilisée et totale) et les détails sur la capacité brute (utilisable, disponible, réserve et total). Vous pouvez également obtenir des informations sur les paires haute disponibilité, les tiroirs disques et les ports.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Nodes**.
2. Dans la vue **Santé : tous les nœuds**, cliquez sur le nœud dont vous souhaitez afficher les détails.

   Les informations détaillées du nœud sélectionné s'affichent sur la page des détails du cluster / intégrité. Le volet gauche affiche la liste des paires HA. Par défaut, les détails de la haute disponibilité sont ouverts, qui affiche les détails d'état de la haute disponibilité et les événements associés à la paire haute disponibilité sélectionnée.

3. Pour afficher d'autres détails sur le nœud, effectuez l'action appropriée :

Pour afficher…	Cliquez sur…
Détails sur les tiroirs disques	**Tiroirs disques**.
Informations relatives aux ports	**Ports**.

Pour plus d'informations, voir :

- "Performance : vue de tous les nœuds"
- "Affichage des valeurs d'IOPS disponibles du nœud et de l'agrégat"
- "Affichage des valeurs de capacité des nœuds et des performances des agrégats utilisées"

Génération d'un rapport d'inventaire du matériel pour le renouvellement du contrat

Vous pouvez générer un rapport contenant une liste complète des informations sur le cluster et le nœud, notamment les numéros de modèle du matériel et les numéros de série, les types et nombres de disques, les licences installées. Ce rapport est utile pour le renouvellement de contrats dans des sites sécurisés (« parc ») qui ne sont pas connectés à la plateforme NetApp Active IQ.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Nodes**.
2. Accédez à la vue **Health: All Nodes** ou **Performance: All Nodes**.
3. Sélectionnez **Rapports** > *** >** Rapport d'inventaire matériel*.

   Le rapport d'inventaire du matériel est téléchargé sous la forme d'un fichier .csv contenant des informations complètes à la date actuelle.

4. Indiquez ces informations à votre contact de support NetApp pour le renouvellement du contrat.

Affichage de la liste des VM de stockage et des détails

Depuis le point de vue Health: All Storage VM, vous pouvez surveiller l'inventaire des machines virtuelles de stockage (SVM). Vous pouvez utiliser la page Storage VM / Health pour afficher des informations détaillées sur les SVM surveillés.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez afficher des détails relatifs aux SVM, comme la capacité, l'efficacité et la configuration d'un SVM. Vous pouvez également afficher des informations sur les périphériques associés et les alertes associées pour ce SVM.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Storage VM**.
2. Choisir l'une des méthodes suivantes pour afficher les détails du SVM :
   - Pour afficher les informations relatives à l'état de santé de tous les SVM de tous les clusters, dans le menu View, sélectionnez Santé : vue tous les VM de stockage.
   - Pour afficher les informations complètes, cliquez sur le nom de la VM de stockage.

Vous pouvez également afficher les détails complets en cliquant sur **Afficher les détails** dans la boîte de dialogue Détails minimaux.

3. Afficher les objets liés à la SVM en cliquant sur **View Related** dans la boîte de dialogue des détails minimaux.

Informations connexes

- "VM de stockage : page Détails de l'état de santé"
- "Performances : vue de toutes les machines virtuelles de stockage"
- "Sécurité : vue anti-ransomware"
- "Affichage de l'état de sécurité pour les clusters et les VM de stockage"
- "Relation : vue de toutes les relations"

Affichage de la liste des agrégats et des détails

Depuis la vue Santé : tous les agrégats, vous pouvez surveiller votre inventaire des agrégats. La vue capacité : tous les agrégats vous permet d'afficher des informations sur la capacité et l'utilisation des agrégats de tous les clusters.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez afficher des informations détaillées, telles que la capacité et la configuration de l'agrégat, ou encore les informations sur le disque depuis la page de détails de l'agrégat/de l'intégrité. 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 **Storage** > **Aggregates**.
2. Choisir l'une des méthodes suivantes pour afficher les détails des agrégats :
   - Pour afficher des informations relatives à l'état de santé de tous les agrégats de tous les clusters, dans le menu View, sélectionnez Santé : vue tous les agrégats.
   - Pour afficher des informations sur la capacité et l'utilisation de tous les agrégats de tous les clusters, sélectionnez la vue capacité : 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 Détails minimaux.
3. Affichez les objets liés à l'agrégat en cliquant sur **Afficher lié** dans la boîte de dialogue Détails minimaux.

Informations connexes

- "Page Détails de l'agrégat/de l'intégrité"
- "Performance : vue de tous les agrégats"
- "Personnalisation des rapports de capacité d'agrégats"

Affichage des informations de capacité FabricPool

Vous pouvez afficher les informations relatives à la capacité FabricPool des clusters, des agrégats et des volumes dans les pages d'inventaire de la capacité et des performances, ainsi que les pages détaillées de ces objets. Ces pages affichent également des informations sur le miroir FabricPool lorsqu'un niveau miroir a été configuré.

Ces pages affichent des informations, telles que la capacité disponible sur le Tier de performance local et sur le Tier cloud, la capacité utilisée dans les deux tiers, des agrégats connectés à un niveau cloud, Et quels volumes implémentent les fonctionnalités FabricPool en déplaçant certaines informations vers le Tier cloud.

Lorsqu'un niveau cloud est mis en miroir vers un autre fournisseur de cloud (le « niveau miroir »), les deux niveaux de cloud sont affichés dans la page des détails agrégat/intégrité.

Étapes

1. Effectuez l'une des opérations suivantes :

Pour afficher les informations de capacité pour…	Procédez comme ça…
Clusters	a. Dans la vue capacité : tous les clusters, cliquez sur un cluster. b. Sur la page Cluster / Health details, cliquez sur l'onglet **Configuration**. L'écran affiche les noms de tous les niveaux de Cloud auxquels le cluster est connecté.
64 bits	a. Dans la vue capacité : tous les agrégats, cliquez sur un agrégat dans lequel le champ Type indique `SD (FabricPool)' ou 'HDD (FabricPool)'. b. Sur la page de détails agrégat / Santé, cliquez sur l'onglet **capacité**. L'écran affiche la capacité totale utilisée dans le Tier cloud. c. Cliquez sur l'onglet **Disk information**. L'affichage indique le nom du Tier cloud ainsi que la capacité utilisée. d. Cliquez sur l'onglet **Configuration**. L'écran affiche le nom du Tier cloud ainsi que d'autres informations détaillées sur le Tier cloud.

Pour afficher les informations de capacité pour…	Procédez comme ça…
Volumes	a. Dans la vue capacité : tous les volumes, cliquez sur un volume dont le nom de la règle apparaît dans le champ « politique de hiérarchisation ». b. Sur la page Détails du volume / Santé, cliquez sur l'onglet **Configuration**. L'affichage indique le nom de la règle de hiérarchisation FabricPool attribuée au volume.

2. Sur la page **Workload Analysis**, vous pouvez sélectionner « Cloud Tier View » dans la zone **Capacity Trend** pour afficher la capacité utilisée dans le Tier de performance local et dans le Tier cloud au cours du mois précédent.

Pour plus d'informations sur les agrégats FabricPool, reportez-vousà la section "Présentation des disques et des agrégats".

Affichage des détails du pool de stockage

Vous pouvez afficher les détails du pool de stockage afin de surveiller l'état du pool de stockage, le cache total et disponible, ainsi que les allocations utilisées et disponibles.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Cliquer sur le nom d'un agrégat.

   Les détails de l'agrégat sélectionné sont affichés.

3. Cliquez sur l'onglet **Disk information**.

   Les informations détaillées du disque s'affichent.

   > La table cache s'affiche uniquement lorsque l'agrégat sélectionné utilise un pool de stockage.

4. Dans la table cache, déplacez le pointeur sur le nom du pool de stockage requis.

   Les détails du pool de stockage s'affichent.

Affichage de la liste des volumes et des détails

Depuis la vue Health: All volumes, vous pouvez surveiller votre inventaire des volumes. Le vue capacité : tous les volumes vous permet d'afficher des informations sur la capacité et l'utilisation des volumes d'un cluster.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez également utiliser la page des détails Volume / intégrité 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 d'un volume spécifique.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **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 View, sélectionnez Health: All volumes View.
   - Pour afficher des informations détaillées sur la capacité et l'utilisation des volumes d'un cluster, sélectionnez la vue Capacity : tous les volumes dans le menu View.
   - Pour afficher les informations complètes, cliquez sur le nom du volume.

     Vous pouvez également afficher les détails complets en cliquant sur **Afficher les détails** dans la boîte de dialogue Détails minimaux.
3. **Facultatif:** Affichez les objets liés au volume en cliquant sur **Voir connexe** dans la boîte de dialogue Détails minimaux.

Informations connexes

- "Volume : page de détails de santé"
- "Performance : vue de 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"

Affichage des détails sur les partages NFS

Vous pouvez afficher des informations détaillées sur tous les partages NFS, notamment son état, le chemin associé au volume (volumes FlexGroup ou volumes FlexVol), les niveaux d'accès des clients aux partages NFS et l'export policy 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 Storage VM / Health details pour afficher tous les partages NFS sur un SVM spécifique.

Ce dont vous aurez besoin

- La licence NFS doit être activée sur le cluster.
- Les interfaces réseau servant les partages NFS doivent être configurées.
- Vous devez avoir le rôle opérateur, administrateur d'applications ou 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 pour un SVM particulier.

Pour…	Suivez ces étapes…
Afficher tous les partages NFS	Cliquez sur **stockage** > **partages NFS**
Affichage des partages NFS pour un seul SVM	a. Cliquez sur **Storage** > **Storage VM** b. Cliquer sur le SVM pour lequel vous souhaitez afficher les détails des partages NFS. c. Dans la page de détails VM de stockage / intégrité, 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".

Affichage des détails sur les partages SMB/CIFS

Vous pouvez afficher les détails de tous les partages SMB/CIFS, notamment le nom du partage, le chemin de jonction, l'contenant les objets, les paramètres de sécurité et les règles 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 Storage VM / Health details pour afficher tous les partages SMB sur un SVM spécifique.

Ce dont vous aurez besoin

- La licence CIFS doit être activée sur le cluster.
- Les interfaces réseau servant les partages SMB/CIFS doivent être configurées.
- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Les partages des 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.

Pour…	Suivez ces étapes…
Afficher tous les partages SMB/CIFS	Cliquez sur **stockage** > **partages SMB**
Affichage des partages SMB/CIFS pour un seul SVM	a. Cliquez sur **Storage** > **Storage VM** b. Cliquer sur le SVM pour lequel vous souhaitez afficher les détails du partage SMB/CIFS. c. Dans la page de détails VM de stockage / intégrité, cliquez sur l'onglet **partages SMB**.

Pour plus d'informations, voir "Provisionnement des partages de fichiers CIFS et NFS à l'aide d'API".

Affichage de la liste des copies Snapshot

Vous pouvez afficher la liste des copies Snapshot d'un volume sélectionné. Vous pouvez utiliser la liste des copies Snapshot pour calculer la quantité d'espace disque pouvant être récupérée si une ou plusieurs copies Snapshot sont supprimées, et vous pouvez supprimer les copies Snapshot si nécessaire.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Le volume contenant les copies Snapshot doit être en ligne.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans la vue **Health: All volumes**, sélectionnez le volume qui contient les copies Snapshot que vous souhaitez afficher.
3. Dans la page **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 en regard de **copies snapshot**.

   Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

Informations connexes

"Page Health/Volume"

Suppression des copies Snapshot

Vous pouvez supprimer une copie Snapshot pour économiser de l'espace disque, libérer de l'espace disque, ou supprimer la copie Snapshot si elle n'est plus nécessaire.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Le volume doit être en ligne.

Pour supprimer une copie Snapshot occupée ou verrouillée, vous devez avoir libéré cette copie de l'application qu'elle utilisait.

- Vous ne pouvez pas supprimer la copie Snapshot de base d'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 et la `Busy` 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 Snapshot est verrouillée et requise pour la prochaine mise à jour.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans la vue **Health: All volumes**, sélectionnez le volume qui contient les copies Snapshot que vous souhaitez afficher.

   La liste des copies Snapshot s'affiche.

3. Dans la page **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 en regard de **copies snapshot**.

   Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

5. Dans la vue **copies snapshot**, sélectionnez les copies Snapshot à supprimer, puis cliquez sur **Supprimer les copies sélectionnées**.

Calcul de 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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Le volume doit être en ligne.
- Le volume doit être un volume FlexVol. Cette fonctionnalité n'est pas prise en charge avec les volumes FlexGroup.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans la vue **Health: All volumes**, sélectionnez le volume qui contient les copies Snapshot que vous souhaitez afficher.

   La liste des copies Snapshot s'affiche.

3. Dans la page **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 en regard de **copies snapshot**.

   Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

5. Dans la vue **copies snapshot**, sélectionnez les copies Snapshot pour lesquelles vous souhaitez calculer l'espace récupérable.
6. Cliquez sur **calculer**.

   L'espace récupérable (en pourcentage, et en Ko, Mo, Go, etc.) sur le volume s'affiche.

7. Pour recalculer l'espace récupérable, sélectionnez les copies Snapshot requises et cliquez sur **Recalculer**.

Description des fenêtres et boîtes de dialogue d'objets de cluster

Vous pouvez afficher tous vos clusters et objets de cluster à partir de la page de stockage objet respective. Vous pouvez également consulter les détails à partir de la page de détails des objets de stockage correspondante. Vous pouvez désormais lancer l'interface utilisateur System Manager à partir des sections DE STOCKAGE et DE PROTECTION suivantes de L'INVENTAIRE.

- Pages Cluster Inventory, Cluster Health et Cluster Performance
- Pages d'inventaire des agrégats, d'état des agrégats et de performances agrégées
- Pages Inventaire des volumes, Santé des volumes et performances des volumes
- Pages Inventaire des nœuds et performances des nœuds
- StorageVM Inventory, StorageVM Health et StorageVM Performance pages
- Pages de relation de protection

Tâches et workflows d'état de Unified Manager communs

Parmi les workflows et tâches d'administration courants associés à Unified Manager figurent la sélection des clusters de stockage à contrôler, le diagnostic des conditions qui affectent négativement la disponibilité des données, la capacité et la protection, la restauration des données perdues, la configuration et la gestion des volumes, le regroupement et l'envoi de données de diagnostic au support technique (si nécessaire).

Unified Manager permet aux administrateurs du 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.

Les problèmes les plus importants liés à un cluster, à un SVM (Storage Virtual machine), à un volume ou à un volume FlexGroup qui affectent la capacité de stockage ou la disponibilité des données des objets de stockage gérés sont affichés dans les graphiques et événements d'état du système sur la page Tableau de bord. Lorsque des problèmes critiques sont identifiés, cette page fournit des liens permettant de prendre en charge les processus de dépannage appropriés.

Unified Manager peut également être inclus dans des flux de production comprenant des outils de gestion associés, tels que OnCommand Workflow Automation (WFA), pour prendre en charge la configuration directe des ressources de stockage.

Ce document décrit les workflows courants relatifs aux tâches administratives suivantes :

- Diagnostic et gestion des problèmes de disponibilité

  Si une défaillance matérielle ou des problèmes de configuration des ressources de stockage entraînent l'affichage des 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, consulter les 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 qui sont

surveillées. Pour "Présentation de la surveillance des performances Active IQ Unified Manager"plus d'informations, reportez-vous à la section.

- Diagnostic et gestion des problèmes de capacité des volumes

  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 relatives à la capacité de stockage du volume affecté, consulter des conseils de dépannage et attribuer la résolution des problèmes à d'autres administrateurs.

- Configuration, contrôle et diagnostic des problèmes de relation au niveau de la protection

  Après avoir créé et configuré des relations de protection, les administrateurs du stockage peuvent voir les problèmes potentiels liés aux relations de protection, l'état actuel des relations de protection, les informations de réussite de la tâche de protection actuelle et historique concernant les relations affectées, ainsi que des conseils de résolution de problèmes. Pour "Création, surveillance et résolution des problèmes de relations de protection"plus d'informations, reportez-vous à la section.

- Création de fichiers de sauvegarde et restauration de données à partir de fichiers de sauvegarde.
- Association d'objets de stockage avec des annotations

  En associant les objets de stockage aux annotations, les administrateurs du stockage peuvent filtrer et afficher les événements associés aux objets de stockage. Ainsi, les administrateurs du stockage peuvent hiérarchiser et résoudre les problèmes associés aux événements.

- Utilisation d'API REST pour vous aider à gérer les clusters en visualisant les informations d'état, de capacité et de performance collectées par Unified Manager. Voir "Mise en route des API REST de Active IQ Unified Manager" pour plus d'informations.
- Envoi d'un pack support au support technique

  Les administrateurs de stockage peuvent récupérer et envoyer un pack au support technique à l'aide de la console de maintenance. Les packs de support doivent être envoyés au support technique si le problème nécessite un diagnostic et une résolution de problèmes plus détaillés que ceux communiqués par un message AutoSupport.

Surveillance et résolution des problèmes de disponibilité des données

Unified Manager contrôle la fiabilité avec laquelle les utilisateurs autorisés peuvent accéder aux données stockées, vous informe des conditions qui les bloquent ou les empêchent d'accéder, et vous aide à diagnostiquer ces conditions ainsi qu'à attribuer et suivre leur résolution.

Les rubriques relatives au workflow de disponibilité de cette section décrivent des exemples de la façon dont un administrateur du stockage peut utiliser l'interface utilisateur Web Unified Manager pour détecter, diagnostiquer et attribuer des conditions matérielles et logicielles de résolution qui affectent négativement la disponibilité des données.

Recherche et résolution des problèmes de liaison d'interconnexion de basculement de stockage

Ce workflow fournit un exemple de numérisation, d'évaluation et de résolution des problèmes de liaison d'interconnexion de basculement du stockage arrêté. Dans ce scénario, vous êtes administrateur à l'aide de Unified Manager pour rechercher les

risques de basculement du stockage avant de lancer la mise à niveau d'une version de ONTAP sur vos nœuds.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Si les interconnexions du basculement du stockage entre les paires haute disponibilité échouent dans le cadre d'une tentative de mise à niveau sans interruption, la mise à niveau échoue. Il est donc courant que l'administrateur surveille et confirme la fiabilité du basculement du stockage sur les nœuds de cluster dont la mise à niveau est prévue avant le début d'une mise à niveau.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.
2. Dans la page d'inventaire **Event Management**, sélectionnez **Active Availability Events**.
3. En haut de la colonne **Event Management** Inventory page **Name**, cliquez ⚌ et entrez `*failover` dans la zone de texte pour limiter l'événement à afficher aux événements de basculement de stockage.

   Tous les événements passés relatifs aux conditions de basculement du stockage sont affichés.

   Dans ce scénario, Unified Manager affiche l'événement, « Storage Failover Interconnect one or more Links Down » dans sa section Availability incidents.

4. Si un ou plusieurs événements liés au basculement de stockage sont affichés sur la page d'inventaire **Event Management**, effectuez les opérations suivantes :

   a. Cliquez sur le lien du titre de l'événement pour afficher les détails de l'événement.

      Dans cet exemple, vous cliquez sur le titre de l'événement "Storage Failover Interconnect one or more Links Down".

   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.
      - Attribuez l'événement à un administrateur.
      - Accuser réception de l'événement.

Informations connexes

"Page de détails de l'événement"

"Fonctionnalités et rôles utilisateur de Unified Manager"

Effectuer une action corrective pour les liaisons d'interconnexion de basculement du 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 éventuelle du problème.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Dans cet exemple, le récapitulatif des événements disponible sur la page des détails de l'événement contient les informations suivantes concernant la condition d'interruption de la liaison d'interconnexion de basculement du 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)
```

L'exemple d'informations d'événement indique qu'une liaison 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. Une liaison étant active, le RDMA (Remote Dynamic Memory Access) fonctionne toujours et une tâche de basculement du stockage peut continuer à réussir.

Cependant, pour vous assurer que la protection contre les liaisons qui échouent et contre le basculement de stockage est totalement désactivée, vous décidez de continuer à diagnostiquer la cause de la panne de Link1.

Étapes

1. Dans la page **Event** details, vous pouvez cliquer sur le lien vers l'événement spécifié dans le champ Source pour obtenir plus de détails sur d'autres événements qui peuvent être liés à la condition d'interconnexion de basculement de stockage.

   Dans cet exemple, la source de l'événement est le nœud nommé aardvark. Lorsque vous cliquez sur ce nom de nœud, les détails de haute disponibilité de la paire HA affectée, aardvark et bonobo, apparaissent sur l'onglet nœuds de la page des détails Cluster/Santé et affichent les autres événements survenus récemment sur la paire HA affectée.

2. Consultez les **Détails HA** pour plus d'informations sur l'événement.

   Dans cet exemple, les informations pertinentes se trouvent dans le tableau Evénements. Le tableau montre l'événement "Storage Failover Connection one or more Link Down", l'heure à laquelle l'événement a été généré, et encore une fois, le nœud d'origine de cet événement.

En utilisant les informations d'emplacement du nœud dans les détails de la haute disponibilité, demander ou effectuer personnellement une inspection physique et la réparation du problème de basculement du stockage sur les nœuds de la paire haute disponibilité affectés.

Informations connexes

"Page de détails de l'événement"

"Fonctionnalités et rôles utilisateur de Unified Manager"

Résolution des problèmes de mise hors ligne des volumes

Ce flux de travail fournit un exemple de l'évaluation et de la résolution d'un événement hors ligne qu'Unified Manager peut afficher sur la page d'inventaire Event Management. Dans ce scénario, vous êtes administrateur qui utilise Unified Manager pour résoudre un ou plusieurs événements de mise hors ligne des volumes.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Les volumes peuvent être signalés hors ligne pour plusieurs raisons :

- L'administrateur du SVM a délibérément mis le volume hors ligne.
- Le nœud de cluster d'hébergement du volume est en panne et le basculement du stockage vers sa paire haute disponibilité partenaire a également échoué.
- La machine virtuelle de stockage (SVM) d'hébergement du volume est arrêtée car le nœud hébergeant le volume root de ce SVM est en panne.
- L'agrégat d'hébergement du volume est en panne due à une défaillance simultanée de deux disques RAID.

Vous pouvez utiliser la page d'inventaire Event Management et les pages Cluster/Health, Storage VM/Health et Volume/Health pour confirmer ou supprimer une ou plusieurs de ces possibilités.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.
2. Dans la page d'inventaire **Event Management**, sélectionnez **Active Availability Events**.
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 n'importe quelle indication que l'administrateur du SVM a mis le volume en question hors ligne.
5. Sur la page **Event** details, vous pouvez consulter les informations d'une ou plusieurs des tâches suivantes :
   - Consulter les informations affichées dans le champ cause pour obtenir un guidage de diagnostic possible.

     Dans cet exemple, les informations du champ cause vous indiquent uniquement que le volume est hors ligne.

   - Vérifier dans la zone Notes et mises à jour si l'administrateur du 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.

- Attribuez l'événement à un administrateur.
- Reconnaissez l'événement ou, le cas échéant, marquez-le comme résolu.

Exécution d'actions de diagnostic pour des conditions hors ligne de volume

Après avoir accédé à la page des détails du volume/de l'état d'intégrité d'un volume signalé comme étant hors ligne, vous pouvez rechercher des informations supplémentaires utiles pour diagnostiquer la condition hors ligne du volume.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Si le volume signalé n'a pas été délibérément hors ligne, ce volume peut être hors ligne pour plusieurs raisons.

À partir de la page d'informations sur le volume / l'intégrité du volume hors ligne, vous pouvez accéder à d'autres pages et volets afin de confirmer ou d'éliminer les causes possibles :

- Cliquez sur les liens de la page **Volume / Santé** pour déterminer si le volume est hors ligne, car son nœud hôte est en panne et le basculement du stockage vers son partenaire de paire haute disponibilité a également échoué.

  Voir "Pour déterminer si une condition de volume hors ligne est causée par un nœud défaillant".

- 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 ce SVM est en panne.

  Voir "Détermination d'un volume hors ligne et arrêt d'un SVM parce qu'un nœud est arrêté".

- Cliquez sur les liens de la page **Volume / Santé** pour déterminer si le volume est hors ligne en raison de disques cassés dans son agrégat hôte.

  Voir "Détermination de la disponibilité d'un volume à cause de disques rompus dans un agrégat".

Informations connexes

"Fonctionnalités et rôles utilisateur de Unified Manager"

Détermination d'un volume hors ligne parce que son nœud hôte est arrêté

Vous pouvez utiliser l'interface utilisateur Web d'Unified Manager pour confirmer ou supprimer la possibilité qu'un volume soit hors ligne, car le nœud hôte est en panne et que le basculement du stockage vers son partenaire de paire haute disponibilité n'a pas réussi.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Pour déterminer si la condition de hors ligne du volume est due à une défaillance du nœud d'hébergement et à un basculement de stockage qui a échoué par la suite, effectuez les opérations suivantes :

Étapes

1. Localisez et cliquez sur le lien hypertexte affiché sous SVM dans le volet **Related Devices** de la page de détails **Volume / Santé** du volume hors ligne.

   La page des détails VM de stockage / intégrité affiche des informations sur le volume offline du serveur virtuel de stockage (SVM)

2. Dans le volet **Related Devices** de la page **Storage VM / Health** details, localisez 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 la SVM.

3. Dans l'en-tête de colonne **Health: All volumes** View State , cliquez sur le symbole de filtre , puis sélectionnez l'option **Offline**.

   Seuls les volumes du SVM dont l'état est hors ligne sont répertoriés.

4. Dans la vue Santé : tous les volumes, cliquez sur le symbole de grille , puis sélectionnez l'option **nœuds de cluster**.

   Vous devrez peut-être faire défiler la zone de sélection de grille pour localiser l'option **Cluster Nodes**.

   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 la colonne nœud de cluster, cliquez sur le nom de son nœud d'hébergement.

   L'onglet nœuds de la page Cluster / Health details affiche l'état de la paire HA de nœuds auxquels le nœud d'hébergement appartient. L'état du nœud d'hébergement et le succès de toute opération de basculement de cluster sont indiqués à l'écran.

Une fois que vous avez confirmé que le volume est hors ligne car le nœud hôte est en panne et que le basculement du stockage vers le partenaire de la paire haute disponibilité a échoué, contactez l'administrateur ou l'opérateur approprié pour redémarrer manuellement le nœud d'arrêt et résoudre le problème de basculement du stockage.

Détermination d'un volume hors ligne et de son SVM arrêté, car un nœud est arrêté

Vous pouvez utiliser l'interface utilisateur Web Unified Manager pour confirmer ou éliminer tout risque qu'un volume soit hors ligne, car sa machine virtuelle de stockage hôte (SVM) est arrêtée du fait du nœud hébergeant le volume racine de ce SVM.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Pour déterminer si le volume hors ligne est provoqué l'arrêt de son SVM hôte car le nœud hébergeant le volume root de ce SVM est arrêté, effectuer les actions suivantes :

Étapes

1. Localisez et cliquez sur le lien hypertexte affiché sous le SVM dans le volet **Related Devices** de la page de détails **Volume / Santé** du volume hors ligne.

La page de détails Storage VM / Health affiche l'état « en cours » ou « en surface » du SVM d'hébergement. Si le statut de la SVM est exécuté, alors la condition de volume offline n'est pas provoquée par le nœud hébergeant le volume root de cette SVM en panne.

2. Si l'état du SVM est arrêté, cliquer sur **View SVM** pour mieux identifier la cause de l'arrêt du SVM d'hébergement.
3. Sur l'en-tête de colonne du SVM de la vue **Health: All Storage VM**, cliquer sur le symbole de filtre puis taper le nom du SVM arrêté.

   Les informations pour ce SVM sont présentées 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 Root est ajoutée à l'inventaire du SVM et affiche le nom du volume root du SVM stopped.

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 root du SVM est (en ligne), la condition hors ligne du volume d'origine n'est pas générée, car le nœud hébergeant le volume root de ce SVM est arrêté.

6. Si le statut du volume root du SVM est (Offline), localiser et cliquer sur le lien hypertexte affiché sous agrégat dans le volet Devices associés de la page details du volume root du SVM / Health.
7. Localisez et cliquez sur le lien hypertexte affiché sous noeud dans le volet **périphériques associés** de la page de détails **agrégat / Santé** de l'agrégat.

   L'onglet nœuds de la page des détails Cluster / Health affiche l'état de la paire HA de nœuds vers lequel le nœud d'hébergement du volume root du SVM appartient. L'état du nœud est indiqué à l'écran.

Après avoir confirmé que la condition de mise hors ligne du volume est provoquée par une condition de SVM hôte hors ligne de ce volume, qui lui-même est causée par le nœud qui héberge le volume racine de ce SVM en panne, contactez l'administrateur ou l'opérateur approprié pour redémarrer manuellement le nœud arrêté.

Détermination de la disponibilité d'un volume à cause de disques rompus dans un agrégat

L'interface utilisateur Web de Unified Manager vous permet de confirmer ou d'éliminer toute possibilité qu'un volume soit hors ligne, car les problèmes de disque RAID ont mis hors ligne son agrégat hôte.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Pour déterminer si la condition de mise hors ligne du volume est provoquée par des problèmes de disque RAID qui chargent la mise hors ligne de l'agrégat d'hébergement, effectuez les opérations suivantes :

Étapes

1. Localisez et cliquez sur le lien hypertexte affiché sous agrégat dans le volet **périphériques associés** de la page de détails **Volume / Santé**.

   La page des détails de l'agrégat/intégrité affiche le statut en ligne ou hors ligne de l'agrégat

d'hébergement. Si l'état de l'agrégat est en ligne, les problèmes de disque RAID ne sont pas à l'origine du volume mis hors ligne.

2. Si l'état de l'agrégat est hors ligne, cliquez sur **Disk information** et recherchez les événements de disque rompu dans la liste **Events** de l'onglet **Disk information**.
3. Pour identifier davantage les disques rompus, cliquez sur le lien hypertexte affiché sous noeud dans le volet **périphériques associés**.

   La page Détails du cluster / Santé s'affiche.

4. Cliquez sur **disques**, puis sélectionnez **Broken** dans le volet **filtres** pour afficher la liste de tous les disques dont l'état est rompu.

   Si les disques sont état Broken et ont provoqué l'état hors ligne de l'agrégat hôte, le nom de l'agrégat est affiché dans la colonne impacté de l'agrégat.

Après avoir confirmé que le volume était provoqué par des disques RAID cassés et les agrégats hôtes hors ligne qui en découlent, contactez l'administrateur ou l'opérateur approprié pour remplacer manuellement les disques défectueux et remettre l'agrégat en ligne.

Résoudre les problèmes de capacité

Ce flux de travail fournit un exemple de résolution d'un problème de capacité. Dans ce scénario, vous êtes administrateur ou opérateur et accédez à la page Unified ManagerDashboard pour voir si l'un des objets de stockage surveillés présente des problèmes de capacité. Vous voulez déterminer la cause possible du problème et la résolution de celui-ci.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Sur la page Tableau de bord, vous recherchez un événement d'erreur « espace de volume plein » dans le panneau capacité sous la liste déroulante événements.

Étapes

1. Dans le panneau **Capacity** de la page **Dashboard**, cliquez sur le nom de l'événement Volume Space Full error.

   La page Détails de l'événement pour l'erreur s'affiche.

2. À partir de la page de détails **Event**, vous pouvez effectuer une ou plusieurs des tâches suivantes :
   - Passez en revue le message d'erreur dans le champ cause et cliquez sur les suggestions sous actions correctives suggérées pour examiner les descriptions des éventuelles corrections.
   - Cliquez sur le nom de l'objet, dans ce cas un volume, dans le champ Source pour obtenir des détails sur l'objet.
   - Recherchez les notes qui ont peut-être été ajoutées à ce sujet.
   - Ajoutez une note à l'événement.
   - Attribuez l'événement à un autre utilisateur.
   - Accuser réception de l'événement.

- Marquer l’événement comme résolu.

Informations connexes

"Page de détails de l’événement"

Exécution de suggestions d’actions correctives pour un volume complet

Après avoir reçu un événement d’erreur « Volume Space Full », vous passez en revue les mesures correctives proposées sur la page Détails de l’événement et décidez d’effectuer l’une des actions suggérées.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.

Un utilisateur possédant n’importe quel rôle peut effectuer toutes les tâches de ce flux de travail qui utilisent Unified Manager.

Dans cet exemple, vous avez vu un événement Volume Space Full error sur la page d’inventaire Unified ManagerEvent Management et vous avez cliqué sur le nom de l’événement.

Les actions correctives possibles pour un volume complet sont les suivantes :

- Activation de la croissance automatique, de la déduplication ou de la compression sur le volume
- Redimensionnement ou déplacement du volume
- Suppression ou déplacement de données du volume

Bien que toutes ces actions doivent être effectuées depuis ONTAP System Manager ou l’interface de ligne de commandes de ONTAP, Unified Manager permet de trouver les informations qui vous permettront éventuellement de déterminer les actions à effectuer.

Étapes

1. Dans la page **Event** details, cliquez sur le nom du volume dans le champ Source pour afficher les détails du volume affecté.
2. Sur la page des détails **Volume/Santé**, cliquez sur **Configuration** et vérifiez que la déduplication et la compression sont déjà activées sur le volume.

   Vous décidez de redimensionner le volume.

3. Dans le volet **Related Devices**, vous cliquez sur le nom de l’agrégat d’hébergement pour voir si l’agrégat peut accueillir un volume plus important.
4. Sur la page **agrégat/Santé**, l’agrégat hébergeant le volume complet présente une capacité non utilisée suffisante. Par conséquent, vous pouvez utiliser ONTAP System Manager pour redimensionner le volume, ce qui lui donne davantage de capacité.

Informations connexes

"Page de détails de l’événement"

Gestion des seuils de santé

Vous pouvez configurer les valeurs des seuils de santé globaux de tous les agrégats, volumes et qtrees pour assurer le suivi des violations de seuils de santé.

Quels sont les seuils d'état de santé de la capacité de stockage

Un seuil d'état de santé de la capacité de stockage est le point à partir duquel le serveur Unified Manager génère des événements pour signaler un problème de capacité au niveau des objets de stockage. Vous pouvez configurer des alertes pour envoyer des notifications chaque fois que de tels événements se produisent.

Les seuils d'état de la capacité de stockage de tous les agrégats, volumes et qtrees sont définis sur les valeurs par défaut. Vous pouvez modifier les paramètres requis pour un objet ou un groupe d'objets.

Configuration des paramètres de seuil de santé global

Vous pouvez configurer des conditions seuils de santé globaux pour la capacité, la croissance, la réserve Snapshot, les quotas et les inodes afin de surveiller de façon efficace la taille de l'agrégat, du volume et du qtree. Vous pouvez également modifier les paramètres de génération d'événements pour des seuils de décalage supérieurs.

Les paramètres de seuil de santé global s'appliquent à tous les objets auxquels ils sont associés, comme les agrégats, les volumes, etc. Lorsque les seuils sont croisés, un événement est généré et, si des alertes sont configurées, une notification d'alerte est envoyée. Les valeurs par défaut des seuils sont définies sur les valeurs recommandées, mais vous pouvez les modifier pour générer des événements à intervalles afin de répondre à vos besoins spécifiques. Lorsque les seuils sont modifiés, les événements sont générés ou obsolètes dans le cycle de surveillance suivant.

Les paramètres des seuils de santé globale sont accessibles depuis la section seuils d'événements du menu de navigation gauche. Vous pouvez également modifier les paramètres de seuil 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 des seuils de santé globaux des agrégats".

  Vous pouvez configurer les paramètres de seuil de santé pour la capacité, la croissance et les copies Snapshot de tous les agrégats afin d'assurer le suivi de tout seuil de non-respect.

- Pour plus d'informations, voir "Configuration des valeurs de seuil de contrôle global du volume".

  Vous pouvez modifier les paramètres du seuil de santé pour la capacité, les copies Snapshot, les quotas qtree, la croissance du volume, l'espace de réserve de remplacement, et des inodes pour tous les volumes afin de suivre les violations de seuil éventuelles.

- Pour plus d'informations, voir "Configuration des valeurs des seuils de santé des qtrees globaux".

  Vous pouvez modifier les paramètres du seuil de santé de la capacité de tous les qtrees pour assurer le suivi d'une éventuelle violation de seuil.

- Pour plus d'informations, voir "Modification des paramètres de seuil d'intégrité de décalage pour les relations de protection non gérées".

  Vous pouvez augmenter ou diminuer le pourcentage de temps de décalage d'avertissement ou d'erreur

afin que les événements soient générés à des intervalles plus adaptés à vos besoins.

Configuration des valeurs des seuils de santé globaux des agrégats

Vous pouvez configurer les valeurs des seuils de santé globaux de tous les agrégats pour suivre tout seuil d'atteinte. Les événements appropriés sont générés pour les violations de seuil et vous pouvez prendre des mesures préventives basées sur ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de bonnes pratiques pour les seuils applicables à tous les agrégats surveillés.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Lorsque vous configurez globalement les options, 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 de l'agrégat sont considérés comme enfreintes en fonction de la taille maximale du volume définie par la croissance automatique, non pas en fonction de la taille du volume initial.

Les valeurs de seuil de santé ne sont pas applicables à l'agrégat racine du nœud.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **seuils d'événements** > **agrégat**.
2. Configurez les valeurs de seuil appropriées pour la capacité, la croissance et les copies Snapshot.
3. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Configuration des valeurs de seuil de contrôle global du volume

Vous pouvez configurer les valeurs de seuil de santé global pour tous les volumes afin de suivre toute violation de seuil. Les événements appropriés sont générés pour les atteintes aux seuils de santé et vous pouvez prendre des mesures préventives basées sur ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de la meilleure pratique pour les seuils qui s'appliquent à tous les volumes surveillés.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

La plupart des options de seuil ont des valeurs par défaut pour une meilleure surveillance. Cependant, vous pouvez modifier les valeurs en fonction des besoins de votre environnement.

Notez que lorsque la croissance automatique est activée sur un volume que les seuils de capacité sont considérés comme enfreintes en fonction de la taille maximale du volume définie par Autogrow, et non pas en fonction de la taille du volume initial.

> La valeur par défaut de 1000 copies Snapshot s'applique uniquement aux volumes FlexVol lorsque la version de ONTAP est 9.4 ou supérieure, et aux volumes FlexGroup lorsque la version de ONTAP est 9.8 ou supérieure. Pour les clusters installés avec d'anciennes versions du logiciel ONTAP, le nombre maximal est de 250 copies Snapshot par volume. Pour ces versions plus anciennes, Unified Manager interprète ce numéro 1000 (et d'autres nombres entre 1000 et 250) comme 250 ; autrement dit, vous continuerez à recevoir des événements lorsque le nombre de copies Snapshot atteint 250. Si vous souhaitez définir ce seuil sur moins de 250 pour ces versions antérieures, vous devez définir le seuil sur 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'événements** > **Volume**.
2. Configurez les valeurs de seuil appropriées pour la capacité, les copies Snapshot, les quotas qtree, la croissance du volume et les inodes.
3. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Configuration des valeurs des seuils de santé des qtrees globaux

Vous pouvez configurer les valeurs du seuil de santé global pour tous les qtrees afin de suivre toute violation de seuil. Les événements appropriés sont générés pour les atteintes aux seuils de santé et vous pouvez prendre des mesures préventives basées sur ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de bonnes pratiques pour les seuils qui s'appliquent à tous les qtrees surveillés.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 utilisateur ou un quota de groupe a dépassé le seuil.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **seuils d'événements** > **qtree**.
2. Configurez les valeurs de seuil de capacité appropriées.
3. Cliquez sur **Enregistrer**.

Configuration des paramètres de seuil de décalage pour les relations de protection non gérées

Vous pouvez modifier les paramètres de seuil d'avertissement de décalage global par défaut et d'intégrité des erreurs pour les relations de protection non gérées afin que les événements soient générés à des intervalles adaptés à vos besoins.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Le temps de décalage ne doit pas dépasser l'intervalle de planification de transfert défini. Par exemple, si la planification de transfert est horaire, la durée de décalage ne doit pas dépasser une heure. Le seuil de décalage indique un pourcentage que le temps de décalage ne doit pas dépasser. Dans l'exemple d'une heure, si le seuil de décalage est défini sur 150 %, vous recevrez un événement lorsque le temps de décalage est supérieur à 1.5 heures.

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'événements** > **relation**.
2. Augmentez ou réduisez le pourcentage de temps d'avertissement ou de retard 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"

Modification des paramètres de seuil d'intégrité des agrégats individuels

Vous pouvez modifier les paramètres du seuil de santé pour la capacité globale, la croissance et les copies Snapshot 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

En fonction des modifications apportées aux valeurs de seuil, les événements sont générés ou obsolètes dans le cycle de surveillance suivant.

Lorsque la croissance automatique est activée sur les volumes qui résident sur l'agrégat, les seuils de capacité de l'agrégat sont considérés comme enfreintes en fonction de la taille maximale du volume définie par la croissance automatique, non pas en fonction de la taille du volume initial.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.

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 d'agrégats**, modifiez les paramètres de seuil de l'une des options suivantes : capacité, croissance ou copies Snapshot en cochant la case appropriée, puis en modifiant les paramètres.
4. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Modification des paramètres de seuil d'intégrité du volume individuel

Vous pouvez modifier les paramètres du seuil d'intégrité pour la capacité du volume, la croissance, les quotas 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

En fonction des modifications apportées aux valeurs de seuil, les événements sont générés ou obsolètes dans le cycle de surveillance suivant.

Notez que lorsque la croissance automatique est activée sur un volume que les seuils de capacité sont considérés comme enfreintes en fonction de la taille maximale du volume définie par Autogrow, et non pas en fonction de la taille du volume initial.

> La valeur par défaut de 1000 copies Snapshot s'applique uniquement aux volumes FlexVol lorsque la version de ONTAP est 9.4 ou supérieure, et aux volumes FlexGroup lorsque la version de ONTAP est 9.8 ou supérieure. Pour les clusters installés avec d'anciennes versions du logiciel ONTAP, le nombre maximal est de 250 copies Snapshot par volume. Pour ces versions plus anciennes, Unified Manager interprète ce numéro 1000 (et d'autres nombres entre 1000 et 250) comme 250 ; autrement dit, vous continuerez à recevoir des événements lorsque le nombre de copies Snapshot atteint 250. Si vous souhaitez définir ce seuil sur moins de 250 pour ces versions antérieures, vous devez définir le seuil sur 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 **Storage** > **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'une des options suivantes : capacité, copies Snapshot, quota qtree, croissance ou inodes en cochant la case appropriée, puis en modifiant les paramètres.
4. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Modification des paramètres de seuil de santé des qtrees individuels

Vous pouvez modifier les paramètres du seuil de santé pour la capacité qtree d'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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

En fonction des modifications apportées aux valeurs de seuil, les événements sont générés ou obsolètes dans le cycle de surveillance suivant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **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 de qtree**, modifiez les seuils de capacité du qtree ou des qtrees sélectionnés et cliquez sur **Enregistrer**.

> Vous pouvez également définir des seuils qtree individuels depuis l'onglet qtrees de la page Storage VM / Health Details.

Gestion des objectifs de sécurité des clusters

Unified Manager fournit un tableau de bord identifiant la sécurité de vos clusters ONTAP, de vos serveurs de stockage virtuels (SVM) et de vos volumes à partir des recommandations définies dans le *guide NetApp de renforcement de la sécurité des environnements ONTAP 9*.

L'objectif du tableau de bord de sécurité est de fournir des informations sur les zones dans lesquelles les clusters ONTAP ne sont pas en adéquation avec les instructions recommandées par NetApp afin de résoudre ces problèmes potentiels. Dans la plupart des cas, vous pouvez résoudre les problèmes à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP. Il se peut que votre organisation ne suive pas toutes les recommandations. Dans certains cas, vous n'aurez donc pas besoin d'apporter de modifications.

Consultez le "Guide NetApp sur le renforcement de la sécurité des environnements ONTAP 9" (TR-4569) pour des recommandations et 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 la gestion des événements et configurer les alertes pour ces événements de sorte que votre administrateur de stockage soit averti en cas de nouveaux événements de sécurité.

Pour plus d'informations, voir "Quels sont les critères de sécurité évalués".

Quels sont les critères de sécurité évalués

De manière générale, les critères de sécurité des clusters ONTAP, des serveurs de stockage virtuels (SVM) et des volumes sont évalués avec les recommandations définies dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9*.

Voici quelques-unes des vérifications de sécurité :

- Indique si un cluster utilise une méthode d'authentification sécurisée, par exemple SAML
- les communications des clusters utilisant des canaux de connexion sont chiffrées
- Indique si le journal des audits d'un serveur virtuel de stockage est activé
- que le chiffrement logiciel ou matériel soit activé pour vos volumes

Reportez-vous aux rubriques relatives aux catégories de conformité et "Guide NetApp sur le renforcement de la sécurité des environnements ONTAP 9" pour obtenir des informations détaillées.

> Les événements de mise à niveau signalés sur la plate-forme Active IQ sont également considérés comme des événements de sécurité. Ces événements identifient les problèmes liés à la résolution des problèmes lorsque vous devez mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les conseils de sécurité). Ces événements ne sont pas affichés dans le panneau sécurité, mais ils sont disponibles dans 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 que Unified Manager évalue, la recommandation NetApp et si le paramètre affecte la détermination globale du cluster plainte ou non.

L'utilisation de SVM non conformes sur un cluster affecte la valeur de conformité du cluster. Dans certains cas, vous devrez peut-être corriger les problèmes de sécurité avec un SVM avant que la sécurité du cluster ne soit considérée comme conforme.

Notez que tous les paramètres répertoriés ci-dessous ne s'affichent pas pour toutes les installations. Par exemple, si vous n'avez pas de cluster avec peering, ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments de peering de cluster ni de transport AutoSupport HTTPS dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
FIPS global	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 les modèles TLSv1.1 et TLSv1.2 sont autorisés.	Activé	Oui
Telnet	Indique si l'accès Telnet au système est activé ou désactivé. NetApp recommande un accès sécurisé à distance (SSH).	Désactivé	Oui
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Non	Oui
Bannière de connexion	Indique si la bannière connexion est activée ou désactivée pour les utilisateurs accédant au système.	Activé	Oui
Peering de clusters	Indique si la communication entre les clusters avec points de connexion est cryptée ou non chiffrée. Le chiffrement doit être configuré sur les clusters source et de destination pour que ce paramètre soit considéré comme conforme.	Chiffrées	Oui

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Protocole de temps réseau	Indique si le cluster possède un ou plusieurs serveurs NTP configurés. Pour la redondance et le meilleur service, NetApp vous recommande d'associer au moins trois serveurs NTP au cluster.	Configuré	Oui
OCSP	Depuis la version 9.14.1, Active IQ Unified Manager fournit des informations d'état du protocole OCSP (Online Certificate Status Protocol) au niveau du SVM (Storage Virtual machine). Cela signifie qu'une validation OCSP est appliquée à toutes les connexions SSL/TLS établies au SVM et assure l'intégrité et la validité des certificats utilisés dans ces connexions.	Activé	Non
Consignation d'audit à distance	Indique si le transfert de journal (Syslog) est crypté ou non.	Chiffrées	Oui
Transport AutoSupport HTTPS	Indique si HTTPS est utilisé comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.	Activé	Oui
Utilisateur Admin par défaut	Indique si l'utilisateur Admin par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tous les comptes intégrés inutiles.	Désactivé	Oui

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Utilisateurs SAML	Indique si SAML est configuré. SAML 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 privilégiés pour les utilisateurs qui accèdent 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 le biais d'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
Coque distante	Indique si le RSH est activé. Pour des raisons de sécurité, la fonction RSH doit être désactivée. Le protocole SSH (Secure Shell) est préféré pour un accès distant sécurisé.	Désactivé	Oui

Paramètre	Description	Recommandation	Concerne la conformité du cluster
MD5 utilisé	Indique si les comptes utilisateur ONTAP utilisent la fonction de hachage MD5 moins sécurisée. Le MD5 hache les comptes utilisateur la migration vers la fonction de hachage cryptographique plus sécurisée comme SHA-512 est préférable.	Non	Oui
Type émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé CA	Non

Catégories de conformité des VM de stockage

Ce tableau décrit les critères de conformité de sécurité de la machine virtuelle de stockage (SVM) que Unified Manager évalue, la recommandation de NetApp et si le paramètre affecte la détermination globale de la plainte ou non de la SVM.

Paramètre	Description	Recommandation	Concerne la conformité des 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 `cbc*`.	Non	Oui
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs qui accèdent aux SVM sur le système.	Activé	Oui
Cryptage LDAP	Indique si le chiffrement LDAP est activé ou désactivé.	Activé	Non
Authentification NTLM	Indique si l'authentification NTLM est activée ou désactivée.	Activé	Non

Paramètre	Description	Recommandation	Concerne la conformité des SVM
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.	Désactivé	Non
État FPolicy actif	Indique si FPolicy est créé ou non.	Oui	Non
Chiffrement SMB activé	Indique si SMB - Signature & scellage n'est pas activé.	Oui	Non
Signature SMB activée	Indique si SMB -Signing n'est pas activé.	Oui	Non

Catégories de conformité des volumes

Ce tableau décrit les paramètres de chiffrement de volume que Unified Manager évalue pour déterminer si les données de vos volumes sont correctement protégées contre tout accès par des utilisateurs non autorisés.

Notez que les paramètres de chiffrement de volume n'affectent pas la conformité du cluster ou de la machine virtuelle de stockage.

Paramètre	Description
Chiffrement logiciel	Affiche le nombre de volumes protégés à l'aide des solutions logicielles de chiffrement NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
Chiffrement matériel	Affiche le nombre de volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).

Paramètre	Description
Cryptage logiciel et matériel	Affiche le nombre de volumes protégés par le chiffrement logiciel et matériel.
Non chiffré	Affiche le nombre de volumes qui ne sont pas chiffrés.

Que signifie pas conforme

Les clusters et les SVM (Storage Virtual machine) sont considérés comme non conformes lorsque l'un des critères de sécurité évalués avec les recommandations définies dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9* n'est pas satisfait. Par ailleurs, un cluster est considéré comme non conforme lorsqu'un SVM n'est pas signalé comme étant non conforme.

Les icônes d'état des cartes de sécurité ont la signification suivante 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 du chiffrement des volumes ne contribue pas à la conformité du cluster ou de la SVM.

Affichage de l'état de sécurité pour les clusters et les VM de stockage

Active IQ Unified Manager permet d'afficher l'état de sécurité des objets de stockage de votre environnement à partir de différents points de l'interface. Il est ainsi possible de collecter et d'analyser des informations et des rapports en fonction de paramètres définis. Il détecte également les comportements suspects ou les modifications non autorisées du système sur les clusters surveillés et les VM de stockage.

Pour connaître les recommandations de sécurité, reportez-vous au "Guide NetApp sur le renforcement de la sécurité des environnements 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 accéder à l'efficacité de sécurité de vos clusters ONTAP et de vos machines virtuelles de stockage au niveau du centre de données et du site. Les objets pris en charge sont le cluster, les VM de stockage et les volumes. Voici la procédure à suivre :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
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.

Si vous cliquez sur les graphiques à barres, les nombres et les `View Reports` liens, vous accédez à la page volumes, clusters ou VM de stockage pour afficher les détails correspondants ou générer des rapports, si

nécessaire.

La page sécurité affiche les panneaux suivants :

- **Cluster Compliance** : état de sécurité (nombre de clusters conformes ou non) de tous les clusters d'un centre de données
- **Conformité des machines virtuelles de stockage** : état de sécurité (nombre de machines virtuelles de stockage conformes ou non) pour toutes les machines virtuelles de stockage de votre centre de données
- **Volume Encryption** : état du chiffrement du volume (nombre de volumes cryptés ou non) de tous les volumes de votre environnement
- **Volume anti-ransomware Status** : état de sécurité (nombre de volumes avec anti-ransomware activé ou désactivé) de tous les volumes de votre environnement
- **Authentification et certificats de cluster** : nombre de clusters utilisant chaque type de méthode d'authentification, tel que SAML, Active Directory, ou via des certificats et l'authentification locale. Le panneau affiche également le nombre de grappes 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 sécurité au niveau du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage > clusters**.
2. Sélectionnez **Affichage > sécurité > tous les clusters**.

Paramètres de sécurité par défaut, tels que Global FIPS, Telnet, paramètres SSH non sécurisés, bannière de connexion, protocole d'heure réseau, Le transport AutoSupport HTTPS et l'état de l'expiration du certificat du cluster sont affichés.

Vous pouvez cliquer sur ⋮ le bouton plus d'options et choisir d'afficher les détails de sécurité sur la page **sécurité** d'Unified Manager ou sur System Manager. Vous devez disposer d'identifiants valides pour afficher les détails dans System Manager.

> Si un cluster a un certificat expiré, vous pouvez cliquer sur `expired` **Cluster Certificate Validity** et le renouveler à partir de System Manager (9.10.1 et versions ultérieures). Vous ne pouvez pas cliquer sur `expired` si l'instance System Manager est d'une version antérieure à 9.10.1.

Afficher les détails de sécurité de tous les clusters à partir de la page VM de stockage

La page de détails **Storage VM / Security** vous permet d'afficher l'état de conformité de sécurité au niveau d'une 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**. La liste des clusters avec les paramètres de sécurité s'affiche.

Vous pouvez afficher la conformité de sécurité des machines virtuelles de stockage par défaut 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 bouton plus d'options et choisir d'afficher les détails de sécurité sur la page **sécurité** d'Unified Manager ou sur System Manager. Vous devez disposer d'identifiants valides pour afficher les détails dans System Manager.

Pour plus d'informations sur la sécurité anti-ransomware pour les volumes et les machines virtuelles de stockage, consultez "Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage"la section .

Affichage des événements de sécurité qui peuvent nécessiter des mises à jour logicielles ou micrologicielles

Certains événements de sécurité ont une zone d'impact de « mise à niveau ». Ces événements sont signalés sur la plateforme Active IQ et ils identifient les problèmes liés à la résolution lorsque vous devez mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les conseils de sécurité).

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez effectuer une action corrective immédiatement pour certains de ces problèmes, alors que d'autres peuvent attendre la prochaine maintenance planifiée. Vous pouvez afficher tous ces événements et les attribuer à des utilisateurs capables de résoudre ces problèmes. En outre, si certains événements de mise à niveau de sécurité que vous ne souhaitez pas être avertis, cette liste peut vous aider à identifier ces événements afin de pouvoir les désactiver.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.

   Par défaut, tous les événements actifs (nouveaux et acquittés) sont affichés sur la page d'inventaire gestion des événements.

2. Dans le menu Affichage, sélectionnez **mettre à niveau les événements**.

   La page affiche tous les événements de sécurité de mise à niveau actifs.

Affichage de la façon dont l'authentification utilisateur 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, conformément à la définition de votre organisation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
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. Affichez la carte **Cluster Authentication** pour voir le nombre d'utilisateurs qui accèdent au système à

l'aide de chaque type d'authentification.

5. Affichez la carte **Cluster Security** 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 si cette méthode n'est pas recommandée par NetApp, vous pouvez la désactiver.

Affichage de l'état de chiffrement de tous les volumes

Vous pouvez afficher la liste de tous les volumes, ainsi que leur état de cryptage actuel, afin de déterminer si les données de vos volumes sont correctement protégées contre tout accès par des utilisateurs non autorisés.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Les types de chiffrement pouvant être appliqués à un volume sont les suivants :

- Logiciels : volumes protégés à l'aide de solutions NetApp Volume Encryption (NVE) ou de chiffrement logiciel de chiffrement d'agrégats NetApp (NAE).
- Matériel : volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
- Logiciel et matériel : volumes protégés par le chiffrement logiciel et matériel.
- Aucun : volumes qui ne sont pas chiffrés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **chiffrement des volumes**
3. Dans la vue **Santé : volumes Encryption**, triez le champ **Type de cryptage** ou utilisez le filtre pour afficher les volumes ayant un type de cryptage spécifique ou qui ne sont pas cryptés (Type de cryptage « aucun »).

Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage

Vous pouvez afficher la liste de tous les volumes et de toutes les machines virtuelles de stockage (SVM) ainsi que leur statut actuel anti-ransomware afin de déterminer si les données de vos volumes et de vos SVM sont correctement protégées contre les attaques par ransomware.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Pour plus d'informations sur les différents statuts de protection contre les ransomware, reportez-vous à "ONTAP : activation d'une protection contre les ransomwares"la section .

Afficher les informations de sécurité de tous les volumes avec la détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.

2. Dans le menu Affichage, sélectionnez **Santé** > **sécurité** > **anti-ransomware**
3. Dans la vue **Security: Anti-ransomware**, vous pouvez trier les différents champs ou utiliser le filtre.

> Une protection contre les ransomwares n'est pas prise en charge pour les volumes hors ligne, les volumes restreints, les volumes SnapLock, les volumes FlexGroup, les volumes FlexCache, Volumes SAN uniquement, volumes des VM de stockage arrêtés, volumes root de VM de stockage, ou volumes de protection des données.

Affichez les informations de sécurité de toutes les machines virtuelles de stockage avec la détection anti-ransomwares

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez **Affichage > sécurité > anti-ransomware**. La liste des SVM avec le statut anti-ransomware est affichée.

> 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.

Affichage de tous les événements de sécurité actifs

Vous pouvez afficher tous les événements de sécurité actifs, puis les attribuer à un utilisateur qui peut résoudre le problème. En outre, si vous ne souhaitez pas recevoir certains événements de sécurité, cette liste peut vous aider à identifier les événements que vous souhaitez désactiver.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.

   Par défaut, les événements nouveaux et acquittés sont affichés sur la page d'inventaire gestion des événements.

2. Dans le menu Affichage, sélectionnez **événements de sécurité actifs**.

   La page affiche tous les événements de sécurité nouveaux et acquittés qui ont été générés au cours des 7 derniers jours.

Ajout d'alertes pour les événements de sécurité

Vous pouvez configurer les alertes pour les événements de sécurité individuels comme pour tous les autres événements reçus par Unified Manager. En outre, si vous souhaitez traiter tous les événements de sécurité, et que vous avez envoyé un e-mail à la même personne, vous pouvez créer une alerte unique pour vous avertir lorsque des événements de sécurité sont déclenchés.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

L'exemple ci-dessous montre comment créer une alerte pour l'événement de sécurité « Protocole Telnet activé ». Une alerte sera envoyée 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 **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez 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 **Evénements** et effectuez les opérations suivantes :
   a. Dans la liste gravité de l'événement, sélectionnez **Avertissement**.
   b. Dans la liste Evénements 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 **Alert thavent Users**.
7. Configurez toutes les autres options de cette page pour la fréquence de notification, l'émission de taps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Désactivation d'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 de notifications pour eux.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Lorsque vous désactivez des événements, les événements générés précédemment dans le système sont signalés comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications de ces événements sont générées à partir du cycle de surveillance suivant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Event Setup**.
2. Dans la page Configuration **Event**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
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 de tous les événements de sécurité. c. Dans la colonne Matching Events, sélectionnez les événements de sécurité que vous souhaitez désactiver, puis cliquez sur la flèche de droite pour déplacer ces événements vers la colonne Disable Events. d. Cliquez sur **Enregistrer et fermer**. e. Vérifiez que les événements que vous avez désactivés s'affichent dans la vue 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 fournissent des informations sur l'état de sécurité des clusters ONTAP, des serveurs de stockage virtuels (SVM) et des volumes basés sur des paramètres définis dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9*. Ces événements vous avertissent des problèmes potentiels afin que vous puissiez évaluer leur gravité et corriger 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 du cluster et de la machine virtuelle de stockage.

La gestion des opérations de sauvegarde et de restauration

Vous pouvez créer des sauvegardes de 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 défaillance du système ou de perte de données.

Il existe trois méthodes de sauvegarde et de restauration selon le système d'exploitation sur lequel vous avez installé Unified Manager, et basées sur le nombre de clusters et de nœuds gérés :

Système d'exploitation	Taille du déploiement	Méthode de sauvegarde recommandée
VMware vSphere	Toutes	Snapshot VMware de l'appliance virtuelle Unified Manager
Red Hat Enterprise Linux ou CentOS Linux	Petit	Unified Manager - dump de base de données MySQL
	Grand	Snapshot NetApp de base de données Unified Manager
Microsoft Windows	Petit	Unified Manager - dump de base de données MySQL
	Grand	NetApp Snapshot de base de données Unified Manager avec protocole iSCSI

Ces différentes méthodes sont décrites dans les sections suivantes.

Sauvegarde et restauration de Unified Manager sur l'appliance virtuelle

Le modèle de sauvegarde et de restauration d'Unified Manager, 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 une copie Snapshot VMware de l'appliance virtuelle Unified Manager.
2. Effectuez une copie NetApp Snapshot du datastore pour capturer le snapshot VMware.

   Si le datastore n'est pas hébergé sur un système exécutant le logiciel ONTAP, suivez les instructions du fournisseur de stockage pour créer une sauvegarde du snapshot VMware.

3. Répliquez la copie NetApp Snapshot, ou équivalent, sur un autre système de stockage.
4. Supprimez le snapshot VMware.

Il est recommandé d'implémenter un programme de sauvegarde à l'aide de ces tâches pour garantir la protection de l'appliance virtuelle Unified Manager en cas de problème.

Pour restaurer la machine virtuelle, vous pouvez utiliser le snapshot VMware que vous avez créé pour restaurer la machine virtuelle à l'état point dans le temps de sauvegarde.

Sauvegarde et restauration à l'aide d'un vidage de base de données MySQL

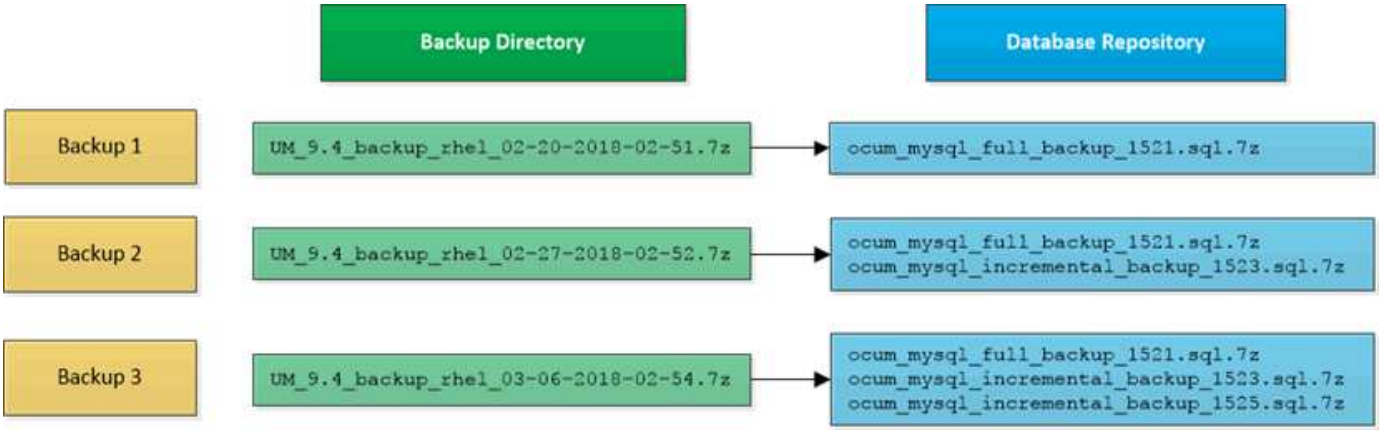
Une sauvegarde de vidage de la base de données MySQL est une copie de la base de données Active IQ Unified Manager et des fichiers de configuration que vous pouvez utiliser en cas de défaillance ou de perte de données du système. Vous pouvez planifier

l'écriture d'une sauvegarde vers une destination locale ou 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 sauvegarder à l'aide de copies Snapshot. Cette fonctionnalité est disponible sur les systèmes Red Hat Enterprise Linux, CentOS Linux et Windows.

Une sauvegarde de vidage de base de données consiste en un seul fichier dans le répertoire de sauvegarde et un ou plusieurs fichiers dans le répertoire de référentiel de base de données. Le fichier du répertoire de sauvegarde est très petit car il ne contient qu'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 de référentiel de base de données qui contient les différences du fichier de sauvegarde complet. Ce processus se poursuit au fur et à mesure que vous créez des sauvegardes supplémentaires, jusqu'au paramètre de rétention maximum, comme indiqué dans la figure suivante.



> Ne renommez pas et 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 un contrôle d'intégrité pour vérifier que tous les fichiers de sauvegarde et répertoires de sauvegarde requis existent et sont inscriptibles. Il vérifie également qu'il y a suffisamment d'espace sur le système pour créer le fichier de sauvegarde.

Configuration de la destination et de la planification pour les sauvegardes de vidage de base de données

Vous pouvez configurer les paramètres de sauvegarde de vidage de la base de données Unified Manager pour définir le chemin de sauvegarde de la base de données, le nombre

de rétention et la planification des sauvegardes. Vous pouvez activer des sauvegardes planifiées quotidiennement ou hebdomadaires. Par défaut, les sauvegardes planifiées sont désactivées, mais vous devez définir un planning de sauvegarde.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Vous devez disposer d'au moins 150 Go d'espace disponible dans 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 les droits de propriété suivants sont définis dans 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 est effectuée moins de temps que les sauvegardes suivantes, car la première sauvegarde est une sauvegarde complète. Une sauvegarde complète peut dépasser 1 Go et peut prendre entre trois et quatre heures. Les sauvegardes suivantes sont incrémentielles et requièrent moins de temps.

- Si le nombre de fichiers de sauvegarde incrémentielle est trop important pour l'espace que vous avez alloué aux sauvegardes, vous pouvez régulièrement effectuer une sauvegarde complète pour remplacer l'ancienne sauvegarde et ses fichiers incrémentiels. Autre option : vous pouvez effectuer une sauvegarde à l'aide des copies Snapshot.
- Il se peut que la sauvegarde effectuée durant les 15 premiers jours d'un nouvel ajout de cluster ne soit pas assez précise pour obtenir l'historique des données de performances.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **sauvegarde de base de données**.
2. Dans la page **sauvegarde de base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Configurez les valeurs appropriées pour un chemin de sauvegarde, le nombre de rétention et la planification.

   La valeur par défaut pour le nombre de rétention est 10 ; vous pouvez utiliser 0 pour créer des sauvegardes illimitées.

4. Sélectionnez le bouton **planifié quotidien** ou **planifié hebdomadaire**, puis spécifiez les détails de l'horaire.
5. Cliquez sur **appliquer**.

Les fichiers de sauvegarde de vidage de la 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

La restauration d'une base de données MySQL est le processus de restauration d'un

fichier de sauvegarde Unified Manager existant sur le même serveur ou sur un serveur Unified Manager différent. Vous effectuez l'opération de restauration à partir de la console de maintenance de 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 à l'aide de l'emplacement par défaut. Si vous effectuez une restauration sur un autre système Unified Manager (un système distant), vous devez copier le ou les fichiers de sauvegarde du stockage secondaire sur le disque local avant d'exécuter l'option de restauration.

Durant le processus de restauration, vous êtes déconnecté de 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

"Génération d'un certificat de sécurité HTTPS"

"Activation de l'authentification SAML"

"Authentification avec Active Directory ou OpenLDAP"

Restauration d'une sauvegarde de base de données MySQL sur un système Linux

En cas de perte ou de corruption des données, Unified Manager peut être restauré vers l'état stable précédent avec un minimum de perte de données. Vous pouvez restaurer la base de données Unified Manager sur un système Red Hat Enterprise Linux ou CentOS local ou distant à l'aide de la console de maintenance Unified Manager.

Ce dont vous aurez besoin

- Vous devez disposer des informations d'identification utilisateur root pour l'hôte Linux sur lequel Unified Manager est installé.
- Vous devez disposer d'un ID utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez avoir copié le fichier de sauvegarde Unified Manager et le contenu du répertoire du référentiel de base de données sur le système sur lequel vous allez effectuer l'opération de restauration.

  Il est recommandé de copier le fichier de sauvegarde dans le répertoire par défaut /`data/ocum`-backup. Les fichiers du référentiel de base de données doivent être copiés dans le /`database-dumps-repo` sous-répertoire situé sous le /`ocum-backup`répertoire.

- Les fichiers de sauvegarde doivent être de `.7z` type.

La fonction de restauration est spécifique à la plate-forme et à la version. La restauration d'une sauvegarde Unified Manager ne peut être effectuée que sur la même version de Unified Manager. Vous pouvez restaurer un fichier de sauvegarde Linux ou un fichier de sauvegarde d'appliance virtuelle sur un système Red Hat Enterprise Linux ou CentOS.

> Si le nom du dossier de sauvegarde contient un espace, vous devez inclure le chemin absolu ou relatif dans des guillemets doubles.

Étapes

1. Si vous effectuez une restauration sur un nouveau serveur, une fois l'installation de Unified Manager terminée, ne lancez pas l'interface utilisateur et ne configurez pas les clusters, les utilisateurs ou les paramètres d'authentification. Le fichier de sauvegarde remplit ces informations lors du processus de restauration.
2. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager.
3. Connectez-vous au système avec le nom et le mot de passe de l'utilisateur de maintenance (umadmin).
4. Entrez la commande `maintenance_console` et appuyez sur entrée.
5. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarder Restaurer**.
6. Saisissez le numéro de **Restore MySQL Backup**.
7. Lorsque vous y êtes invité, entrez le chemin absolu du fichier de sauvegarde.

   ```
   Bundle to restore from: /data/ocum-
   backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
   ```

   Une fois l'opération de restauration terminée, vous pouvez vous connecter à Unified Manager.

Après la restauration de la sauvegarde, si le serveur OnCommand Workflow Automation ne fonctionne pas, effectuez les opérations suivantes :

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.

Restauration d'une sauvegarde de base de données MySQL sous Windows

En cas de perte ou de corruption des données, la fonctionnalité de restauration permet de restaurer l'état stable précédent de Unified Manager avec une perte minimale. Vous pouvez restaurer la base de données MySQL Unified Manager sur un système Windows local ou un système Windows distant en utilisant la console de maintenance Unified Manager.

Ce dont vous aurez besoin

- Vous devez disposer des privilèges d'administrateur Windows.

- Vous devez avoir copié le fichier de sauvegarde Unified Manager et le contenu du répertoire du référentiel de base de données sur le système sur lequel vous allez effectuer 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 situé sous le `\backup` répertoire.

- Les fichiers de sauvegarde doivent être de `.7z` type.

La fonction de restauration est spécifique à la plate-forme et à la version. Vous ne pouvez restaurer une sauvegarde MySQL Unified Manager que sur la même version de 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 relatif du fichier de sauvegarde dans des guillemets doubles.

Étapes

1. Si vous effectuez une restauration sur un nouveau serveur, une fois l'installation de Unified Manager terminée, ne lancez pas l'interface utilisateur et ne configurez pas les clusters, les utilisateurs ou les paramètres d'authentification. Le fichier de sauvegarde remplit ces informations lors du processus de restauration.
2. Connectez-vous au système Unified Manager avec les identifiants 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**, saisissez le numéro de l'option **Sauvegarder Restaurer**.
6. Saisissez le numéro de **Restore MySQL Backup**.
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 la restauration de la sauvegarde, si le serveur OnCommand Workflow Automation ne fonctionne pas, effectuez les opérations suivantes :

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 des copies NetApp snapshots

Une copie NetApp Snapshot crée une image instantanée de la base de données Unified

Manager et des fichiers de configuration qui permet de restaurer les données en cas de défaillance du système ou de perte de données. Vous pouvez planifier régulièrement l'écriture d'une copie Snapshot sur un volume de l'un de vos clusters ONTAP, afin de toujours avoir une copie à jour.

> Cette fonctionnalité n'est pas disponible pour Active IQ Unified Manager installé sur une appliance virtuelle.

Configuration de la sauvegarde sous Linux

Si votre Active IQ Unified Manager est installé sur un ordinateur Linux, vous pouvez décider de configurer votre sauvegarde et restauration à l'aide des snapshots NetApp.

Les copies Snapshot prennent très peu de temps, en général quelques minutes seulement, et la base de données Unified Manager est verrouillée pendant un très court laps de temps. Vous n'avez donc que peu d'interruptions dans votre installation. L'image consomme un espace de stockage minimal et entraîne une surcharge minime des performances, car elle enregistre uniquement les modifications apportées aux fichiers depuis la dernière copie Snapshot. Comme la copie Snapshot est créée sur un cluster ONTAP, vous pouvez utiliser d'autres fonctionnalités NetApp, telles que SnapMirror, pour créer une protection secondaire, si nécessaire.

Avant de lancer une opération de sauvegarde, Unified Manager effectue une vérification d'intégrité afin de vérifier que le système de destination est disponible.

> - Vous ne pouvez restaurer une copie Snapshot que sur la même version de Active IQ Unified Manager.
>
> Par exemple, si vous avez créé une sauvegarde sur Unified Manager 9.14, la sauvegarde ne peut être restaurée que sur les systèmes Unified Manager 9.14.
>
> - Si une modification est apportée à la configuration de Snapshot, celle-ci peut ne pas être valide.

Configuration de l'emplacement de la copie Snapshot

Vous pouvez configurer le volume sur lequel les copies Snapshot seront stockées sur l'un de vos clusters ONTAP à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes ONTAP.

Ce dont vous aurez besoin

Le cluster, la VM de stockage et le volume doivent satisfaire aux exigences suivantes :

- Configuration requise pour le cluster :
  - ONTAP 9.3 ou version ultérieure doit être installé
  - Elle doit se trouver géographiquement proche du serveur Unified Manager
  - Il peut être surveillé par Unified Manager, mais ce n'est pas nécessaire
- Configuration requise pour les machines virtuelles de stockage :
  - Le commutateur de nom et le mappage de nom doivent être définis pour utiliser « fichiers ».

    - Les utilisateurs locaux créés pour correspondre aux utilisateurs côté client
    - Assurez-vous que tous les accès en lecture/écriture sont sélectionnés
    - Assurez-vous que Superuser Access est défini sur « n'importe quel » dans la politique d'exportation
    - NFS pour NetApp Snapshot pour Linux
    - NFSv4 doit être activé sur le serveur NFS et le domaine ID NFSv4 spécifié sur le client et le VM de stockage
    - Le volume doit avoir au moins deux fois la taille du répertoire Unified Manager/opt/netapp/Data

      Utilisez la commande du -sh /opt/netapp/data/ pour vérifier la taille actuelle.

- Volume requis :
    - Le volume doit avoir au moins deux fois la taille du répertoire Unified Manager /opt/netapp/data
    - Le style de sécurité doit être défini sur UNIX
    - La stratégie de snapshot local doit être désactivée
    - La taille automatique du volume doit être activée
    - Le niveau de services de performance doit être défini à une règle avec des IOPS élevées et une faible latence, telles que « extrême »

Pour obtenir des instructions détaillées sur la création du volume NFS, reportez-vous aux sections "Comment configurer NFSv4 dans ONTAP 9" et "Guide de configuration rapide ONTAP 9 NFS" .

Spécification de l'emplacement de destination des copies Snapshot

Vous devez configurer l'emplacement de destination des copies Snapshot Active IQ Unified Manager 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 utilisateur root pour l'hôte Linux sur lequel Active IQ Unified Manager est installé.
- Vous devez disposer d'un ID 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 de 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 FQDN du système Active IQ Unified Manager.
2. Connectez-vous au système avec le nom et le mot de passe de l'utilisateur de maintenance (umadmin).
3. Entrez la commande `maintenance_console` et appuyez sur entrée.
4. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarder Restaurer**.
5. Entrez le numéro **configurer la sauvegarde NetApp Snapshot**.
6. Indiquez le nombre de configurations NFS.

7. Vérifiez les informations que vous devez fournir, puis saisissez le numéro de **entrer les détails de la configuration de sauvegarde**.
8. Pour identifier le volume sur lequel la copie Snapshot sera écrite, entrez l'adresse IP de l'interface de gestion du cluster, le nom du VM de stockage, le nom du volume, le nom de la 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 avec le 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 de 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 de la copie Snapshot si vous ne l'avez pas encore fait.

Configuration de la sauvegarde sous Windows

Active IQ Unified Manager prend en charge les sauvegardes et les restaurations à l'aide de snapshots NetApp sur le système d'exploitation Windows à l'aide du protocole iSCSI.

Une sauvegarde basée sur des snapshots peut être effectuée pendant l'exécution de tous les services Unified Manager. Un état cohérent de la base de données est capturé dans le cadre de la copie Snapshot, tandis que la sauvegarde place un verrouillage de lecture global sur l'ensemble de la base de données, ce qui empêche toute écriture simultanée. Pour que votre système Unified Manager soit installé sur le système d'exploitation Windows pour effectuer des sauvegardes et des restaurations à l'aide des snapshots NetApp, vous devez d'abord configurer la sauvegarde Unified Manager sur des copies Snapshot 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.

- Configurez le cluster ONTAP
- Configurer la machine hôte Windows

Configuration de l'emplacement de sauvegarde pour Windows

Il est recommandé de configurer le volume de stockage des copies Snapshot après les sauvegardes de Unified Manager sur Windows.

Ce dont vous aurez besoin

Le cluster, la VM de stockage et le volume doivent satisfaire aux exigences suivantes :

- Configuration requise pour le cluster :
  - ONTAP 9.3 ou version ultérieure doit être installé

    - Elle doit se trouver géographiquement proche du serveur Unified Manager
    - Il est surveillé par Unified Manager
- Configuration requise pour les machines virtuelles 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'une LUN dédiés pour la configuration de sauvegarde. Le volume sélectionné ne doit contenir qu'une seule LUN et rien d'autre.
    - La taille de la LUN doit être au moins deux fois supérieure à la taille de données prévue pour les 9.9 Active IQ Unified Manager.

      Cela permet également de définir la même taille pour le volume.
    - Assurez-vous que tous les accès en lecture/écriture sont sélectionnés
    - Assurez-vous que Superuser Access est défini sur « n'importe quel » dans la politique d'exportation
- Configuration requise pour le volume et les LUN :
    - Le volume doit être au moins le double de la taille du répertoire de données MySQL Unified Manager.
    - Le style de sécurité doit être défini sur Windows
    - La stratégie de snapshot local doit être désactivée
    - La taille automatique du volume doit être activée
    - Le niveau de services de performance doit être défini à une règle avec des IOPS élevées et une faible latence, telles que « extrême »

Configuration du cluster ONTAP

Avant de pouvoir sauvegarder et restaurer des Active IQ Unified Manager à l'aide d'une copie Snapshot sur les systèmes ONTAP, vous devez effectuer quelques étapes de préconfiguration sur les clusters.

Vous pouvez configurer le cluster ONTAP à l'aide de l'invite de commandes ou de l'interface utilisateur de System Manager. La configuration du cluster ONTAP implique la configuration des LIFs de données à disponibilité à attribuer en tant que LIFs iSCSI à la VM de stockage. L'étape suivante consiste à configurer une machine virtuelle de stockage iSCSI à l'aide de l'interface utilisateur de System Manager. Vous devrez configurer une route réseau statique pour cette VM de stockage afin de contrôler la façon dont les LIF utilisent le réseau pour le trafic sortant.

> Vous devez disposer d'un volume dédié et d'une LUN pour la configuration de sauvegarde. Le volume sélectionné ne doit inclure qu'une seule LUN. La taille de la LUN doit être au moins deux fois supérieure à la taille de données que les Active IQ Unified Manager devraient traiter.

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. Configurer une route réseau pour la VM de stockage configurée
3. Configurez un volume de capacité appropriée et une LUN unique à l'intérieur, en veillant à ce que le

volume soit dédié uniquement à cette LUN.

> Dans un scénario où la LUN est créée sur System Manager, son annulation peut entraîner la suppression du groupe initiateur et l'échec de la restauration. Pour éviter ce scénario, veillez à ce que la création d'une LUN soit explicitement créée et n'ait pas été supprimée lorsque le mappage de la LUN est annulé.

4. Configurez un groupe initiateur sur la machine virtuelle de stockage.
5. Configurez un ensemble de ports.
6. Intégrez le groupe initiateur avec l'ensemble de ports.
7. Mappez la LUN sur le groupe initiateur.

Configuration de l'ordinateur hôte Windows

Vous devez configurer votre serveur hôte Windows avant d'utiliser NetApp Snapshot pour sauvegarder et restaurer Active IQ Unified Manager. Pour démarrer l'initiateur iSCSI Microsoft sur une machine hôte Windows, saisissez « iscsi » dans la barre de recherche et cliquez sur **iSCSI Initiator**.

Ce dont vous aurez besoin

Vous devez nettoyer toutes les configurations précédentes sur l'ordinateur hôte.

Si vous essayez de démarrer l'initiateur iSCSI lors d'une nouvelle installation de Windows, vous êtes invité à confirmer et, à votre 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 qui tente de se connecter. Vous devez donc vous assurer que toutes les configurations précédentes sur l'hôte Windows sont supprimées.

Étapes

1. Nettoyez toutes les configurations précédentes sur l'ordinateur hôte.
2. Découvrir le portail cible.
3. Connectez-vous au portail cible.
4. Connectez-vous via un chemins d'accès multiples au portail cible.
5. Découvrez les deux LIF.
6. Découvrez le LUN configuré sur l'ordinateur Windows en tant que périphérique.
7. Configurez la LUN découverte en tant que nouveau lecteur de volume dans Windows.

Spécification de l'emplacement de destination des copies Snapshot sous Windows

Vous devez configurer l'emplacement de destination des copies Snapshot Active IQ Unified Manager 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 ID 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 de cluster, du nom de la machine virtuelle de stockage, du nom du volume, du nom de 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 du shell d'alimentation, 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 et le mot de passe de l'utilisateur de maintenance (umadmin).
3. Entrez la commande `maintenance_console` et appuyez sur entrée.
4. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarder Restaurer**.
5. Entrez le numéro **configurer la sauvegarde NetApp Snapshot**.
6. Entrez le nombre de configurations iSCSI.
7. Vérifiez les informations que vous devez fournir, puis saisissez le numéro de **entrer les détails de la configuration de sauvegarde**.
8. Pour identifier le volume sur lequel la copie Snapshot sera écrite, entrez l'adresse IP de l'interface de gestion du cluster, le nom de la machine virtuelle de stockage, le nom du volume, le nom de la LUN, le nom d'utilisateur et le mot de passe du système de stockage, ainsi que le disque de montage.
9. Vérifiez ces informations et entrez `y`.

   Le système effectue les tâches suivantes :

   - La VM de stockage est validée
   - Le volume est validé
   - Le disque de montage et l'état sont validés
   - Existence et statut de la LUN
   - Lecteur réseau existant
   - L'existence de l'espace recommandé (plus de deux fois du répertoire de données mysql) au volume monté est validée
   - Chemin LUN correspondant à la LUN dédiée dans le volume
   - nom d'igroup
   - 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 des copies Snapshot.

Configuration de la sauvegarde par copie Snapshot à partir de la console de maintenance

Pour sauvegarder Active IQ Unified Manager à l'aide de la copie Snapshot, vous devez effectuer quelques étapes de configuration à partir de la console de maintenance.

Ce dont vous aurez besoin

Vous devez disposer des informations suivantes pour votre système :

- Adresse IP de cluster
- Nom de la VM de stockage
- Nom du volume
- Nom du LUN
- Chemin de montage
- Identifiants du système de stockage

Étapes

1. Accédez à la console de maintenance de Unified Manager.
2. Entrez 4 pour sélectionner **Backup Restore**.
3. Entrez 2 pour sélectionner **sauvegarde et restauration à l'aide de NetApp Snapshot**.

> Si vous souhaitez modifier la configuration de sauvegarde, entrez 3 pour sélectionner **mettre à jour la configuration de sauvegarde Snapshot NetApp**. Vous pouvez uniquement mettre à jour le mot de passe.

4. Dans le menu, entrez 1 pour sélectionner **configurer NetApp Snapshot Backup**.
5. Entrez 1 pour fournir les informations requises.
6. Indiquez le nom d'utilisateur et le mot de passe de la console de maintenance, puis indiquez la confirmation du montage de la LUN sur l'hôte.

   Le processus vérifie ensuite que le répertoire des données, le chemin LUN, la VM de stockage, les volumes, la disponibilité de l'espace, conduire, et ainsi de suite fournis par vous est correct. Les opérations qui se sont effectuées en arrière-plan sont les suivantes :

   - Les services sont arrêtés
   - Le répertoire de base de données est déplacé vers le stockage monté
   - Le répertoire de la base de données est supprimé et des symlinks sont établis
   - Les services sont redémarrés une fois la configuration terminée dans l'interface Active IQ Unified Manager, le type de sauvegarde est modifié dans NetApp Snapshot et reflète dans l'interface utilisateur en tant que sauvegarde de base de données (basée sur Snapshot).

Avant de commencer une opération de sauvegarde, vous devez vérifier s'il existe une modification dans la configuration de snapshot, car cela pourrait rendre le snapshot non valide. Supposons que vous ayez configuré la sauvegarde du lecteur G et de l'instantané pris. Vous avez ensuite reconfiguré la sauvegarde sur le disque E et les données sont enregistrées sur le disque E, conformément à la nouvelle configuration. Si vous essayez de restaurer l'instantané pris alors qu'il était dans le lecteur G, il échoue avec une erreur indiquant que le lecteur G n'existe pas.

Définition d'un planning de sauvegarde pour Linux et Windows

Vous pouvez configurer la planification à laquelle les copies Snapshot de Unified Manager sont créées à l'aide de l'interface utilisateur d'Unified Manager.

Ce dont vous aurez besoin

- Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.
- Vous devez avoir configuré les paramètres de création de copies Snapshot depuis la console de maintenance pour identifier la destination où les snapshots seront créés.

Les copies Snapshot sont créées en quelques minutes seulement et la base de données Unified Manager est verrouillée pendant quelques secondes seulement.

> Il se peut que la sauvegarde effectuée durant les 15 premiers jours d'un nouvel ajout de cluster ne soit pas assez précise pour obtenir l'historique des données de performances.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **sauvegarde de base de données**.
2. Dans la page **sauvegarde de base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Saisissez le nombre maximal de copies Snapshot que vous souhaitez conserver dans le champ **Retention Count**.

   La valeur par défaut pour le nombre de rétention 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 de ONTAP.

4. Sélectionnez le bouton **planifié quotidien** ou **planifié hebdomadaire**, puis spécifiez les détails de l'horaire.
5. Cliquez sur **appliquer**.

Les copies Snapshot sont créées en fonction du planning. 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 snapshots, il est possible que vous souhaitiez créer une ou deux alertes pour ce volume. Vous êtes donc averti lorsque :

- L'espace du volume est plein à 90 %. Utilisez l'événement **Volume Space Full** pour configurer l'alerte.

  Vous pouvez ajouter de la capacité au volume à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes ONTAP, de sorte que la base de données Unified Manager ne manque pas d'espace.

- Le nombre d'instantanés est proche d'atteindre le nombre maximal. Utilisez l'événement **trop de copies snapshot** pour configurer l'alerte.

  Vous pouvez supprimer d'anciens snapshots à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes ONTAP afin qu'il reste de la place pour les nouvelles copies Snapshot.

Vous configurez les alertes dans la page Configuration des alertes.

Restauration de Unified Manager à l'aide des copies Snapshot

En cas de perte ou de corruption des données, Unified Manager peut être restauré vers l'état stable précédent avec un minimum de perte de données. Vous pouvez restaurer la base de données Snapshot Unified Manager sur un système d'exploitation local ou distant via la console de maintenance Unified Manager.

Ce dont vous aurez besoin

- Vous devez disposer des informations d'identification 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 ID utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

La fonction de restauration est spécifique à la plate-forme et à la version. La restauration d'une sauvegarde Unified Manager ne peut être effectuée que sur la même version de Unified Manager.

Étapes

1. Connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager.
   - Linux : Secure Shell
   - Fenêtres : Power Shell
2. Connectez-vous au système à l'aide des 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 **Sauvegarder Restaurer**.
5. Entrez 2 pour sélectionner **sauvegarde et restauration à l'aide de NetApp Snapshot**.

   Si vous effectuez une restauration sur un nouveau serveur, une fois l'installation de Unified Manager terminée, ne lancez pas l'interface utilisateur et ne configurez pas les clusters, les utilisateurs ou les paramètres d'authentification. Entrez 1 pour sélectionner **configurer NetApp Snapshot Backup** et configurez les paramètres des copies Snapshot comme ils se trouvent sur le système d'origine.

6. Entrez 3 pour sélectionner **Restore Using NetApp Snapshot**.
7. Sélectionnez la copie Snapshot 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 Unified Manager.

Après avoir restauré la sauvegarde, si le serveur Workflow Automation ne fonctionne pas, effectuez les opérations suivantes :

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.

Modification du type de sauvegarde

Pour modifier le type de sauvegarde de votre système Active IQ Unified Manager, vous pouvez utiliser les options de la console de maintenance. L'option **Unconfigure NetApp Snapshot Backup** vous permet de revenir à la sauvegarde MySQL.

Ce dont vous aurez besoin

Vous devez disposer d'un ID 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 **Unconfigure NetApp Snapshot Backup**.

   Les actions exécutées sont affichées, qui sont : arrêter les services, interrompre le symlink, 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 Snapshot 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 de Active IQ Unified Manager pour générer des sauvegardes à la demande à tout moment. La sauvegarde à la demande vous permet de créer instantanément une sauvegarde à l'aide de la méthode de sauvegarde existante. La sauvegarde à la demande ne fait pas de différence entre la sauvegarde MySQL ou NetApp Snapshot.

Vous pouvez effectuer une sauvegarde à la demande à l'aide du bouton **Sauvegarder maintenant** de la page sauvegarde de base de données. La sauvegarde à la demande ne dépend pas des plannings que vous avez configurés pour Active IQ Unified Manager.

Migration d'une appliance virtuelle Unified Manager vers un système Linux

Vous pouvez restaurer une sauvegarde de vidage de base de données Unified Manager MySQL à partir d'une appliance virtuelle vers un système Red Hat Enterprise Linux ou CentOS Linux si vous souhaitez modifier le système d'exploitation hôte sur lequel Unified Manager s'exécute.

Ce dont vous aurez besoin

- Sur l'appliance virtuelle :
  - Vous devez avoir le rôle opérateur, administrateur d'applications ou 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 la section "Installation de Unified Manager sur des systèmes Linux".
  - La version d'Unified Manager sur ce serveur doit être identique à celle de 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 remplit ces informations lors du processus de restauration.
  - Vous devez disposer des informations d'identification 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 le système Red Hat Enterprise Linux ou CentOS, puis restaurer la sauvegarde de la base de

données sur le nouveau système.

Étapes

1. Sur l'appliance virtuelle, cliquez sur **Management** > **Database Backup**.
2. Dans la page **sauvegarde de base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Définissez le chemin de sauvegarde sur /jail/support.
4. Dans la section planification, sélectionnez **programmé quotidien** et entrez quelques minutes après l'heure actuelle pour que la sauvegarde soit créée sous peu.
5. Cliquez sur **appliquer**.
6. Attendre quelques heures la génération de la sauvegarde.

   Une sauvegarde complète peut dépasser 1 Go et peut prendre entre trois et 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 de 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 utilisateur Web de Unified Manager.

Vous devez effectuer les tâches suivantes :

- Générez un nouveau certificat de sécurité HTTPS et redémarrez le serveur Unified Manager.
- Définissez le chemin de sauvegarde sur le paramètre par défaut de votre système Linux (/data/ocum-backup) ou sur 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.

Une fois que vous avez vérifié que tout s'exécute correctement sur votre système Linux, vous pouvez arrêter et supprimer l'appliance virtuelle Unified Manager.

Gestion des 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 les scripts vers Unified Manager et de les exécuter est activée par défaut. Si votre

entreprise ne souhaite pas autoriser cette fonctionnalité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité à partir de **Storage Management** > **Feature Settings**.

Fonctionnement des scripts avec les alertes

Vous pouvez associer une alerte à votre script afin que le script soit exécuté lorsqu'une alerte est générée pour un événement dans Unified Manager. Vous pouvez utiliser ces 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, des actions sont prises en fonction de votre script personnalisé pour ce type d'événement, et les actions **Fix it** ne sont pas disponibles par défaut sur la page actions de gestion ou 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 de vos scripts et recueillir des informations d'événement associées ou modifier des objets de stockage.

Exemple pour obtenir des 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 les valeurs de sortie suivantes s'affichent :

```
-eventID : 290
-eventSourceID : 4138
```

Ajout de scripts

Vous pouvez ajouter des scripts dans Unified Manager et les associer aux alertes. Ces scripts sont exécutés automatiquement lorsqu'une alerte est générée. Ils vous permettent d'obtenir des informations sur les objets de stockage pour lesquels l'événement est généré.

Ce dont vous aurez besoin

- Vous devez avoir créé et enregistré les scripts que vous souhaitez ajouter au serveur Unified Manager.
- Les formats de fichier pris en charge pour les scripts sont Perl, Shell, PowerShell, Python et les `.bat` fichiers.

Plateforme sur laquelle Unified Manager est installé	Langues prises en charge
VMware	Scripts Perl et Shell
Linux	Scripts Perl, Python et Shell
Fenêtres	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 ne prennent en charge que 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 pas créés à un endroit quelconque du dossier d'installation d'Unified Manager.

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez télécharger des scripts personnalisés et collecter des informations détaillées sur 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 à partir de **Storage Management** > **Feature Settings**.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **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**.

Suppression de scripts

Vous pouvez supprimer un script d'Unified Manager lorsque le script n'est plus nécessaire ou valide.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Le script ne doit pas être associé à une alerte.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **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 le script s'exécute correctement lorsqu'une alerte est générée pour un objet de stockage.

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir téléchargé un script au format de fichier pris en charge vers Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **scripts**.
2. Dans la page scripts, ajoutez votre script de test.
3. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
4. Dans la page **Configuration des alertes**, effectuez l'une des opérations suivantes :

Pour…	Procédez comme ça…
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 **Test**.

   Le script est exécuté avec l'argument "`-test", et une alerte de notification est envoyée aux adresses électroniques spécifiées lors de la création de l'alerte.

Gestion et suivi des groupes

La création de groupes dans Unified Manager permet de gérer les objets de stockage.

Présentation des groupes

La création de groupes dans Unified Manager permet de gérer les objets de stockage. Pour gérer les objets de stockage de votre environnement, il est important de comprendre les concepts relatifs aux groupes et la manière dont les règles de groupe permettent d'ajouter des objets de stockage à un groupe.

Qu'est-ce qu'un groupe

Un groupe est un ensemble dynamique d'objets de stockage hétérogènes (clusters, SVM ou volumes). La création de groupes dans Unified Manager permet de gérer facilement un ensemble d'objets de stockage. Il est possible que les membres d'un groupe changent, en fonction des objets de stockage surveillés par Unified Manager à un point dans le temps.

- 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 les clusters, SVM ou volumes.
- Les objets de stockage sont ajoutés dynamiquement à un groupe selon l'heure à laquelle une règle de groupe est créée ou à la fin d'un cycle de surveillance par Unified Manager.
- Vous pouvez appliquer simultanément des actions sur tous les objets de stockage d'un groupe, par exemple la définition de seuils pour les volumes.

Fonctionnement des règles de groupe pour les groupes

Une règle de groupe est un critère que vous définissez pour activer l'inclure dans un groupe spécifique des objets de stockage (volumes, clusters ou SVM). Vous pouvez utiliser des groupes de condition 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 à une règle de groupe ; un seul type d'objet est associé à 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 condition et chaque groupe de condition 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 condition et chaque groupe de condition peut avoir une ou plusieurs conditions. Vous pouvez appliquer tous les groupes de conditions définis dans une règle de groupe aux groupes afin de spécifier les objets de stockage inclus dans le groupe.

Les conditions d'un groupe de conditions sont exécutées à l'aide de LA commande LOGIQUE ET. 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 s'applique, sélectionne et regroupe uniquement les objets de stockage qui répondent à toutes les conditions du groupe de conditions. Vous pouvez utiliser plusieurs conditions dans un groupe de conditions lorsque vous souhaitez restreindre l'étendue 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
Volumétrie	• 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 annotation comme opérande pour un objet de stockage, l'opérateur « is » est disponible. Pour tous les autres opérandes, vous pouvez sélectionner « is » 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 du SVM 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 « is » et « contient ».

  Lorsque vous sélectionnez l'opérateur « is », la condition est évaluée en fonction de la correspondance exacte entre la valeur d'opérande et la valeur fournie pour l'opérande sélectionné.

  Lorsque vous sélectionnez l'opérateur « contient », la condition est évaluée pour satisfaire à l'un des critères suivants :

  - La valeur d'opérande correspond exactement à la valeur fournie pour l'opérande sélectionné

    - La valeur opérande contient la valeur fournie pour l'opérande sélectionné
- Valeur

  Le champ 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 ».
- Nom du SVM est « `date_svm' »

Ce groupe de condition sélectionne tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur des SVM sous le nom « data_svm ».

Groupes de condition

Les groupes de condition sont exécutés à l'aide D'UN OU logique, puis appliqués aux objets de stockage. Les objets de stockage doivent satisfaire l'un des groupes de condition à inclure dans un groupe. Les objets de stockage de tous les groupes de condition 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 groupes de condition

Considérons deux groupes de condition pour un volume, chaque groupe contenant les deux conditions suivantes :

- Groupe condition 1
  - Le nom contient « vol ».
  - SVM name 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 sous le nom « data_svm ».
- Groupe condition 2
  - Le nom contient « vol ».
  - La valeur d'annotation de la priorité de données est le groupe de condition « critique » 2 sélectionne tous les volumes qui incluent « vol » dans leurs noms et qui sont annotés avec la valeur d'annotation de priorité de données comme « critique ».

Lorsqu'une règle de groupe contenant ces deux groupes de condition est appliquée aux 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 la SVM sous le nom « data_svm ».
- Tous les volumes qui incluent « vol » dans leurs noms et qui sont annotés avec la valeur d'annotation prioritaire des données « critique ».

Fonctionnement des 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 de groupe de seuils 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'action de groupe uniques. Vous pouvez avoir un groupe avec un seul type d'action de groupe de seuils d'intégrité de volume. Toutefois, vous pouvez configurer un autre type d'action de groupe, si disponible, pour le même groupe. Le classement 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 seuils de contrôle de volume suivantes sont configurées pour ces groupes :

- `Change_capacity_threshold` action de groupe avec rang 1, pour la configuration de la capacité du volume
- `Change_snapshot_copies` Action de groupe avec rang 2, pour la configuration des copies Snapshot du volume

L'`Change_capacity_threshold`action de groupe est toujours prioritaire sur l' `Change_snapshot_copies`action de groupe et appliquée au volume A. lorsque Unified Manager termine un cycle de surveillance, les événements liés au seuil d'intégrité du volume A sont réévalués par action de groupe. `Change_capacity_threshold` Vous ne pouvez pas configurer un autre type d'action de groupe de seuil de volume pour le groupe G1 ou G2.

Ajout de groupes

La création de groupes permet de combiner les clusters, les volumes et les SVM (Storage Virtual machine) pour une gestion simplifiée.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez définir des règles de groupe pour ajouter ou supprimer des membres du groupe et modifier les actions de groupe pour ce dernier.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **groupes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un groupe**, entrez un nom et une description pour le groupe.
4. Cliquez sur **Ajouter**.

Modification de groupes

Vous pouvez modifier le nom et la description d'un groupe créé dans Unified Manager.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Lorsque vous modifiez un groupe pour le mettre à jour, 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 **Storage Management** > **Groups**.
2. Dans l'onglet **groupes**, sélectionnez le groupe à modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le groupe**, modifiez le nom, la description ou les deux pour le groupe.
4. Cliquez sur **Enregistrer**.

Suppression de groupes

Vous pouvez supprimer un groupe depuis Unified Manager lorsque ce dernier n'est plus nécessaire.

Ce dont vous aurez besoin

- Aucun des objets de stockage (clusters, SVM ou volumes) ne doit être associé à toute règle de groupe associée au groupe que vous souhaitez supprimer.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **groupes**, sélectionnez le groupe à 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. Toutefois, ces actions de groupe seront démappées après la suppression du groupe.

Ajout de règles de groupe

Vous pouvez créer des règles de groupe pour ajouter de manière dynamique des objets de stockage tels que les volumes, les clusters ou les SVM (Storage Virtual machine) au groupe. Vous devez configurer au moins un groupe de conditions avec au moins une condition pour créer une règle de groupe.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Les objets de stockage actuellement surveillés sont ajoutés dès la création de la règle de groupe. Les nouveaux objets sont ajoutés uniquement une fois le cycle de surveillance terminé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
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 :

Pour créer	Procédez comme ça…
Une condition	a. Sélectionnez un opérande dans la liste des opérandes. b. Sélectionnez **contient** ou **est** comme opérateur. c. Entrez 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. Entrez une valeur ou sélectionnez une valeur dans la liste disponible. e. Cliquez sur **Ajouter une condition** pour créer d'autres conditions si nécessaire, puis répétez les étapes a à d pour chaque condition.

7. Cliquez sur **Ajouter**.

Exemple de création d'une règle de groupe

Procédez comme suit 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

1. Spécifiez un nom pour la règle de groupe.
2. Sélectionnez le type d'objet en tant que machine virtuelle de stockage (SVM).
3. Sélectionnez un groupe dans la liste des groupes.
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 **priorité données** comme opérande à l'étape 8, **is** comme opérateur à l'étape 9 et **critique** comme valeur à l'étape 10.
13. Cliquez sur **Ajouter** pour créer la condition de la règle de groupe.

Modification des règles de groupe

Vous pouvez modifier des règles de groupe pour modifier les groupes de condition et les conditions d'un groupe de conditions afin d'ajouter ou de supprimer des objets de stockage dans ou d'un groupe spécifique.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **règles de groupe**, sélectionnez la règle de groupe à 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 condition et les conditions selon les besoins.

   Vous ne pouvez pas modifier le type d'objet cible d'une règle de groupe.

4. Cliquez sur **Enregistrer**.

Suppression de règles de groupe

Vous pouvez supprimer une règle de groupe de Active IQ Unified Manager lorsque la règle de groupe n'est plus nécessaire.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 **Storage Management** > **Groups**.
2. Dans l'onglet **règles de groupe**, sélectionnez la règle de groupe à supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Ajout d'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 individuellement à chaque objet.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.

2. Dans l'onglet **actions de groupe**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une action de groupe**, entrez 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 **action Type**, sélectionnez un type d'action.

   La boîte de dialogue se développe, ce qui vous permet 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**.

Modification des actions de groupe

Vous pouvez modifier les paramètres d'action de groupe que vous avez configurés dans Unified Manager, tels que le nom d'action de groupe, la description, le nom de groupe associé et les paramètres du type d'action.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **actions de groupe**, sélectionnez l'action de groupe à 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 les besoins.
4. Cliquez sur **Enregistrer**.

Configuration des seuils d'intégrité des volumes pour les groupes

Vous pouvez configurer des seuils d'état du volume au niveau du groupe pour la capacité, les copies Snapshot, les quotas qtree, la croissance et les inodes.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Le type de seuil d'intégrité du volume de l'action de groupe est appliqué uniquement sur les volumes d'un groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **actions de groupe**, cliquez sur **Ajouter**.
3. Entrez un nom et une description pour l'action de groupe.
4. Dans la liste déroulante **Groupe**, sélectionnez un groupe pour lequel vous souhaitez configurer l'action de groupe.
5. Sélectionnez **action Type** comme seuil de contrôle 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**.

Suppression des actions de groupe

Vous pouvez supprimer une action de groupe de Unified Manager lorsque l'action de groupe n'est plus nécessaire.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Lorsque vous supprimez l'action de groupe pour le seuil d'intégrité du volume, des seuils globaux sont appliqués aux objets de stockage de ce groupe. Les seuils de santé des niveaux objet définis sur l'objet de stockage ne sont pas affectés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **actions de groupe**, sélectionnez l'action de groupe à supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Réorganisation des actions de groupe

Vous pouvez modifier l'ordre des actions de groupe à appliquer aux objets de stockage d'un groupe. Les actions de groupe sont appliquées aux objets de stockage de façon séquentielle en fonction de leur rang. Le rang le plus bas est affecté à l'action de groupe que vous avez configurée en dernier. Vous pouvez modifier le classement de l'action de groupe en fonction de vos besoins.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez sélectionner une ou plusieurs lignes, puis effectuer plusieurs opérations glisser-déposer pour modifier le rang des actions de groupe. Cependant, vous devez enregistrer les modifications pour que la nouvelle hiérarchisation soit reflétée dans la grille des actions de groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Groups**.
2. Dans l'onglet **actions de groupe**, cliquez sur **Réordonner**.
3. Dans la boîte de dialogue **Réordonner les actions de groupe**, faites glisser les lignes pour réorganiser la séquence des actions de groupe, si nécessaire.
4. Cliquez sur **Enregistrer**.

Hiérarchiser les événements d’objet de stockage à l’aide d’annotations

Vous pouvez créer et appliquer des règles d’annotation aux objets de stockage afin d’identifier et de filtrer ces objets en fonction du type d’annotation appliqué et de sa priorité.

En savoir plus sur les annotations

La compréhension des concepts liés aux annotations vous aide à gérer les événements liés aux objets de stockage de votre environnement.

Quelles 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 de façon dynamique aux 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 associés. Vous pouvez appliquer des annotations aux clusters, volumes et 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 "centre des données" avec les valeurs "Boston" et "Canada". Vous pouvez ensuite appliquer l’annotation "deata-centre" avec la valeur "Boston" au volume v1. Lorsqu’une alerte est générée pour tout événement sur un volume v1 annoté par « centre de données », l’e-mail généré indique l’emplacement du volume, « Boston », ce qui vous permet de hiérarchiser et de résoudre le problème.

Fonctionnement des règles d’annotation dans Unified Manager

Une règle d’annotation est un critère que vous définissez pour annoter les objets de stockage (volumes, clusters ou SVM). Vous pouvez utiliser des groupes de condition 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 à une règle d’annotation ; un seul type d’objet peut être associé à une règle d’annotation.
- Unified Manager ajoute ou supprime des annotations des objets de stockage après chaque cycle de surveillance ou lors de la création, de la modification, de la suppression ou de la réorganisation d’une règle.
- Une règle d’annotation peut avoir un ou plusieurs groupes de condition et chaque groupe de condition 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 condition et chaque groupe de condition peut avoir une ou plusieurs conditions. Vous pouvez appliquer tous les groupes de condition définis dans une règle d'annotation d'une annotation afin d'annoter les objets de stockage.

Les conditions d'un groupe de conditions sont exécutées à l'aide de LA commande LOGIQUE ET. 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 s'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
Volumétrie	• 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 annotation comme opérande pour un objet de stockage, l'opérateur « is » est disponible. Pour tous les autres opérandes, vous pouvez sélectionner « is » ou « contient » comme opérateur. Lorsque vous sélectionnez l'opérateur « is », la condition est évaluée pour une correspondance exacte entre la valeur de l'opérande et la valeur fournie pour l'opérande sélectionné. Lorsque vous sélectionnez l'opérateur « contient », la condition est évaluée pour satisfaire à l'un des critères suivants :

- La valeur d'opérande correspond exactement à la valeur de l'opérande sélectionné.
- La valeur opérande contient la valeur fournie pour l'opérande sélectionné.

Exemple de règle d'annotation avec des conditions

Envisagez une règle d'annotation avec un groupe de conditions pour un volume avec les deux conditions suivantes :

- Le nom contient « vol ».
- Nom du SVM est « `date_svm' »

Cette règle d'annotation annote tous les volumes qui incluent « vol » dans leurs noms et qui sont hébergés sur des SVM sous le nom « `date_svm' » avec l'annotation sélectionnée et le type d'annotation.

Groupes de condition

Les groupes de condition sont exécutés à l'aide D'UN OU logique, puis appliqués aux objets de stockage. Les objets de stockage doivent répondre aux exigences de l'un des groupes de condition à annoter. Les objets de stockage qui répondent aux conditions de tous les groupes de condition 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 groupes de condition

Considérons une règle d'annotation avec deux groupes de condition pour un volume ; chaque groupe contient les deux conditions suivantes :

- Groupe condition 1
  - Le nom contient « vol ».
  - SVM name est « data_svm » cette condition group annote tous les volumes, y compris « vol », dans leurs noms et qui sont hébergés sur des SVM sous le nom « `date_svm ».
- Groupe condition 2
  - Le nom contient « vol ».
  - La valeur d'annotation de la priorité des données est « critique » ce groupe de condition annote tous les volumes qui incluent « vol » dans leurs noms et qui sont annotés avec la valeur d'annotation prioritaire des données comme « critique ».

Lorsqu'une règle d'annotation contenant ces deux groupes de condition 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 sous le nom « data_svm ».
- Tous les volumes qui incluent « vol » dans leurs noms et qui sont annotés avec la valeur d'annotation prioritaire des données comme « critique ».

Description des valeurs d'annotation prédéfinies

Priorité des données est une annotation prédéfinie qui a les valeurs Mission critique, haute et basse. Ces valeurs vous permettent d'annoter les objets de stockage en fonction de la priorité des données qu'ils contiennent. Vous ne pouvez ni modifier ni supprimer les valeurs d'annotation prédéfinies.

- **Priorité des données:critique**

  Cette annotation est appliquée aux objets de stockage qui contiennent des données stratégiques. Par exemple, les objets qui contiennent des applications de production peuvent être considérés comme critiques.

- **Priorité de données:élevée**

  Cette annotation est appliquée aux objets de stockage qui contiennent des données à priorité élevée. Par exemple, les objets qui hébergent des applications métier peuvent être considérés comme prioritaires.

- **Priorité de données : faible**

  Cette annotation est appliquée aux objets de stockage qui contiennent des données à faible priorité. Par exemple, les objets qui se trouvent sur un système de stockage secondaire, comme les destinations de

sauvegarde et de miroir, peuvent être en priorité faible.

Ajout dynamique d'annotations

Lorsque vous créez des annotations personnalisées, Unified Manager associe de façon dynamique les clusters, les machines virtuelles de stockage et les volumes avec les annotations à l'aide de règles. Ces règles affectent automatiquement les annotations aux objets de stockage.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **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**.

Ajout de valeurs aux annotations

Vous pouvez ajouter des valeurs aux annotations, puis associer des objets de stockage à une paire nom-valeur d'annotation spécifique. L'ajout de valeurs aux annotations permet de gérer plus efficacement les objets de stockage.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous ne pouvez pas ajouter de valeurs aux annotations prédéfinies.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **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**.

Suppression d'annotations

Vous pouvez supprimer des annotations personnalisées et leurs valeurs lorsqu'elles ne sont plus nécessaires.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou 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 **Storage Management** > **Annotations**.
2. Dans l'onglet **Annotations**, sélectionnez l'annotation à supprimer.

   Les détails de l'annotation sélectionnée s'affichent.

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.

Affichage de la liste d'annotations et des détails

Vous pouvez afficher la liste des annotations dynamiquement associées aux clusters, aux volumes et aux machines virtuelles de stockage (SVM). Vous pouvez également afficher des détails tels que la description, créée par, créée par, valeurs, règles, et les objets associés à l'annotation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Annotations**.
2. Dans l'onglet **Annotations**, cliquez sur le nom de l'annotation pour afficher les détails associés.

Suppression de valeurs des annotations

Vous pouvez supprimer les valeurs associées aux annotations personnalisées lorsque cette valeur ne s'applique plus à l'annotation.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou 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 de valeurs des annotations prédéfinies.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Annotations**.
2. Dans la liste des annotations de l'onglet **Annotations**, sélectionnez l'annotation à partir de laquelle vous souhaitez supprimer une valeur.
3. Dans la zone **valeurs** de l'onglet **Annotations**, sélectionnez la valeur à supprimer, puis cliquez sur **Supprimer**.
4. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

   La valeur est supprimée et ne s'affiche plus dans la liste de valeurs pour l'annotation sélectionnée.

Création de règles d'annotation

Unified Manager permet également de créer des règles d'annotations dynamiques pour

les objets de stockage tels que les volumes, les clusters ou les SVM.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Les objets de stockage actuellement surveillés sont annotés dès la création de la règle d'annotation. 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 **Storage Management** > **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 à annoter.
5. Dans les champs **appliquer une 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…	Procédez comme ça…
Une condition	a. Sélectionnez un opérande dans la liste des opérandes. b. Sélectionnez **contient** ou **est** comme opérateur. c. Entrez 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. Entrez une valeur ou sélectionnez une valeur dans la liste disponible. e. Cliquez sur **Ajouter une condition** pour créer d'autres conditions si nécessaire, puis répétez les étapes a à d pour chaque condition.

7. Cliquez sur **Ajouter**.

Exemple de création d'une règle d'annotation

Procédez comme suit dans la boîte de dialogue Ajouter une règle d'annotation pour créer une règle d'annotation, notamment configurer une condition et ajouter un groupe de conditions :

Étapes

1. Spécifiez un nom pour la règle d'annotation.
2. Sélectionnez le type d'objet cible en tant que 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 **priorité données** comme opérande à l'étape 8, **is** comme opérateur à l'étape 9 et **critique** comme valeur à l'étape 10.
13. Cliquez sur **Ajouter**.

Ajout manuel d'annotations à des objets de stockage individuels

Vous pouvez annoter manuellement les volumes, les clusters et les SVM sélectionnés sans utiliser de règles d'annotation. Vous pouvez annoter un ou plusieurs objets de stockage et spécifier la combinaison de paires nom-valeur requise pour l'annotation.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Accédez aux objets de stockage à annoter :

Pour ajouter une annotation à…	Procédez comme ça…
Clusters	a. Cliquez sur **Storage** > **clusters**. b. Sélectionnez un ou plusieurs clusters.
Volumes	a. Cliquez sur **Storage** > **volumes**. b. Sélectionnez un ou plusieurs volumes.
SVM	a. Cliquez sur **Storage** > **SVM**. b. Sélectionnez un ou plusieurs SVM.

2. Cliquez sur **Annotate** et sélectionnez une paire nom-valeur.
3. Cliquez sur **appliquer**.

Modification des règles d'annotation

Vous pouvez modifier des règles d'annotation pour modifier les groupes de conditions et les conditions au sein du groupe de conditions afin d'ajouter des annotations à des objets

de stockage ou de les supprimer.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 **Storage Management** > **Annotations**.
2. Dans l'onglet **règles d'annotation**, sélectionnez la règle d'annotation à modifier, puis cliquez sur **actions** > **Modifier**.
3. Dans la boîte de dialogue **Modifier règle d'annotation**, modifiez le nom de la règle, le nom et la valeur de l'annotation, les groupes de condition et les conditions comme requis.

   Vous ne pouvez pas modifier le type d'objet cible d'une règle d'annotation.

4. Cliquez sur **Enregistrer**.

Configuration des conditions pour les règles d'annotation

Vous pouvez configurer une ou plusieurs conditions pour créer des règles d'annotation qui s'appliquent aux objets de stockage par Unified Manager. Les objets de stockage correspondant à la règle d'annotation sont annotés avec la valeur spécifiée dans la règle.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Annotations**.
2. Dans l'onglet **règles d'annotation**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle d'annotation**, entrez un nom pour la règle.
4. Sélectionnez un type d'objet dans la liste Type d'objet cible, puis sélectionnez un nom d'annotation et une valeur 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

Prenons l'exemple d'une condition du SVM de type objet, où le nom d'objet contient "svm_data".

Pour configurer la condition, procédez comme suit dans la boîte de dialogue Ajouter une règle d'annotation :

Étapes

1. Entrez un nom pour la règle d'annotation.
2. Sélectionner le type d'objet cible en tant que SVM.

3. Sélectionnez une annotation dans la liste d'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**.

Suppression de règles d'annotation

Vous pouvez supprimer des règles d'annotation de Active IQ Unified Manager lorsque les règles ne sont plus nécessaires.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 **Storage Management** > **Annotations**.
2. Dans l'onglet **règles d'annotation**, sélectionnez la règle d'annotation à supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui** pour confirmer la suppression.

Réorganisation des règles d'annotation

Vous pouvez modifier l'ordre dans lequel Unified Manager applique des règles d'annotation aux objets de stockage. Les règles d'annotation sont appliquées de façon séquentielle aux objets de stockage en fonction de leur rang. Lorsque vous configurez une règle d'annotation, le rang est le moins. Toutefois, vous pouvez modifier le rang de la règle d'annotation en fonction de vos besoins.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez sélectionner une ou plusieurs lignes et effectuer de nombreuses opérations glisser-déposer pour modifier le rang des règles d'annotation. Cependant, vous devez enregistrer les modifications pour que la repriorisation s'affiche dans l'onglet règles des annotations.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Annotations**.
2. Dans l'onglet **règles d'annotation**, cliquez sur **Réordonner**.
3. Dans la boîte de dialogue **Réordonner 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 s'affiche.

Envoi d'un bundle via l'interface utilisateur Web et la console de maintenance

Vous devez envoyer un pack de support si le problème que vous rencontrez nécessite des diagnostics et des dépannages plus détaillés qu'un message AutoSupport. Vous pouvez envoyer un pack au support technique à l'aide de l'interface utilisateur Web et de la console de maintenance d'Unified Manager.

Unified Manager stocke un maximum de deux packs de support complets et trois packs de support légers à la fois.

Informations connexes

"Fonctionnalités et rôles utilisateur de Unified Manager"

Envoi des messages AutoSupport et des packs de support 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 préserver l'intégrité de votre environnement. AutoSupport est activé par défaut et ne doit pas être désactivé pour bénéficier des avantages de NetAppActive IQ.

Vous pouvez envoyer des informations relatives au système de diagnostic et des données détaillées sur le serveur Unified Manager dans un message selon les besoins, planifier l'envoi périodique d'un message, ou même générer et envoyer des packs de support à l'équipe de support technique.

> Un utilisateur doté d'un rôle d'administrateur de stockage peut générer et envoyer à la demande des messages AutoSupport et des packs de support au support technique. Cependant, seul un administrateur ou un utilisateur de maintenance peut activer ou désactiver l'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 du stockage puisse envoyer des messages AutoSupport à la demande et des packs de support au support technique.

Envoi de messages AutoSupport à la demande

Vous pouvez générer et envoyer un message à la demande au support technique, à un destinataire d'e-mail spécifié, ou aux deux.

Étapes

1. Accédez à **général** > **AutoSupport** et effectuez l'une ou les deux opérations 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 spécifique de l'e-mail, cochez la case **Envoyer au destinataire** et entrez l'adresse e-mail du destinataire.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **générer et Envoyer AutoSupport**.

Activation du AutoSupport périodique

Vous pouvez envoyer régulièrement des messages spécifiques et prédéfinis au support technique pour le diagnostic et la résolution des problèmes. Cette fonctionnalité est activée par défaut. S'il est désactivé, 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 de données AutoSupport vers Active IQ**.
3. Si nécessaire, définissez le nom, le port et les informations d'authentification du serveur proxy HTTP comme indiqué dans la section Configuration du serveur proxy HTTP.
4. Cliquez sur **Enregistrer**.

Téléchargement de l'offre d'assistance à la demande

Vous pouvez générer et envoyer un bundle de support au support technique en fonction des exigences de résolution de problèmes. Unified Manager ne stocke que les deux derniers packs de support générés. Les anciens packs de support sont supprimés du système.

Comme certains types de données de support peuvent utiliser un grand nombre de ressources de cluster ou prendre beaucoup de temps, lorsque vous sélectionnez le pack de support complet, vous pouvez inclure ou exclure des types de données spécifiques pour réduire la taille du paquet de support. Vous avez également la possibilité de créer un pack de support léger qui contient seulement 30 jours de journaux et d'enregistrements de base de données de configuration — cela exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage du segment de mémoire du serveur.

Étapes

1. Accédez à **général** > **AutoSupport**.
2. Dans la section offre de support à la demande, cliquez sur **générer et envoyer un pack de support**.
3. Pour envoyer un bundle léger de support au support technique, dans la fenêtre contextuelle générer et envoyer un support, cochez la case **générer un support léger**.
4. Sinon, pour envoyer un pack de support complet, cochez la case **générer le bundle de support complet**. Sélectionnez les types de données spécifiques à inclure ou exclure dans le bundle 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 dans le serveur Unified Manager. Le support bundle 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**.

Configuration du serveur proxy HTTP

Vous pouvez désigner un proxy qui fournit l'accès Internet afin d'envoyer du contenu AutoSupport à l'assistance si votre environnement ne fournit pas un accès direct depuis le serveur Unified Manager. Cette section est disponible uniquement pour les utilisateurs de maintenance et d'administrateur.

- **Utiliser le proxy HTTP**

  Cochez cette case pour identifier le serveur utilisé comme proxy HTTP.

  Entrez 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.

  Entrez le nom d'utilisateur et le mot de passe requis pour s'authentifier auprès du proxy HTTP.

> Les proxys HTTP qui fournissent uniquement l'authentification de base ne sont pas pris en charge.

Accès à la console de maintenance

Si l'interface utilisateur Unified Manager n'est pas en cours de fonctionnement ou si vous devez effectuer 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.

Ce dont vous aurez besoin

Vous devez avoir installé et configuré Unified Manager.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.

> Lorsqu'il est installé sur VMware, si vous 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. La procédure suivante permet d'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 à l'aide de votre nom d'utilisateur et de votre mot de passe de maintenance.

Sur ce système d'exploitation…	Suivez ces étapes…
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 et le mot de passe de l'utilisateur de maintenance (umadmin). c. Entrez la commande `maintenance_console` et appuyez sur entrée.
Fenêtres	a. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Entrez la commande `maintenance_console` et appuyez sur entrée.

Le menu de la console de maintenance Unified Manager s'affiche.

Génération et téléchargement d'un bundle de support

Vous pouvez générer un pack contenant les informations de diagnostic, de manière à pouvoir l'envoyer au support technique pour obtenir de l'aide au dépannage.

Depuis Unified Manager 9.8, si votre serveur Unified Manager est connecté à Internet, vous pouvez également charger le pack de support à NetApp à partir de la console de maintenance.

Ce dont vous aurez besoin

Comme utilisateur de maintenance, vous devez avoir accès à la console de maintenance.

Comme certains types de données de support peuvent utiliser une grande quantité de ressources de cluster ou prendre beaucoup de temps, lorsque vous sélectionnez le bundle de support complet, vous pouvez spécifier des types de données à inclure ou exclure pour réduire la taille du paquet de support. Vous avez également la possibilité de créer un pack de support léger qui contient seulement 30 jours de journaux et d'enregistrements de base de données de configuration — cela exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage du segment de mémoire du serveur.

Unified Manager ne stocke que les deux derniers packs de support générés. Les anciens packs de support sont supprimés du système.

Étapes

1. Dans la console de maintenance **Menu principal**, sélectionnez **support/Diagnostics**.
2. Sélectionnez **Generate Light support Bundle** ou **Generate support Bundle** selon le niveau de détails que vous souhaitez obtenir dans le pack de support.
3. Si vous choisissez le bundle de support complet, sélectionnez ou désélectionnez les types de données suivants à inclure ou exclure dans le bundle de support :

- **vidage de base de données**

  Un vidage de la base de données MySQL Server.

- **vidage du tas**

  Snapshot de l'état des principaux processus du serveur Unified Manager. Cette option est désactivée par défaut et doit être sélectionnée uniquement sur demande du service client.

- * 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 support est toujours généré avec d'autres données Unified Manager.

4. Tapez `g`, puis appuyez sur entrée pour générer le paquet de support.

   Comme la génération d'un bundle de support est une opération consommant beaucoup de mémoire, vous êtes invité à vérifier que vous voulez bien générer le bundle de support à ce moment-là.

5. Tapez `y`, puis appuyez sur entrée pour générer le paquet de support.

   Si vous ne souhaitez pas générer le bundle de support pour le moment, tapez `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 inclure les statistiques de performances. Y compris les statistiques de performances, vous pouvez prendre beaucoup de temps et d'espace ; vous pouvez donc également vider la base de données sans y inclure les statistiques de performances :

   a. Entrez la date de début au format AAAAMMJJ.

      Par exemple, entrez `20210101` pour le 1er janvier 2021. Saisissez `n` si vous ne souhaitez pas inclure les statistiques de performances.

   b. Entrez le nombre de jours de statistiques à inclure, à partir de 12 h, à la date de début spécifiée.

      Vous pouvez entrer un nombre compris entre 1 et 10.

   Si vous ajoutez des statistiques de performances, le système affiche la période pendant laquelle les statistiques de performances seront collectées.

7. Une fois le pack créé, vous êtes invité à le télécharger sur NetApp. Tapez `y`, puis appuyez sur entrée.

   Vous devez saisir votre numéro de dossier de support.

8. Si vous avez déjà un numéro de dossier, saisissez-le et appuyez sur entrée. Sinon, appuyez simplement sur entrée.

   Le bundle de support est téléchargé vers NetApp.

Si votre serveur Unified Manager n'est pas connecté à Internet ou si vous ne pouvez pas télécharger le pack de support pour une autre raison, vous pouvez le récupérer et l'envoyer manuellement. Vous pouvez le récupérer à l'aide d'un client SFTP ou à l'aide des commandes CLI UNIX ou Linux. Sur les installations

Windows, vous pouvez utiliser Remote Desktop (RDP) pour récupérer le pack de prise en charge.

Le bundle de support généré réside dans le répertoire /support des systèmes VMware, dans /opt/netapp/data/support/ sur les systèmes Linux, et dans ProgramData\NetApp\OnCommandAppData\ocum\support sur les systèmes Windows.

Informations connexes

"Fonctionnalités et rôles utilisateur de Unified Manager"

Récupération du bundle 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 bundle de support à partir de votre serveur Unified Manager. Vous pouvez envoyer le pack d'assistance au support technique pour obtenir un diagnostic plus détaillé d'un problème. FileZilla ou WinSCP sont des exemples d'outils que vous pouvez utiliser.

Ce dont vous aurez besoin

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 support bundle.
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 permet d'afficher tous les modules de support existants.

4. Sélectionnez le répertoire de destination du bundle de support que vous souhaitez copier.
5. Sélectionnez le bundle de support que vous souhaitez copier et utilisez l'outil pour copier le fichier du serveur Unified Manager vers votre système local.

Récupération du bundle de support à l'aide d'un client UNIX ou Linux

Si vous êtes un utilisateur UNIX ou Linux, vous pouvez récupérer le bundle 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.

Ce dont vous aurez besoin

Vous devez être l'utilisateur de maintenance pour effectuer cette tâche.

Vous devez avoir généré un support bundle à l'aide de la console de maintenance et avoir le nom du support bundle disponible.

Étapes

1. Accédez à l'interface de ligne de commande via Telnet ou la console, à l'aide de votre serveur client Linux.

2. Accédez au /`support` répertoire.
3. Récupérez le pack support et copiez-le dans le répertoire local à l'aide de la commande suivante :

Si vous utilisez…	Ensuite, utilisez la commande suivante…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

Le nom du pack de support vous est fourni lorsque vous le générez à l'aide de la console de maintenance.

4. Saisissez le mot de passe utilisateur de maintenance.

Exemples

L'exemple suivant utilise SCP pour récupérer le pack de support :

```
        `$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

L'exemple suivant utilise SFTP pour récupérer le pack de support :

```
        `$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_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
```

Envoi d'un pack support au support technique

Pour obtenir des informations plus détaillées sur le diagnostic et le dépannage d'un problème que ne fournit un message AutoSupport, vous pouvez envoyer un pack d'assistance au support technique.

Ce dont vous aurez besoin

Vous devez accéder au pack pour l'envoyer au support technique.

Vous devez obtenir un numéro de dossier généré par le biais du site Web de support technique.

Étapes

1. Connectez-vous au site de support NetApp.
2. Téléchargez le fichier.

   "Télécharger un fichier vers NetApp"

Tâches et informations relatives à plusieurs flux de travail

Certaines tâches et textes de référence qui peuvent vous aider à comprendre et à effectuer un flux de travail sont courants pour de nombreux flux de travail dans Unified Manager. Vous pouvez notamment ajouter et revoir des notes concernant un événement, attribuer un événement, accuser réception et résoudre des événements, ainsi que des détails sur les volumes, les SVM (Storage Virtual machine), les agrégats, et ainsi de suite.

Les composants du cluster et les conflits

Vous pouvez identifier les problèmes de performance du cluster lorsqu'un composant du cluster entre en conflit. Les performances des charges de travail qui utilisent le ralentissement du composant et leur temps de réponse (latence) augmente pour les requêtes client, ce qui déclenche un événement dans Unified Manager.

Un composant en conflit ne peut pas se faire à un niveau optimal. Ses performances ont diminué, et la performance des autres composants et charges de travail du cluster, appelés *victimes*, peut avoir augmenté la latence. Pour mettre un composant à l'extérieur des conflits, vous devez réduire sa charge de travail ou augmenter sa capacité à gérer davantage de travail, de sorte que les performances puissent revenir à des niveaux normaux. Unified Manager collecte et analyse les performances des charges de travail toutes les cinq minutes. En effet, il ne détecte que lorsqu'un composant du cluster est constamment sur-utilisé. Les pics transitoires de surutilisation qui durent pendant une courte durée dans l'intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être soumis à des conflits car une ou plusieurs charges de travail y sont en concurrence pour que leurs demandes d'E/S soient traitées. Des charges de travail peuvent être affectées sur l'agrégat, ce qui entraîne une baisse des performances. Pour réduire la quantité d'activité sur l'agrégat, différentes étapes sont possibles : déplacer une ou plusieurs charges de travail vers un agrégat ou un nœud moins occupé, par exemple, afin de réduire les besoins globaux de la charge de travail sur l'agrégat en cours. Pour un groupe de règles de qualité de service, vous pouvez ajuster la limite de débit ou déplacer les workloads vers un autre groupe de règles, de sorte que les charges de travail ne soient plus restreintes.

Unified Manager contrôle les composants de cluster suivants pour vous alerter en cas de 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 la fin des transactions « de transfert prêt » avant que le cluster puisse répondre à une demande d'E/S. Si le composant réseau constitue un 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 de plusieurs charges de travail.

- **Traitement réseau**

Composant logiciel dans le cluster impliqué dans le traitement des E/S entre la couche de protocole et le cluster. Le traitement du réseau de traitement des nœuds a peut-être changé depuis la détection de l'événement. Si le composant de traitement de réseau est en conflit, son utilisation élevée au niveau du nœud de traitement réseau a un impact sur la latence d'une ou de plusieurs charges de travail.

Lors de l'utilisation d'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 de qualité de service max**

  Représente le paramètre de débit maximal (crête) du groupe de règles de qualité de service (QoS) de stockage affecté à la charge de travail. Si le composant de groupe de règles conflits, cela signifie que toutes les charges de travail du groupe de règles sont restreintes par la limite de débit définie, qui a un impact sur la latence d'une ou plusieurs de ces charges de travail.

- **Limite de qualité de service min**

  Représente la latence pour une charge de travail générée par le paramètre de débit de QoS minimal (attendu) attribué à d'autres workloads. Si, pour certaines charges de travail, la qualité de service minimale est définie sur la majorité de la bande passante pour garantir le débit promis, d'autres charges de travail sont restreintes et affichent une latence plus élevée.

- * Interconnexion de cluster*

  La représente les câbles et adaptateurs avec lesquels les nœuds en cluster sont physiquement connectés. Si le composant d'interconnexion de cluster est en conflit, cela signifie un temps d'attente élevé pour les demandes d'E/S au niveau de l'interconnexion de cluster se répercute sur la latence d'une ou de plusieurs charges de travail.

- **Traitement de données**

  Composant logiciel dans le cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient la charge de travail. Le traitement des données de traitement du nœud peut avoir changé depuis la détection de l'événement. Si le composant de traitement des données conflit, une utilisation élevée au niveau du nœud de traitement des données affecte la latence d'un ou de plusieurs workloads.

- **Activation du volume**

  Processus permettant de suivre l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1000 volumes sont actifs, ce processus surveille en même temps le nombre de volumes stratégiques devant accéder aux ressources par le biais du nœud. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques subissent une latence telle qu'elle est identifiée ici.

- **Ressources MetroCluster**

  La représente les ressources MetroCluster, y compris la NVRAM et les liens ISL, utilisés pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster rencontre des conflits, il s'agit d'un débit d'écriture élevé avec les charges de travail sur le cluster local ou d'un problème d'état de santé de la liaison ayant un impact sur la latence d'une ou de plusieurs charges de travail sur le cluster local. Si le cluster ne se trouve pas dans une configuration MetroCluster, cette icône n'est pas affichée.

- **Agrégat ou agrégat SSD**

  Agrégat de stockage sur lequel les charges de travail s'exécutent. Si le composant de l'agrégat est en conflit, une utilisation élevée de l'agrégat a un impact sur la latence d'une ou de plusieurs charges de travail. Un agrégat se compose de tous les disques durs, ou d'un mélange de disques durs et de disques SSD (un agrégat Flash Pool), ou d'une combinaison de disques durs et d'un niveau de cloud (un agrégat FabricPool). Un « agrégat SD » se compose de tous les SSD (un agrégat 100 % Flash), ou d'une combinaison de SSD et d'un niveau cloud (un agrégat FabricPool).

- * Latence 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 dans le cloud conflits, une grande quantité de lectures sur les volumes hébergés sur le Tier cloud ont une incidence sur la latence d'un ou de plusieurs workloads.

- **SnapMirror de synchronisation**

  Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur depuis le volume primaire vers le volume secondaire dans une relation SnapMirror synchrone. Si le composant SnapMirror synchrone entre en conflit, l'activité des opérations SnapMirror synchrone a un impact sur la latence d'un ou de plusieurs workloads.

Page de détails sur le volume / la santé

Vous pouvez utiliser la page de détails Volume / Santé pour afficher des informations détaillées sur un volume sélectionné, telles que la capacité, l'efficacité du stockage, la configuration, la protection, annotation et événements générés. Vous pouvez également afficher des informations sur les objets associés et les alertes associées pour ce volume.

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes pour le volume sélectionné :

- **Basculer vers l'affichage des performances**

  Vous permet de naviguer jusqu'à la page Détails du volume / performances.

- **Actions**

  - Ajouter une alerte

    Permet d'ajouter une alerte au volume sélectionné.

  - Modifier les seuils

    Permet de modifier les paramètres de seuil du volume sélectionné.

  - Annoter

    Permet d'annoter le volume sélectionné.

- Protéger

  Permet de créer des relations SnapMirror ou SnapVault pour le volume sélectionné.

- Relations

  Permet d'exécuter les opérations de relation de protection suivantes :

  - Modifier

    Lance la boîte de dialogue Modifier une relation qui vous permet de modifier les règles SnapMirror, les planifications et les taux de transfert maximum pour une relation de protection existante.

  - Abandonner

    Annule les transferts en cours pour une relation sélectionnée. Vous pouvez également 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 ligne de base.

  - Mise au repos

    Désactive temporairement les mises à jour programmées pour une relation sélectionnée. Les transferts déjà en cours doivent être terminés avant la suspension de la relation.

  - Pause

    Rompt la relation entre les volumes source et destination et modifie la destination en un volume en lecture-écriture.

  - Déposer

    Supprime définitivement la relation entre la source et la destination sélectionnées. Les volumes ne sont pas détruits et les copies Snapshot des volumes ne sont pas supprimées. Cette opération ne peut pas être annulée.

  - Reprendre

    Active les transferts programmés pour une relation mise en veille. Lors de l'intervalle de transfert planifié suivant, un point de contrôle de redémarrage est utilisé, s'il en existe un.

  - Resynchroniser

    Permet de resynchroniser une relation interrompue au préalable.

  - Initialiser/mettre à jour

    Permet d'effectuer un transfert de base de première fois sur une nouvelle relation de protection ou d'effectuer une mise à jour manuelle si la relation est déjà initialisée.

  - Resynchronisation inverse

    Permet de rétablir une relation de protection interrompue précédemment, en inversant la fonction de la source et de la destination en créant la copie de la destination d'origine de la source. Le contenu de la source est écrasé par le contenu sur la destination. De plus, les données plus récentes que les données de la copie Snapshot commune sont supprimées.

- Restaurer

  Permet de restaurer les 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/intégrité".

  > Le bouton Restaurer et les boutons d'opération de relation ne sont pas disponibles pour les volumes qui se trouvent dans des relations de protection synchrones.

- **Voir volumes**

  Permet de naviguer vers 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 la capacité des snapshots

    Affiche l'espace de données utilisé par les copies Snapshot.

  - Utilisé

    Affiche l'espace utilisé par les données du volume.

  - Avertissement

    Indique que l'espace du volume est presque plein. Si ce seuil est atteint, l'événement espace presque plein est généré.

  - Erreur

    Indique que l'espace du volume est plein. Si ce seuil est atteint, l'événement espace plein est généré.

  - Inutilisable

    Indique que l'événement espace de volume à provisionnement fin en cas de risque est généré et que l'espace dans le volume à provisionnement fin est menacé en raison des problèmes de capacité de l'agrégat. La capacité inutilisable s'affiche uniquement pour les volumes à provisionnement fin.

  - Graphique de données

    Affiche la capacité totale des 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 pouvant être utilisé par les données du volume, lequel peut être l'un des éléments suivants :

    - Capacité de données réelle du volume pour les conditions suivantes :

        - Croissance automatique désactivée.
        - Le volume activé pour la croissance automatique a atteint la taille maximale.
        - Le volume provisionné de manière automatique ne peut pas augmenter davantage.
    - Capacité des données du volume après avoir pris en compte la taille maximale du volume (pour les volumes à provisionnement fin et pour les volumes à provisionnement fin lorsque l'agrégat dispose d'espace pour que ce volume atteigne la taille maximale)
    - Capacité de données du volume après avoir examiné la taille de croissance automatique suivante possible (pour les volumes en provisionnement fin qui ont un seuil de pourcentage de croissance automatique)
  - Graphique sur les copies Snapshot

    Ce graphique s'affiche uniquement lorsque la capacité Snapshot utilisée ou la réserve Snapshot n'est pas égale à zéro.

  Les deux graphiques affichent la capacité par laquelle la capacité Snapshot dépasse la réserve Snapshot si la capacité Snapshot utilisée dépasse la réserve Snapshot.

- **Logique de capacité**

  Affiche les caractéristiques d'espace logique du volume. L'espace logique indique la taille réelle des données stockées sur disque sans appliquer les économies réalisées grâce aux technologies d'efficacité du stockage ONTAP.

  - Rapport sur l'espace logique

    Indique si le volume a configuré un rapport d'espace logique. La valeur peut être activée, désactivée ou non applicable. « Non applicable » s'affiche pour les volumes situés sur des versions plus anciennes d'ONTAP ou sur des volumes qui ne prennent pas en charge la création de rapports sur l'espace logique.

  - Utilisé

    Affiche la quantité d'espace logique utilisée par les données du volume ainsi que le pourcentage d'espace logique utilisé en fonction de la capacité totale des données.

  - Application de l'espace logique

    Indique si l'application de l'espace logique est configurée pour les volumes à provisionnement fin. Lorsque cette option est activée, la taille logique utilisée du volume ne peut pas être supérieure à la taille du volume physique actuellement définie.

- **Croissance automatique**

  Indique si le volume augmente automatiquement lorsqu'il est en manque d'espace.

- **Garantie d'espace**

  Affiche le contrôle de réglage du volume FlexVol lorsqu'un volume supprime des blocs libres d'un agrégat. Ces blocs sont alors garantis pour être disponibles pour les écritures dans les fichiers du volume. La garantie d'espace peut être définie sur l'une des options suivantes :

  - Aucune

Aucune garantie d'espace n'est configurée pour le volume.

- Fichier

  La taille complète des fichiers peu écrits (par exemple, LUN) est garantie.

- Volumétrie

  La taille totale du volume est garantie.

- Partiel

  Le volume FlexCache réserve de l'espace en fonction de sa taille. Si la taille du volume FlexCache est supérieure ou égale à 100 Mo, la garantie d'espace minimale est définie par défaut sur 100 Mo. Si la taille du volume FlexCache est inférieure à 100 Mo, la garantie d'espace minimale est définie sur la taille du volume FlexCache. Si la taille du volume FlexCache augmente plus tard, la garantie d'espace minimale n'est pas incrémentée.

> La garantie d'espace est partielle lorsque le volume est de type Data-cache.

- **Détails (physique)**

  Affiche les caractéristiques physiques du volume.

- **Capacité totale**

  Affiche la capacité physique totale du volume.

- **Capacité de données**

  Affiche la quantité d'espace physique utilisé par le volume (capacité utilisée) et la quantité d'espace physique toujours disponible (capacité libre) dans le volume. Ces valeurs sont également affichées sous forme de pourcentage de la capacité physique totale.

  Lorsque l'événement Volume Space at Risk 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 ne peut pas être utilisée (capacité inutilisable) en raison de problèmes de capacité de l'agrégat sont affichés.

- **Réserve snapshot**

  Affiche l'espace utilisé par les copies Snapshot (capacité utilisée) et la quantité d'espace disponible pour les copies Snapshot (capacité disponible) dans le volume. Ces valeurs sont également affichées sous forme de pourcentage de la réserve d'instantanés totale.

  Lorsque l'événement Volume Space at Risk est généré pour les volumes à provisionnement fin, l'espace utilisé par les copies Snapshot (capacité utilisée) et la quantité d'espace disponible sur le volume, mais ne peut pas être utilisé pour les copies Snapshot (capacité inutilisable) du fait des problèmes de capacité de l'agrégat s'affiche.

- **Seuils de volume**

  Affiche les seuils de capacité de volume suivants :

  - Presque plein seuil

Spécifie le pourcentage auquel un volume est presque plein.

- Seuil maximal

  Spécifie le pourcentage auquel un volume est plein.

- **Autres détails**
  - Taille de croissance automatique max

    Affiche la taille maximale jusqu'à laquelle le volume peut augmenter automatiquement. La valeur par défaut est 120 % de la taille du volume lors de sa création. Ce champ s'affiche uniquement lorsque la croissance automatique est activée pour le volume.

  - Quota qtree en fonction de la capacité effective

    Affiche l'espace réservé dans les quotas.

  - Quota qtree en excès de capacité

    Affiche la quantité d'espace pouvant être utilisée avant que le système ne génère l'événement Volume qtree quota overengage.

  - 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 de sorte que les objets soient entièrement protégés pour les écrasements. Si la réserve fractionnaire est inférieure à 100 %, l'espace réservé de tous les fichiers réservés dans ce volume est réduit au pourcentage de réserve fractionnaire.

  - Taux de croissance quotidien des instantanés

    Affiche la modification (en pourcentage, ou en Ko, Mo, Go, etc.) qui a lieu toutes les 24 heures des copies Snapshot du volume sélectionné.

  - Nombre de jours de snapshot à plein

    Affiche le nombre estimé de jours restants avant que l'espace réservé pour les copies Snapshot du volume n'atteigne le seuil spécifié.

    Le champ jours instantanés à pleins affiche une valeur non applicable lorsque le taux de croissance des copies Snapshot du volume est nul ou négatif, ou lorsque des données insuffisantes sont utilisées pour calculer le taux de croissance.

  - Suppression automatique de l'instantané

    Spécifie si les copies Snapshot sont automatiquement supprimées de l'espace disponible lorsqu'une écriture sur un volume échoue en raison d'un manque d'espace dans l'agrégat.

  - Copies Snapshot

    Affiche des informations sur les copies Snapshot du volume.

    Le nombre de copies Snapshot du volume s'affiche sous la forme d'un lien. Lorsque vous cliquez sur le lien, la boîte de dialogue copies Snapshot s'affiche dans un volume, qui affiche le détail des copies

Snapshot.

Le nombre de copies Snapshot est mis à jour environ toutes les heures. Toutefois, la liste des copies Snapshot est mise à jour au moment où vous cliquez sur l'icône. Il peut y avoir une différence entre le nombre de copies Snapshot affichées dans la topologie et le nombre de copies Snapshot répertoriées lorsque vous cliquez sur l'icône.

- **Déplacement de volume**

  Affiche l'état de l'opération de déplacement de volume en cours ou de la dernière opération de déplacement de volume 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 et l'heure de fin, et 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 des informations détaillées sur le volume sélectionné, telles que la stratégie d'exportation, le type RAID, les fonctions liées à la capacité et à l'efficacité du stockage du volume :

- **Aperçu**
  - Nom complet

    Affiche le nom complet du volume.
  - 64 bits

    Affiche le nom de l'agrégat sur lequel réside le volume ou le nombre d'agrégats sur lequel réside le volume FlexGroup.
  - Règle de hiérarchisation

    Affiche le jeu de règles de Tiering du volume ; si le volume est déployé sur un agrégat compatible FabricPool. La règle peut être aucun, Snapshot uniquement, sauvegarde, Auto ou tous.
  - VM 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 d'accès du SVM vers lequel le volume est monté est également affiché. Vous pouvez cliquer sur le lien **Historique** pour afficher les cinq dernières modifications apportées au chemin de jonction.
  - Export policy

    Affiche le nom de l'export policy créée pour le volume. Vous pouvez cliquer sur le lien pour afficher des détails sur les export-policies, les protocoles d'authentification et l'accès activé sur les volumes appartenant à la 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.

  > Il est possible d'afficher plusieurs types RAID pour les volumes FlexGroup, car les volumes constitutifs de FlexGroups peuvent se trouver sur des agrégats de différents types.

- Type de SnapLock

  Affiche le type SnapLock de l'agrégat qui contient le volume.

- Expiration du SnapLock

  Affiche la date d'expiration du volume SnapLock.

- **Capacité**
  - Provisionnement fin

    Indique si le provisionnement fin est configuré pour le volume.

  - Croissance automatique

    Indique si le volume flexible augmente automatiquement au sein d'un agrégat.

  - Suppression automatique de l'instantané

    Spécifie si les copies Snapshot sont automatiquement supprimées de l'espace disponible lorsqu'une écriture sur un volume échoue en raison d'un manque d'espace dans l'agrégat.

  - Quotas

    Indique si les quotas sont activés pour le volume.

- **Efficacité**
  - Compression

    Indique si la compression est activée ou désactivée.

  - Déduplication

    Indique 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 des règles. Si le mode est défini sur planifié, le programme d'opérations 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 fait partie d'une relation SnapVault, le type affiché est SnapVault. Pour tout autre volume, le type est affiché comme normal.

- Règles d'efficacité du stockage

  Spécifie le nom de la règle d'efficacité du stockage qui a été attribuée à ce volume par l'intermédiaire d'Unified Manager. Cette règle peut contrôler les paramètres de compression et de déduplication.

- **Protection**
  - Copies Snapshot

    Indique si les copies Snapshot automatiques sont activées ou désactivées.

Onglet de protection

L'onglet protection affiche des 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 reprise après incident de la machine virtuelle de stockage) pour un volume sélectionné. Pour tout autre type de relation, seule la propriété Type de relation est affichée. Si un volume primaire est sélectionné, seules les stratégies de copie Snapshot gérées et locales sont affichées. Les propriétés affichées pour les relations SnapMirror et SnapVault sont les suivantes :

  - Volume source

    Affiche le nom de la source du volume sélectionné si le volume sélectionné est une destination.

  - Etat de décalage

    Affiche l'état de mise à jour ou de décalage de transfert pour une relation de protection. L'état peut être erreur, Avertissement ou critique.

    L'état de décalage n'est pas applicable pour les relations synchrones.

  - Durée du décalage

    Affiche l'heure à laquelle les données du miroir sont en retard derrière 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 à et est géré par un service de stockage.

- Réplication flexible des versions

  Affiche Oui, Oui avec option de sauvegarde ou aucun. Oui indique que la réplication SnapMirror est possible même si les volumes source et de destination exécutent différentes versions du logiciel ONTAP. Oui avec l'option de sauvegarde indique l'implémentation de la protection SnapMirror avec la possibilité de conserver plusieurs versions de copies de sauvegarde sur le volume de destination. Aucun indique que la réplication de version flexible n'est pas activée.

- Capacité de relation

  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 n'importe quel type de relation, y compris Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync, Et Sync.

- État de la relation

  Affiche l'état de la relation SnapMirror ou SnapVault. Cet état peut être non initialisé, SnapMirror ou Broken-off. 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 du transfert pour la relation de protection. Le statut du transfert peut être l'un des suivants :

  - Abandon

    Les transferts SnapMirror sont activés. Cependant, une opération d'abandon du transfert susceptible d'inclure la suppression du point de contrôle est en cours.

  - Vérification

    Le volume de destination fait l'objet d'un contrôle 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.

  - In-Sync

    Les données des deux volumes de 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 en cours.

- Suspendu

  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 le transfert est en cours.

- La transition

  Le transfert asynchrone des données du volume source vers le volume de destination est terminé, et la transition vers le volume synchrone a démarré.

- En attente

  Un transfert SnapMirror a été initié, mais certaines tâches associées attendent d'être mises en file d'attente.

◦ Taux de transfert max

Affiche le taux de transfert maximal de la relation. Le taux de transfert maximal peut être une valeur numérique en kilo-octets par seconde (Kbps), mégaoctets par seconde (Mbps), gigaoctets par seconde (Gbit/s) ou téraoctets par seconde (Tbit/s). Si aucune limite n'est affichée, le transfert de base entre les relations est illimité.

◦ Règle SnapMirror

Affiche la règle de protection du volume. DPDefault indique la règle de protection par défaut de miroir asynchrone, XDPDefault indique la stratégie de coffre-fort asynchrone par défaut, et DPSyncDefault indique la stratégie par défaut de MirrorVault asynchrone. StrictSync indique la règle de protection synchrone par défaut et Sync indique la règle synchrone par défaut. Vous pouvez cliquer sur le nom de la stratégie pour afficher les détails associés à cette stratégie, notamment les informations suivantes :

- Priorité de transfert
- Ignorer le réglage de l'heure d'accès
- Limite de tentatives
- Commentaires

        - Étiquettes SnapMirror
        - Paramètres de conservation
        - Copies Snapshot réelles
        - Conservez les copies Snapshot
        - Seuil d'avertissement de rétention
        - Copies Snapshot 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.
    - Mettre à jour le planning

      Affiche la planification SnapMirror affectée à la relation. Le fait de placer le curseur sur l'icône d'information affiche les détails de l'horaire.

    - Règle Snapshot locale

      Affiche la règle de copie Snapshot du volume. La règle est définie par défaut, aucun ou aucun nom donné à une règle personnalisée.

    - Protégé par

      Affiche le type de protection utilisé pour le volume sélectionné. Par exemple, si un volume est protégé par des relations de groupe de cohérence et de volume SnapMirror, ce champ affiche à la fois SnapMirror et Groupe de cohérence. Ce champ fournit également un lien qui vous redirige vers la page des relations pour afficher l'état de la relation unifiée. Ce lien ne s'applique qu'aux relations constitutives.

    - Groupe de cohérence

      Pour les volumes protégés par des 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 inclut des représentations graphiques de tous les volumes associés au volume sélectionné. Le volume sélectionné est indiqué par une bordure grise foncée et les lignes entre volumes de 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 gras doubles spécifient une relation miroir asynchrone, une ligne Bold unique spécifie une relation de coffre-fort asynchrone, des lignes simples doubles spécifient une relation MirrorVault asynchrone, et une ligne Bold et une ligne non Bold spécifie 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 dans lequel vous pouvez choisir de protéger le volume ou de restaurer les données. Un clic droit sur une relation permet d'afficher un menu dans lequel vous pouvez modifier, abandonner, arrêter, interrompre, supprimer, ou reprendre une relation.

  Les menus ne s'affichent pas dans les cas suivants :

    - Si les paramètres RBAC n'autorisent pas cette action, par exemple, si vous disposez uniquement des privilèges d'opérateur
    - Si le volume se trouve dans une relation de protection synchrone

- Lorsque l'ID du volume est inconnu, par exemple, lorsque vous disposez d'une relation intercluster et que le cluster de destination n'a pas encore été découvert en cliquant sur un autre volume de la topologie sélectionne et affiche les informations correspondant au volume en question. 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. Il peut également indiquer que les informations relatives à la capacité sont manquantes. Si vous positionnez votre curseur sur le point d'interrogation, des informations supplémentaires s'affichent, y compris des suggestions d'actions correctives.

La topologie affiche les informations relatives à la capacité du volume, au décalage, aux copies Snapshot et au dernier transfert de données réussi s'il est conforme à l'un des plusieurs modèles de topologie communs. Si une topologie n'est pas conforme à l'un de ces modèles, les informations relatives au décalage du volume et au dernier transfert de données réussi sont affichées dans une table de relations sous la topologie. Dans ce cas, la ligne en surbrillance du 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 de topologie incluent les informations suivantes :

- Capacité

  Affiche la capacité totale utilisée par le volume. Lorsque vous placez le curseur sur un volume de la topologie, les paramètres d'avertissement et de seuil critique actuels de ce volume s'affichent 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 **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 **LAG** est grisée, les informations de décalage du volume sélectionné s'affichent dans la table de relations sous la topologie, ainsi que les informations de décalage pour tous les volumes associés.

- Snapshot

  Affiche le nombre de copies Snapshot disponibles pour un volume. En désactivant la case **Snapshot**, toutes les informations de copie Snapshot sont masqués pour tous les volumes de la topologie. Si vous cliquez sur l'icône d'une copie Snapshot ( ), la liste des copies Snapshot d'un volume s'affiche. Le nombre de copies Snapshot affichées à côté de l'icône est mis à jour environ toutes les heures. Toutefois, la liste des copies Snapshot est mise à jour au moment où vous cliquez sur l'icône. Il peut y avoir une différence entre le nombre de copies Snapshot affichées dans la topologie et le nombre de copies Snapshot répertoriées lorsque vous cliquez sur l'icône.

- Dernier transfert réussi

  Affiche la quantité, la durée, l'heure et la date du dernier transfert de données réussi. Lorsque la case **dernier transfert réussi** est grisée, le dernier transfert réussi pour le volume sélectionné s'affiche dans la table de relations sous la topologie, ainsi que les dernières informations de transfert réussies 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 historiques sont disponibles : la durée du décalage de la relation entrante, la durée du transfert de la relation entrante et la 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 primaire, les graphiques sont vides et le message aucune donnée trouvée s'affiche. Si les volumes sont protégés par des relations synchrones du groupe de cohérence et SnapMirror, les informations relatives à la durée du transfert de la relation et à la taille du transfert de la relation ne s'affichent pas.

Vous pouvez sélectionner un type de graphique dans la liste déroulante située en haut du volet Historique. Vous pouvez également afficher les détails d'une période donnée en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques historiques peuvent vous aider à identifier les tendances : par exemple, si de grandes quantités de données sont transférées en même temps que le jour ou la semaine, ou si le seuil d'avertissement de décalage ou d'erreur de décalage est constamment dépassé, vous pouvez prendre l'action appropriée. En outre, vous pouvez cliquer sur le bouton **Exporter** pour créer un rapport au format CSV pour le graphique que vous consultez.

Les graphiques de l'historique de protection affichent les informations suivantes :

- **Durée du décalage de la relation**

  Affiche les secondes, minutes ou heures sur l'axe vertical (y) et affiche les jours, les mois ou les années sur l'axe horizontal (x), en fonction de la période de durée sélectionnée. La valeur supérieure sur l'axe y indique la durée maximale de décalage atteinte dans la période de durée indiquée dans l'axe 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. Si vous placez le curseur sur ces lignes, le réglage du seuil s'affiche. La ligne horizontale bleue indique la durée du décalage. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant le curseur sur une zone d'intérêt.

- **Durée du transfert de la relation**

  Affiche les secondes, minutes ou heures sur l'axe vertical (y) et affiche les jours, les mois ou les années sur l'axe horizontal (x), en fonction de la période de durée sélectionnée. La valeur supérieure de l'axe y indique la durée maximale de transfert atteinte dans la période de durée indiquée dans l'axe X. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant le curseur sur la zone d'intérêt.

  Ce graphique n'est pas disponible pour les volumes qui se trouvent dans des relations de protection synchrone.

- **Relation transférée taille**

  Affiche les octets, kilo-octets, 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 de l'axe y indique la taille de transfert maximale atteinte dans la période de durée indiquée dans l'axe x. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant le curseur sur une zone d'intérêt.

  Ce graphique n'est pas disponible pour les volumes qui se trouvent dans des relations de protection synchrone.

Zone historique

La zone Historique affiche des graphiques qui fournissent des informations sur la capacité et les réservations

d’espace du volume sélectionné. En outre, vous pouvez cliquer sur le bouton **Exporter** pour créer un rapport au format CSV pour le graphique que vous consultez.

Les graphiques peuvent être vides et le message aucune donnée trouvée s’affiche lorsque les données ou l’état du volume restent inchangés pendant un certain temps.

Vous pouvez sélectionner un type de graphique dans la liste déroulante située en haut du volet Historique. Vous pouvez également afficher les détails d’une période donnée en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques de l’historique peuvent vous aider à identifier les tendances. Par exemple, si l’utilisation du volume dépasse systématiquement le seuil presque plein, vous pouvez prendre l’action appropriée.

Les graphiques de l’historique affichent les informations suivantes :

- **Capacité en volume utilisée**

  Affiche la capacité utilisée dans le volume et la tendance dans la façon dont la capacité de volume est utilisée en fonction de l’historique d’utilisation, sous forme de graphiques en octets, kilo-octets, mégaoctets, etc., sur l’axe vertical (y). La période s’affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende capacité utilisée du volume, la ligne du graphique capacité utilisée du volume 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 de l’utilisation, ainsi que la capacité utilisée, la capacité totale et les économies d’espace réalisées grâce à la déduplication et à la compression, sous forme de graphiques en ligne, en octets, en kilo-octets, en mégaoctets, et ainsi de suite, sur l’axe vertical (y). La période s’affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Trend Capacity Used, la ligne de graphique Trend Capacity Used est masquée.

- **Capacité en volume utilisée (%)**

  Affiche la capacité utilisée dans le volume et la tendance dans la façon dont la capacité de volume est utilisée en fonction de l’historique d’utilisation, sous forme de graphiques linéaires, en pourcentage, sur l’axe vertical (y). La période s’affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende capacité utilisée du volume, la ligne du graphique capacité utilisée du volume est masquée.

- **Capacité de snapshot utilisée (%)**

  Affiche le seuil d’avertissement de la réserve Snapshot et des snapshots sous forme de graphiques en ligne, ainsi que la capacité utilisée par les copies Snapshot sous forme de graphique de zone, en pourcentage, sur l’axe vertical (y). Le débordement de l’instantané est représenté avec des couleurs différentes. La période s’affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende de réserve Snapshot, la ligne du graphique de réserve Snapshot est masquée.

Liste des événements

La liste Evénements affiche des détails sur les événements nouveaux et acquittés :

- **Gravité**

  Affiche la gravité de l'événement.

- **Événement**

  Affiche le nom de l'événement.

- **Temps déclenché**

  Affiche le temps écoulé depuis la génération de l'événement. Si le temps écoulé dépasse une semaine, l'heure à laquelle l'événement a été généré s'affiche.

Volet Annotations associées

Le volet Annotations associées permet d'afficher les détails d'annotation associés au volume sélectionné. Les détails incluent le nom de l'annotation et les valeurs d'annotation qui sont appliquées au volume. Vous pouvez également supprimer des annotations manuelles du volet Annotations associées.

Panneau périphériques 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 liés 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 contenant le volume sélectionné. Pour les volumes FlexGroup, le nombre d'agrégats composant le FlexGroup est indiqué.

- **Volumes dans l'agrégat**

  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, sur la base 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 affichent l'état critique, l'état affiché est critique. Ce composant n'apparaît pas pour les volumes FlexGroup.

- **Qtrees**

  Affiche le nombre de qtrees que le volume sélectionné contient et la capacité de qtrees avec quota que le volume sélectionné contient. La capacité des qtrees avec quota est affichée en fonction de la capacité des données du volume. L'état de santé des qtrees est également affiché, selon le niveau de sévérité le plus élevé. Par exemple, si un volume a dix qtrees, cinq sont associés à l'état Avertissement et les cinq autres ayant l'état critique, l'état affiché est critique.

- **Partages NFS**

  Affiche le nombre et l'état des partages NFS associés au volume.

- **Partages SMB**

  Affiche le nombre et l'état des partages SMB/CIFS.

- **LUN**

  Affiche le nombre et la taille totale de toutes les LUN du volume sélectionné. L'état de santé des LUN est également affiché, sur la base 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 sont affichés uniquement 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 n'est affiché que si le volume sélectionné est un volume FlexClone.

Volet groupes associés

Le volet groupes associés 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 en modifiant une alerte existante en cliquant sur le nom de l'alerte.

VM de stockage / page de détails d'intégrité

Vous pouvez utiliser la page Storage VM / Health details pour afficher des informations détaillées sur la VM de stockage sélectionnée, notamment son intégrité, sa capacité, sa configuration, les règles de données, les interfaces logiques (LIF), LUN, qtrees, utilisateur, quotas de groupe d'utilisateurs et détails de protection . Vous pouvez également afficher des informations sur les objets associés et les alertes associées pour la VM de stockage.

> Vous pouvez surveiller uniquement les machines virtuelles de stockage des données.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes pour la VM de stockage sélectionnée :

- **Basculer vers l'affichage des performances**

  Permet de naviguer vers la page Storage VM / Performance Details.

- **Actions**
  - Ajouter une alerte

    Permet d'ajouter une alerte à la machine virtuelle de stockage sélectionnée.

  - Annoter

    Permet d'annoter la machine virtuelle de stockage sélectionnée.

- **Afficher les machines virtuelles de stockage**

  Permet de naviguer vers la vue intégrité : 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 liés à divers objets tels que les volumes, les agrégats, les LIF NAS, les LIF SAN, les LUN, Protocoles, services, partages NFS et 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 des volumes qui affiche des avertissements pour afficher la liste des volumes ayant des problèmes de capacité avec la gravité correspondante.

- **Problèmes de disponibilité**

  Affiche, sous forme de graphique, le nombre total d'objets, y compris les objets ayant des problèmes de disponibilité et les objets qui n'ont aucun problème de disponibilité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations figurant sous le graphique fournissent des informations détaillées sur les problèmes de disponibilité susceptibles d'avoir un impact ou d'avoir déjà affecté la disponibilité des données dans la machine virtuelle de stockage. Par exemple, des informations s'affichent concernant les LIF NAS et les LIF SAN qui sont en panne et 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 qui présentent des problèmes de capacité et des objets qui n'ont aucun problème de capacité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations figurant sous le graphique fournissent des informations détaillées sur les problèmes de capacité susceptibles d'avoir un impact ou qui ont déjà eu un impact sur la capacité des données de la machine virtuelle de stockage. Par exemple, des informations s'affichent concernant les agrégats susceptibles d'enfreindre les valeurs de seuil définies.

- **Questions de protection**

  Fournit un aperçu rapide de l'état de protection de ces machines virtuelles en affichant, dans une boîte de dialogue de champ, le nombre total de relations, y compris les relations qui ont des problèmes de protection et des relations qui n'ont aucun problème de protection. Vous pouvez également afficher l'état de la relation DR de la machine virtuelle de stockage pour la VM de stockage sélectionnée. Les événements de relations de reprise après incident de la machine virtuelle de stockage sont affichés ici et un clic sur les événements vous permet d'accéder à la page de détails de l'événement. Lorsque des volumes non protégés sont présents, un clic sur le lien indique l'état : tous les volumes. La vue à partir de

laquelle vous pouvez afficher une liste filtrée des volumes non protégés sur la machine virtuelle de stockage est affichée. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Lorsque vous cliquez sur un graphique, vous accédez à la relation : vue toutes les relations, où vous pouvez afficher une liste filtrée des détails de la relation de protection. Les informations figurant sous le graphique fournissent des informations détaillées sur les problèmes de protection qui peuvent avoir un impact ou ont déjà affecté la protection des données dans la VM de stockage. Par exemple, des informations s'affichent concernant les volumes dont la réserve Snapshot est presque pleine ou qui présentent 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 s'affichent pour un VM de stockage avec volume FlexVol ou 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.

  - Garantie disponible

    Affiche l'espace disponible garanti pour les données disponibles pour les volumes de 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 ayant des problèmes de capacité**

  La liste volumes avec problèmes de capacité affiche, sous forme de tableau, des informations détaillées sur les volumes ayant des problèmes de capacité :

  - État

    Indique que le volume a un problème lié à la capacité d'une gravité indiquée.

    Vous pouvez déplacer le pointeur de la souris 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 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 affecté 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 s'affichent avec des informations telles que le nom de l'événement, l'heure et la date du déclenchement des événements, ainsi que le nom de l'administrateur auquel l'événement est affecté. 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 même gravité ou différents niveaux de gravité. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un volume a deux événements avec des niveaux d'erreur et d'avertissement, seul le niveau d'erreur est affiché.

- Volumétrie

  Affiche le nom du volume.

- Capacité de données utilisée

  Affiche, sous forme de graphique, des informations sur l'utilisation de la capacité du volume (en pourcentage).

- Jours avant la date complète

  Affiche le nombre estimé de jours restants avant que le volume n'atteigne sa capacité maximale.

- Provisionnement fin

  Indique si la garantie d'espace est définie pour le volume sélectionné. Les valeurs valides sont Oui et non

- 64 bits

  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 la FlexGroup.

Onglet Configuration

L'onglet Configuration affiche des détails de configuration sur la machine virtuelle de stockage sélectionnée, tels que son cluster, son volume root, le type de volumes qu'elle contient (volumes FlexVol), les règles et la protection créée sur le VM de stockage :

- **Aperçu**
  - Cluster

    Affiche le nom du cluster auquel appartient la VM de stockage.

  - Type de volume autorisé

    Affiche le type de volumes pouvant être créés sur la machine virtuelle de stockage. Il peut s'agir de FlexVol ou de FlexVol/FlexGroup.

  - Volume racine

    Affiche le nom du volume root de la VM de stockage.

- Protocoles autorisés

  Affiche le type de protocoles pouvant être configurés sur la VM de stockage. Indique également si un protocole est actif ( ), inactif ( ) ou n'est pas configuré ( ).

- **Interfaces de réseau de données**
  - NAS

    Affiche le nombre d'interfaces NAS associées à la machine virtuelle de stockage. Indique également si les interfaces sont en cours ( ) ou en panne ( ).

  - SAN

    Affiche le nombre d'interfaces SAN associées à la machine virtuelle de stockage. Indique également si les interfaces sont en cours ( ) ou en panne ( ).

  - NVMe-FC

    Affiche le nombre d'interfaces FC-NVMe associées à la machine virtuelle de stockage. Indique également si les interfaces sont en cours ( ) ou en panne ( ).

- * 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 en cours ( ) ou en panne ( ).

- **Politiques**
  - Snapshots

    Affiche le nom de la règle Snapshot créée sur la machine virtuelle de stockage.

  - Export-règles

    Affiche le nom de l'export policy si une seule policy est créée ou affiche le nombre de export policy si plusieurs policies sont créées.

- **Protection**
  - Reprise après incident des machines virtuelles de stockage

    Indique si la machine virtuelle de stockage sélectionnée est protégée, de destination ou non protégée, ainsi que le nom de la destination sur laquelle la machine virtuelle de stockage est protégée. Si la VM de stockage sélectionnée est destination, les détails de la VM de stockage source sont affichés. En cas de « Fan-Out », ce champ affiche le nombre total de machines virtuelles de stockage de destination sur lesquelles la machine virtuelle de stockage est protégée. La liaison de nombre vous amène à la grille des relations de VM 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 à partir du nombre total de volumes. Si vous visualisez une machine virtuelle de stockage de destination, le lien numérique est destiné aux 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. Ce type peut être DNS (Domain Name System) ou NIS (Network information Service).

  - État

    Affiche l'état du service, qui peut être Haut ( ), Bas ( ) ou non configuré ( ).

  - Nom de domaine

    Affiche les noms de domaine complets (FQDN) du serveur DNS pour les services DNS ou le 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 FQDN 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 Network interfaces (interfaces réseau) affiche des détails sur les interfaces de réseau de données créées sur la machine virtuelle de stockage sélectionnée :

- **Interface réseau**

  Affiche le nom de l'interface créée sur la machine virtuelle de stockage sélectionnée.

- **État opérationnel**

  Affiche l'état opérationnel de l'interface, qui peut être Haut ( ), Bas ( ) ou Inconnu ( ). Le statut opérationnel d'une interface est déterminé par le statut de ses ports physiques.

- **Statut administratif**

  Affiche l'état administratif de l'interface, qui peut être Haut ( ), Bas ( ) ou Inconnu ( ). Le statut administratif d'une interface est contrôlé par l'administrateur du stockage pour modifier la configuration ou la maintenance. Le statut administratif peut être différent du statut opérationnel. Cependant, si le statut administratif d'une interface est arrêté, le statut opérationnel est désactivé par défaut.

- **Adresse IP / WWPN**

  Affiche l'adresse IP des interfaces Ethernet et le WWPN (World Wide Port Name) des 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 données ou gestion.

- **Port domicile**

  Affiche le port physique auquel l'interface a été associée à l'origine.

- **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'accueil.

- **Port Set**

  Affiche le port 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 règle de basculement par défaut est « Next » (Suivant). La règle de basculement ne s'applique pas aux interfaces FC et iSCSI.

- **Groupes de routage**

  Affiche le nom du groupe de routage. Vous pouvez afficher plus d'informations sur les routes et la passerelle de destination en cliquant sur le nom du groupe de routage.

  Les groupes de routage ne sont pas pris en charge par ONTAP 8.3 ou version ultérieure et une colonne vide s'affiche donc pour ces clusters.

- **Groupe de basculement**

  Affiche le nom du groupe de basculement.

Onglet qtrees

L'onglet qtrees affiche des informations détaillées 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 de la capacité qtree d'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 qtree 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 pour tous les clusters de votre data Center. Certains champs de qtrees supplémentaires apparaissent dans le fichier CSV exporté.

- **Statut**

  Affiche le statut actuel du qtree. L'état 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 le statut 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 à laquelle l'événement a été déclenché, le nom de l'administrateur à qui l'événement est affecté, 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 s'affichent avec des informations telles que le nom de l'événement, l'heure et la date du déclenchement des événements, et le nom de l'administrateur à qui l'événement est affecté. 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 différents niveaux d'importance. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un qtree possède deux événements ayant des niveaux de gravité d'erreur et d'avertissement, seul le niveau de gravité de l'erreur est affiché.

- **Qtree**

  Affiche le nom du qtree.

- **Cluster**

  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 de la souris sur le nom du volume pour afficher plus d'informations sur ce dernier.

- **Ensemble de quotas**

  Indique si un quota est activé ou désactivé sur le qtree.

- **Type de quota**

  Spécifie si le quota est pour un utilisateur, un groupe d'utilisateurs ou 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 de disque est définie, cette valeur est basée sur la limite matérielle du disque. Si le quota est défini sans limite Hard disque, la valeur est

basée sur l'espace de données du volume. Si le quota n'est pas défini ou si des quotas sont définis sur le volume auquel appartient le qtree, « non applicable » s'affiche sur la page de la grille et le champ est vide dans les données d'exportation CSV.

- **Limite matérielle disque**

  Affiche la quantité maximale d'espace disque alloué au qtree. Unified Manager génère un événement critique lorsque cette limite est atteinte et qu'aucune autre écriture de disque n'est autorisée. La valeur s'affiche sous la forme « illimitée » pour les conditions suivantes : si le quota est défini sans limite matérielle de disque, si le quota n'est pas défini ou si des quotas sont situés sur le volume auquel appartient le qtree.

- **Limite logicielle du disque**

  Affiche la quantité d'espace disque alloué au qtree avant de générer un événement d'avertissement. La valeur s'affiche sous la forme « illimitée » pour les conditions suivantes : si le quota est défini sans limite logicielle de disque, si le quota n'est pas défini ou si des quotas sont situés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

- **Seuil de disque**

  Affiche la valeur de seuil définie sur l'espace disque. La valeur s'affiche sous la forme « illimitée » pour les conditions suivantes : si le quota est défini sans limite de disque, si le quota n'est pas défini ou si des quotas sont situés 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 matérielle du fichier est définie, cette valeur est basée sur la limite matérielle du fichier. Aucune valeur n'est affichée si le quota est défini sans limite matérielle de fichier. Si le quota n'est pas défini ou si des quotas sont définis sur le volume auquel appartient le qtree, « non applicable » s'affiche sur la page de la grille et le champ est vide dans les données d'exportation CSV.

- **Limite matérielle de fichier**

  Affiche la limite matérielle du nombre de fichiers autorisés sur les qtrees. La valeur s'affiche sous la forme « illimitée » pour les conditions suivantes : si le quota est défini sans limite matérielle de fichier, si le quota n'est pas défini ou si des quotas sont situés sur le volume auquel appartient le qtree.

- **Limite logicielle de fichier**

  Affiche la limite soft pour le nombre de fichiers autorisés sur les qtrees. La valeur s'affiche sous la forme « illimitée » pour les conditions suivantes : si le quota est défini sans limite logicielle de fichier, si le quota n'est pas défini ou si des quotas sont situés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

Onglet quotas d'utilisateur et de groupe

Affiche des 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 logicielles et matérielles définies sur les disques et les fichiers, la quantité d'espace disque et le nombre de fichiers utilisés, ainsi que la valeur de 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 adresse e-mail**

Ouvre la boîte de dialogue Modifier l'adresse électronique, qui affiche l'adresse électronique actuelle de l'utilisateur ou du groupe d'utilisateurs sélectionné. Vous pouvez modifier l'adresse e-mail. 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 s'affichent sous la forme de valeurs séparées par des virgules. De même, la règle par défaut n'est pas utilisée pour générer l'adresse e-mail ; vous devez donc fournir l'adresse e-mail requise pour l'envoi des notifications.

- **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'utilisateurs ou de groupes d'utilisateurs configurés sur la machine virtuelle de stockage. Une notification est envoyée à l'adresse e-mail spécifiée lorsqu'une violation de quota est constatée.

- **Statut**

  Affiche l'état actuel du quota. L'état 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 auquel l'événement est affecté 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 du déclenchement des événements, ainsi que le nom de l'administrateur auquel l'événement est affecté. 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 même gravité ou différents niveaux de gravité. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un quota a deux événements avec des niveaux d'erreur et d'avertissement, seul le niveau d'erreur est affiché.

- **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 s'affichent sous la forme de valeurs séparées par des virgules.

  La valeur s'affiche sous la forme « Inconnu » lorsque ONTAP ne fournit pas de nom d'utilisateur valide en raison d'erreurs de type SECD.

- **Type**

  Spécifie si le quota est pour un utilisateur ou un groupe d'utilisateurs.

- **Volume ou qtree**

  Affiche le nom du volume ou 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 qtree pour afficher plus d'informations sur le volume ou le qtree.

- **Disque utilisé %**

  Affiche le pourcentage d'espace disque utilisé. La valeur est affichée comme « non applicable » si le quota est défini sans limite matérielle du disque.

- **Limite matérielle disque**

  Affiche la quantité maximale d'espace disque alloué au quota. Unified Manager génère un événement critique lorsque cette limite est atteinte et qu'aucune autre écriture de disque n'est autorisée. La valeur s'affiche sous la forme « illimitée » si le quota est défini sans limite matérielle du disque.

- **Limite logicielle du disque**

  Affiche la quantité d'espace disque alloué au quota avant qu'un événement d'avertissement ne soit généré. La valeur s'affiche sous la forme « illimitée » si le quota est défini sans limite logicielle du disque. Par défaut, cette colonne est masquée.

- **Seuil de disque**

  Affiche la valeur de seuil définie sur l'espace disque. La valeur est affichée comme « illimitée » 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 matérielle de fichier.

- **Limite matérielle de fichier**

  Affiche la limite matérielle du nombre de fichiers autorisés sur le quota. La valeur est affichée comme « illimitée » si le quota est défini sans limite matérielle de fichier.

- **Limite logicielle de fichier**

  Affiche la limite logicielle du nombre de fichiers autorisés sur le quota. La valeur est affichée comme « illimitée » si le quota est défini sans limite logicielle de fichier. Par défaut, cette colonne est masquée.

- **Adresse e-mail**

  Affiche l'adresse e-mail de l'utilisateur ou du groupe d'utilisateurs auquel les notifications sont envoyées en cas de violation des quotas.

Onglet NFS Shares

L'onglet NFS Shares affiche des informations sur les partages NFS, telles que son état, le chemin associé au volume (volumes FlexGroup ou volumes FlexVol), les niveaux d'accès des clients aux partages NFS et l'export policy 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 l'export policy pour le volume ne contiennent pas de partages NFS.

- **Statut**

Affiche l'état actuel des partages NFS. L'état peut être erreur ( ) ou Normal ( ).

- **Chemin de jonction**

  Affiche le chemin vers lequel le volume est monté. Lorsqu'une règle d'exportations NFS explicite est appliquée à un qtree, la colonne affiche le chemin d'accès du volume par le biais duquel il est possible d'accéder au qtree.

- **Chemin de jonction actif**

  Indique si le chemin d'accès au volume monté est actif ou inactif.

- **Volume ou qtree**

  Affiche le nom du volume ou qtree vers lequel la export policy NFS est appliquée. Si une export policy NFS est appliquée à un qtree du volume, la colonne affiche 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 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, limité 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.

  - Limitée

    Les opérations limitées, telles que la reconstruction de parité, sont autorisées, mais l'accès aux données n'est pas autorisé.

  - Mixte

    Les composants d'un volume FlexGroup ne sont pas tous du même état.

- **Style de sécurité**

  Affiche l'autorisation d'accès pour les volumes exportés. Le style de sécurité peut être UNIX, unifié, NTFS ou Mixed.

  - UNIX (clients NFS)

    Les fichiers et les répertoires du volume disposent d'autorisations UNIX.

  - Unifiée

    Les fichiers et les répertoires du volume possèdent une méthode de sécurité unifiée.

  - NTFS (clients CIFS)

Les fichiers et les répertoires du volume disposent d'autorisations Windows NTFS.

- Mixte

  Les fichiers et les répertoires du volume peuvent disposer d'autorisations UNIX ou NTFS Windows.

- **Autorisation UNIX**

  Affiche les bits d'autorisation UNIX dans un format octal de chaîne, qui est défini pour les volumes exportés. Elle est similaire aux bits d'autorisation de style UNIX.

- **Politique d'exportation**

  Affiche les règles qui définissent l'autorisation d'accès pour les volumes qui sont exportés. Vous pouvez cliquer sur le lien pour afficher les détails des règles associées à la stratégie d'exportation, telles que les protocoles d'authentification et l'autorisation d'accès.

Onglet SMB Shares

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 de partage, le chemin associé à la VM de stockage, l'état de la Junction path du partage, l'état du volume contenant, les données de sécurité du partage et les règles d'exportation définies pour le partage. Vous pouvez également déterminer s'il existe un chemin NFS équivalent pour le partage SMB.

> Les partages des dossiers ne sont pas affichés dans l'onglet partages SMB.

- **Bouton de commande Afficher le mappage utilisateur**

  Lance la boîte de dialogue mappage utilisateur.

  Vous pouvez afficher les détails des mappages des utilisateurs pour la VM de stockage.

- **Afficher le bouton de commande ACL**

  Lance la boîte de dialogue contrôle d'accès pour le partage.

  Vous pouvez afficher les détails des utilisateurs et des autorisations pour le partage sélectionné.

- **Statut**

  Affiche l'état actuel du partage. L'état 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**

  Indique si le chemin d'accès au partage est actif ou inactif.

- **Objet contenant**

  Affiche le nom de l'objet contenant auquel le partage appartient. L'objet contenant peut être un volume ou un qtree.

  En cliquant sur le lien, vous pouvez afficher les détails de l'objet contenant dans la page Détails correspondante. Si l'objet contenant est un qtree, les liens s'affichent à la fois pour qtree et volume.

- **État du volume**

  Affiche l'état du volume en cours d'exportation. L'état peut être hors ligne, en ligne, limité 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.

  - Limitée

    Les opérations limitées, telles que la reconstruction de parité, sont autorisées, mais l'accès aux données n'est pas autorisé.

  - Mixte

    Les composants d'un volume FlexGroup ne sont pas tous du même état.

- **Sécurité**

  Affiche l'autorisation d'accès pour les volumes exportés. Le style de sécurité peut être UNIX, unifié, NTFS ou Mixed.

  - UNIX (clients NFS)

    Les fichiers et les répertoires du volume disposent d'autorisations UNIX.

  - Unifiée

    Les fichiers et les répertoires du volume possèdent une méthode de sécurité unifiée.

  - NTFS (clients CIFS)

    Les fichiers et les répertoires du volume disposent d'autorisations Windows NTFS.

  - Mixte

    Les fichiers et les répertoires du volume peuvent disposer d'autorisations UNIX ou NTFS Windows.

- **Politique d'exportation**

  Affiche le nom de l'export policy applicable au partage. Si une export policy n'est pas spécifiée pour la VM de stockage, la valeur s'affiche comme non activée.

  Vous pouvez cliquer sur ce lien pour afficher des détails sur les règles associées à la stratégie

d’exportation, telles que les protocoles d’accès et les autorisations. Le lien est désactivé si l’export policy est désactivée pour la machine virtuelle de stockage sélectionnée.

- **Équivalent NFS**

  Indique s’il existe un équivalent NFS pour le partage.

Onglet SAN

Affiche des informations détaillées sur les LUN, les groupes initiateurs et les initiateurs de la machine virtuelle de stockage sélectionnée. Par défaut, la vue LUN est affichée. Dans l’onglet groupes initiateurs, vous pouvez afficher des informations détaillées sur les groupes initiateurs dans l’onglet initiateurs.

- **Onglet LUN**

  Affiche des détails sur les LUN appartenant à la machine virtuelle de stockage sélectionnée. Vous pouvez afficher des informations telles que le nom de la LUN, son état (en ligne ou hors ligne), le nom du système de fichiers (volume ou qtree) qui contient la LUN, le type de système d’exploitation hôte, la capacité totale de données et le numéro de série de la LUN. La colonne performances de LUN fournit un lien vers la page des détails relatifs aux LUN/performances.

  Vous pouvez également consulter les informations relatives à l’activation du provisionnement fin sur la LUN et si celle-ci est mappée sur un groupe initiateur. Si elle est mappée sur un initiateur, vous pouvez afficher les groupes initiateurs et les initiateurs qui sont mappés sur la LUN sélectionnée.

- **Onglet groupes initiateurs**

  Affiche des détails sur les groupes initiateurs. Vous pouvez afficher des détails tels que le nom du groupe initiateur, 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 de la colonne État d’accès, vous pouvez afficher l’état d’accès actuel du groupe initiateur.

  - **Normal**

    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**

    Aucun chemin d’accès n’est connecté au groupe initiateur.

    Vous pouvez voir si les groupes initiateurs sont mappés sur toutes les interfaces ou des interfaces spécifiques via un ensemble de ports. Lorsque vous cliquez sur le lien nombre dans la colonne interfaces mappées, toutes les interfaces s’affichent ou des interfaces spécifiques pour un ensemble de ports s’affichent. Les interfaces mappées via le portail cible ne sont pas affichées. Le nombre total d’initiateurs et de LUN mappés sur un groupe initiateur s’affiche.

  Vous pouvez également afficher les LUN et les initiateurs mappés sur le groupe initiateur sélectionné.

- **Onglet initiateurs**

  Affiche le nom et le type de l’initiateur et le nombre total de groupes d’initiateurs mappés sur 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. Elle comprend également le nom de l'annotation et les valeurs d'annotation qui sont appliquées à la machine virtuelle de stockage. Vous pouvez également supprimer des annotations manuelles du volet Annotations associées.

Panneau périphériques associés

Le volet périphériques associés vous permet d'afficher le cluster, les agrégats et les volumes associés à la machine virtuelle de stockage :

- **Cluster**

  Affiche l'état de santé du cluster auquel appartient la VM de stockage.

- **Agrégats**

  Affiche le nombre d'agrégats qui appartiennent à la machine virtuelle de stockage sélectionnée. L'état de santé des agrégats s'affiche également, sur la base du niveau de gravité le plus élevé. Par exemple, si un serveur virtuel de stockage contient dix agrégats, dont cinq affichent le statut d'avertissement et les cinq autres affichent l'état critique, l'état affiché est critique.

- **Agrégats affectés**

  Affiche le nombre d'agrégats affectés à une machine virtuelle de stockage. L'état de santé des agrégats s'affiche également, sur la base 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, sur la base du niveau de gravité le plus élevé. Lorsque il existe des volumes FlexGroup dans la machine virtuelle de stockage, le nombre inclut également FlexGroups, il n'inclut pas les composants FlexGroup.

Volet groupes associés

Le volet groupes associés 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 en modifiant une alerte existante en cliquant sur le nom de l'alerte.

Page Cluster / Health Details

La page de détails Cluster / Health fournit des informations détaillées sur un cluster sélectionné, notamment son état de santé, sa capacité et sa configuration. Vous pouvez également afficher des informations sur les interfaces réseau (LIF), les nœuds, les disques, les périphériques associés et les alertes associées au cluster.

L'état situé à côté du nom du cluster, par exemple (Good), 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 permettent d'effectuer les tâches suivantes pour le cluster sélectionné :

- **Basculer vers l'affichage des performances**

  Permet de accéder à la page des détails sur le cluster / les performances.

- **Actions**

  - 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, qui permet à Unified Manager de détecter les dernières modifications apportées au cluster.

    En cas d'association avec Unified Manager et OnCommand Workflow Automation, l'opération de redécouverte acquiert également les données 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 : permet d'annoter le cluster sélectionné.

- **Afficher les clusters**

  Permet de naviguer vers la vue Santé : tous les clusters.

Onglet Santé

Affiche des informations détaillées sur les problèmes de disponibilité et de capacité des données liés aux différents objets du cluster tels que les nœuds, les SVM et les agrégats. Les problèmes de disponibilité sont liés à la fonctionnalité de service des données des objets de cluster. Les problèmes de capacité sont liés à la capacité de stockage des données des objets du cluster.

Vous pouvez cliquer sur le graphe d'un objet pour afficher une liste filtrée des objets. Par exemple, vous pouvez cliquer sur le graphique de capacité du SVM qui affiche les avertissements pour afficher une liste filtrée des SVM. Cette liste contient les SVM contenant des volumes ou des qtrees dont les problèmes de capacité sont indiqués avec un niveau de sévérité avertissement. Vous pouvez également cliquer sur le graphique disponibilité des SVM qui affiche des avertissements pour afficher la liste des SVM ayant des problèmes de disponibilité avec un niveau de sévérité avertissement.

Problèmes de disponibilité

Affiche graphiquement le nombre total d'objets, y compris les objets qui présentent des problèmes de disponibilité et des objets qui n'ont aucun problème lié à la disponibilité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations ci-dessous fournissent des informations détaillées sur les problèmes de disponibilité qui peuvent avoir un impact ou ont déjà affecté la disponibilité des données dans le cluster. Par exemple, des informations s'affichent concernant les tiroirs disques qui sont en panne et les agrégats qui sont hors ligne.

> Les données affichées pour le graphique à barres du 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 sous forme graphique le nombre total d'objets, y compris les objets qui présentent des problèmes de capacité et des objets qui n'ont aucun problème lié à la capacité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations ci-dessous fournissent des informations détaillées sur les problèmes de capacité qui peuvent avoir un impact ou qui ont déjà affecté la capacité des données du cluster. Par exemple, des informations s'affichent concernant les agrégats susceptibles d'enfreindre les valeurs de seuil définies.

Onglet capacité

Affiche des informations détaillées sur la capacité du cluster sélectionné.

Capacité

Affiche le graphique de capacité des données sur 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 aux technologies d'efficacité du stockage ONTAP. Cela n'inclut pas les copies Snapshot.

- Réduction des données

  Affiche le ratio sans copies Snapshot et avec deux chiffres significatifs, par exemple, 1.8 pour 1. Ce taux est basé sur les paramètres d'efficacité du stockage ONTAP configurés.

- Utilisé

  Capacité physique utilisée par les données sur tous les agrégats. Cette opération n'inclut pas la capacité utilisée pour la parité, le dimensionnement adapté et la réservation.

- Disponibilité

  Affiche la capacité disponible pour les données.

- Pièces de rechange

  Affiche la capacité de stockage disponible pour le stockage de tous les disques de réserve.

- Provisionnée

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 de l'agrégat 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. Cette opération n'inclut pas la capacité utilisée pour la parité, le dimensionnement adapté et la réservation.

- Disponibilité

  Affiche la capacité disponible pour les données.

- Provisionnée

  Affiche la capacité provisionnée pour tous les volumes sous-jacents.

- Pièces de rechange

  Affiche la capacité de stockage disponible pour le stockage de tous les disques de réserve.

Tier dans le cloud

Affiche la capacité totale du Tier cloud utilisé ainsi que la capacité utilisée pour chaque Tier 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 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 dans l'onglet disques.

- Capacité exploitable totale

  Affiche la capacité disponible et la capacité disponible des disques de données.

- DISQUES DURS

  Affiche graphiquement la capacité utilisée et la capacité disponible de tous les disques de données HDD du cluster. La ligne en pointillés correspond à la capacité disponible des disques de données du disque dur.

- Flash
  - Données SSD

    Affiche sous forme graphique la capacité utilisée et la capacité disponible des disques de données SSD du cluster.

- Cache SSD

  Affiche sous forme graphique la capacité de stockage des disques SSD cache du cluster.

- Disque de secours SSD

  Affiche graphiquement la capacité disponible du disque SSD, ainsi que les données et les disques en cache dans le cluster.

- Disques non assignés

  Affiche le nombre de disques non assignés dans le cluster.

Agrégats avec liste de problèmes de capacité

Affiche sous forme de tableau des informations détaillées sur la capacité utilisée et la capacité disponible des agrégats qui présentent des problèmes de risque de capacité.

- État

  Indique que l'agrégat présente un problème de capacité d'une gravité spécifique.

  Vous pouvez déplacer le pointeur de la souris sur l'état pour afficher plus d'informations sur l'événement ou les événements générés pour l'agrégat.

  Si le statut 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 à laquelle l'événement a été déclenché, le nom de l'administrateur auquel l'événement est affecté 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 s'affichent avec des informations telles que le nom de l'événement, l'heure et la date du déclenchement des événements, ainsi que le nom de l'administrateur à qui l'événement est affecté. 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 divers niveaux d'importance. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un agrégat a 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 les informations relatives à l'utilisation de la capacité de l'agrégat (en pourcentage).

- Jours avant la date complète

  Affiche le nombre estimé de jours restants avant que l'agrégat n'atteigne sa capacité maximale.

Onglet Configuration

Affiche des détails sur le cluster sélectionné, tels que l'adresse IP, le contact et l'emplacement :

Présentation du cluster

- Interface de gestion

  Affiche la LIF de cluster-management que Unified Manager utilise pour se connecter au cluster. Le statut opérationnel de l'interface est également affiché.

- Nom d'hôte ou adresse IP

  Affiche le FQDN, le nom court ou l'adresse IP de la LIF de cluster-management que Unified Manager utilise pour se connecter au cluster.

- FQDN

  Affiche le nom de domaine complet (FQDN) du cluster.

- Version du système d'exploitation

  Affiche la version ONTAP que le cluster exécute. Si les nœuds du cluster exécutent différentes versions de ONTAP, la version la plus ancienne de ONTAP s'affiche.

- Contactez

  Affiche des détails sur l'administrateur que vous devez contacter en cas de problème avec le cluster.

- Emplacement

  Affiche l'emplacement du cluster.

- Personnalité

  Indique s'il s'agit d'un cluster configuré pour toutes les baies SAN.

Présentation du cluster distant

Fournit des détails sur le cluster distant dans une configuration MetroCluster. Ces informations s'affichent uniquement dans les configurations MetroCluster.

- Cluster

  Affiche le nom du cluster distant. Vous pouvez cliquer sur le nom du cluster pour accéder à la page détaillée du cluster.

- Nom d'hôte ou adresse IP

  Affiche le FQDN, le nom court ou l'adresse IP du cluster distant.

- Emplacement

  Affiche l'emplacement du cluster distant.

Présentation de MetroCluster

Fournit des informations détaillées sur le cluster local dans les configurations MetroCluster over FC ou MetroCluster over IP. Ces informations s'affichent uniquement pour les configurations MetroCluster sur FC ou IP.

- Type

  Indique si le type MetroCluster est à deux ou quatre nœuds. Pour MetroCluster sur IP, seuls les quatre nœuds sont pris en charge.

- Configuration

  Affiche la configuration MetroCluster sur FC et IP, qui peut avoir les valeurs suivantes :

Pour FC

- Configuration Stretch avec câbles SAS
- Configuration Stretch avec Bridge FC-SAS
- Configuration de la structure avec commutateurs FC

> Dans le cas d'un système MetroCluster à quatre nœuds, seule la configuration Fabric avec commutateurs FC est prise en charge.

Pour IP

- Configuration IP avec commutateurs Ethernet (L2 ou L3, selon la configuration du cluster)
  - Basculement automatisé et non planifié

    Indique si le basculement automatique non planifié est activé pour le cluster local. Par défaut, AUSO est activé pour tous les clusters d'une configuration MetroCluster à deux nœuds dans Unified Manager. Vous pouvez utiliser l'interface de ligne de commande pour modifier le paramètre AUSO. Cela est pris en charge uniquement pour MetroCluster over FC.

  - Mode basculement

    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 haut ( ) ou en bas ( ) dans le cluster.

- Versions d'OS

  Affiche les versions ONTAP que les nœuds exécutent ainsi que le nombre de nœuds exécutant une version particulière de ONTAP. Par exemple, 9.6 (2), 9.3 (1) indique que deux nœuds exécutent ONTAP 9.6 et qu'un nœud exécute ONTAP 9.3.

Ordinateurs virtuels de stockage

- Disponibilité

  Affiche le nombre de SVM qui sont en hausse ( ) ou en baisse ( ) dans le cluster.

Interfaces réseau

- Disponibilité

  Affiche le nombre de LIFs non-data qui sont en hausse ( ) ou en baisse ( ) dans le cluster.

- Interfaces de gestion du cluster

  Affiche le nombre de LIF cluster-management.

- Interfaces node-Management

  Affiche le nombre de LIFs de node-management.

- Interfaces de cluster

  Affiche le nombre de LIF de cluster.

- Interfaces intercluster

  Affiche le nombre de LIFs intercluster.

Protocoles

- Protocoles de données

  Affiche la liste des protocoles de données sous licence qui sont activés pour le cluster. Les protocoles de données incluent iSCSI, CIFS, NFS, NVMe et FC/FCoE.

La protection

- Médiateurs

  Indique si le cluster prend en charge les médiateurs et l'état de connectivité du médiateur. Elle indique si le médiateur est configuré et, s'il est configuré, elle affiche l'état des médiateurs.

  - Sans objet

    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. L'état du médiateur est indiqué par la couleur. La couleur verte indique que l'état du médiateur est accessible.

La couleur rouge indique que l'état du médiateur est inaccessible.

Tiers cloud

Le 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 l'état des tiers cloud (disponibles ou non).

Onglet MetroCluster Connectivity

Affiche les problèmes et l'état de connectivité des composants du cluster dans la configuration MetroCluster over FC. Un cluster s'affiche dans une zone rouge lorsque le partenaire de reprise sur incident du cluster a des problèmes.

> L'onglet MetroCluster Connectivity s'affiche uniquement pour les clusters qui se trouvent dans une configuration MetroCluster over FC.

Pour accéder à la page de détails d'un cluster distant, cliquez sur le nom du cluster distant. Vous pouvez également afficher les détails des composants en cliquant sur le lien nombre d'un composant. Par exemple, si vous cliquez sur le lien nombre de nœuds du cluster, l'onglet nœud s'affiche sur la page de détails du cluster. Si vous cliquez sur le lien nombre de disques du cluster distant, l'onglet disque s'affiche dans la page de détails du cluster distant.

> Lors de la gestion d'une configuration MetroCluster à huit nœuds, un clic sur le lien nombre de tiroirs disques affiche uniquement les tiroirs locaux de la paire haute disponibilité par défaut. Il n'existe aucun moyen d'afficher les tiroirs locaux sur l'autre paire haute disponibilité.

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 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 affecté 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 du déclenchement des événements, ainsi que le nom de l'administrateur auquel l'événement est affecté. 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 over FC. Vous pouvez utiliser l'onglet MetroCluster Replication pour assurer la protection des données en réalisant une mise en miroir synchrone des données avec les clusters déjà peering. Un cluster s'affiche dans une zone rouge lorsque le partenaire de reprise sur incident du cluster a des problèmes.

> L'onglet MetroCluster Replication s'affiche uniquement pour les clusters qui se trouvent dans une configuration MetroCluster over 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 afficher la représentation objective des composants du cluster avec leurs connexions logiques. Cela permet d'identifier les problèmes susceptibles de se produire lors de la mise en miroir des métadonnées et des données.

Dans l'onglet MetroCluster Replication, le cluster local fournit la représentation graphique détaillée du cluster sélectionné et le partenaire MetroCluster fait référence au cluster distant.

Onglet interfaces réseau

Affiche des détails sur toutes les LIFs autres que les données créées sur le cluster sélectionné.

Interface réseau

Affiche le nom de la LIF créée sur le cluster sélectionné.

Statut opérationnel

Affiche l'état opérationnel de l'interface, qui peut être Haut ( ), Bas ( ) ou Inconnu ( ). L'état opérationnel d'une interface réseau est déterminé par le statut de ses ports physiques.

Statut administratif

Affiche l'état administratif de l'interface, qui peut être Haut ( ), Bas ( ) ou Inconnu ( ). Vous pouvez contrôler le statut administratif d'une interface lorsque vous modifiez la configuration ou pendant la maintenance. Le statut administratif peut être différent du statut opérationnel. Cependant, si le statut administratif d'une LIF est arrêté, le statut opérationnel est arrêté par défaut.

Adresse IP

Affiche l'adresse IP de l'interface.

Rôle

Affiche le rôle de l'interface. Les rôles possibles sont les LIF Cluster-Management, les LIF Node Management, les LIF Cluster et les LIF intercluster.

Port de départ

Affiche le port physique auquel l'interface a été associée à l'origine.

Port actuel

Affiche le port physique auquel l'interface est actuellement associée. Après la migration de LIF, le port actuel peut être différent du port de home.

Règle 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 routes et la passerelle de destination en cliquant sur le nom du groupe de routage.

Les groupes de routage ne sont pas pris en charge par ONTAP 8.3 ou version ultérieure et une colonne vide s'affiche donc 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 haute disponibilité, les tiroirs disques et les ports :

Détails DE LA HAUTE DISPONIBILITÉ

La fournit une représentation schématique de l'état de haute disponibilité et de l'état de santé des nœuds de la paire haute disponibilité. 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 relais du nœud partenaire ou il rencontre des problèmes environnementaux.

- **Rouge**

  Le nœud ne fonctionne pas.

Vous pouvez afficher les informations relatives à la disponibilité de la paire haute disponibilité et prendre les mesures nécessaires pour éviter tout risque. Par exemple, en cas d'opération de basculement possible, le message suivant s'affiche : basculement du stockage possible.

Vous pouvez afficher la liste des événements relatifs à la paire haute disponibilité et à son environnement, tels que les ventilateurs, les alimentations, la batterie NVRAM, les cartes Flash, processeur de service et connectivité des tiroirs disques. Vous pouvez également afficher l'heure à laquelle les événements ont été déclenchés.

Vous pouvez afficher d'autres informations relatives au nœud, telles que le numéro de modèle.

Si des clusters à un seul nœud sont disponibles, vous pouvez également afficher les détails relatifs aux nœuds.

Tiroirs disques

Affiche des informations sur les tiroirs disques de la paire haute disponibilité.

Vous pouvez également afficher les événements générés pour les tiroirs disques et les composants environnementaux, ainsi que la date à laquelle les événements ont été déclenchés.

- **ID étagère**

  Affiche l'ID du shelf où est situé le disque.

- **Etat du composant**

Affiche les détails environnementaux des tiroirs disques, comme les alimentations, les ventilateurs, les capteurs de température, les capteurs actuels, la connectivité des disques, et les capteurs de tension. Les détails relatifs à l'environnement s'affichent 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 du tiroir disque. Les États possibles sont hors ligne, en ligne, pas de statut, initialisation requise, manquant, Et inconnu.

- **Modèle**

  Affiche le numéro de modèle du tiroir disque.

- **Plateau de disque local**

  Indique si le tiroir disque est situé sur le cluster local ou le cluster distant. Cette colonne s'affiche uniquement pour les clusters dans une configuration MetroCluster.

- **ID unique**

  Affiche l'identifiant unique du tiroir disque.

- **Version du micrologiciel**

  Affiche la version du firmware du tiroir disque.

Ports

Affiche des informations sur les ports FC, FCoE et Ethernet associés. Vous pouvez afficher des détails sur les ports et les LIF associées en cliquant sur les icônes de ports.

Vous pouvez également afficher les événements générés pour les ports.

Vous pouvez afficher les détails de port suivants :

- ID de port

  Affiche le nom du port. Par exemple, les noms de ports peuvent être e0M, e0a et e0b.

- Rôle

  Affiche le rôle du port. Les rôles possibles sont Cluster, Data, intercluster, Node Management et Undefined.

- Type

  Affiche le protocole de couche physique utilisé pour le port. Les types possibles sont Ethernet, Fibre Channel et FCoE.

- WWPN

  Affiche le WWPN (World Wide Port Name) du port.

- Révision du micrologiciel

  Affiche la révision du micrologiciel du port FC/FCoE.

- État

  Affiche l'état actuel du port. Les États possibles sont Haut, Bas, lien non connecté ou Inconnu (?).

  Vous pouvez afficher les événements liés au port dans la liste Evénements. Vous pouvez également afficher les détails des LIF associées, tels que le nom LIF, le statut opérationnel, l'adresse IP ou WWPN, les protocoles, le nom du SVM associé à la LIF, le port actuel, la politique de basculement et le groupe de basculement.

Onglet disques

Affiche des détails sur les disques du cluster sélectionné. Vous pouvez afficher les informations relatives aux disques, telles que le nombre de disques utilisés, les disques de rechange, les disques défectueux et les disques non affectés. Vous pouvez également afficher d'autres détails, tels que le nom du disque, le type de disque et le nœud propriétaire du disque.

Récapitulatif du pool de disques

Affiche le nombre de disques, classés par type effectif (FCAL, SAS, SATA, MSATA, SSD, SSD NVMe, CAPACITÉ SSD, Array LUN et VMDISK) et état des disques. Vous pouvez également afficher d'autres informations, telles que le nombre d'agrégats, de disques partagés, de disques de rechange, des disques endommagés, des disques non assignés, et des disques non pris en charge. Si vous cliquez sur le lien effectif Disk type count, les disques de l'état sélectionné et du type effectif sont affichés. Par exemple, si vous cliquez sur le lien count pour le type SAS d'état disque rompu et effectif, tous les disques dont l'état de disque est rompu et le type SAS effectif sont affichés.

Disque

Affiche le nom du disque.

Groupes RAID

Affiche le nom du groupe RAID.

Nœud propriétaire

Affiche le nom du nœud auquel le disque appartient. Si le disque n'est pas affecté, aucune valeur n'est affichée dans cette colonne.

État

Affiche l'état du disque : agrégat, partagé, Spare, Broken, non affecté, Non pris en charge ou inconnu. Par défaut, cette colonne est triée pour afficher les États dans l'ordre suivant : Broken, Unattribués, Unsupported, Spare, Aggregate, Et partagé.

Disque local

Affiche Oui ou non pour indiquer si le disque se trouve sur le cluster local ou 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 concernés

Affiche le nombre d'agrégats affectés par la défaillance du disque. Vous pouvez déplacer le pointeur de la souris sur le lien du nombre 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 d'agrégats pour afficher la liste des agrégats impactés dans la vue Santé : tous les agrégats.

Aucune valeur n'est affichée dans cette colonne dans 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 disque défectueux

Pool de stockage

Affiche le nom du pool de stockage auquel le disque SSD appartient. 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 de disque disponible.

Capacité brute

Affiche la capacité du disque brut non formaté avant le dimensionnement approprié et la configuration RAID. Par défaut, cette colonne est masquée.

Type

Affiche les types de disques, par exemple ATA, SATA, FCAL ou VMDISK.

Type effectif

Affiche le type de disque attribué par ONTAP.

Certains types de disques ONTAP sont considérés comme équivalents lors de la création et de l'ajout d'agrégats, ainsi que pour la gestion des disques de secours. ONTAP attribue un type de disque efficace à chaque type de disque.

Blocs de réserve consommés %

Affiche, par pourcentage, les blocs de spare qui sont utilisés dans le disque SSD. Cette colonne est vide pour les disques autres que les disques SSD.

Durée de vie nominale en %

Affiche, en pourcentage, une estimation de la durée de vie des disques SSD utilisés, en fonction de l'utilisation réelle des disques SSD et des prévisions du fabricant concernant la durée de vie des disques SSD. Une valeur supérieure à 99 indique que l'endurance estimée a été consommée, mais qu'elle n'indique pas une panne de disque SSD. Si la valeur est inconnue, le disque est omis.

Micrologiciel

Affiche la version du micrologiciel du disque.

TR/MIN

Affiche le nombre de tours par minute (tr/min) 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 du tiroir

Affiche l'ID du shelf où est situé le disque.

Baie

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 comprennent le nom de l'annotation et les valeurs d'annotation qui sont appliquées au cluster. Vous pouvez également supprimer des annotations manuelles du volet Annotations associées.

Panneau périphériques 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 effectuer une analyse plus approfondie sur ce périphérique particulier.

Vous pouvez utiliser le volet partenaires de MetroCluster pour obtenir des chiffres, ainsi que des informations sur le partenaire MetroCluster distant avec les composants de cluster associés, tels que les nœuds, les agrégats et les SVM. Le volet partenaire MetroCluster s'affiche uniquement pour les clusters d'une configuration MetroCluster.

Le volet périphériques associés vous permet d'afficher et de naviguer vers les nœuds, SVM et agrégats liés au cluster :

Partenaire MetroCluster

Affiche le statut de santé du partenaire MetroCluster. En utilisant le lien nombre, 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. Capacité indique la capacité totale utilisable par rapport à la capacité disponible.

Ordinateurs virtuels de stockage

Affiche le nombre de SVM appartenant au cluster sélectionné.

64 bits

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 incluant le cluster sélectionné.

Volet alertes associées

Le volet alertes associées vous permet d'afficher la liste des alertes du cluster sélectionné. Vous pouvez également ajouter une alerte en cliquant sur le lien Ajouter une alerte ou en modifiant une alerte existante en cliquant sur le nom de l'alerte.

Informations connexes

"Page volumes" "Affichage de la liste et des détails des clusters"

Page Détails de l'agrégat/de l'intégrité

Vous pouvez utiliser la page des détails agrégat/intégrité pour afficher des informations détaillées sur l'agrégat sélectionné, telles que la capacité, des informations sur le disque, les détails de la 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 validées et survalidées affichées sur cette page concernent uniquement la capacité locale, ou de Tier de performance. La quantité d'espace disponible dans le Tier cloud n'est pas reflétée dans les valeurs survalidées. De la même façon, les valeurs seuils agrégées ne sont pertinentes que pour le Tier de performance local.

Les boutons de commande permettent d'effectuer les tâches suivantes pour l'agrégat sélectionné :

- **Basculer vers l’affichage des performances**

  Accès à la page des détails sur les agrégats / performances.

- **Actions**
  - Ajouter une alerte

    Permet d’ajouter une alerte à l’agrégat sélectionné.

  - Modifier les seuils

    Permet de modifier les paramètres de seuil de l’agrégat sélectionné.

- **Afficher les agrégats**

  Permet de naviguer vers 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. En outre, les valeurs de seuil utilisées par Unified Manager ne s’appliquent pas aux agrégats racine de nœud. Seul un représentant du support technique peut modifier les paramètres de ces événements. 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 copies Snapshot, qui affiche les détails de capacité sur l’agrégat :

  - Espace logique utilisé

    La taille réelle des données stockées dans l’agrégat sans appliquer les économies obtenues grâce aux technologies d’efficacité du stockage de ONTAP.

  - Utilisé

    Capacité physique utilisée par les données dans l’agrégat.

  - Surengagement

    Lorsqu’un espace dans l’agrégat est surengagé, le graphique affiche un indicateur avec le montant excédentaire.

  - Avertissement

    Affiche une ligne pointillée à l’emplacement où le seuil d’avertissement est défini ; l’espace dans l’agrégat est donc presque plein. Si ce seuil est atteint, l’événement espace presque plein est généré.

  - Erreur

    Affiche une ligne continue à l’emplacement où le seuil d’erreur est défini ; c’est-à-dire l’espace dans l’agrégat est plein. Si ce seuil est atteint, l’événement espace plein est généré.

- Graphique sur les copies Snapshot

  Ce graphique s'affiche uniquement lorsque la capacité Snapshot utilisée ou la réserve Snapshot n'est pas égale à zéro.

Les deux graphiques affichent la capacité par laquelle la capacité Snapshot dépasse la réserve Snapshot si la capacité Snapshot utilisée dépasse la réserve Snapshot.

- **Tier cloud**

  Affiche l'espace utilisé par les données dans le Tier cloud pour les agrégats compatibles FabricPool. Un FabricPool peut être sous licence ou sans licence.

  Lorsque le niveau cloud est mis en miroir vers un autre fournisseur de cloud (le « niveau miroir »), les deux niveaux de cloud s'affichent ici.

- **Détails**

  Affiche des informations détaillées sur la capacité.

  - Capacité totale

    Affiche la capacité totale de l'agrégat.

  - Capacité des données

    Affiche la quantité d'espace utilisée par l'agrégat (capacité utilisée) et la quantité d'espace disponible dans l'agrégat (capacité libre).

  - Réserve Snapshot

    Affiche la capacité Snapshot utilisée et disponible de l'agrégat.

  - Capacité excessive

    Affiche le surengagement de l'agrégat. La surallocation d'agrégat vous permet de fournir une quantité de stockage qui est réellement disponible à partir d'un agrégat donné, tant que cette partie n'est pas utilisée. Lorsque le provisionnement fin est utilisé, la taille totale des volumes de l'agrégat peut dépasser la capacité totale de l'agrégat.

    > Si vous avez surallouné votre agrégat, vous devez surveiller soigneusement son espace disponible et ajouter du stockage à la demande pour éviter les erreurs en écriture dues à la quantité d'espace insuffisante.

  - Tier dans le cloud

    Affiche l'espace utilisé par les données dans le Tier cloud pour les agrégats compatibles FabricPool. Un FabricPool peut être sous licence ou sans licence. Lorsque le niveau cloud est mis en miroir vers un autre fournisseur de cloud (niveau miroir), les deux niveaux de cloud sont affichés ici

  - Espace total du cache

    Affiche l'espace total des disques SSD ou unités d'allocation ajouté à un agrégat Flash Pool. Si vous avez activé Flash Pool pour un agrégat, mais que vous n'avez ajouté aucun disque SSD, l'espace du cache s'affiche sous la forme 0 Ko.

Ce champ est masqué si Flash Pool est désactivé pour un agrégat.

- Seuils des agrégats

  Affiche les seuils de capacité d'agrégat suivants :

  - Presque plein seuil

    Spécifie le pourcentage où un agrégat est presque plein.

  - Seuil maximal

    Spécifie le pourcentage lorsqu'un agrégat est plein.

  - Seuil presque dépassé

    Spécifie le pourcentage auquel un agrégat est presque surengagé.

  - Seuil de surengagement

    Spécifie le pourcentage de surallocation d'un agrégat.

- Autres détails: Taux de croissance quotidien

  Affiche l'espace disque utilisé dans l'agrégat 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 6 h, le taux de croissance quotidien (Go) de cet agrégat est de 2 Go.

- Déplacement de volumes

  Affiche le nombre d'opérations de déplacement de volumes en cours :

  - Volumes hors service

    Affiche le nombre et la capacité des volumes qui sont déplacés hors de l'agrégat.

  Vous pouvez cliquer sur le lien pour afficher plus d'informations, notamment le nom du volume, l'agrégat vers lequel le volume est déplacé, l'état de l'opération de déplacement de volume et l'heure de fin estimée.

  - Volumes dans

    Affiche le nombre et la capacité restante des volumes qui sont déplacés vers l'agrégat.

Vous pouvez cliquer sur le lien pour afficher plus d'informations, notamment le nom du volume, l'agrégat depuis lequel le volume est déplacé, l'état de l'opération de déplacement de volume et l'heure de fin estimée.

- Capacité utilisée estimée après le déplacement de volume

  Affiche la quantité estimée d'espace utilisé (en pourcentage, en Ko, Mo, Go, etc.) dans l'agrégat une fois les opérations de déplacement de volume terminées.

- **Présentation de la capacité - volumes**

  Affiche des graphiques fournissant des informations sur la capacité des volumes de 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 Volume Space at Risk 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 ne peut pas être utilisée (capacité inutilisable) en raison de problèmes de capacité de l'agrégat sont affichés.

  Vous pouvez sélectionner le graphique à afficher dans les listes déroulantes. Vous pouvez trier les données affichées sur le graphique pour afficher des informations telles 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 SVM qui contiennent les volumes de l'agrégat. Vous pouvez également afficher des détails sur les volumes à provisionnement fin. Vous pouvez afficher les détails de points spécifiques sur le graphique en positionnant le curseur sur la zone d'intérêt. Par défaut, le graphique affiche les 30 principaux volumes filtrés dans l'agrégat.

Onglet informations sur le disque

Affiche des informations détaillées sur les disques de l'agrégat sélectionné, y compris le type et la taille RAID, et le type de disques utilisés dans l'agrégat. L'onglet affiche également sous forme graphique les groupes RAID et les types de disques utilisés (SAS, ATA, FCAL, SSD ou VMDISK, par exemple). Pour plus d'informations, telles que la baie, le tiroir et la vitesse de rotation des disques, vous pouvez positionner votre curseur sur les disques de parité et de données.

- **Données**

  Affiche graphiquement des informations 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 RAID**

    Les détails RAID s'affichent uniquement pour les disques dédiés.

    - Type

      Affiche le type RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

    - Taille du groupe

      Affiche le nombre maximum de disques autorisés dans le groupe RAID.

    - Groupes

      Affiche le nombre de groupes RAID de l'agrégat.

  - **Disques utilisés**

    - Type effectif

      Affiche les types de disques de données (par exemple, ATA, SATA, FCAL, SSD, Ou VMDISK) dans l'agrégat.

- Disques de données

  Affiche le nombre et la capacité des disques de données affectés à un agrégat. Les informations détaillées du disque de données ne sont pas affichées lorsque l'agrégat contient uniquement des disques partagés.

- Disques de parité

  Affiche le nombre et la capacité des disques de parité affectés à un agrégat. Les informations détaillées du disque de parité ne sont pas affichées lorsque l'agrégat contient uniquement des disques partagés.

- Disques partagés

  Affiche le nombre et la capacité des disques de données partagés affectés à un agrégat. Les détails des disques partagés ne sont affichés que lorsque l'agrégat contient des disques partagés.

◦ **Disques de rechange**

Affiche le type, le nombre et la capacité effectifs des disques de données disponibles pour le nœud de l'agrégat sélectionné.

> Lorsqu'un agrégat est basculée vers le nœud partenaire, Unified Manager n'affiche pas tous les disques de spare compatibles avec l'agrégat.

- **Cache SSD**

La section fournit des informations détaillées sur les disques SSD cache dédiés et les disques SSD cache partagés.

Les détails suivants pour les disques SSD en cache dédiés sont affichés :

◦ **Détails RAID**

- Type

  Affiche le type RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

- Taille du groupe

  Affiche le nombre maximum de disques autorisés dans le groupe RAID.

- Groupes

  Affiche le nombre de groupes RAID de l'agrégat.

◦ **Disques utilisés**

- Type effectif

  Indique que les disques utilisés pour le cache dans l'agrégat sont de type SSD.

- Disques de données

  Affiche le nombre et la capacité des disques de données affectés à un agrégat pour le cache.

- Disques de parité

  Affiche le nombre et la capacité des disques de parité affectés à un agrégat pour le cache.

- **Disques de rechange**

Affiche le type, le nombre et la capacité effectifs des disques de réserve disponibles pour le nœud de l'agrégat sélectionné pour la mise en cache.

> Lorsqu'un agrégat est basculée vers le nœud partenaire, Unified Manager n'affiche pas tous les disques de spare compatibles avec l'agrégat.

Fournit les détails suivants pour le cache partagé :

- **Pool 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 :

  - État

    Affiche l'état du pool de stockage, qui peut être sain ou malsain.

  - Nombre total d'allocations

    Affiche le nombre total d'unités d'allocation et la taille dans le pool de stockage.

  - Taille de l'unité d'allocation

    Affiche la quantité minimale d'espace du pool de stockage pouvant être alloué 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 correspondant à ce pool de stockage ne correspondent pas, cela indique qu'un ou plusieurs disques sont rompus et que le pool de stockage est défectueux.

  - 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 cet 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 de l'agrégat.

- **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**
  - Pool de stockage

    Affiche le nombre de pools de stockage.

  - Taille totale

    Affiche la taille totale des pools de stockage.

- **Tier cloud**

  Affiche le nom du Tier cloud si vous avez configuré un agrégat compatible FabricPool et affiche l'espace total utilisé. Lorsque le niveau cloud est mis en miroir vers un autre fournisseur cloud (niveau en miroir), les détails des deux niveaux cloud s'affichent 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 RAID, sa taille RAID et le 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 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 de l'agrégat.

  - Type de SnapLock

    Affiche le type SnapLock de l'agrégat.

- **Tier cloud**

  Si cet agrégat est compatible avec FabricPool, les détails du Tier cloud sont affichés. Certains champs diffèrent selon le fournisseur de stockage. Lorsque le niveau cloud est mis en miroir vers un autre fournisseur de cloud (le « niveau miroir »), les deux niveaux de cloud s'affichent 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 Tier cloud lors de sa création par ONTAP.

- Serveur

  Affiche le FQDN du niveau de cloud.

- Port

  Port utilisé pour communiquer avec le fournisseur cloud.

- Clé d'accès ou compte

  Affiche la clé d'accès ou le compte pour le niveau de Cloud.

- Nom du conteneur

  Affiche le nom du compartiment ou du conteneur du Tier cloud.

- SSL

  Indique si le chiffrement SSL est activé pour le niveau cloud.

Zone historique

La zone Historique affiche des graphiques fournissant des informations sur la capacité de l'agrégat sélectionné. En outre, vous pouvez cliquer sur le bouton **Exporter** pour créer un rapport au format CSV pour le graphique que vous consultez.

Vous pouvez sélectionner un type de graphique dans la liste déroulante située en haut du volet Historique. Vous pouvez également afficher les détails d'une période donnée en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques historiques peuvent vous aider à identifier les tendances : par exemple, si l'utilisation de l'agrégat dépasse constamment le seuil presque plein, vous pouvez prendre l'action appropriée.

Les graphiques de l'historique affichent les informations suivantes :

- **Capacité agrégée utilisée (%)**

  Affiche la capacité utilisée dans l'agrégat et la tendance dans la façon dont la capacité d'agrégat est utilisée en fonction de l'historique d'utilisation sous forme de graphiques en pourcentage sur l'axe vertical (y). La période s'affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne 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 agrégée utilisée par rapport à capacité totale**

  Affiche la tendance d'utilisation de la capacité d'agrégat en fonction de l'historique d'utilisation, ainsi que de

la capacité utilisée et de la capacité totale, sous forme de graphiques linéaires, en octets, en kilo-octets, en mégaoctets, et ainsi de suite, sur l'axe vertical (y). La période s'affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Trend Capacity Used, la ligne de graphique Trend Capacity Used est masquée.

- **Capacité agrégée utilisée (%) par rapport à engagé (%)**

  Affiche la tendance dans la façon dont la capacité d'agrégat est utilisée en fonction de l'historique d'utilisation, ainsi que de l'espace alloué sous forme de graphiques linéaires, sous forme de pourcentage, sur l'axe vertical (y). La période s'affiche 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 le curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique en ligne 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 Evénements affiche des détails sur les événements nouveaux et acquittés :

- **Gravité**

  Affiche la gravité de l'événement.

- **Événement**

  Affiche le nom de l'événement.

- **Temps déclenché**

  Affiche le temps écoulé depuis la génération de l'événement. Si le temps écoulé dépasse une semaine, l'horodatage de la génération de l'événement s'affiche.

Panneau périphériques associés

Le volet périphériques associés permet d'afficher le nœud de cluster, les volumes et les disques associés à l'agrégat :

- **Nœud**

  Affiche l'état de capacité et d'intégrité du nœud qui contient l'agrégat. Capacité indique la capacité totale utilisable par rapport à la capacité disponible.

- **Agrégats dans le noeud**

  Affiche le nombre et la capacité de tous les agrégats du nœud de cluster contenant l'agrégat sélectionné. L'état de santé des agrégats s'affiche également, sur la base du niveau de gravité le plus élevé. Par exemple, si un nœud du cluster contient dix agrégats, dont cinq affichent le statut d'avertissement et les cinq restants qui affichent l'état critique, l'état affiché est critique.

- **Volumes**

  Affiche le nombre et la capacité des volumes FlexVol et FlexGroup de l'agrégat, mais pas les composants

FlexGroup. L’état de santé des volumes est également affiché, sur la base du niveau de gravité le plus élevé.

- **Pool de ressources**

  Affiche les pools de ressources associés à l’agrégat.

- **Disques**

  Affiche le nombre de disques de 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 en modifiant une alerte existante en cliquant sur le nom de l’alerte.

Informations connexes

"Affichage des détails du pool de stockage"

Protégez et restaurez les données

Création, surveillance et résolution des problèmes de relations de protection

Unified Manager vous permet de créer des relations de protection, de surveiller et de résoudre les problèmes de protection en miroir et de sauvegarde des données stockées sur les clusters gérés, et de restaurer les données lorsqu'elles sont remplacées ou perdues.

Types de protection SnapMirror

Selon le déploiement de la 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 contre les basculements après incident, mais elles proposent plusieurs fonctionnalités en performances, une flexibilité de version et une protection contre les copies de sauvegarde différentes.

Relations de protection asynchrones SnapMirror classiques

La protection asynchrone traditionnelle de SnapMirror protège les miroirs de réplication de blocs entre les volumes source et de destination.

Dans les relations SnapMirror traditionnelles, les opérations de mise en miroir s'exécutent plus rapidement que dans d'autres relations SnapMirror, car l'opération de mise en miroir est basée sur la réplication de blocs. La protection traditionnelle par SnapMirror implique cependant que le volume de destination s'exécute sous la même version mineure du logiciel ONTAP ou une version ultérieure, que le volume source soit au sein de la même version principale (par exemple, version 8.x vers 8.x ou 9.x vers 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 de SnapMirror avec réplication flexible de la version

La protection asynchrone de SnapMirror avec la réplication flexible de la version protège les miroirs de réplication logique entre les volumes source et de destination, même si ces volumes sont exécutés sous différentes versions du logiciel ONTAP 8.3 ou version ultérieure (par exemple, la 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 la réplication flexible de la version, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

Compte tenu du ralentissement d'exécution, SnapMirror avec protection de réplication flexible de la version ne convient pas à implémenter dans l'un ou l'autre des cas suivants :

- L'objet source contient plus de 10 millions de fichiers à protéger.
- L'objectif de point de restauration des données protégées est de deux heures maximum. (La destination doit donc toujours contenir des données mises en miroir et récupérables datant d'au plus deux heures que les données de la source.)

Dans l'un ou l'autre des cas répertoriés, l'exécution plus rapide de la protection SnapMirror par défaut basée sur la réplication des blocs est requise.

Protection asynchrone de SnapMirror avec l'option de réplication et de sauvegarde flexibles de la version

La protection asynchrone de SnapMirror avec l'option de réplication et de sauvegarde flexible de la version protège les données en miroir entre les volumes source et de destination, et permet de stocker plusieurs copies des données en miroir sur la destination.

L'administrateur du stockage peut spécifier quelles copies Snapshot sont mises en miroir de la source vers la destination et spécifier également la durée de conservation de ces copies au niveau de la destination, même si elles sont supprimées à la source.

Dans les relations SnapMirror avec l'option de réplication et de sauvegarde flexibles de la version, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

Réplication unifiée SnapMirror (mise en miroir et archivage sécurisé)

La réplication unifiée SnapMirror vous permet de configurer la reprise après incident et l'archivage sur le même volume de destination. Comme pour SnapMirror, la protection unifiée des données effectue un transfert de base dès le premier appel que vous l'appelez. Un transfert de base placé sous la règle de protection unifiée des données par défaut « irriorAndVault » effectue une copie Snapshot du volume source, puis transfère cette copie et les données qu'elle renvoie au volume de destination. Comme SnapVault, la protection unifiée des données n'inclut pas d'anciennes copies Snapshot de la configuration de base.

Protection SnapMirror synchrone avec synchronisation stricte

La protection SnapMirror synchrone avec synchronisation « par suppression » garantit que les volumes primaires et secondaires sont toujours une copie authentique les uns des autres. En cas de défaillance de réplication lors d'une tentative d'écriture de données sur le volume secondaire, les E/S du client vers le volume primaire sont interrompues.

Protection SnapMirror synchrone avec synchronisation régulière

La protection synchrone de SnapMirror avec la synchronisation « granulaire » n'exige pas que les volumes primaire et secondaire soient toujours une copie authentique des uns des autres, ce qui assure la disponibilité du volume primaire. Si une défaillance de réplication se produit lors d'une tentative d'écriture de données sur le volume secondaire, les volumes primaire et secondaire sont désynchronisés et les E/S client continuent sur le volume primaire.

> Le bouton Restaurer et les boutons d'opération de relation ne sont pas disponibles lors de la surveillance des relations de protection synchrone à partir de la vue Santé : tous les volumes ou de la page Détails du volume / intégrité.

Synchronisation active SnapMirror

La fonction de synchronisation active SnapMirror est disponible avec ONTAP 9.8 et versions ultérieures. Elle vous permet de protéger les applications avec les LUN. Ainsi, les applications basculent en toute transparence, assurant ainsi la continuité de l'activité en cas d'incident.

Elle vous permet de détecter et de surveiller les relations SnapMirror synchrones pour les groupes de cohérence disponibles sur les clusters et les machines virtuelles de stockage de Unified Manager. La synchronisation active SnapMirror est prise en charge sur les clusters AFF ou All SAN Array (ASA), dans lesquels les clusters principal et secondaire peuvent être AFF ou ASA. La synchronisation active SnapMirror 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 afficher une vue unifiée des relations de protection et des groupes de cohérence dans l'inventaire des volumes, afficher la topologie de protection des 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 récapitulatif des relations de groupe de cohérence, rechercher le support des relations de 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 protégée par le groupe de cohérence.

Pour en savoir plus sur la synchronisation active SnapMirror, reportez-vous "Documentation ONTAP 9 pour SnapMirror Active Sync (anciennement SM-BC)"à la section .

Configuration des relations de protection dans Unified Manager

Il existe plusieurs étapes à effectuer pour utiliser Unified Manager et OnCommand Workflow Automation afin de configurer les relations SnapMirror et SnapVault afin de protéger vos données.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir établi des relations entre deux clusters ou deux SVM (Storage Virtual machine).
- OnCommand Workflow Automation doit être intégré avec Unified Manager :
  - "Configurer OnCommand Workflow Automation".
  - "Vérification de la mise en cache des sources de données 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 stratégie pour la relation, en fonction du type de relation que vous créez, effectuez l'une des opérations suivantes :
   - "Création d'une règle SnapVault".
   - "Créer une règle SnapMirror".
3. "Créer une planification SnapMirror ou SnapVault".

Configuration d'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 flux de travail de configuration SnapMirror et SnapVault, ainsi que des commandes pour gérer les relations SnapMirror.

Ce dont vous aurez besoin

- La version installée de Workflow Automation doit être égale ou supérieure à 5.1.

> Le pack WFA pour la gestion de clustered Data ONTAP est inclus dans WFA 5.1. Il n'est donc pas nécessaire de télécharger ce pack sur le site NetApp Storage Automation Store et de l'installer séparément sur votre serveur WFA, comme requis par le passé. "WFA pack pour la gestion de 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 utilisateur du schéma d'intégration.

- Vous devez être affecté soit au rôle Administrateur, soit au rôle architecte dans Workflow Automation.
- L'adresse de l'hôte, le numéro de port 443, le nom d'utilisateur et le mot de passe doivent être définis pour Workflow Automation.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Workflow Automation**.
2. Dans la zone **Database User** de la page **Workflow Automation**, 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 **Workflow Automation Credentials** de la page, entrez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6), ainsi que le nom d'utilisateur et le mot de passe de la configuration de Workflow Automation.

   Vous devez utiliser le port de 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 Workflow Automation s'affiche.

6. Cliquez sur **Oui** pour recharger l'interface utilisateur Web et ajouter les fonctions Workflow Automation.

Informations connexes

"Documentation NetApp : OnCommand Workflow Automation (versions actuelles)"

Vérification de la mise en cache des sources de données Unified Manager dans Workflow Automation

Vous pouvez déterminer si la mise en cache des sources de données Unified Manager fonctionne correctement en vérifiant si l'acquisition des sources de données dans Workflow Automation fonctionne correctement. Vous pouvez le faire lorsque vous intégrez Workflow Automation à Unified Manager pour vous assurer que la fonctionnalité Workflow Automation est disponible après l'intégration.

Ce dont vous aurez besoin

Pour effectuer cette tâche, vous devez être affecté soit au rôle Administrateur, soit au rôle architecte dans Workflow Automation.

Étapes

1. Dans l'interface utilisateur Workflow Automation, sélectionnez **exécution** > **sources de données**.
2. Cliquez avec le bouton droit de la souris sur le nom de la source de données Unified Manager, puis sélectionnez **acquérir maintenant**.
3. Vérifiez que l'acquisition réussit sans erreur.

   Pour que l'intégration de Workflow Automation à Unified Manager réussisse, les erreurs d'acquisition doivent être résolues.

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 toutes les tâches OnCommand Workflow Automation en cours d'exécution ou planifiées sont arrêtées.

Vous devez également supprimer manuellement Unified Manager de OnCommand Workflow Automation.

Après avoir réinstallé ou mis à niveau OnCommand Workflow Automation, vous devez de nouveau configurer la connexion avec Unified Manager.

Suppression de la configuration OnCommand Workflow Automation depuis Unified Manager

Vous pouvez supprimer la configuration OnCommand Workflow Automation d'Unified Manager si vous ne souhaitez plus utiliser Workflow Automation.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Workflow Automation** dans le menu de configuration de gauche.
2. Dans la page **Workflow Automation**, cliquez sur **Supprimer la configuration**.

Effectuer un basculement et un retour arrière 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 incident, vous pouvez utiliser les fonctions de relation de protection de Unified Manager pour rendre les données de destination de protection accessibles en lecture/écriture et basculer vers le volume jusqu'à ce que la source soit à nouveau en ligne. vous pouvez ensuite revenir à la source d'origine lorsqu'il est disponible pour transmettre les données.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation pour effectuer cette opération.

Étapes

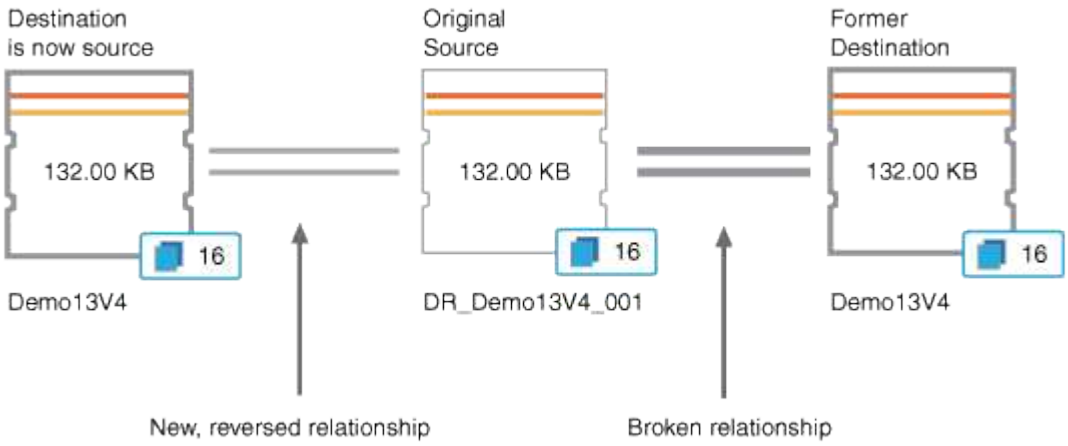
1. "Interrompre la relation SnapMirror".

   Vous devez interrompre la relation avant de pouvoir convertir la destination d'un volume de protection des données en volume de lecture/écriture, et avant d'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. 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 Snapshot de base est créée pour la nouvelle relation.

   La relation inversée ressemble à une relation en cascade :



3. "Interrompre la relation SnapMirror inversée".

   Lorsque le volume source d'origine est resynchronisé et peut à nouveau transmettre les données, utilisez l'opération de coupure pour interrompre 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.

Briser une relation SnapMirror depuis la page des détails du volume / intégrité

Vous pouvez interrompre une relation de protection à partir de la page des détails de volume/intégrité et arrêter les transferts de données entre un volume source et un volume cible dans une relation SnapMirror. Vous pouvez briser une relation lorsque vous souhaitez migrer des données, pour la reprise d'activité ou pour le test d'application. Le volume de destination est modifié en volume de lecture-écriture. Vous ne pouvez pas

interrompre une relation SnapVault.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez interrompre.
2. Cliquez avec le bouton droit de la souris 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.

Inversion des relations de protection à partir de la page Détails du volume/intégrité

Lorsqu'un incident désactive le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour transmettre des données en les convertissant en lecture/écriture pendant que vous réparez ou remplacez la source. Lorsque la source est de 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 de la source avec celles de la destination de lecture/écriture.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.
- 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 règles et les planifications créées sur la relation de resynchronisation inverse sont identiques à celles de la relation de protection d'origine.

  Si des stratégies et des plannings n'existent pas, ils sont créés.

Étapes

1. Dans l'onglet **protection** de la page de détails **Volume/Santé**, localisez dans la topologie la relation SnapMirror sur laquelle vous souhaitez inverser la source et la destination, et cliquez avec le bouton droit de la souris.

2. Sélectionnez **Reverse Resync** dans le menu.

   La boîte de dialogue Reverse Resync s'affiche.

3. Vérifiez que la relation affichée dans la boîte de dialogue **Reverse Resync** est celle pour laquelle vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Submit**.

   La boîte de dialogue Reverse Resync est fermée et un lien de tâche s'affiche en haut de la page Volume / Health details.

4. **Facultatif:** cliquez sur **Afficher les travaux** sur la page **Volume / Santé** pour suivre l'état de chaque tâche de resynchronisation inverse.

   Une liste filtrée des travaux 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 de travail sont terminées avec succès.

Suppression d'une relation de protection de la page Détails du volume/intégrité

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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page d'informations **Volume/Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez supprimer.
2. Cliquez avec le bouton droit de la souris 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 Volume / Health details.

Resynchronisation des relations de protection à partir de la page Détails du volume/intégrité

Vous pouvez resynchroniser les données d'une relation SnapMirror ou SnapVault interrompue, puis la destination a été créée en lecture/écriture afin que les données de la source correspondent aux données de destination. Vous pouvez également resynchroniser lorsqu'une copie Snapshot commune requise sur le volume source est

supprimée, entraînant l'échec des mises à jour de SnapMirror ou de SnapVault.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page de détails **Volume / Santé**, localisez 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.

   Vous pouvez également sélectionner **relations** > **Resynchroniser** dans le menu **actions** pour resynchroniser la relation pour laquelle vous consultez actuellement les détails.

   La boîte de dialogue Resynchroniser s'affiche.

3. Dans l'onglet **Resynchronisation Options**, sélectionnez une priorité de transfert et le taux de transfert maximal.
4. Cliquez sur **copies snapshot source**, puis, dans la colonne **copie snapshot**, cliquez sur **par défaut**.

   La boîte de dialogue Sélectionner une copie Snapshot source s'affiche.

5. Pour spécifier une copie Snapshot existante plutôt que de transférer la copie Snapshot par défaut, cliquez sur **copie Snapshot existante** et sélectionnez une copie Snapshot 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 **default** pour la source suivante pour laquelle vous souhaitez spécifier une copie Snapshot existante.
8. Cliquez sur **Submit** pour lancer le travail de resynchronisation.

   Le travail de resynchronisation est lancé, vous êtes renvoyé à la page Détails du volume / intégrité et un lien tâches s'affiche en haut de la page.

9. **Facultatif:** cliquez sur **Afficher les travaux** dans la page **Détails du volume / de l'état de santé** pour suivre l'état de chaque travail de resynchronisation.

   Une liste filtrée des travaux s'affiche.

10. **Facultatif:** cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

    La tâche de resynchronisation est terminée lorsque toutes les tâches de travail sont terminées avec succès.

Résolution de l'échec d'une tâche de protection

Ce flux de travail fournit un exemple d'identification et de résolution d'une défaillance de tâche de protection à partir du tableau de bord Unified Manager.

Ce dont vous aurez besoin

Comme certaines tâches de ce flux de travail nécessitent de vous connecter à l'aide du rôle Administrateur, vous devez connaître les rôles requis pour utiliser diverses fonctionnalités.

Dans ce scénario, vous accédez à la page Tableau de bord pour voir s'il y a des problèmes avec vos tâches de protection. Dans la zone incident de protection, vous remarquez qu'un incident de fin de tâche est survenu, indiquant une erreur d'échec de tâche de protection sur un volume. Vous étudiez cette erreur afin de déterminer la cause possible et la résolution potentielle.

Étapes

1. Dans le panneau protection incidents de la zone Tableau de bord incidents et risques non résolus, cliquez sur l'événement **protection job failed**.

   > Le texte lié à l'événement est écrit sous la forme `object_name:/object_name - Error Name`, par exemple `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 mesures correctives possibles.

   Voir "Identification du problème et exécution d'actions correctives pour une tâche de protection ayant échoué".

Identification du problème et exécution d'actions correctives pour une tâche de protection ayant échoué

Vous examinez le message d'erreur d'échec du travail dans le champ cause de la page Détails de l'événement et déterminez que le travail a échoué en raison d'une erreur de copie Snapshot. Vous allez ensuite à la page Volume / Health details pour recueillir plus d'informations.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Le message d'erreur fourni dans le champ cause de la page Détails de l'événement contient le texte suivant concernant le travail en échec :

```
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 miroir ne s'est pas terminée avec succès.

  Cette tâche impliquait une relation de protection entre le volume source `cluster2_src_vol2` du 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 Snapshot 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. Toutefois, pour résoudre ce problème, vous devez accéder à l'interface utilisateur Web de System Manager ou aux commandes de l'interface de ligne de commande de ONTAP.

Étapes

1. Vous passez en revue le message d'erreur et déterminez qu'une tâche de copie Snapshot a échoué sur le volume source, ce qui indique qu'il y a probablement un problème avec le volume source.

   Vous pouvez également cliquer sur le lien **Détails du travail** à la fin du message d'erreur, mais pour ce scénario, vous choisissez de ne pas le faire.

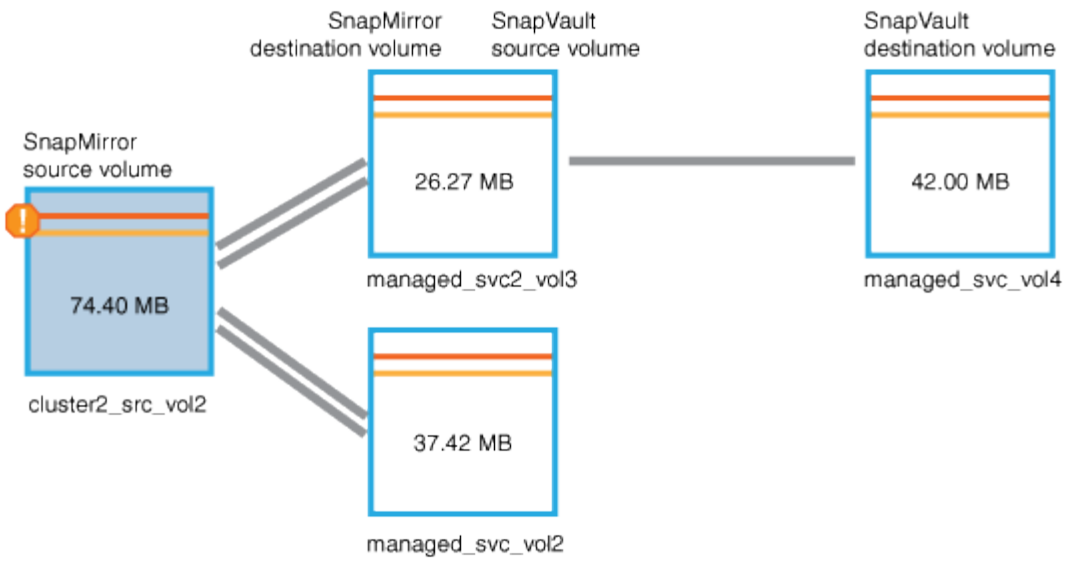
2. Vous décidez que vous voulez essayer de résoudre l'événement, vous devez donc procéder comme suit :
   a. Cliquez sur le bouton **affecter à** et sélectionnez **Me** dans le menu.
   b. Cliquez sur le bouton **Acknowledge** pour ne pas continuer à recevoir de notifications d'alerte répétées si des alertes ont été définies pour l'événement.
   c. Vous pouvez également ajouter des remarques à propos de l'événement.
3. Cliquez sur le champ **Source** dans le volet **Résumé** pour afficher les détails du volume source.

   Le champ **Source** contient le nom de l'objet source : dans ce cas, le volume sur lequel le travail de copie Snapshot a été planifié.

   La page de détails Volume / Santé s'affiche pour `cluster2_src_vol2`, affichant le contenu de l'onglet protection.

4. Sur le graphique de topologie de protection, une icône d'erreur s'affiche, associée au premier volume de la topologie, qui correspond au 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. Placez le curseur sur l'icône d'erreur pour afficher la boîte de dialogue contextuelle qui affiche les paramètres de seuil et voir que le volume a dépassé le seuil d'erreur, ce qui indique un problème de capacité.
6. Cliquez sur l'onglet **capacité**.

   Informations de capacité sur les affichages de volume `cluster2_src_vol2`.

7. Dans le panneau **Capacity**, une icône d'erreur s'affiche dans le graphique à barres, indiquant que la capacité de volume a dépassé le niveau de seuil défini pour le volume.
8. Sous le graphique capacité, vous constatez que la croissance automatique du volume a été désactivée et qu'une garantie d'espace volume a été définie.

   Vous pourriez décider d'activer la croissance automatique, mais dans le cadre de ce scénario, vous décidez d'en approfondir avant de prendre une décision sur la manière de résoudre le problème de capacité.

9. Vous faites défiler la liste **Events** et voyez que les événements protection Job failed, Volume Days jusqu'à Full et Volume Space Full ont été générés.
10. Dans la liste **Evénements**, vous cliquez sur l'événement **Volume Space Full** pour obtenir plus d'informations, ayant décidé que cet événement semble le plus pertinent pour votre problème de capacité.

    La page Détails de l'événement affiche l'événement Volume Space Full 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 suggestions d'actions correctives.

    > Les actions correctives suggérées s'affichent uniquement pour certains événements. Vous ne voyez donc pas cette zone pour tous les types d'événements.

    Vous pouvez cliquer sur la liste des actions suggérées pour résoudre l'événement Volume Space Full :

    - Activer la croissance automatique sur ce volume.
    - Redimensionner le volume.

- Activer et exécuter la déduplication sur ce volume.
- Activer et exécuter la compression sur ce volume.

13. Vous décidez d'activer la croissance automatique sur le volume. 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 liés**.

    > Vous pouvez cliquer sur le nom de l'agrégat pour obtenir plus de détails sur celui-ci.

    Vous avez établi que l'agrégat dispose d'un espace suffisant pour activer la croissance automatique de volumes.

    b. En haut de la page, regardez l'icône indiquant un incident critique et passez en revue le texte au-dessous de l'icône.

    Vous déterminez que « jours complets : moins d'une journée | taux de croissance quotidien : 5.4 % ».

14. Accédez à System Manager ou à l'interface de ligne de commandes ONTAP pour activer l' `volume autogrow`option.

    > Notez les noms du volume et de l'agrégat pour qu'ils soient disponibles en cas d'activation de la croissance automatique.

15. Après avoir résolu le problème de capacité, revenez à la page Détails Unified Manager **Event** et marquez l'événement comme résolu.

Résolution des problèmes de décalage

Ce flux de travail fournit un exemple de résolution d'un problème de décalage. Dans ce scénario, vous êtes un administrateur ou un opérateur qui accède à la page Tableau de bord Unified ManagerLe cas échéant, pour voir s'il y a des problèmes avec vos relations de protection et, le cas échéant, pour trouver des solutions.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Sur 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 protection risques.

Étapes

1. Dans le volet **protection** de la page **Dashboard**, localisez l'erreur de décalage de la 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 **Event**, vous pouvez effectuer une ou plusieurs des tâches suivantes :
   - Passez en revue le message d'erreur dans le champ cause de la zone Résumé pour déterminer s'il y a 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.

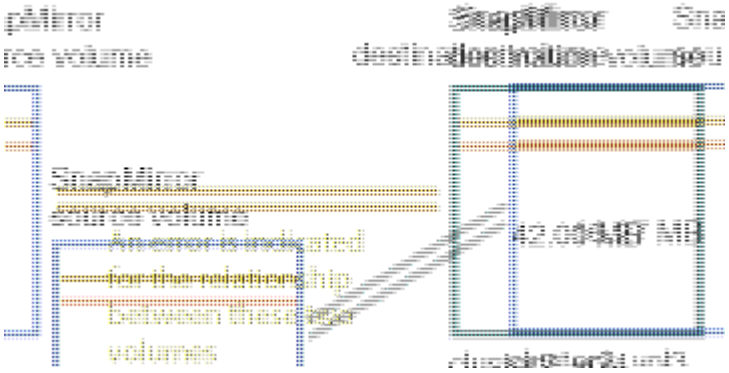
- Recherchez les notes qui ont peut-être été ajoutées à ce sujet.
- Ajoutez une note à l'événement.
- Attribuez l'événement à un utilisateur spécifique.
- Accuser réception ou résoudre l'événement.

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 du volume/intégrité s'affiche.

4. Dans l'onglet **protection**, vous examinez le diagramme de topologie.

   Vous remarquerez que le volume avec l'erreur de décalage est le dernier volume d'une cascade SnapMirror à trois volumes. Le volume sélectionné est en gris foncé et une ligne double orange du volume source indique une erreur de relation SnapMirror.



5. Cliquer sur chacun des volumes de la cascade SnapMirror.

   Lorsque vous sélectionnez chaque volume, les informations de protection dans le récapitulatif, topologie, Historique, événements, périphériques associés, Les zones alertes associées changent pour afficher les détails relatifs au volume sélectionné.

6. Vous regardez la zone **Résumé** et placez votre curseur sur l'icône d'information dans le champ **mettre à jour le programme** pour chaque volume.

   Dans ce scénario, vous remarquerez que la règle SnapMirror est DPDefault et que la planification SnapMirror est mise à jour toutes les heures à cinq minutes après l'heure. Vous avez conscience que tous les volumes de la relation tentent de réaliser 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.

Gestion et surveillance des 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 primaire au volume secondaire est déterminée par une planification.

- Synchrone

  La réplication s'effectue simultanément sur les volumes primaire et secondaire.

Vous pouvez effectuer jusqu'à 10 tâches de protection en même temps, sans affecter les performances. Vous pouvez avoir un impact certain sur les performances lorsque vous exécutez simultanément entre 11 et 30 tâches. Il n'est pas recommandé d'exécuter plus de 30 tâches simultanément.

Affichage de l'état de protection du volume

La page protection des données présente une vue globale des détails de protection des données pour tous les volumes protégés d'un cluster unique, ou tous les clusters d'un data Center.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
2. Selon que vous souhaitez afficher l'état de la protection des données pour tous les clusters surveillés ou pour un seul cluster, sélectionnez **tous les clusters** ou sélectionnez un cluster unique dans le menu déroulant.
3. Cliquez sur la flèche droite en haut du panneau protection des données. La page **Data protection** s'affiche.

Selon que vous avez sélectionné un seul ou l'ensemble des clusters de votre data Center, cette page affiche l'état de protection des données des volumes protégés par les copies Snapshot ou les stratégies SnapMirror, ainsi que le nombre de volumes non protégés.

Si vous sélectionnez un cluster dans la liste **Individual Cluster**, la protection Snapshot et l'état des relations SnapMirror des volumes protégés de ce cluster s'affichent.

Cliquez sur les événements de cette page pour accéder 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 gestion des événements. Vous pouvez positionner le curseur de la souris pour afficher les comptages et légendes respectifs. Vous pouvez cliquer sur :

- Les graphiques à barres des volumes et volumes non protégés par les copies Snapshot permettent d'accéder à la page volumes et d'afficher les détails.
- Les graphiques à barres permettant d'accéder à la page relations, où les détails sont filtrés par le groupe source.

Afficher l'état de protection des volumes protégés par des copies Snapshot

Présentation des copies Snapshot : vue d'ensemble des volumes protégés par les copies Snapshot, par exemple :

- Le nombre total de volumes protégés et non protégés par les copies Snapshot.
- Nombre total de volumes qui utilisent ou dépassent l'espace de réserve pour les copies Snapshot.

Analyse des copies Snapshot fournit les informations suivantes :

- Événements individuels pour les copies Snapshot, y compris les événements survenus au cours des dernières 24 heures.
- Tableau détaillé des volumes protégés et non protégés par les copies Snapshot.
- Volumes utilisant, sans utiliser ni enfreindre la capacité de copie Snapshot réservée.
- Répartition du nombre de volumes en termes de nombre de copies Snapshot.

Points à noter pour les copies Snapshot

- Pour comptabiliser les volumes protégés par des copies Snapshot, il convient d'envisager des volumes source et de destination.
- Le nombre de copies Snapshot renvoyées correspond uniquement aux volumes en ligne et disponibles.
- La plage de graphiques correspondant au nombre de copies Snapshot est dynamique. Il est généré en fonction du nombre de snapshots présents dans le cluster sélectionné.
- Si vous envisagez de protéger un volume, la planification de la copie Snapshot du volume doit être activée.
- La valeur de l'espace de réserve pour les copies Snapshot est importante pour afficher la quantité d'espace disque utilisée ou pour calculer l'espace pouvant être récupéré si une ou plusieurs copies Snapshot sont supprimées.

Affichez l'état de protection des relations SnapMirror

Présentation de SnapMirror : présentation des volumes protégés par des règles SnapMirror, notamment :

- Le nombre de volumes protégés par les règles SnapMirror respectives, comme les relations SnapMirror volume, la reprise après incident de stockage virtuel (SVM-DR) et leurs combinaisons.
- Le nombre total de relations SnapMirror avec décalage par rapport à l'état de décalage (RPO).

SnapMirror Analysis fournit les informations suivantes :

- Événements individuels soulevés pour les relations SnapMirror, y compris les événements survenus au cours des dernières 24 heures
- Le nombre de volumes protégés par chaque type de règle SnapMirror.
- Nombre de relations protégées par les types de relations SnapMirror, telles que Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, le groupe de cohérence de synchronisation actif SnapMirror et Sync.
- Le nombre de relations saines et malsaines.
- Répartition du nombre de relations de volume. Vous pouvez basculer les graphiques en fonction du temps et de l'état du décalage RPO.
- Seuils de décalage pour la relation non gérée. 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 décalage pour les relations de protection non gérées".

Points à noter pour les relations SnapMirror

- Pour comptabiliser les relations SnapMirror, les volumes source, 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 de données repose sur la relation SnapMirror. L'état 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 compté pour le décalage RPO.
- Les relations de volume sont considérées comme malsaines en cas de problèmes de réplication des données entre la source et la destination, par exemple lorsque la relation est rompue.

Afficher les clusters protégés par une configuration MetroCluster

Le panneau **MetroCluster protection** de la page **Data protection** affiche le nombre de clusters protégés ou non protégés par MetroCluster sur FC ou par la configuration IP de votre site. Cliquez sur les graphiques à barres de ce panneau pour accéder à la page clusters dans laquelle 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, reportez-vous à "Contrôle des configurations MetroCluster"la section .

Affichage des relations de protection des volumes

Depuis la vue relation : toutes les relations, et depuis la page Volume relations, vous pouvez afficher l'état des relations SnapMirror volume et SnapVault existantes. Vous pouvez également examiner des détails sur les relations de protection, notamment le statut de transfert et de décalage, les informations sur la source et la destination, les informations de planification et de stratégie, etc.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 **Storage** > **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 informations de protection des volumes :

   - Pour afficher les informations actuelles sur toutes les relations de volume, rester sur la page par défaut **toutes les relations**.
   - Pour afficher des informations détaillées sur les tendances de transfert de volume sur une période de temps, dans le menu Affichage, sélectionnez relation : vue État transfert du dernier mois.
   - Pour afficher des informations détaillées sur l'activité de transfert de volume jour en jour, dans le menu Affichage, sélectionnez relation : vue du dernier 1 mois du taux de transfert.

Les vues de transfert de volume affichent des informations sur les volumes dans les relations asynchrones uniquement - les volumes dans les relations synchrones ne sont pas affichés.

Contrôle des 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 contrôler ces LUN sur Active IQ Unified Manager.

La synchronisation active SnapMirror garantit un objectif de délai de restauration nul en cas de basculement dans des environnements SAN. Dans un déploiement typique prenant en charge la synchronisation active SnapMirror, les LUN sur des volumes sont protégées par des relations de groupe de cohérence.

Ces LUN primaires et secondaires sont des LUN composites ou une paire de LUN de réplica avec le même UUID et le même numéro de série. Les opérations d'E/S (lecture et écriture) sont multiplexées entre les sites source et de destination sur ces LUN composites, pour une meilleure transparence.

Pour afficher les LUN composites, vous devez ajouter et découvrir les clusters principal et secondaire avec les LUN faisant partie de la relation de groupe de cohérence sur Unified Manager. Seules les LUN iSCSI et FCP sont prises en charge.

Pour plus d'informations sur la synchronisation active SnapMirror, reportez-vous à "Documentation ONTAP 9 pour SnapMirror Active Sync (anciennement SM-BC)"la section .

Pour afficher les LUN composites dans votre environnement, effectuez la procédure suivante :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **LUNs**.
2. Dans le menu Affichage, sélectionnez **relation** > **tous les LUN**.

   La relation : toutes les LUN s'affichent.

Vous pouvez afficher les détails de la LUN, tels que le nom de la LUN, le volume, la machine virtuelle de stockage hébergeant la LUN, le cluster, le groupe de cohérence et la LUN partenaire. Vous pouvez cliquer sur chacun de ces composants pour accéder à une vue détaillée. Cliquez sur Groupe de cohérence pour accéder à la page relations.

Cliquez sur le LUN partenaire pour afficher les détails de configuration dans l'onglet SAN de la page Storage VM Details de la VM de stockage correspondant à la VM de stockage sur laquelle est hébergée la LUN partenaire. Les informations telles que les initiateurs et les groupes initiateurs, ainsi que d'autres aspects de la LUN partenaire s'affichent.

Vous pouvez exécuter les fonctions standard de tri, de filtrage, de génération et de téléchargement des rapports des LUN protégées de votre environnement au niveau de la grille.

Création d'une relation de protection SnapVault depuis 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 une même VM de stockage afin de permettre la

sauvegarde des données à des fins de protection.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Le menu **Protect** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans la vue **Santé : tous les volumes**, sélectionnez un volume à protéger et cliquez sur **protéger**.

   Sinon, 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 relatives au volume secondaire.
5. Cliquez sur **Advanced** pour définir la déduplication, la compression, la croissance automatique et la garantie d'espace selon les besoins, puis cliquez sur **Apply**.
6. Renseignez la zone **destination information** et la zone **Relationship Settings** de l'onglet **SnapVault**.
7. Cliquez sur **appliquer**.

   Vous êtes renvoyé à la vue Santé: Tous les volumes.

8. Cliquez sur le lien du travail 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. Cependant, 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'un seul travail, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de protection et déterminer quand la tâche est terminée.
   - Si vous avez plusieurs travaux :
     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 à la tâche de configuration de protection et déterminer quand la tâche est terminée.
     iii. Utilisez le bouton **Retour** pour revenir à la liste filtrée et afficher un autre travail.

Création d’une relation de protection SnapVault à partir de la page des détails du volume / intégrité

Vous pouvez créer une relation SnapVault à l’aide de la page des détails de volume/intégrité, de sorte que les sauvegardes de données soient activées à des fins de protection sur des volumes.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation pour effectuer cette tâche.

Le menu **Protect** ne s’affiche pas dans les cas suivants :

- Si les paramètres RBAC n’autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d’opérateur
- Lorsque l’ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster 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 de la souris 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 de ressource secondaire.
4. Cliquez sur **Advanced** pour définir la déduplication, la compression, la croissance automatique et la garantie d’espace selon les besoins, puis cliquez sur **Apply**.
5. Renseignez la zone **destination information** et la zone **Relationship Settings** de la boîte de dialogue **Configure protection**.
6. Cliquez sur **appliquer**.

   Vous êtes renvoyé à la page Volume / Health details.

7. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page **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 à la tâche de configuration de protection et déterminer quand la tâche est terminée.

   Une fois les tâches terminées, les nouvelles relations s’affichent dans la vue topologique de la page Volume / Health details.

Création d’une relation de protection SnapMirror depuis la vue Santé : tous les volumes

A partir de la vue Santé : tous les volumes, vous pouvez créer plusieurs relations de

protection SnapMirror simultanément en sélectionnant plusieurs volumes sur la même VM de stockage.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Le menu **Protect** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert

Étapes

1. Dans la vue **Health: All volumes**, sélectionnez un volume que vous souhaitez protéger.

   Alternativement, pour créer plusieurs relations de protection sur le même SVM, sélectionnez un ou plusieurs volumes dans la vue Health: All volumes, et cliquez sur **Protect** > **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 les besoins, puis cliquez sur **appliquer**.
4. Renseignez la zone **destination information** et la zone **Relationship Settings** de l'onglet **SnapMirror**.
5. Cliquez sur **appliquer**.

   Vous êtes renvoyé à la vue Santé: Tous les volumes.

6. Cliquez sur le lien du travail 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. Cependant, si vous créez plusieurs relations de protection, la 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'un seul travail, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de protection et déterminer quand la tâche est terminée.
   - Si vous avez plusieurs travaux :
     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 à la tâche de configuration de protection et déterminer quand la tâche est terminée.
     iii. Utilisez le bouton **Retour** pour revenir à la liste filtrée et afficher un autre travail.

En fonction du SVM de destination que vous avez spécifié lors de la configuration ou des options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut être l'une des variantes suivantes :

- Si vous avez spécifié un SVM de destination qui s'exécute sous la même version ou plus récente de ONTAP que celui du volume source, une relation SnapMirror basée sur la réplication de bloc est le résultat par défaut.
- Si vous avez spécifié un SVM de destination qui s'exécute sous la même version ou plus récente de ONTAP que celui du volume source, mais que vous avez activé la réplication flexible de version dans les paramètres avancés, il en résulte une relation SnapMirror avec la réplication flexible de la version.
- Si vous avez spécifié un SVM de destination qui s'exécute sous une version antérieure de ONTAP par rapport au volume source, et la version précédente prend en charge la réplication flexible de la version, une relation SnapMirror avec la réplication flexible de la version est le résultat automatique.

Création d'une relation de protection SnapMirror à partir de la page des détails du volume / intégrité

Vous pouvez utiliser la page de détails volume/intégrité pour créer une relation SnapMirror de sorte que la réplication des données soit activée à des fins de protection. La réplication SnapMirror vous permet de restaurer les données à partir du volume de destination en cas de perte de données sur la source.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Le menu **Protect** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert

Vous pouvez effectuer jusqu'à 10 tâches de protection en même temps, sans affecter les performances. Vous pouvez avoir un impact certain sur les performances lorsque vous exécutez simultanément entre 11 et 30 tâches. Il n'est pas recommandé d'exécuter plus de 30 tâches simultanément.

Étapes

1. Dans l'onglet **protection** de la page **Volume / Santé**, cliquez avec le bouton droit de la souris dans la vue topologique sur le nom d'un volume que vous souhaitez protéger.
2. Sélectionnez **Protect** > **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 les besoins, puis cliquez sur **appliquer**.
5. Renseignez la zone **destination information** et la zone **Relationship Settings** de la boîte de dialogue **Configure protection**.
6. Cliquez sur **appliquer**.

   Vous êtes renvoyé à la page Volume / Health details.

7. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page **Volume / Santé**.

Les tâches et les détails du travail s'affichent sur la page Détails du travail.

8. Dans la page **Job** details, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails de la tâche associée à la tâche de configuration de la protection et déterminer quand la tâche est terminée.
9. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails **Volume / Santé**.

   La nouvelle relation s'affiche dans la vue topologique de la page Volume / Health details.

En fonction du SVM de destination que vous avez spécifié lors de la configuration ou des options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut être l'une des variantes suivantes :

- Si vous avez spécifié un SVM de destination qui s'exécute sous la même version ou plus récente de ONTAP que celui du volume source, une relation SnapMirror basée sur la réplication de bloc est le résultat par défaut.
- Si vous avez spécifié un SVM de destination qui s'exécute sous la même version ou plus récente de ONTAP que celui du volume source, mais que vous avez activé la réplication flexible de version dans les paramètres avancés, il en résulte une relation SnapMirror avec la réplication flexible de la version.
- Si vous avez spécifié un SVM de destination qui s'exécute sous une version antérieure de ONTAP, ou une version supérieure à celle du volume source et que la version précédente prend en charge la réplication flexible de la version, il s'agit du résultat automatique d'une relation SnapMirror avec la réplication flexible de la version.

Création d'une relation SnapMirror avec la réplication flexible de la version

Vous pouvez créer une relation SnapMirror avec la réplication flexible de la version. La réplication flexible de la version vous permet d'implémenter la protection SnapMirror, même si les volumes source et de destination s'exécutent sous différentes versions d'ONTAP.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.
- Les SVM source et destination doivent tous deux disposer d'une licence SnapMirror activée.
- Les SVM source et de destination doivent être exécutés sous une version du logiciel ONTAP qui prend en charge la réplication flexible de la version.

SnapMirror avec la réplication flexible de la version vous permet d'implémenter la protection SnapMirror, même dans des environnements de stockage hétérogènes où tout le stockage n'est pas exécuté sous une version d'ONTAP. Toutefois, les opérations de mise en miroir effectuées sous SnapMirror avec une réplication flexible de la version ne s'exécutent pas aussi rapidement que sous SnapMirror de réplication de blocs traditionnelle.

Étapes

1. Affichez la boîte de dialogue **Configure protection** pour le volume que vous souhaitez protéger.
   - Si vous consultez l'onglet protection de la page Détails du volume/intégrité, cliquez avec le bouton droit de la souris dans la vue topologique portant le nom d'un volume à protéger et sélectionnez **protéger** > **SnapMirror** dans le menu.

- Si vous affichez la vue Santé : tous les volumes, localisez 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. Renseignez la zone **destination information** et la zone **Relationship Settings** de la boîte de dialogue **Configure protection**.

   Si vous spécifiez un SVM de destination qui s'exécute sous une version antérieure de ONTAP par rapport au volume source que vous protégez. Si cette version antérieure prend en charge la réplication flexible de la version, cette tâche configure automatiquement SnapMirror avec la réplication flexible de la version.

4. Si vous spécifiez un SVM de destination qui s'exécute sous la même version de ONTAP que le volume source, mais que vous souhaitez toujours configurer SnapMirror avec une réplication flexible de la version, cliquez sur **Advanced** pour activer la réplication flexible de la version, puis sur **Apply**.
5. Cliquez sur **appliquer**.

   Vous êtes renvoyé à la page Volume / Health details.

6. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page **Volume / Santé**.

   Les tâches et les détails des travaux s'affichent dans la page Détails du travail.

7. Dans la page **Job** details, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails de la tâche associée à la tâche de configuration de la protection et déterminer quand la tâche est terminée.
8. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails **Volume / Santé**.

   La nouvelle relation s'affiche dans la vue topologique de la page Volume / Health details.

Création de relations SnapMirror avec la réplication flexible de la version avec l'option de sauvegarde

Vous pouvez créer une relation SnapMirror avec la fonctionnalité d'option de réplication et de sauvegarde flexible de la version. La fonctionnalité d'option de sauvegarde vous permet d'implémenter la protection SnapMirror et de conserver plusieurs versions de copies de sauvegarde sur l'emplacement de destination.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.
- Les SVM source et destination doivent tous deux disposer d'une licence SnapMirror activée.
- Les SVM source et destination doivent chacun avoir une licence SnapVault activée.
- Les SVM source et de destination doivent être exécutés sous une version du logiciel ONTAP qui prend en charge la réplication flexible de la version.

La configuration de SnapMirror avec l'option de sauvegarde vous permet de protéger vos données avec les fonctionnalités de reprise après incident SnapMirror, telles que le basculement de volume, tout en offrant des fonctionnalités SnapVault, comme la protection pour plusieurs copies de sauvegarde.

Étapes

1. Affichez la boîte de dialogue **Configure protection** pour le volume que vous souhaitez protéger.
   - Si vous consultez l'onglet protection de la page Détails du volume/intégrité, cliquez avec le bouton droit de la souris dans la vue topologique sur le nom d'un volume à protéger et sélectionnez **protéger** > **SnapMirror** dans le menu.
   - Si vous affichez la vue Santé : tous les volumes, localisez 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. Renseignez la zone **destination information** et la zone **Relationship Settings** de la boîte de dialogue **Configure protection**.
4. Cliquez sur **Avancé** pour afficher la boîte de dialogue **Paramètres de destination avancés**.
5. Si la case **version-flexible Replication** n'est pas déjà cochée, sélectionnez-la maintenant.
6. Cochez la case **avec option de sauvegarde** pour activer la fonctionnalité de l'option de sauvegarde, puis cliquez sur **appliquer**.
7. Cliquez sur **appliquer**.

   Vous êtes renvoyé à la page Volume / Health details.

8. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page **Volume / Santé**.

   Les tâches et les détails des travaux s'affichent dans la page Détails du travail.

9. Dans la page **Job** details, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails des tâches associés à la tâche de configuration de la protection et déterminer quand la tâche est terminée.
10. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails **Volume / Santé**.

    La nouvelle relation s'affiche dans la vue topologique de la page Volume / Health details.

Configuration des paramètres d'efficacité de la destination

Vous pouvez configurer des 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. Ces paramètres permettent d'optimiser l'utilisation de l'espace sur un volume de destination ou secondaire.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Par défaut, les paramètres d'efficacité correspondent à ceux du volume source, sauf pour les paramètres de compression d'une relation SnapVault, qui sont désactivés par défaut.

Étapes

1. Cliquez sur l'onglet **SnapMirror** ou **SnapVault** de la boîte de dialogue **configurer la protection**, selon le type de relation que vous configurez.

2. Cliquez sur **Avancé** dans la zone **informations de 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 les besoins.
4. Cliquez sur **appliquer** pour enregistrer vos sélections et revenir à la boîte de dialogue **configurer la protection**.

Création de planifications SnapMirror et SnapVault

Vous pouvez créer des planifications SnapMirror et SnapVault de base ou avancées pour activer les transferts automatiques sur un volume source ou primaire. Les transferts ont ainsi lieu plus ou moins fréquemment, selon la fréquence à laquelle les données sont modifiées sur vos volumes.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir déjà terminé la zone informations sur la destination dans la boîte de dialogue configurer la protection.
- Vous devez avoir configuré Workflow Automation 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 un programme** dans la zone **Paramètres de relation**.

   La boîte de dialogue Créer un programme s'affiche.

2. Dans le champ **Nom de l'horaire**, saisissez le nom que vous souhaitez donner à l'horaire.
3. Sélectionnez l'une des options suivantes :
   - **De base**

     Sélectionnez cette option si vous souhaitez créer une planification de base de style d'intervalle.

   - **Avancé**

     Sélectionnez cette option pour créer une planification de style cron.

4. Cliquez sur **Créer**.

   La nouvelle planification est affichée dans la liste déroulante planification SnapMirror ou planification SnapVault.

Création de relations en cascade ou en sortie pour étendre la protection à partir d'une relation de protection existante

Vous pouvez étendre la protection à partir d'une relation existante en créant soit un fanout à partir du volume source, soit une cascade à partir du volume de destination d'une relation existante. Pour cela, il vous suffit de copier des données d'un site vers de

nombreux sites ou de renforcer la protection en créant davantage de sauvegardes.

Vous pouvez étendre la protection aux volumes à l'aide d'un groupe de cohérence, un conteneur qui contient plusieurs volumes de manière à pouvoir gérer tous les volumes en tant qu'entité unique. Vous pouvez afficher le groupe de cohérence de la synchronisation active SnapMirror et la relation de groupe de cohérence synchrone dans la page relations d'Unified Manager.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Cliquez sur **protection** > **relations**. Vous pouvez également afficher les relations à partir de la page des détails du volume.
2. Dans la page **Volume Relationship**, sélectionnez la relation SnapMirror depuis laquelle vous souhaitez étendre la protection.
3. Dans la barre d'actions, cliquez sur **prolonger la protection**.
4. Dans le menu, sélectionnez **à partir de Source** ou **à partir de destination**, selon que vous créez une relation de sortie à partir de la source ou d'une relation de 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 Unified Relationship / Volume Relationship et Volume / Health details.

6. Renseignez les informations indiquées dans la boîte de dialogue **configurer la protection**.

Modification des 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 stratégie de protection ou le planning de protection. Vous pouvez modifier une relation pour diminuer la bande passante utilisée pour les transferts ou pour augmenter la fréquence des transferts programmés car les données changent souvent.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Les volumes sélectionnés doivent être des destinations de relation de protection. Vous ne pouvez pas modifier les relations lorsque les volumes source, les volumes de partage de charge ou les volumes qui ne sont pas de destination d'une relation SnapMirror ou SnapVault sont sélectionnés.

Étapes

1. Dans la page **Volume Relationship**, sélectionnez dans la liste des volumes un ou plusieurs volumes du même SVM pour lesquels vous souhaitez modifier les paramètres de relation, puis sélectionnez **Edit** 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 stratégie de protection ou le calendrier de protection, selon les besoins.
3. Cliquez sur **appliquer**.

   Les modifications sont appliquées aux relations sélectionnées.

Modification des relations de protection à partir de la page Détails du volume/intégrité

Vous pouvez modifier les relations de protection existantes pour modifier le taux de transfert maximal actuel, la stratégie de protection ou la planification de protection. Vous pouvez modifier une relation pour diminuer la bande passante utilisée pour les transferts ou pour augmenter la fréquence des transferts programmés car les données changent souvent.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou 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 les volumes source, les volumes de partage de charge ou les volumes qui ne sont pas de destination d'une relation SnapMirror ou SnapVault sont sélectionnés.

Étapes

1. Dans l'onglet **protection** de la page **Volume / Santé**, localisez 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.

   Dans le menu **actions**, vous pouvez également sélectionner **relation** > **Modifier** pour modifier la relation pour laquelle vous consultez actuellement les détails.

   La boîte de dialogue **Modifier 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 les besoins.
4. Cliquez sur **appliquer**.

   Les modifications sont appliquées aux relations sélectionnées.

Création d'une règle SnapMirror pour optimiser l'efficacité du transfert

Vous pouvez créer une règle SnapMirror pour spécifier la priorité de transfert SnapMirror pour les relations de protection. Les règles SnapMirror vous permettent d'optimiser l'efficacité du transfert entre la source et la destination en définissant des priorités. De cette manière, les transferts avec priorité inférieure doivent être programmés pour s'exécuter après les transferts prioritaires.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.
- Cette tâche suppose que vous avez déjà terminé la zone informations de destination dans la boîte de dialogue configurer la protection.

Étapes

1. Dans l'onglet **SnapMirror** de la boîte de dialogue **Configure protection**, cliquez sur le lien **Create Policy** dans la zone **Relationship Settings**.

   La boîte de dialogue Créer une règle SnapMirror s'affiche.

2. Dans le champ **Policy Name**, saisissez le nom que vous souhaitez attribuer à la stratégie.
3. Dans le champ **priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la stratégie.
4. Dans le champ **Commentaire**, entrez un commentaire facultatif pour la stratégie.
5. Cliquez sur **Créer**.

   La nouvelle règle s'affiche dans la liste déroulante SnapMirror Policy.

Création d'une règle SnapVault pour optimiser l'efficacité du transfert

Vous pouvez créer une nouvelle règle SnapVault afin de définir la priorité d'un transfert SnapVault. Vous utilisez des règles pour optimiser l'efficacité des transferts du stockage primaire au stockage secondaire dans une relation de protection.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.
- Vous devez avoir déjà terminé la zone informations sur la 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 **Policy Name**, saisissez le nom que vous souhaitez attribuer à la stratégie.
3. Dans le champ **priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la stratégie.
4. **Facultatif:** dans le champ **Commentaire**, entrez un commentaire pour la police.
5. Dans la zone **Replication Label**, ajoutez ou modifiez une étiquette de réplication, selon les besoins.
6. Cliquez sur **Créer**.

   La nouvelle stratégie s'affiche dans la liste déroulante Créer une stratégie.

Abandon d'un transfert actif de protection des données à partir de la page relations de volume

Vous pouvez annuler le transfert actif de protection des données 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 annuler un transfert en cas de conflit avec une autre opération, par exemple un déplacement de volume.

> Vous ne pouvez pas abandonner les relations de volumes protégées par le groupe de cohérence.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

L'action d'abandon ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert

Vous ne pouvez pas effacer le point de contrôle de redémarrage pour un transfert de ligne de base.

Étapes

1. Pour abandonner 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 **abandonner**.

   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 du travail d'abandon s'affiche en haut de la page relations de volume, avec un lien vers les détails du travail.

4. **Facultatif:** cliquez sur le lien **Afficher les détails** pour accéder à la page **travail** pour plus de détails et pour afficher la progression du travail.

Abandon d'un transfert actif de protection des données à partir de la page Détails du volume/intégrité

Vous pouvez annuler le transfert actif de protection des données 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 annuler un transfert en cas de conflit avec une autre opération, par exemple un déplacement de volume.

Vous ne pouvez pas abandonner les relations de volumes protégées par le groupe de cohérence.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

L'action d'abandon ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action : par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert

Vous ne pouvez pas effacer le point de contrôle de redémarrage pour un transfert de ligne de base.

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 du transfert de données que vous souhaitez abandonner et sélectionnez **abandonner**.

   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 / intégrité, ainsi qu'un lien vers les détails du travail.

4. **Facultatif:** cliquez sur le lien **Afficher les détails** pour accéder à la page **travail** pour plus de détails et pour afficher la progression du travail.
5. Cliquez sur chaque tâche pour afficher ses détails.
6. Cliquez sur la flèche Précédent de votre navigateur pour revenir à la page de détails **Volume / Santé**.

   L'opération d'abandon est terminée lorsque toutes les tâches ont réussi.

Mise en veille d'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 afin d'empêcher temporairement les transferts de données. Vous pouvez suspendre une relation lorsque vous souhaitez créer une copie Snapshot d'un volume de destination SnapMirror qui contient une base de données. Vous devez également vous assurer que son contenu est stable pendant l'opération de copie Snapshot.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

- Vous devez avoir configuré Workflow Automation.

L'action de mise en veille ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action ; par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu ; par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert
- Si vous n'avez pas associé Workflow Automation et Unified Manager

Étapes

1. Pour suspendre les transferts pour une ou plusieurs relations de protection, sélectionnez un ou plusieurs volumes dans la page **relations de volume** et, dans la barre d'outils, cliquez sur **Quiesce**.

   La boîte de dialogue Quiesce s'affiche.

2. Cliquez sur **Continuer**.

   L'état de la tâche de mise en attente s'affiche en haut de la page Détails du volume/intégrité, ainsi qu'un lien vers les détails de la tâche.

3. Cliquez sur le lien **Afficher les détails** pour accéder à la page **travail** des détails supplémentaires et à la progression du travail.
4. **Facultatif:** cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Volume relations**.

   La tâche de mise en attente est terminée lorsque toutes les tâches du travail sont terminées avec succès.

Mise au repos d'une relation de protection à partir de la page Volume / informations d'intégrité

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 qui contient une base de données. Vous devez également vous assurer que son contenu est stable pendant la copie Snapshot.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

L'action de mise en veille ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC n'autorisent pas cette action, par exemple, si vous disposez uniquement des privilèges d'opérateur
- Lorsque l'ID du volume est inconnu, par exemple, lorsque vous avez une relation intercluster et que le cluster destination n'a pas encore été découvert
- Si 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 mettre en veille.
2. Sélectionnez **Quiesce** dans le menu.
3. Cliquez sur **Oui** pour continuer.

   L'état de la tâche de mise en attente s'affiche en haut de la page Détails du volume/intégrité, ainsi qu'un lien vers les détails de la tâche.

4. Cliquez sur le lien **Afficher les détails** pour accéder à la page **travail** des détails supplémentaires et à la progression du travail.
5. **Facultatif:** cliquez sur la flèche Précédent de votre navigateur pour revenir à la page de détails **Volume / Santé**.

   La tâche de mise en attente est terminée lorsque toutes les tâches du travail sont terminées avec succès.

Rompre une relation SnapMirror depuis la page Volume relations

Vous pouvez interrompre 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 briser une relation lorsque vous souhaitez migrer des données, pour la reprise d'activité ou pour le test d'application. Le volume de destination est modifié en volume de lecture/écriture. Vous ne pouvez pas interrompre une relation SnapVault.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans la page **Volume relations**, 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 **Break**.

   La boîte de dialogue rompre la relation s'affiche.

2. Cliquez sur **Continuer** pour rompre la relation.
3. Dans la page **Volume Relationship**, vérifiez dans la colonne **Relationship State** que la relation est rompue.

   La colonne Etat de la relation est masquée par défaut, vous devrez peut-être la sélectionner dans la liste Afficher/masquer la colonne .

Suppression d'une relation de protection de la page relations de volume

Dans 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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans la page **Volume relations**, sélectionnez un ou plusieurs volumes avec des relations de protection que vous souhaitez supprimer et, dans la barre d'outils, cliquez sur **Remove**.

   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.

Reprise des transferts programmés sur une relation mise en veille à partir de la page de relations de volume

Une fois que vous avez suspendu une relation pour arrêter les transferts programmés, vous pouvez utiliser **Resume** pour réactiver les transferts programmés afin que les données sur le volume source ou primaire soient protégées. Les transferts reprennent à partir d'un point de contrôle, le cas échéant, à l'intervalle de transfert planifié suivant.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Vous ne pouvez sélectionner pas plus de 10 relations suspendues pour reprendre les transferts.

Étapes

1. Dans la page Volume **relations**, 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 revenez à la page Volume relations.

3. Pour afficher les tâches associées et suivre leur progression, cliquez sur le lien du travail affiché en haut de la page **Volume relations**.
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 à la tâche de configuration de protection et déterminer quand la tâche est terminée.
   - Si plusieurs travaux sont affichés,
     i. Dans la page travaux, cliquez sur le travail pour lequel 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 de la tâche associée à la tâche de configuration de protection et déterminer quand la tâche

est terminée. Une fois les tâches terminées, les transferts de données sont repris à l'intervalle de transfert planifié suivant.

Reprise des transferts programmés sur une relation mise en veille à partir de la page Volume / informations de santé

Une fois que vous avez suspendu une relation pour arrêter les transferts programmés, vous pouvez utiliser **Resume** sur la page Volume / Détails de l'état de santé pour réactiver les transferts programmés afin que les données sur le volume source ou primaire soient protégées. Les transferts reprennent à partir d'un point de contrôle, le cas échéant, à l'intervalle de transfert planifié suivant.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page d'informations **Volume / Santé**, cliquez avec le bouton droit de la souris dans la vue topologique d'une relation mise au repos 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 Volume / Health details.

3. Pour afficher les tâches associées et suivre leur progression, cliquez sur le lien du travail qui s'affiche en haut de la page **Volume / Santé**.
4. Dans la page **Job** details, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails de la tâche associée à la tâche de configuration de la protection et déterminer quand la tâche est terminée.

   Une fois les travaux terminés, les transferts de données sont repris au prochain intervalle de transfert programmé.

Initialisation ou mise à jour des relations de protection à partir de la page relations de volume

À partir de la page Volume relations, vous pouvez effectuer un transfert de base pour la première fois 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 et non planifiée pour le transfert immédiatement.

> Vous ne pouvez ni initialiser ni mettre à jour des volumes protégés par des groupes de cohérence.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans la page **Volume relations**, cliquez avec le bouton droit de la souris sur un volume et sélectionnez un ou plusieurs volumes avec des relations que vous souhaitez mettre à jour ou initialiser, puis, dans la barre d'outils, cliquez sur **Initialize/Update**.

   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 snapshot source**, puis, dans la colonne **copie snapshot**, cliquez sur **par défaut**.

   La boîte de dialogue Sélectionner une copie Snapshot source s'affiche.

4. Pour spécifier une copie Snapshot existante plutôt que de transférer la copie Snapshot par défaut, cliquez sur **copie Snapshot existante** et sélectionnez une copie Snapshot dans la liste.
5. Cliquez sur **soumettre**.

   Vous revenez à la boîte de dialogue **Initialize/Update**.

6. Si vous avez sélectionné plusieurs sources à initialiser ou à mettre à jour, cliquez sur **default** pour la source suivante pour laquelle vous souhaitez spécifier une copie Snapshot existante.
7. Cliquez sur **Submit** pour lancer la tâche d'initialisation ou de mise à jour.

   La tâche d'initialisation ou de mise à jour est démarrée, vous êtes renvoyé à la page relations de volume et un lien de travaux s'affiche en haut de la page.

8. **Facultatif:** cliquez sur **View Jobs** dans la vue **Health: All volumes** pour suivre l'état de chaque travail d'initialisation ou de mise à jour.

   Une liste filtrée des travaux s'affiche.

9. **Facultatif:** cliquez sur chaque travail pour en voir les détails.
10. **Facultatif:** cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Volume relations**.

    L'opération d'initialisation ou de mise à jour est terminée lorsque toutes les tâches sont terminées.

Initialisation ou mise à jour des relations de protection à partir de la page Détails du volume/intégrité

Vous pouvez effectuer un transfert de base initial sur une nouvelle relation de protection, ou mettre à jour une relation si elle est déjà initialisée et si vous souhaitez effectuer une mise à jour incrémentielle manuelle et non planifiée pour transférer immédiatement les données.

REMARQUE : vous ne pouvez pas initialiser ni mettre à jour des volumes protégés par des groupes de cohérence.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **protection** de la page **Volume / Santé**, localisez 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.

   Vous pouvez également sélectionner **relations** > **initialiser/mettre à jour** dans le menu **actions** pour initialiser ou mettre à jour la relation pour laquelle 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 snapshot source**, puis, dans la colonne **copie snapshot**, cliquez sur **par défaut**.

   La boîte de dialogue Sélectionner une copie Snapshot source s'affiche.
5. Pour spécifier une copie Snapshot existante plutôt que de transférer la copie Snapshot par défaut, cliquez sur **copie Snapshot existante** et sélectionnez une copie Snapshot 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 **default** pour la source de lecture/écriture suivante pour laquelle vous souhaitez spécifier une copie Snapshot existante.

   Vous ne pouvez pas sélectionner une autre copie Snapshot pour les volumes de protection des données.
8. Cliquez sur **Submit** pour lancer la tâche d'initialisation ou de mise à jour.

   La tâche d'initialisation ou de mise à jour est démarrée, vous êtes renvoyé à la page Volume / Health details et un lien travaux s'affiche en haut de la page.
9. **Facultatif:** cliquez sur **Afficher les travaux** sur la page **Volume / Santé** pour suivre l'état de chaque tâche d'initialisation ou de mise à jour.

   Une liste filtrée des travaux s'affiche.
10. **Facultatif:** cliquez sur chaque travail pour en voir les détails.
11. **Facultatif:** cliquez sur la flèche Précédent 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.

Resynchronisation des relations de protection à partir de la page Volume relations

Dans la page Volume relations, vous pouvez resynchroniser une relation pour effectuer une restauration à partir d'un événement qui a désactivé votre volume source ou si vous souhaitez modifier la source actuelle vers un autre volume.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans la page **Volume relations**, 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 **Resynchronisation Options**, sélectionnez une priorité de transfert et le taux de transfert maximal.
3. Cliquez sur **copies snapshot source**, puis, dans la colonne **copie snapshot**, cliquez sur **par défaut**.

   La boîte de dialogue Sélectionner une copie Snapshot source s'affiche.

4. Pour spécifier une copie Snapshot existante plutôt que de transférer la copie Snapshot par défaut, cliquez sur **copie Snapshot existante** et sélectionnez une copie Snapshot 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 **default** pour la source suivante pour laquelle vous souhaitez spécifier une copie Snapshot existante.
7. Cliquez sur **Submit** pour lancer le travail de resynchronisation.

   Le travail de resynchronisation est démarré, vous êtes renvoyé à la page relations de volume et un lien de travaux s'affiche en haut de la page.

8. **Facultatif:** cliquez sur **Afficher les travaux** sur la page **relations de volume** pour suivre l'état de chaque travail de resynchronisation.

   Une liste filtrée des travaux s'affiche.

9. **Facultatif:** cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Volume relations**.

   L'opération de resynchronisation est terminée lorsque toutes les tâches du travail ont été terminées avec succès.

Inversion des relations de protection à partir de la page relations de volume

Lorsqu'un incident désactive le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour transmettre des données en le convertissant en volume de lecture/écriture pendant que vous réparez ou remplacez la source. Lorsque la source est de 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 de la source avec celles de la destination de lecture/écriture.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré Workflow Automation.

- 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 règles et les planifications créées pour les relations de resynchronisation inverse sont identiques à celles de la relation de protection d'origine.

  Si des stratégies et des plannings n'existent pas, ils sont créés.

Étapes

1. Dans la page **Volume relations**, sélectionnez un ou plusieurs volumes avec des relations que vous souhaitez inverser et, dans la barre d'outils, cliquez sur **Reverse Resync**.

   La boîte de dialogue Reverse Resync s'affiche.

2. Vérifiez que les relations affichées dans la boîte de dialogue **Reverse Resync** sont celles pour lesquelles vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Submit**.

   L'opération de resynchronisation inverse est lancée, vous êtes renvoyé à la page relations de volume et un lien de travaux s'affiche en haut de la page.

3. **Facultatif:** cliquez sur **Afficher les travaux** sur la page **relations de volume** pour suivre l'état de chaque travail de resynchronisation inverse.

   Une liste filtrée des travaux associés à cette opération s'affiche.

4. **Facultatif:** cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Volume relations**.

   L'opération de resynchronisation inverse est terminée lorsque toutes les tâches du travail sont terminées avec succès.

Restauration des données à l'aide des pages de détails Volume et Volume/intégrité

Vous pouvez restaurer des fichiers, des répertoires ou un volume entier à partir d'une copie Snapshot remplacés ou supprimés. Pour ce faire, utilisez la fonctionnalité de restauration des pages d'informations sur le volume et le volume/l'état.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 du volume est inconnu : par exemple, lorsque vous disposez d'une relation intercluster et que le

cluster destination n'a pas encore été découvert.

- Le volume est configuré pour la réplication SnapMirror synchrone.

Étapes

1. Dans le volet de navigation de gauche, accédez à **Storage > volumes**.
2. Sélectionnez le volume et cliquez sur le bouton **Restaurer**. Vous pouvez également cliquer sur le volume pour accéder à **Volume / Détails de l'état de santé > actions > Restaurer**. La boîte de dialogue Restaurer s'affiche. Pour plus d'informations sur cette page, reportez-vous "Restaurer la boîte de dialogue"à la section .
3. Sélectionnez le volume et la copie Snapshot depuis lesquels vous souhaitez restaurer les données, si elles sont différentes de celles par défaut.
4. Sélectionnez les éléments à restaurer, par exemple la LUN source.

   Vous pouvez restaurer tout le volume ou spécifier les dossiers et les fichiers à restaurer.

5. Sélectionnez l'emplacement auquel vous souhaitez restaurer les éléments sélectionnés : **emplacement d'origine** ou **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 d'accès de l'emplacement auquel 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 opérations suivantes :
     i. Sélectionnez le cluster de destination, la VM de stockage (SVM) et le volume vers lequel vous souhaitez restaurer.
     ii. Dans la table Nom, sélectionnez un nom de répertoire à restaurer.
     iii. Cliquez sur **Sélectionner répertoire**.
7. Cliquez sur **Restaurer**.

   Le processus de restauration commence. Un travail est créé en arrière-plan pour terminer le processus de restauration.

8. Pour afficher la progression du travail, accédez à **protection > travaux** dans le volet de navigation de gauche pour afficher l'état du travail de restauration dans 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 console NetApp .

En quoi sont les pools de ressources

Les pools de ressources sont des groupes d'agrégats créés par un administrateur de stockage via Unified Manager pour fournir le provisionnement aux applications partenaires pour la gestion des sauvegardes.

Vous pouvez regrouper vos ressources au sein d'un pool en fonction de critères tels que les performances, les coûts, 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 plus efficace du stockage.

Lors du provisionnement de stockage secondaire, Unified Manager détermine l'agrégat le plus approprié du pool de ressources à des fins de protection, à l'aide des critères suivants :

- L'agrégat est un agrégat de données (pas un agrégat root) qui est EN LIGNE.
- L'agrégat se trouve sur un nœud de cluster cible 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 le provisionnement du volume de destination, l'espace de l'agrégat se trouve dans le seuil presque atteint et quasi dépassé 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 plateforme.

Création de pools de ressources

Vous pouvez utiliser la boîte de dialogue Créer un pool de ressources pour regrouper les agrégats à des fins de provisionnement.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 des pools de ressources différents.

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 donner un nom et une description et pour ajouter des agrégats comme membres au pool de ressources que vous souhaitez créer.

Modification de pools de ressources

Vous pouvez modifier un pool de ressources existant lorsque vous souhaitez modifier le nom du pool de ressources et sa description.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Le bouton **Modifier** n'est activé que lorsqu'un pool de ressources est sélectionné. Si plusieurs pools de ressources sont sélectionnés, le bouton **Edit** 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 sont affichés dans la liste des pools de ressources.

Affichage de 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **protection** > **pools de ressources**.

   L'inventaire du pool de ressources s'affiche.

Ajout de membres de pool de ressources

Un pool de ressources est constitué d'un certain nombre d'agrégats membres. Vous pouvez ajouter des agrégats à des pools de ressources existants pour augmenter l'espace disponible pour le provisionnement du volume secondaire.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou 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 Aggregates 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 membre du pool de ressources, cliquez sur **Ajouter**.

   La boîte de dialogue Aggregates s'affiche.

4. Sélectionnez un ou plusieurs agrégats.
5. Cliquez sur **Ajouter**.

   La boîte de dialogue est fermée et les agrégats s'affichent dans la liste des membres du pool de ressources sélectionné.

Suppression d’agrégats des pools de ressources

Vous pouvez supprimer des agrégats d’un pool de ressources existant : par exemple, si vous souhaitez utiliser un agrégat à d’autres fins.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.

Les membres du pool de ressources ne sont affichés que 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 dans lequel vous souhaitez supprimer des agrégats membres.

   La liste des agrégats membres est affichée 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.

Suppression de pools de ressources

Vous pouvez supprimer des pools de ressources lorsqu’ils ne sont plus nécessaires. Par exemple, vous pouvez vouloir redistribuer les agrégats membres d’un pool de ressources vers plusieurs autres pools de ressources, ce qui rend le pool de ressources d’origine obsolète.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.

Le bouton **Supprimer** n’est activé que 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 à 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 contre les reprises après incident des machines virtuelles de stockage

Active IQ Unified Manager prend en charge la surveillance des relations de reprise après incident des VM de stockage, qui assure la reprise après incident au niveau de la granularité d'une VM de stockage. La reprise après incident de l'ordinateur virtuel de stockage permet de récupérer les données présentes dans les volumes constitutifs du serveur virtuel de stockage et la restauration de la configuration de cette machine virtuelle de stockage.

Une relation de reprise après incident de machine virtuelle de stockage est créée à partir de la machine virtuelle de stockage source vers la machine virtuelle de stockage cible afin de permettre une reprise après incident asynchrone. Vous pouvez choisir de répliquer l'ensemble ou un sous-ensemble de la configuration de la machine virtuelle de stockage (à l'exception de la configuration du réseau et du protocole) ainsi que les volumes de données basés sur le cluster setup.

Après la relation de reprise après incident de la machine virtuelle de stockage est configurée, lorsque la machine virtuelle de stockage source devient indisponible en raison d'une défaillance matérielle ou d'un incident environnemental, la machine virtuelle de stockage de destination démarre, ce qui permet d'accéder aux données avec une interruption minimale. De la même façon, lorsque la machine virtuelle de stockage source est disponible, elle est resynchronisée sur la machine virtuelle de stockage de destination, puis elle redémarre pour fournir les données. Vous pouvez utiliser des commandes SnapMirror pour configurer et gérer la relation de reprise d'activité des machines virtuelles de stockage.

Surveillance des VM de stockage à l'aide de la page relations

Vous pouvez surveiller vos relations de reprise après incident de machine virtuelle de stockage depuis la page relations de la section PROTECTION de l'INVENTAIRE. Par défaut, la page relations répertorie uniquement les relations de premier niveau lorsque le filtre de relations composant est appliqué.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous utilisez des filtres pour afficher les relations de reprise après incident 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 Storage VM.

2. Cliquez sur **Filter**, puis sélectionnez **Relationship Object Type** et **Storage VM** pour afficher uniquement les relations de reprise après sinistre des VM de stockage.
3. Cliquez sur **appliquer le filtre**.

   > Vous devez effacer le filtre des relations constituant pour afficher toutes les relations de protection.

   La page affiche uniquement les relations de reprise après incident des machines virtuelles de stockage.

Affichage des relations de protection à partir de la page Storage VM

Grâce à la page machines virtuelles de stockage, vous pouvez afficher l'état des relations de reprise sur incident des machines virtuelles de stockage existantes.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez également examiner les détails des relations de protection, notamment l'état du transfert et du décalage, les détails source et de destination. Vous pouvez planifier des rapports ou télécharger des rapports existants au format requis. Le bouton **Afficher/Masquer** 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 **STORAGE** > **Storage VM**.
2. Dans le menu **VIEW**, sélectionnez **Relationship** > **All Relationship**.

   La vue relation : toutes les relations s'affiche avec toutes les machines virtuelles de stockage configurées.

Affichage des VM de stockage en fonction de l'état de protection

Vous pouvez utiliser la page Storage VM de l'inventaire pour afficher toutes les machines virtuelles de stockage de Active IQ Unified Manager et filtrer les machines virtuelles de stockage en fonction de leur état de protection.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Un nouveau rôle de protection est ajouté dans la vue des VM de stockage qui fournit des informations sur la protection ou non de la machine virtuelle de stockage.

> Si un cluster source n'est pas ajouté à Active IQ Unified Manager, toutes les informations relatives à ce cluster sont indisponibles dans les grilles.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **STORAGE** > **Storage VM**.
2. Dans le menu **VIEW**, sélectionnez **Health** > **All Storage VM**.

   The Health : tous les ordinateurs virtuels de stockage s'affichent.

3. Cliquez sur **Filter** pour afficher l'une des machines virtuelles de stockage suivantes.

Pour afficher	Valeur du filtre
Machines virtuelles de stockage protégées	**Le rôle de protection** est **protégé**
Machines virtuelles 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 par la reprise après sinistre de la machine virtuelle de stockage en fonction de vos sélections de filtre.

Présentation des associations d'ordinateurs virtuels de stockage

Les associations de machines virtuelles de stockage sont mises en correspondance entre une machine virtuelle de stockage source et une machine virtuelle de stockage de destination utilisée 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 pour créer une association avec une machine virtuelle de stockage de destination tertiaire.

En tant qu'administrateur d'applications ou administrateur de stockage, vous pouvez afficher les associations de machines virtuelles de stockage de 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 primaire et un ou plusieurs SVM de destination. Cela signifie que tous les SVM existants qui nécessitent actuellement une protection, ainsi que tous les SVM créés à l'avenir, sont associés aux SVM de destination spécifiés. Par exemple, vous pouvez sauvegarder des applications de plusieurs sources situées à différents emplacements sur un ou plusieurs SVM de destination au sein d'un emplacement unique.
- **Association d'une machine virtuelle de stockage** spécifique : vous pouvez créer une association entre une machine virtuelle de stockage source spécifique et un ou plusieurs SVM de destination spécifiques. Par exemple, si vous proposez des services de stockage à de nombreux clients dont les données doivent être séparées les uns des autres, vous pouvez choisir cette option pour associer une VM de stockage source spécifique à une VM de stockage de destination spécifique qui n'est attribuée qu'à ce client.
- **Associer avec 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 Create Storage Virtual machine associations permet aux applications de protection partenaires d'associer une machine virtuelle de stockage source à une machine virtuelle de stockage de destination pour 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

Ce dont vous aurez besoin

- La machine virtuelle de stockage que vous associez doit déjà exister.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Selon le type de relation et d'ordinateur virtuel de stockage source, il n'est possible de choisir qu'une seule machine virtuelle de stockage de destination sur chaque cluster de destination.

La modification d'associations à l'aide des fonctions DELETE et create n'affecte que les opérations de provisioning futures. Les volumes de destination existants ne sont pas déplacés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **protection** > **associations de machines virtuelles de stockage**.
2. Sur la page **Storage VM associations**, cliquez sur **Create**.

   L'assistant **Créer des associations de machines virtuelles de stockage** est lancé.

3. Sélectionnez l'une des sources suivantes :
   - **Tout**

     Sélectionnez cette option si vous souhaitez créer une association entre une source de VM de stockage primaire et une ou plusieurs VM de stockage de destination. Cela signifie que toutes les machines virtuelles de stockage existantes qui nécessitent actuellement une protection, ainsi que toute machine virtuelle de stockage créée à l'avenir, sont associées à la machine virtuelle de stockage de destination spécifiée. Vous pouvez, par exemple, vouloir des applications issues de plusieurs sources situées à différents emplacements sauvegardés sur une ou plusieurs machines virtuelles de stockage de destination sur un emplacement unique.

   - **Unique**

     Sélectionnez cette option si vous souhaitez sélectionner une VM de stockage source spécifique associée à une ou plusieurs machines virtuelles de stockage de destination. Par exemple, si vous proposez des services de stockage à de nombreux clients dont les données doivent être séparées les uns des autres, sélectionnez cette option pour associer une source de VM de stockage à une destination de VM de stockage spécifique affectée uniquement à ce client.

   - **Aucun (externe)**

     Sélectionnez cette option lorsque vous souhaitez créer une association entre un VM de stockage source et un volume flexible externe d'une VM de stockage de destination.

4. Sélectionnez 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 VM de stockage.
7. Cliquez sur **Terminer**.

Supprimez les associations de VM de stockage

Vous pouvez supprimer les associations de machines virtuelles de stockage des applications partenaires afin de supprimer la relation de provisionnement secondaire entre la machine virtuelle de stockage source et celle

de destination. Par exemple, lorsque la machine virtuelle de stockage de destination est saturée, vous souhaitez créer de nouvelles associations de protection des machines virtuelles de stockage.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Le bouton **Supprimer** est désactivé jusqu'à ce qu'au moins une association de VM de stockage soit sélectionnée. La modification d'associations à l'aide des fonctions DELETE et create affecte uniquement les opérations de provisioning 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 VM 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 VM de stockage sélectionnée est supprimée de la liste.

Les exigences en termes de SVM et de pool de ressources pour prendre en charge les services de stockage

Vous pouvez mieux assurer la conformité aux applications partenaires en respectant certaines exigences en matière d'association des SVM et de pool de ressources spécifiques aux services de stockage : Par exemple, lorsque vous associez SVM et que vous 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 sont partenaires avec le serveur Unified Manager pour fournir des services qui configurent et exécutent automatiquement une protection de sauvegarde SnapMirror ou SnapVault entre les volumes source et les volumes de protection sur des sites secondaires ou tertiaires. Pour prendre en charge ces services de stockage de protection, Unified Manager vous devez utiliser pour configurer les associations de SVM et les pools de ressources nécessaires.

Pour la prise en charge de la protection en cascade ou à sauts uniques du service de stockage, y compris la réplication depuis un volume primaire SnapMirror source ou SnapVault vers un volume de sauvegarde SnapMirror de destination ou vers des volumes de sauvegarde SnapVault qui résident sur des emplacements secondaires ou tertiaires, observez les exigences suivantes :

- Les associations de SVM doivent être configurées entre le SVM contenant le volume primaire SnapMirror source ou SnapVault et tout SVM sur lequel réside un volume secondaire ou tertiaire.
  - Par exemple, pour prendre en charge une topologie de protection dans laquelle le volume source vol_A réside sur SVM_1, et 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 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, une association SnapMirror ou une 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 les ressources des agrégats du cluster disponibles pour les SVM associés.

  Vous pouvez configurer des pools de ressources via l'interface utilisateur Web Unified Manager, puis les attribuer par l'intermédiaire de l'application partenaire la cible secondaire du service de stockage et les nœuds cibles tertiaires.

Quels sont les emplois

Un travail est une série de tâches que vous pouvez contrôler à l'aide d'Unified Manager. L'affichage des travaux et de leurs tâches associées vous permet de déterminer s'ils ont réussi.

Les tâches sont lancées lorsque vous créez des relations SnapMirror et SnapVault lorsque vous effectuez une quelconque opération de relation (rompre, éditer, suspendre, supprimer, reprendre, resynchroniser, et resynchroniser), lorsque vous effectuez des tâches de restauration des données, lorsque vous vous connectez à un cluster, etc.

Lorsque vous lancez un travail, vous pouvez utiliser la page travaux et la page Détails du travail pour surveiller le travail et la progression des tâches associées.

Surveillance des tâches

Vous pouvez utiliser la page travaux pour contrôler l'état des travaux et afficher les propriétés des travaux, telles que le type de service de stockage, l'état, l'heure de soumission et l'heure de fin pour déterminer si un travail s'est terminé avec succès ou non.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **protection** > **travaux**.

   La page travaux s'affiche.

2. Affichez la colonne **State** pour déterminer l'état de ces travaux en cours d'exécution.
3. Cliquez sur le nom d'un travail pour afficher les détails de ce travail.

   La page Détails du travail s'affiche.

Affichage des détails du travail

Après avoir démarré un travail, vous pouvez suivre sa progression à partir de la page Détails du travail et contrôler les tâches associées pour détecter d'éventuelles erreurs.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **protection** > **travaux**.
2. Dans la page travaux, cliquez sur un nom de travail dans la colonne **Nom** pour afficher la liste des tâches associées au travail.
3. Cliquez sur une tâche pour afficher des informations supplémentaires dans le volet **Détails de la tâche** et dans le volet **messages de la tâche** à droite de la liste des tâches.

Abandon des travaux

Vous pouvez utiliser la page travaux pour abandonner un travail s'il prend trop de temps à terminer, qu'il rencontre trop d'erreurs ou qu'il n'est plus nécessaire. Vous ne pouvez abandonner un travail que si son état et son type l'autorisent. Vous pouvez abandonner tout travail en cours d'exécution.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **protection** > **travaux**.
2. Dans la liste des travaux, sélectionnez un travail, puis cliquez sur **abandonner**.
3. À l'invite de confirmation, cliquez sur **Oui** pour abandonner le travail sélectionné.

Nouvelle tentative d'échec d'une tâche de protection

Une fois que vous avez pris des mesures pour corriger un échec de la tâche de protection, vous pouvez utiliser **Réessayer** pour exécuter à nouveau le travail. La nouvelle tentative d'un travail crée un nouveau travail à l'aide de l'ID de travail d'origine.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous ne pouvez réessayer qu'un seul travail ayant échoué à la fois. La sélection de plusieurs travaux désactive le bouton **Réessayer**. Seules les tâches du type protection Configuration and protection relations Operation peuvent être relancées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **protection** > **travaux**.
2. Dans la liste des travaux, sélectionnez un seul travail de type d'opération de configuration de protection ou

de protection contre les échecs.

Le bouton **Réessayer** est activé.

3. Cliquez sur **Réessayer**.

   Le travail est redémarré.

Description des fenêtres et boîtes de dialogue protection relations

Vous pouvez afficher et gérer les informations relatives à la protection, telles que les pools de ressources, les associations de SVM et les tâches de protection. Vous pouvez utiliser la page seuils de santé appropriée pour configurer les valeurs des seuils de santé globaux des agrégats, des volumes et des relations.

Page pools de ressources

La page pools de ressources affiche les pools de ressources existants et leurs membres, et vous permet de créer, contrôler et gérer des pools de ressources à des fins de provisionnement.

Boutons de commande

Les boutons de commande 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**

  Permet de modifier le nom et la description des pools de ressources que vous créez.

- **Supprimer**

  Permet de supprimer un ou plusieurs pools de ressources.

Liste Resource pools

La liste pools de ressources affiche (au format tabulaire) les propriétés des pools de ressources existants.

- **Pool de ressources**

  Affiche le nom du pool de ressources.

- **Description**

  Décrit le pool de ressources.

- **Type SnapLock**

  Affiche le type SnapLock utilisé par les agrégats du pool de ressources. Les valeurs valides pour le type

SnapLock sont Compliance, Enterprise et non SnapLock. Un pool de ressources ne peut contenir que des agrégats d'un seul type de 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 l'espace disponible (en Mo, Go, etc.) 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 liste 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 de membres

La liste membres affiche (au format tabulaire) les membres du pool de ressources et leurs propriétés lorsqu'un pool de ressources est sélectionné.

- **Statut**

  Affiche le statut actuel de l'agrégat membre. L'état peut être critique ( ), erreur ( ), Avertissement ( ) ou Normal ( ).

- **Nom d'agrégat**

  Affiche le nom de l'agrégat membre.

- **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.

- Limitée

  Les opérations limitées (par exemple, la reconstruction avec parité) sont autorisées, mais l’accès aux données n’est pas autorisé.

- Création

  L’agrégat est en cours de création.

- Destruction

  L’agrégat est en cours de destruction.

- Échec

  L’agrégat ne peut pas être mis en ligne.

- Congelé

  L’agrégat ne transmet pas (temporairement) de demandes.

- Incohérent

  L’agrégat a été marqué comme corrompu ; vous devez contacter le support technique.

- Fer limité

  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 ou plusieurs disques sont manquants.

- Mise au repos

  L’agrégat est en cours de suspension.

- Suspendu

  L’agrégat est suspendu.

- Rétablie

  La restauration d’un agrégat est terminée.

- Démonté

  L’agrégat a été démonté.

- Démontage

L'agrégat est mis hors ligne.

- Inconnu

  L'agrégat est détecté, mais les informations d'agrégat ne sont pas encore récupérées par le serveur Unified Manager.

Par défaut, cette colonne est masquée.

- **Cluster**

  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 utilisé dans l'agrégat (en Mo, Go, etc.).

- **Capacité disponible**

  Affiche la quantité d'espace disponible (en Mo, Go, etc.) dans l'agrégat.

- **Utilisé %**

  Affiche le pourcentage d'espace utilisé dans l'agrégat.

- **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 RAID groupes sont de type RAID-DP.
  - RAID-TEC : tous les RAID groupes sont de type RAID-TEC.
  - RAID mixte : l'agrégat contient des groupes RAID de différents types (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, ainsi que pour ajouter des agrégats à et supprimer des agrégats de ce pool de ressources.

Nom du pool de ressources

Les zones de texte permettent d'ajouter les informations suivantes pour créer un pool de ressources :

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 permettent d'effectuer les tâches suivantes :

- **Ajouter**

  Ouvre la boîte de dialogue agrégats pour vous permettre d'ajouter des agrégats d'un cluster spécifique au pool de ressources. Vous pouvez ajouter des agrégats depuis différents clusters, mais les mêmes agrégats ne peuvent pas être ajoutés à plusieurs pools de ressources.

- **Supprimer**

  Permet de supprimer des agrégats sélectionnés du pool de ressources.

- **Créer**

  Crée le pool de ressources. Ce bouton n'est activé que si les informations ont été saisies dans les champs Nom du pool de ressources ou Description.

- **Annuler**

  Supprime 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 afin qu'ils soient plus précis.

Zones de texte

Les zones de texte permettent de modifier les informations suivantes pour le pool de ressources sélectionné :

- **Nom du pool de ressources**

  Permet d'entrer un nouveau nom.

- **Description**

  Permet de saisir une nouvelle description.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Enregistrer**

  Enregistre les modifications apportées au nom et à la description du pool de ressources.

- **Annuler**

  Supprime les modifications et ferme la boîte de dialogue Modifier le pool de ressources.

Boîte de dialogue Aggregates

Vous pouvez utiliser la boîte de dialogue Aggregates pour sélectionner les agrégats que vous souhaitez ajouter à votre pool de ressources.

Boutons de commande

Les boutons de commande 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**

  Supprime les modifications et ferme la boîte de dialogue agrégats.

Liste d'agrégats

La liste Aggregates affiche (au format tabulaire) les noms et propriétés des agrégats surveillés.

- **Statut**

  Affiche l'état actuel d'un volume. L'état peut être critique ( ), erreur ( ), Avertissement ( ) ou Normal ( ).

  Vous pouvez déplacer le pointeur de la souris sur l'état pour afficher plus d'informations sur l'événement ou les événements générés pour le volume.

- **Nom d'agrégat**

  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.

  - Limitée

Les opérations limitées (par exemple, la reconstruction avec 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.

- Création

  L'agrégat est en cours de création.

- Destruction

  L'agrégat est en cours de destruction.

- Échec

  L'agrégat ne peut pas être mis en ligne.

- Congelé

  L'agrégat ne transmet pas (temporairement) de demandes.

- Incohérent

  L'agrégat a été marqué comme corrompu ; vous devez contacter le support technique.

- Fer limité

  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 ou plusieurs disques sont manquants.

- Mise au repos

  L'agrégat est en cours de suspension.

- Suspendu

  L'agrégat est suspendu.

- Rétablie

  La restauration d'un agrégat est terminée.

- Démonté

  L'agrégat est mis hors ligne.

- Démontage

L’agrégat est mis hors ligne.

- Inconnu

  L’agrégat est détecté, mais les informations d’agrégat ne sont pas encore récupérées par le serveur Unified Manager.

- **Cluster**

  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 utilisé dans l’agrégat (en Mo, Go, etc.).

- **Capacité disponible**

  Affiche la quantité d’espace disponible (en Mo, Go, etc.) pour les données de l’agrégat. Par défaut, cette colonne est masquée.

- **Disponible %**

  Affiche le pourcentage d’espace disponible pour les données de l’agrégat. Par défaut, cette colonne est masquée.

- **Utilisé %**

  Affiche le pourcentage d’espace utilisé par les données de l’agrégat.

- **Type RAID**

  Affiche le type RAID du volume sélectionné. Le type RAID peut être RAID0, RAID4, RAID-DP, RAID-TEC ou Mixed RAID.

Page travaux

La page travaux 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 les tâches terminées. Vous pouvez utiliser ces informations pour voir quels travaux sont toujours en cours d’exécution et si un travail a réussi ou échoué.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Abort**

  Interrompt 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 protection Configuration ou protection relation Operation. Vous ne pouvez réessayer qu'un seul travail ayant échoué à la fois. Si plusieurs travaux en échec sont sélectionnés, le bouton **Réessayer** est désactivé. Vous ne pouvez pas réessayer les travaux de service de stockage ayant échoué.

- * Actualiser*

  Actualise la liste des travaux et les informations qui leur sont associées.

Liste des travaux

La liste travaux affiche, au format tabulaire, la liste des travaux en cours. Par défaut, la liste affiche uniquement les travaux générés au cours de la semaine passée. Vous pouvez utiliser le tri et le filtrage des colonnes pour personnaliser les travaux affichés.

- **Statut**

  Affiche l'état actuel d'un travail. L'état peut être erreur (⚠️) ou Normal ( )✅.

- **ID 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 travail particulier en saisissant le numéro d'identification du travail dans la zone de texte fournie par le filtre de colonne.

- **Nom**

  Affiche le nom du travail.

- **Type**

  Affiche le type de travail. Les types de travail sont les suivants :

  - * Acquisition de groupe*

    Une tâche Workflow Automation redécouvre un cluster.

  - **Configuration de la protection**

    Une tâche de protection consiste à lancer les flux de travail Workflow Automation, par exemple les planifications cron, la création de règles SnapMirror, etc.

  - * Opération de relation de protection*

Une tâche de protection exécute des opérations SnapMirror.

- **Chaîne de flux de travail de protection**

  Une tâche Workflow Automation exécute plusieurs flux de travail.

- **Restaurer**

  Une tâche de restauration est en cours d'exécution.

- **Nettoyage**

  Le travail nettoie les artefacts des membres du service de stockage qui ne sont plus nécessaires à des fins de restauration.

- **Conforme**

  La tâche consiste à vérifier la configuration des membres du service de stockage pour s'assurer qu'ils sont conformes.

- **Détruire**

  Le travail détruit un service de stockage.

- **Importer**

  Le travail importe des objets de stockage non gérés dans un service de stockage existant.

- **Modifier**

  Le travail modifie les attributs d'un service de stockage existant.

- **Abonnez-vous**

  Le travail s'abonner à un service de stockage.

- * Se désinscrire*

  Le travail annule l'abonnement des membres d'un service de stockage.

- **Mise à jour**

  Une tâche de mise à jour de protection est en cours d'exécution.

- **Configuration WFA**

  Une tâche Workflow Automation pousse les informations d'identification du cluster et synchronise les caches des bases de données.

• **État**

Affiche l'état d'exécution du travail. Les options d'état sont les suivantes :

- **Abandonné**

  Le travail a été abandonné.

- **Aborting**

  Le travail est en cours d’abandon.

- * Terminé*

  Le travail est terminé.

- **En cours d’exécution**

  La tâche est en cours d’exécution.

- **Heure de soumission**

  Affiche l’heure à laquelle le travail a été soumis.

- **Durée**

  Affiche la durée de réalisation du travail. Cette colonne est affichée par défaut.

- **Temps de réalisation**

  Affiche l’heure de fin du travail. Par défaut, cette colonne est masquée.

Page des détails du travail

La page Détails du travail vous permet d’afficher l’état et d’autres informations sur des 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 résoudre les échecs de tâches.

Récapitulatif du travail

Le récapitulatif des tâches affiche les informations suivantes :

- ID de la tâche
- Type
- État
- Heure de soumission
- Heure de fin
- Durée

Boutons de commande

Les boutons de commande permettent d’effectuer les tâches suivantes :

- * Actualiser*

  Actualise la liste des tâches et les propriétés associées à chaque tâche.

- **Afficher les travaux**

Vous renvoie à la page travaux.

Liste des tâches du travail

La liste tâches du travail affiche dans une table toutes les tâches associées à un travail spécifique et les propriétés associées 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.

- **Type**

  Affiche le type de tâche.

- **État**

  État d'une tâche particulière :

  - * Terminé*

    La tâche est terminée.

  - **Queued**

    La tâche est sur le point d'être exécutée.

  - **En cours d'exécution**

    La tâche est en cours d'exécution.

  - **En attente**

    Un travail a été soumis et certaines tâches associées sont en attente d'être mises en file d'attente et exécutées.

- **Statut**

  Affiche l'état de la tâche :

  - **Erreur ( )**

    La tâche a échoué.

  - **Normal ( )**

    La tâche a réussi.

  - **Ignoré ( )**

    Une tâche a échoué, ce qui entraîne le renvoi des tâches suivantes.

- **Durée**

  Affiche le temps écoulé depuis le début de la tâche.

- **Temps de réalisation**

  Affiche l'heure de fin de la tâche. Par défaut, cette colonne est masquée.

- **ID 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 affecté à la première tâche. Par défaut, cette colonne est masquée.

- **Volet Détails de la tâche**

  Affiche des informations supplémentaires sur chaque tâche, y compris le nom de la tâche, la description de la tâche et, si la tâche a échoué, une raison de l'échec.

- **Volet messages de tâche**

  Affiche les messages spécifiques à la tâche sélectionnée. Les messages peuvent comprendre une raison pour 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 de la version, la sauvegarde de plusieurs copies et les paramètres d'espace sur un volume secondaire. Vous pouvez utiliser la boîte de dialogue Paramètres secondaires avancés pour modifier ou désactiver les paramètres actuels.

Les paramètres liés à l'espace optimisent la quantité des données stockées, notamment : déduplication, compression des données, croissance automatique et garantie de l'espace.

La boîte de dialogue comprend les champs suivants :

- **Activer la réplication de version flexible**

  SnapMirror avec réplication flexible de la version. La réplication flexible de la version permet de protéger SnapMirror d'un volume source, même si le volume de destination est exécuté sous une version antérieure d'ONTAP par rapport au volume source.

  - Activez la sauvegarde

    Si la réplication flexible de la version est activée, plusieurs copies Snapshot des données source SnapMirror peuvent également être transférées et conservées au niveau de la destination SnapMirror.

- **Activer la déduplication**

  Active la déduplication sur le volume secondaire dans une relation SnapVault afin de supprimer les blocs de données dupliqués pour économiser de l'espace. Vous pouvez utiliser la déduplication lorsque les économies d'espace sont d'au moins 10 % et lorsque le taux de remplacement 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. Lorsqu'elle est activée, cette

opération est lancée après chaque transfert.

- Activer la compression

  Permet la 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 existe suffisamment de ressources système pour la compression pendant les heures creuses. Dans une relation SnapVault, ce paramètre est désactivé par défaut. La compression n'est disponible que lorsque la déduplication est sélectionnée.

- Compresser à la volée

  Permet un gain d'espace immédiat grâce à la compression des données avant leur écriture sur le disque. Vous pouvez utiliser la compression à la volée lorsque votre système n'a pas une utilisation supérieure à 50 % pendant les heures de pointe, et lorsque le système peut prendre en charge de nouvelles écritures et des ressources de processeur supplémentaires pendant les heures de pointe. Ce paramètre n'est disponible que lorsque l'option « Activer la compression » est sélectionnée.

- **Activer croissance automatique**

  Vous permet d'étendre automatiquement le volume de destination lorsque le pourcentage d'espace libre est inférieur au seuil spécifié, tant qu'un espace est disponible sur l'agrégat associé.

- **Taille maximale**

  Définit le pourcentage maximal sur lequel un volume peut croître. La valeur par défaut est 20 % supérieure à la taille du volume source. Un volume n'augmente pas automatiquement si la taille actuelle est supérieure ou égale au pourcentage de croissance automatique maximal. Ce champ est activé uniquement lorsque le réglage de croissance automatique est activé.

- **Taille d'incrément**

  Spécifie l'incrément de pourcentage d'augmentation automatique du volume avant d'atteindre le pourcentage maximal du volume source.

- **Garantie d'espace**

  Capacité allouée sur le volume secondaire suffisante pour que les transferts de données puissent toujours réussir. Le paramètre de garantie d'espace peut être l'un des suivants :

  - Fichier
  - Volumétrie
  - Aucun + par exemple, un volume de 200 Go peut contenir des fichiers d'une capacité totale de 50 Go. Cependant, ces fichiers ne contiennent que 10 Go de données. La garantie du 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 l'espace est suffisant pour les fichiers sur la source. Si vous sélectionnez aucun dans ce scénario, seuls 10 Go sont alloués à la destination pour l'espace réel utilisé par les données de fichier sur la source.

  La garantie d'espace est définie par défaut sur Volume.

Boutons de commande

Les boutons de commande 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**

  Supprime 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

L'espace disponible est alloué au volume de destination, ce qui garantit le succès continu des transferts de données. Le paramètre de garantie d'espace peut être l'un des suivants :

- Fichier
- Volumétrie
- Aucune

Par exemple, vous pouvez disposer d'un volume de 200 Go contenant des fichiers d'un total de 50 Go. Cependant, ces fichiers ne contiennent que 10 Go de données. La garantie du volume alloue 200 Go au volume de destination, quel que soit le contenu de la source. La garantie de fichier alloue 50 Go pour s'assurer que l'espace est suffisant pour les fichiers source sur la destination ; si vous sélectionnez **aucun** dans ce scénario, seuls 10 Go sont alloués à la destination pour l'espace réel utilisé par les données de fichier sur la source.

La garantie d'espace est définie par défaut sur Volume.

Restaurer la boîte de dialogue

La boîte de dialogue Restaurer permet de restaurer les données sur un volume à partir d'une copie Snapshot spécifique.

Source de restauration

La zone Restaurer à partir de vous permet de spécifier l'emplacement de restauration des 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 contenant tous les volumes avec des relations de protection sur le volume sur lequel vous avez lancé l'action de restauration.

- **Copie snapshot**

  Spécifie la copie Snapshot que vous souhaitez utiliser pour restaurer les données. Par défaut, la copie Snapshot la plus récente est sélectionnée. Vous pouvez également sélectionner une autre copie Snapshot dans la liste déroulante. La liste des copies Snapshot change en fonction du volume sélectionné.

- **Liste maximum de 995 fichiers et répertoires**

  Par défaut, un maximum de 995 objets sont affichés dans la liste. Vous pouvez désélectionner cette case pour afficher tous les objets du 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 le volume entier ou les fichiers et dossiers spécifiques que vous souhaitez restaurer. Vous pouvez sélectionner un maximum de 10 fichiers, dossiers ou une combinaison des deux. Lorsque le nombre maximum d'éléments est sélectionné, les cases à cocher de sélection d'élément sont désactivées.

- **Champ chemin**

  Affiche le chemin d'accès aux données à restaurer. Vous pouvez naviguer vers le dossier et les fichiers que vous souhaitez restaurer ou saisir le chemin d'accès. Ce champ est vide jusqu'à ce que vous sélectionniez ou tapez un chemin. Cliquer sur une fois que vous avez choisi un chemin vous déplace d'un niveau vers le haut dans la structure de répertoires.

- **Liste de dossiers et de fichiers**

  Affiche le contenu du chemin que vous avez entré. Par défaut, le dossier racine s'affiche initialement. Cliquez sur un nom de dossier pour afficher le contenu du dossier.

Vous pouvez sélectionner les éléments à restaurer comme suit :

- Lorsque vous entrez le chemin d'accès avec un nom de fichier particulier spécifié dans le champ chemin d'accès, le fichier spécifié s'affiche dans les dossiers et les 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 pour 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 désélectionner la case « liste maximale de 995 fichiers et répertoires » si vous souhaitez afficher tous les objets du volume sélectionné.

> Vous ne pouvez pas restaurer les flux de fichiers NTFS.

Cible de restauration

La zone Restaurer à vous permet de spécifier l'emplacement où vous souhaitez restaurer les données.

- **Emplacement d'origine dans Nom_volume**

  Restaure les données sélectionnées dans le répertoire de la source à partir duquel les données ont été

sauvegardées à l'origine.

- **Autre emplacement**

  Restaure les données sélectionnées à un nouvel emplacement :

  - Chemin de restauration

    Spécifie un chemin alternatif pour restaurer les données sélectionnées. Le chemin doit déjà exister. Vous pouvez utiliser le bouton **Browse** pour naviguer jusqu'à l'emplacement où vous souhaitez restaurer les données, ou entrer le chemin manuellement en utilisant le format cluster://svm/volume/path.

  - Conserver la hiérarchie du répertoire

    Lorsque cette case est cochée, conserve la structure du fichier ou du répertoire d'origine. Par exemple, si la source est /A/B/C/MyFile.txt et que la destination est /X/y/Z, Unified Manager restaure les données à l'aide de la structure de répertoires suivante sur la destination : /X/y/Z/A/B/C/monfile.txt.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Annuler**

  Supprime vos sélections et ferme la boîte de dialogue Restaurer.

- **Restaurer**

  Applique vos sélections et lance le processus de restauration.

Boîte de dialogue Parcourir les répertoires

Vous pouvez utiliser la boîte de dialogue Browse Directories si vous souhaitez restaurer des données dans un répertoire sur un cluster et un SVM différent de la source d'origine. Le cluster et le volume source d'origine sont sélectionnés par défaut.

La boîte de dialogue Browse Directories vous permet de sélectionner le cluster, le SVM, le volume et le chemin d'accès au répertoire auquel vous souhaitez restaurer les données.

- **Cluster**

  Le répertorie les destinations de cluster disponibles pour lesquelles vous pouvez restaurer. Par défaut, le cluster du volume source d'origine est sélectionné.

- **Liste déroulante SVM**

  Le répertorie le SVM disponible pour le cluster sélectionné. Par défault le SVM du volume source d'origine est sélectionné.

- **Volume**

  Répertorie tous les volumes en lecture/écriture d'un SVM sélectionné. Vous pouvez filtrer les volumes par nom et par espace disponible. Le volume ayant 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 chemin de 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. Si vous cliquez sur un dossier dans la liste Nom, les sous-dossiers s'affichent, le cas échéant. Les fichiers contenus dans les dossiers ne sont pas affichés. Cliquer sur après avoir sélectionné un dossier vous déplace d'un niveau vers le haut dans la structure de répertoires.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Sélectionnez répertoire**

  Applique vos sélections et ferme la boîte de dialogue Parcourir les répertoires. Si aucun répertoire n'est sélectionné, ce bouton est désactivé.

- **Annuler**

  Supprime vos sélections et ferme la boîte de dialogue Parcourir les répertoires.

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 des clusters, afin de vous assurer que les données d'un volume source ou primaire sont répliquées.

Onglet Source

- **Vue topologie**

  Affiche une représentation visuelle de la relation que vous créez. La source de la topologie est mise en évidence par défaut.

- **Information source**

  Affiche des détails sur les volumes source sélectionnés, y compris les informations suivantes :

  - Nom du cluster source
  - Nom du SVM source
  - Taille totale cumulée du volume

    Affiche la taille totale de tous les volumes source sélectionnés.

  - Taille cumulée du volume utilisé

Affiche la taille cumulée du volume utilisé pour tous les volumes source sélectionnés.

- Volume source

  Affiche les informations suivantes dans un tableau :

  - Volume source

    Affiche les noms des volumes source sélectionnés.

  - Type

    Affiche le type de volume.

  - Type de SnapLock

    Affiche le type SnapLock du volume. Les options sont Compliance, Enterprise et non SnapLock.

  - Copie Snapshot

    Affiche la copie Snapshot utilisée pour le transfert de base. Si le volume source est lu/écrit, la valeur par défaut dans la colonne copie Snapshot indique qu'une nouvelle copie Snapshot est créée par défaut et 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 Snapshot indique qu'aucune nouvelle copie Snapshot n'est créée et que toutes les copies Snapshot existantes sont transférées vers la destination. Si vous cliquez sur la valeur de la copie Snapshot, la liste des copies Snapshot disponibles permet de sélectionner une copie Snapshot existante à utiliser pour le transfert de base. Si le type de source est la protection des données, vous ne pouvez pas sélectionner une autre copie Snapshot par défaut.

Onglet SnapMirror

Permet de spécifier un cluster de destination, un SVM (Storage Virtual machine) et un agrégat pour une relation de protection, ainsi qu'une convention de nom pour les destinations lors de la création d'une relation SnapMirror. Vous pouvez également spécifier une règle et une planification SnapMirror.

- **Vue topologie**

  Affiche une représentation visuelle de la relation que vous créez. La ressource de destination SnapMirror dans la topologie est mise en évidence par défaut.

- **Informations sur la destination**

  Vous permet de sélectionner les ressources de destination d'une relation de protection :

  - Lien avancé

    Lance la boîte de dialogue Paramètres de destination avancés lorsque vous créez une relation SnapMirror.

  - Cluster

    Le répertorie les clusters disponibles comme hôtes de destination de protection. Ce champ est obligatoire

- Serveur virtuel de stockage (SVM)

  Le répertorie les SVM disponibles sur le cluster sélectionné. Un cluster doit être sélectionné avant que la liste des SVM ne soit remplie. Ce champ est obligatoire

- Agrégat

  Le répertorie les agrégats disponibles sur le SVM sélectionné. Vous devez sélectionner un cluster avant de renseigner la liste des agrégats. Ce champ est obligatoire La liste des agrégats affiche les informations suivantes :

  - Rang

    Lorsque plusieurs agrégats répondent à toutes les exigences d'une destination, le rang indique la priorité de l'agrégat, selon les conditions suivantes :

    A. Un agrégat situé sur un nœud différent de celui du nœud de volume source est préféré afin d'activer la séparation de domaine de pannes.
    B. Un agrégat d'un nœud avec moins de volumes est recommandé pour permettre l'équilibrage de la charge entre les nœuds d'un cluster.
    C. Pour équilibrer la capacité, il est préférable d'utiliser un agrégat qui dispose de plus d'espace libre que les autres agrégats. Un classement de 1 signifie que l'agrégat est le plus privilégié selon les trois critères.

  - Nom de l'agrégat

    Nom de l'agrégat

  - Capacité disponible
  - Quantité d'espace disponible sur l'agrégat pour les données
  - Pool de ressources

    Nom du pool de ressources auquel appartient l'agrégat

- Convention d'appellation

  Spécifie la convention de nommage par défaut appliquée au volume de destination. Vous pouvez accepter la convention de dénomination fournie ou créer une convention personnalisée. La convention de nommage peut avoir les attributs suivants : %C, %M, %V et %N, où %C est le nom du cluster, %M le nom du SVM, %V est le volume source et %N le nom du nœud cible de la topologie.

Le champ convention de dénomination est mis en surbrillance en rouge si votre entrée n'est pas valide. En cliquant sur le lien « Prévisualiser le nom », vous accédez à un aperçu de la convention de dénomination que vous avez saisie, et le texte d'aperçu est mis à jour de manière dynamique lorsque vous saisissez une convention de dénomination dans le champ de texte. Un suffixe compris entre 001 et 999 est ajouté au nom de destination lorsque la relation est créée, remplaçant le nnn qui s'affiche dans le texte d'aperçu, avec 001 étant attribué en premier, 002 attribué en seconde, etc.

- **Paramètres de relation**

  Permet de spécifier le taux de transfert maximal, la règle SnapMirror et de planifier les utilisations de la relation de protection :

  - Taux de transfert max

Spécifie la vitesse maximale à laquelle les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser un taux de transfert maximal, le transfert de base entre les relations est illimité.

- Règle SnapMirror

  Spécifie la règle ONTAP SnapMirror pour la relation. La valeur par défaut est DPDefault.

- Créer la règle

  Lance la boîte de dialogue Créer une règle SnapMirror qui vous permet de créer et d'utiliser une nouvelle règle SnapMirror.

- Planification SnapMirror

  Spécifie la règle ONTAP SnapMirror pour la relation. Horaires disponibles : aucun, 5 min, 8 heures, tous les jours, toutes les heures, et hebdomadaires. La valeur par défaut est aucun, ce qui indique qu'aucun programme n'est associé à la relation. Les relations sans planifications n'ont aucune valeur d'état de décalage à moins qu'elles n'appartiennent à un service de stockage.

- Créer un planning

  Lance la boîte de dialogue Créer un calendrier, qui vous permet de créer une nouvelle planification SnapMirror.

Onglet SnapVault

Permet de spécifier un cluster secondaire, un SVM et un agrégat dans le cadre d'une relation de protection, ainsi qu'une convention de nom pour les volumes secondaires lors de la création d'une relation SnapVault. Vous pouvez également spécifier une règle et une planification SnapVault.

- **Vue topologie**

  Affiche une représentation visuelle de la relation que vous créez. La ressource secondaire SnapVault de la topologie est mise en évidence par défaut.

- **Informations secondaires**

  Vous permet de sélectionner les ressources secondaires d'une relation de protection :

  - Lien avancé

    Lance la boîte de dialogue Paramètres secondaires avancés.

  - Cluster

    Le répertorie les clusters disponibles en tant qu'hôtes de protection secondaire. Ce champ est obligatoire

  - Serveur virtuel de stockage (SVM)

    Le répertorie les SVM disponibles sur le cluster sélectionné. Un cluster doit être sélectionné avant que la liste des SVM ne soit remplie. Ce champ est obligatoire

  - Agrégat

Le répertorie les agrégats disponibles sur le SVM sélectionné. Vous devez sélectionner un cluster avant de renseigner la liste des agrégats. Ce champ est obligatoire La liste des agrégats affiche les informations suivantes :

- Rang

  Lorsque plusieurs agrégats répondent à toutes les exigences d'une destination, le rang indique la priorité de l'agrégat, selon les conditions suivantes :

  A. Un agrégat situé sur un nœud différent de celui du nœud de volume principal est préféré afin d'activer la séparation de domaine de pannes.
  B. Un agrégat d'un nœud avec moins de volumes est recommandé pour permettre l'équilibrage de la charge entre les nœuds d'un cluster.
  C. Pour équilibrer la capacité, il est préférable d'utiliser un agrégat qui dispose de plus d'espace libre que les autres agrégats. Un classement de 1 signifie que l'agrégat est le plus privilégié selon les trois critères.

- Nom de l'agrégat

  Nom de l'agrégat

- Capacité disponible
- Quantité d'espace disponible sur l'agrégat pour les données
- Pool de ressources

  Nom du pool de ressources auquel appartient l'agrégat

◦ Convention d'appellation

  Spécifie la convention de nommage par défaut appliquée au volume secondaire. Vous pouvez accepter la convention de dénomination fournie ou créer une convention personnalisée. La convention de nommage peut avoir les attributs suivants : %C, %M, %V et %N, où %C est le nom du cluster, %M le nom du SVM, %V est le volume source et %N est le nom du nœud secondaire de la topologie.

Le champ convention de dénomination est mis en surbrillance en rouge si votre entrée n'est pas valide. En cliquant sur le lien « Prévisualiser le nom », vous accédez à un aperçu de la convention de dénomination que vous avez saisie, et le texte d'aperçu est mis à jour de manière dynamique lorsque vous saisissez une convention de dénomination 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 entre 001 et 999 est ajouté au nom secondaire lorsque la relation est créée, remplaçant le nnn qui s'affiche dans le texte d'aperçu, avec 001 étant attribué en premier, 002 attribué en seconde, etc.

- **Paramètres de relation**

  Permet de spécifier le taux de transfert maximal, la règle SnapVault et la planification SnapVault utilisée par la relation de protection :

◦ Taux de transfert max

  Spécifie la vitesse maximale à laquelle les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser un taux de transfert maximal, le transfert de base entre les relations est illimité.

◦ Règles SnapVault

Spécifie la règle ONTAP SnapVault pour la relation. La valeur par défaut est XDPDefault.

- Créer la règle

  Lance la boîte de dialogue Créer une stratégie SnapVault qui vous permet de créer et d'utiliser une nouvelle stratégie SnapVault.

- Planification SnapVault

  Spécifie le planning ONTAP SnapVault de la relation. Horaires disponibles : aucun, 5 min, 8 heures, tous les jours, toutes les heures, et hebdomadaires. La valeur par défaut est aucun, ce qui indique qu'aucun programme n'est associé à la relation. Les relations sans planifications n'ont aucune valeur d'état de décalage à moins qu'elles n'appartiennent à un service de stockage.

- Créer un planning

  Lance la boîte de dialogue Créer un programme qui vous permet de créer un programme SnapVault.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Annuler**

  Supprime vos sélections et ferme la boîte de dialogue configurer la protection.

- **Appliquer**

  Applique vos sélections et lance le processus de protection.

Créer un programme

La boîte de dialogue Créer un planning de protection permet de créer une planification de base ou avancée pour les transferts de relations SnapMirror et SnapVault. Vous pouvez créer un nouveau programme pour augmenter la fréquence des transferts de données en raison de mises à jour fréquentes de données, ou vous pouvez créer un programme moins fréquent lorsque les données changent rarement.

Impossible de configurer le planning pour les relations SnapMirror synchrone.

- **Cluster de destination**

  Nom du cluster sélectionné dans l'onglet SnapVault ou SnapMirror de la boîte de dialogue configurer la protection.

- **Nom de l'annexe**

  Nom que vous indiquez pour le planning. Les noms d'horaires peuvent comprendre les caractères A à Z, a à z, 0 à 9, ainsi que l'un des caractères spéciaux suivants : ! @ # $ % ^ et * ( ) _ -. Les noms d'horaires ne peuvent pas comprendre les caractères suivants : < >.

- **De base ou Avancé**

  Le mode de planification que vous souhaitez utiliser.

Le mode de base comprend les éléments suivants :

- Recommencez

  Fréquence d'un transfert planifié. Vous pouvez choisir entre l'heure, le jour et la semaine.

- Jour

  Lorsqu'une répétition hebdomadaire est sélectionnée, le jour de la semaine où un transfert a lieu.

- Heure

  Lorsque l'option quotidien ou hebdomadaire est sélectionnée, l'heure du jour où un transfert a lieu.

  Le mode avancé comprend les éléments suivants :

- Mois

  Liste numérique séparée par des virgules représentant les mois de l'année. Les valeurs valides sont de 0 à 11, zéro représentant janvier, etc. Cet élément est facultatif. Si vous quittez le champ vide, les transferts se produisent tous les mois.

- Jours

  Liste numérique séparée par des virgules représentant le jour du mois. Les valeurs valides sont comprises entre 1 et 31. Cet élément est facultatif. Si vous quittez le champ vide, un transfert se produit tous les jours du mois.

- Jours de semaine

  Liste numérique séparée par des virgules représentant les jours de la semaine. Les valeurs valides sont de 0 à 6, 0 représentant le dimanche, etc. Cet élément est facultatif. Si vous quittez le champ vide, un transfert se produit 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 n'a lieu que le jour spécifié de la semaine et non tous les jours.

- Heures

  Liste numérique séparée par des virgules représentant le nombre d'heures d'un jour. Les valeurs valides sont de 0 à 23, 0 représentant minuit. Cet élément est facultatif.

- Quelques minutes

  Liste numérique séparée par des virgules représentant les minutes en une heure. Les valeurs valides sont comprises entre 0 et 59. Cet élément est requis.

Boîte de dialogue Créer une règle SnapMirror

La boîte de dialogue Créer une règle SnapMirror vous permet de créer une règle afin de définir la priorité des transferts SnapMirror. Les règles vous permettent d'optimiser l'efficacité des transferts entre la source et la destination.

- **Cluster de destination**

  Nom du cluster sélectionné dans l'onglet SnapMirror de la boîte de dialogue configurer la protection.

- **SVM de destination**

  Nom du SVM que vous avez sélectionné dans l'onglet SnapMirror de la boîte de dialogue configurer la protection.

- **Nom de la politique**

  Nom que vous indiquez pour la nouvelle stratégie. Les noms des polices peuvent être composés des caractères A à Z, a à z, 0 à 9, point (.), tiret (-), et trait de soulignement (_).

- **Priorité de transfert**

  Priorité à laquelle un transfert s'exécute pour les opérations asynchrones. Vous pouvez sélectionner Normal ou Bas. Transférez des relations avec des stratégies qui spécifient une priorité de transfert normale exécutée avant celles qui disposent de stratégies définissant une priorité de transfert faible.

- **Commentaire**

  Champ facultatif dans lequel vous pouvez ajouter des commentaires sur la stratégie.

- **Redémarrage de transfert**

  Indique l'action de redémarrage à effectuer lorsqu'un transfert est interrompu par une opération d'abandon ou tout type de défaillance, par exemple une panne réseau. Vous pouvez sélectionner l'une des options suivantes :

  - Toujours

    Spécifie qu'une nouvelle copie Snapshot est créée avant de redémarrer un transfert. Si elle existe, le transfert est redémarré à partir d'un point de contrôle, suivi d'un transfert incrémentiel à partir de la nouvelle copie Snapshot créée.

  - Jamais

    Spécifie que les transferts interrompus ne sont jamais redémarrés.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Annuler**

  Supprime les sélections et ferme la boîte de dialogue configurer la protection.

- **Appliquer**

  Applique vos sélections et lance le processus de protection.

Boîte de dialogue Créer une stratégie SnapVault

La boîte de dialogue Créer une stratégie de SnapVault vous permet de créer une règle afin de définir la priorité des transferts SnapVault. Vous utilisez les règles pour optimiser l'efficacité des transferts du volume primaire vers le volume secondaire.

- **Cluster de destination**

  Nom du cluster que vous avez sélectionné dans l'onglet SnapVault de la boîte de dialogue configurer la protection.

- **SVM de destination**

  Nom du SVM que vous avez sélectionné dans l'onglet SnapVault de la boîte de dialogue configurer la protection.

- **Nom de la politique**

  Nom que vous indiquez pour la nouvelle stratégie. Les noms des polices peuvent être composés des caractères A à Z, a à z, 0 à 9, point (.), tiret (-), et trait de soulignement (_).

- **Priorité de transfert**

  Priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner Normal ou Bas. Transférez des relations avec des stratégies qui spécifient une priorité de transfert normale exécutée avant celles qui disposent de stratégies définissant une priorité de transfert faible. Le paramètre par défaut est Normal.

- **Commentaire**

  Champ facultatif dans lequel vous pouvez ajouter un commentaire sur la stratégie SnapVault d'un maximum de 255 caractères.

- **Ignorer le temps d'accès**

  Indique si les transferts incrémentiels sont ignorés pour les fichiers dont le temps d'accès a seulement été modifié.

- **Libellé de réplication**

  Répertorie dans un tableau les règles associées aux copies Snapshot sélectionnées par ONTAP qui ont une étiquette de réplication spécifique dans une règle. Les informations et actions suivantes sont également disponibles :

  - Boutons de commande

    Les boutons de commande permettent d'effectuer les opérations suivantes :

    - Ajouter

      Permet de créer une étiquette de copie Snapshot et un nombre de conservation.

    - Modifier le nombre de rétention

      Permet de modifier le nombre de rétention d'une étiquette de copie Snapshot existante. Le nombre de rétention doit être compris entre 1 et 251. La somme de tous les comptes de rétention pour toutes les règles ne peut pas dépasser 251.

    - Supprimer

      Permet de supprimer une étiquette de copie Snapshot existante.

  - Étiquette de copie Snapshot

Affiche l'étiquette de copie Snapshot. Si vous sélectionnez un ou plusieurs volumes avec la même règle de copie Snapshot locale, une entrée pour chaque étiquette de la règle s'affiche. Si vous sélectionnez plusieurs volumes disposant d'au moins deux règles de copie Snapshot locales, le tableau affiche toutes les étiquettes de toutes les règles

- Planification

  Affiche la planification associée à chaque étiquette de copie Snapshot. Si plusieurs horaires sont associés à une étiquette, les planifications de cette étiquette s'affichent dans une liste séparée par des virgules. Si vous sélectionnez plusieurs volumes avec le même libellé mais avec des planifications différentes, la planification affiche « divers » pour indiquer que plusieurs planifications sont associées aux volumes sélectionnés.

- Nombre de rétention de destination

  Affiche le nombre de copies Snapshot avec l'étiquette spécifiée qui sont conservées sur le serveur secondaire SnapVault. Le nombre de rétention pour les étiquettes comportant plusieurs horaires affiche la somme des comptages de rétention de chaque paire d'étiquettes et d'horaires. Si vous sélectionnez plusieurs volumes avec au moins deux règles de copie Snapshot locales, le nombre de rétention est vide.

Boîte de dialogue Modifier la relation

Vous pouvez modifier une relation de protection existante pour modifier le taux de transfert maximal, la stratégie de protection ou le planning de protection.

Informations de destination

- **Cluster de destination**

  Nom du cluster de destination sélectionné.

- **SVM de destination**

  Nom du SVM sélectionné

- **Paramètres de relation**

  Permet de spécifier le taux de transfert maximal, la règle SnapMirror et de planifier les utilisations de la relation de protection :

  - Taux de transfert max

    Spécifie la vitesse maximale à laquelle les données de base sont transférées entre les clusters sur le réseau. Lorsque cette option est sélectionnée, la bande passante réseau est limitée à la valeur que vous spécifiez. Vous pouvez entrer une valeur numérique, puis sélectionner kilo-octets par seconde (Kbit/s), mégaoctets par seconde (Mbit/s), gigaoctets par seconde (Gbit/s) ou téraoctets par seconde (Tbit/s). La vitesse de transfert maximale que vous spécifiez doit être supérieure à 1 kbps et inférieure à 4 Tbit/s. Si vous choisissez de ne pas utiliser un 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.

  - Règle SnapMirror

Spécifie la règle ONTAP SnapMirror pour la relation. La valeur par défaut est DPDefault.

- Créer la règle

  Lance la boîte de dialogue Créer une règle SnapMirror qui vous permet de créer et d'utiliser une nouvelle règle SnapMirror.

- Planification SnapMirror

  Spécifie la règle ONTAP SnapMirror pour la relation. Horaires disponibles : aucun, 5 min, 8 heures, tous les jours, toutes les heures, et hebdomadaires. La valeur par défaut est aucun, ce qui indique qu'aucun programme n'est associé à la relation. Les relations sans planifications n'ont aucune valeur d'état de décalage à moins qu'elles n'appartiennent à un service de stockage.

- Créer un planning

  Lance la boîte de dialogue Créer un calendrier, qui vous permet de créer une nouvelle planification SnapMirror.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Annuler**

  Supprime 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 transfert de base de première fois 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 programmée et incrémentielle.

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**

  Priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner Normal ou Bas. Relations avec des stratégies qui spécifient une priorité de transfert normale avant celles qui spécifient une priorité de transfert faible. Normal est sélectionné par défaut.

- **Taux de transfert max**

  Spécifie la vitesse maximale à laquelle les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser un 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 de relations individuelles

  Lorsque cette option est sélectionnée, les opérations d'initialisation et de mise à jour utilisent la vitesse de transfert maximale spécifiée lors 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.

- Illimitée

  Indique qu'il n'y a pas de limitation de bande passante sur les transferts entre relations. Ce champ est disponible uniquement lorsque plusieurs relations avec des taux de transfert différents sont initialisées ou mises à jour.

- Limitez la bande passante à

  Lorsque cette option est sélectionnée, la bande passante réseau est limitée à la valeur que vous spécifiez. Vous pouvez entrer une valeur numérique, puis sélectionner kilo-octets par seconde (Kbit/s), mégaoctets par seconde (Mbit/s), gigaoctets par seconde (Gbit/s) ou téraoctets par seconde (Tbit/s). La vitesse de transfert maximale que vous spécifiez doit être supérieure à 1 kbps et inférieure à 4 Tbit/s.

Onglet copies Snapshot source

L'onglet copies Snapshot source affiche les informations suivantes sur la copie Snapshot source utilisée pour le transfert de base :

- **Volume source**

  Affiche les noms des volumes source correspondants.

- **Volume de destination**

  Affiche les noms des volumes de destination sélectionnés.

- **Type de source**

  Affiche le type de volume. Ce type peut être soit lecture/écriture, soit protection des données.

- **Copie snapshot**

  Affiche la copie Snapshot utilisée pour le transfert de données. Si vous cliquez sur la valeur de la copie Snapshot, la boîte de dialogue Select source Snapshot Copy s'affiche. Vous pouvez alors sélectionner une copie Snapshot spécifique pour votre transfert, en fonction du type de relation de protection dont vous disposez et de l'opération que vous effectuez. La possibilité de spécifier une autre copie Snapshot n'est pas disponible pour les sources de type de protection des données.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Annuler**

  Supprime vos sélections et ferme la boîte de dialogue initialiser/mettre à jour.

- **Soumettre**

  Enregistre vos sélections et lance la tâche d'initialisation ou de mise à jour.

Boîte de dialogue resynchroniser

La boîte de dialogue Resynchroniser vous permet de resynchroniser les données d'une relation SnapMirror ou SnapVault précédemment interrompue, puis la destination a été créée un volume de lecture/écriture. Vous pouvez également resynchroniser lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, entraînant l'échec des mises à jour de SnapMirror ou de SnapVault.

Onglet Options de resynchronisation

L'onglet Resynchronisation Options vous permet de définir la priorité de transfert et la vitesse de transfert maximale pour la relation de protection que vous êtes en cours de resynchronisation.

- **Priorité de transfert**

  Priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner Normal ou Bas. Relations avec des stratégies qui spécifient une priorité de transfert normale exécutée avant celles qui disposent de stratégies définissant une priorité de transfert faible.

- **Taux de transfert max**

  Spécifie la vitesse maximale à laquelle les données sont transférées entre les clusters sur le réseau. Lorsque cette option est sélectionnée, la bande passante réseau est limitée à la valeur que vous spécifiez. Vous pouvez entrer une valeur numérique, puis sélectionner kilo-octets par seconde (Kbit/s), mégaoctets par seconde (Mbit/s), gigaoctets par seconde (Gbit/s) ou Tbit/s. Si vous choisissez de ne pas utiliser un taux de transfert maximal, le transfert de base entre les relations est illimité.

Onglet copies Snapshot source

L'onglet copies Snapshot source affiche les informations suivantes sur la copie Snapshot source utilisée pour le transfert de base :

- **Volume source**

  Affiche les noms des volumes source 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 snapshot**

  Affiche la copie Snapshot utilisée pour le transfert de données. Si vous cliquez sur la valeur de la copie Snapshot, la boîte de dialogue Sélectionner une copie Snapshot source s'affiche. Elle permet de sélectionner une copie Snapshot 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**

  Lance le processus de resynchronisation et ferme la boîte de dialogue Resynchroniser.

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Resynchroniser.

Sélectionnez la boîte de dialogue copie Snapshot source

La boîte de dialogue Select source Snapshot Copy permet de sélectionner une copie Snapshot afin de transférer des données entre les relations de protection, ou de sélectionner le comportement par défaut. Cette opération varie selon que vous êtes en cours d'initialisation, de mise à jour ou de resynchronisation d'une relation, et que la relation est une SnapMirror ou SnapVault.

Valeur par défaut

Vous permet de sélectionner le comportement par défaut pour déterminer la copie Snapshot 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 :

Fonctionnement	Comportement SnapVault par défaut lorsque la source est en lecture/écriture	Comportement SnapVault par défaut lorsque la source est Data protection (DP)
Initialiser	Crée une nouvelle copie Snapshot et la transfère.	Transfère la dernière copie Snapshot exportée.
Mise à jour	Transfert des copies Snapshot étiquetées uniquement, tel que spécifié dans la règle.	Transfère la dernière copie Snapshot exportée.
Resynchroniser	Transfère toutes les copies Snapshot étiquetées créées à l'issue de la dernière copie Snapshot commune.	Transfère la dernière marque nommée copie Snapshot.

Si vous effectuez un transfert SnapMirror, le comportement par défaut de chaque opération est le suivant :

Fonctionnement	Comportement SnapMirror par défaut	Comportement SnapMirror par défaut lorsqu'une relation est un second 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 à partir 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 à partir 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 nouvelle copie Snapshot commune.

Copie Snapshot existante

Vous permet de sélectionner une copie Snapshot existante dans la liste si la sélection de copie Snapshot est autorisée pour cette opération.

- **Copie snapshot**

  Affiche les copies Snapshot existantes depuis lesquelles vous pouvez sélectionner pour un transfert.

- **Date de création**

  Affiche la date et l'heure de création de la copie Snapshot. Les copies Snapshot sont répertoriées des versions les plus récentes au moins récentes, avec les plus récentes 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, chaque opération se déroule comme suit :

Fonctionnement	Comportement de SnapVault lors de la définition d'une copie Snapshot	Comportement de SnapVault lors de la spécification d'une copie Snapshot dans une cascade
Initialiser	Transfère la copie Snapshot spécifiée.	La sélection de copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.

Fonctionnement	Comportement de SnapVault lors de la définition d'une copie Snapshot	Comportement de SnapVault lors de la spécification d'une copie Snapshot dans une cascade
Mise à jour	Transfère la copie Snapshot spécifiée.	La sélection de copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.
Resynchroniser	Transfère la copie Snapshot sélectionnée.	La sélection de copie Snapshot 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, chaque opération se déroule comme suit :

Fonctionnement	Comportement de SnapMirror lors de la définition d'une copie Snapshot	Comportement de SnapMirror lors de la spécification d'une copie Snapshot dans une cascade
Initialiser	Transfère toutes les copies Snapshot de la source, jusqu'à la copie Snapshot spécifiée.	La sélection de copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.
Mise à jour	Transfère toutes les copies Snapshot de la source, jusqu'à la copie Snapshot spécifiée.	La sélection de copie Snapshot 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 nouvelle copie Snapshot commune.	La sélection de copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Soumettre**

  Soumet vos sélections et ferme la boîte de dialogue Sélectionner une copie Snapshot source.

- **Annuler**

  Supprime vos sélections et ferme la boîte de dialogue Sélectionner une copie Snapshot source.

Boîte de dialogue Reverse Resync

Lorsque la relation de protection est rompue car le volume source est désactivé et la destination est créée un volume en lecture/écriture, la resynchronisation inverse vous permet d'inverser la direction de la relation. La destination devient ainsi la nouvelle source et la nouvelle destination devient la nouvelle destination.

Lorsqu'un incident désactive le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour transmettre des données en les 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 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**

  Nom et emplacement du volume source avant une opération de resynchronisation inverse.

- **Volume de destination**

  Nom et emplacement du volume de destination avant une opération de resynchronisation inverse.

Après resynchronisation inverse

Affiche la source et la destination d'une relation après une opération de resynchronisation de réserve.

- **Volume source**

  Nom et emplacement du volume source après une opération de resynchronisation inverse.

- **Volume de destination**

  Nom et emplacement du volume de destination après une opération de resynchronisation inverse.

Boutons de commande

Les boutons de commande permettent d'effectuer les opérations suivantes :

- **Soumettre**

  Démarre le processus de resynchronisation inverse.

- **Annuler**

  Ferme la boîte de dialogue Reverse Resync sans lancer une opération de resynchronisation inverse.

Relation : vue de toutes les relations

La vue relations : 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 premier niveau 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 limiter la liste des données affichées, d'ajouter/supprimer/réorganiser des colonnes de la page et d'exporter les données de la page vers un fichier .csv, .PDF, ou fichier .xlsx. Après avoir personnalisé la page, vous pouvez enregistrer les résultats sous forme de vue personnalisée, puis planifier régulièrement un rapport de ces données à générer et à envoyer par e-mail. Par défaut, lorsque vous sélectionnez le menu **relations**, le rapport affiché inclut des relations de protection pour les volumes et les machines virtuelles de stockage de votre datacenter. Vous pouvez utiliser l'option **Filter** pour afficher uniquement les systèmes de stockage sélectionnés comme 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 de volume ou de VM de stockage, vous pouvez accéder à la page **Storage** > **volumes** > **relationship : toutes les relations** ou à la page **protection** > **relations** > **relations** > **relationship : Toutes les relations**, et utilisez l'option **Relationship Object Type** dans **Filter** pour filtrer uniquement les volumes ou les données des VM de stockage.

La page relations qui répertorie toutes les relations de protection contient 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.

  L'état peut être erreur ( ), Avertissement ( ) ou OK ( ).

- **VM de stockage source**

  Affiche le nom du SVM source. Pour plus de détails sur la SVM source, cliquez sur le nom du SVM.

  Lorsqu'un SVM existe sur le cluster, mais qu'il 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 est vide. Vous devez vous assurer que la SVM existe ou effectuer une nouvelle découverte sur le cluster pour actualiser la liste des ressources.

- **Source**

  Affiche le volume source ou la machine virtuelle de stockage source protégée en fonction de votre sélection. Vous pouvez afficher des informations plus détaillées sur le volume source ou la VM de stockage en cliquant sur le nom du volume ou de la VM de stockage.

  Si le message `Resource-key not discovered` est affiché, cela peut indiquer que le volume existe sur le cluster, mais qu'il 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 nouvelle découverte 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. Pour plus d'informations sur le volume de destination ou la VM de stockage, cliquez sur le nom de l'objet correspondant.

- **Type d'objet de relation**

  Affiche le type d'objet utilisé dans la relation, tel que machine virtuelle de stockage, volume et groupe de cohérence. Pour les objets d'une relation de cohérence, la source de la relation et les destinations affichent le groupe de cohérence et lorsque vous cliquez sur ces derniers, vous accédez à la page LUN pour afficher la relation.

- **Politique**

  Affiche le nom de la règle de protection de la relation SnapMirror. Vous pouvez cliquer sur le nom de la stratégie pour afficher les détails associés à cette stratégie, notamment 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 de priorité normale sont programmés avant les transferts de priorité faible. La valeur par défaut est Normal.

  - Ignorer l'heure d'accès

    S'applique uniquement aux relations SnapVault. Cette option indique si les transferts incrémentiels ignorent les fichiers dont le temps d'accès a seulement changé. Les valeurs sont soit vrai soit Faux. La valeur par défaut est False.

  - Lorsque la relation est désynchronisée

    Spécifie l'action ONTAP effectuée lorsqu'une relation synchrone ne peut pas être synchronisée. Les relations StrictSync limitent l'accès au volume principal en cas d'échec de la synchronisation avec le volume secondaire. Les relations de synchronisation ne limitent pas l'accès au primaire en cas d'échec de la synchronisation avec le secondaire.

  - Limite de tentatives

    Spécifie le nombre maximal de tentatives de chaque 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 stratégie sélectionnée.

  - Étiquette SnapMirror

    Spécifie l'étiquette SnapMirror pour la première planification associée à la règle de copie Snapshot. L'étiquette SnapMirror est utilisée par le sous-système SnapVault lors de la sauvegarde des copies Snapshot sur une destination SnapVault.

  - Paramètre de conservation

    Indique la durée de conservation des sauvegardes, en fonction de la durée ou du nombre de sauvegardes.

  - Copies Snapshot réelles

Spécifie le nombre de copies Snapshot sur ce volume qui correspond à l'étiquette spécifiée.

- Conservez les copies Snapshot

  Spécifie le nombre de copies SnapVault Snapshot qui ne sont pas supprimées automatiquement, même si la limite maximale de la règle est atteinte. Les valeurs sont soit vrai soit Faux. La valeur par défaut est False.

- Seuil d'avertissement de rétention

  Spécifie la limite de copie Snapshot à laquelle un avertissement est envoyé pour indiquer que la limite de conservation maximale est presque atteinte.

- * Durée du décalage*

  Affiche la durée pendant laquelle les données du miroir sont en retard par rapport à la source.

  La durée du décalage doit être proche ou égale à 0 secondes pour les relations StrictSync.

- **Etat de décalage**

  Affiche l'état de décalage pour les relations gérées et pour les relations non gérées qui ont un planning associé à cette relation. Le statut de 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 se situe dans les limites normales.

  - Sans objet

    L'état de décalage n'est pas applicable pour les relations synchrones car un planning ne peut pas être configuré.

- **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*

  Indique 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 :

  - Mise en miroir asynchrone

- Coffre-fort asynchrone
- MirrorVault asynchrone
- StrictSync
- Synchrone

- **État du transfert**

  Affiche l'état du transfert pour la relation de protection. Le statut du transfert peut être l'un des suivants :

  - Abandon

    Les transferts SnapMirror sont activés. Cependant, une opération d'abandon du transfert susceptible d'inclure la suppression du point de contrôle est en cours.

  - Vérification

    Le volume de destination fait l'objet d'un contrôle 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.

  - In-Sync

    Les données des deux volumes de 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 en cours.

  - Suspendu

    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 le transfert est en cours.

- La transition

  Le transfert asynchrone des données du volume source vers le volume de destination est terminé, et la transition vers le volume synchrone a démarré.

- En attente

  Un transfert SnapMirror a été initié, mais certaines tâches associées attendent d'être mises en file d'attente.

- **Durée du dernier transfert**

  Affiche le temps de fin du dernier transfert de données.

  La durée du transfert n'est pas applicable aux relations StrictSync car le transfert doit être simultané.

- **Dernière taille de transfert**

  Affiche la taille, en octets, du dernier transfert de données.

  La taille de transfert n'est pas applicable aux relations StrictSync.

- **Médiateurs**

  Affiche l'état du médiateur.

  - Sans objet

    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 à Unified Manager.

  - Adresse IP du médiateur

    S'il est configuré et que les clusters source et de destination sont tous les deux ajoutés dans Unified Manager.

- **État**

  Affiche l'état de la relation SnapMirror ou SnapVault. Cet état peut être non initialisé, SnapMirror ou Broken-off. Si un volume source est sélectionné, l'état de la relation n'est pas applicable et n'est pas affiché.

- * Relation Santé*

  Affiche l'état de santé de la relation 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 de priorité normale sont programmés avant les transferts de priorité faible.

La priorité de transfert n'est pas applicable aux relations synchrones car tous les transferts sont traités avec la même priorité.

- **Annexe**

  Affiche le nom du planning de protection attribué à la relation.

  Le planning n'est pas applicable pour les relations synchrones.

- **Réplication flexible de version**

  Affiche Oui, Oui avec option de sauvegarde ou aucun.

- **Cluster source**

  Affiche le FQDN, le nom court ou l'adresse IP du cluster source pour la relation SnapMirror.

- **FQDN du cluster source**

  Affiche le nom du cluster source de la relation SnapMirror.

- **Nœud source**

  Affiche le nom de la liaison nom du nœud source pour la relation SnapMirror d'un volume et affiche le lien SnapMirror relationship node count lorsque l'objet est une VM 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 dans lesquels les volumes de ces groupes de cohérence appartiennent à une relation de synchronisation active SnapMirror.

Lorsque vous cliquez sur le lien nombre de nœuds, vous accédez à la page des nœuds associés à cette relation. Lorsque le nombre de nœuds est égal à 0, aucune valeur n'est affichée car aucun nœud n'est associé à la relation.

- **Nœud de destination**

  Affiche le nom de la liaison nom du nœud de destination pour la relation SnapMirror d'un volume et affiche le lien entre le nombre de nœuds de relations SnapMirror lorsque l'objet est une VM de stockage ou un groupe de cohérence.

  Lorsque vous cliquez sur le lien nombre de nœuds, vous accédez à la page des nœuds associés à cette relation. Lorsque le nombre de nœuds est égal à 0, aucune valeur n'est affichée car aucun nœud n'est associé à la relation.

- **Cluster de destination**

  Affiche le nom du cluster de destination de la relation SnapMirror.

- **FQDN du cluster de destination**

  Affiche le FQDN, 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 volumes et groupes de cohérence pour les clusters et les machines virtuelles de stockage, notamment :

  - SnapMirror
  - Reprise après incident des machines virtuelles de stockage
  - SnapMirror, reprise après incident des VM de stockage
  - Groupe de cohérence
  - SnapMirror, groupe de cohérence.

Informations connexes

- Pour plus d'informations sur la vue **relation : MetroCluster**, voir "Contrôle des configurations MetroCluster".
- Pour plus d'informations sur la vue **Relationship: Last 1 Month Transfer Status**, voir "Relation : vue État transfert du dernier mois".
- Pour plus d'informations sur la vue **relation : toutes les relations**, voir "Relation : vue du taux de transfert du dernier mois".

Relation : vue État transfert du dernier mois

La vue relation : état du transfert sur les 1 derniers mois vous permet d'analyser les tendances de transfert sur une période de temps pour les volumes et les machines virtuelles de stockage dans les 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, créer et appliquer des filtres pour affiner la liste des données affichées, ajouter/supprimer/réorganiser des colonnes sur la page et exporter les données de la page vers un `.csv` fichier , `.pdf` ou `.xlsx` . Après avoir personnalisé la page, vous pouvez enregistrer les résultats sous forme de vue personnalisée, puis planifier régulièrement un rapport de ces données à générer et à envoyer par e-mail. Vous pouvez utiliser l'option **Filter** pour afficher uniquement les systèmes de stockage sélectionnés comme 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 de volume, vous pouvez accéder soit au rapport relation : 1 mois dernier état du transfert pour les machines virtuelles de stockage soit à partir du menu **Storage** > **Storage VM** > **relationship : 1 mois dernier Etat du transfert**, soit à partir du menu **protection** > **relations** > **relationship : Le menu État transfert** du dernier mois et utilisez **Filter** 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 d'opération**

  Indique 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 de transfert**

  Affiche la taille (en Mo) du volume transféré.

- **SVM source**

  Affiche le nom de la machine virtuelle de stockage (SVM).

- **Cluster source**

  Affiche le nom du cluster source.

- **SVM de destination**

  Affiche le nom du SVM de destination.

- **Cluster de destination**

  Affiche le nom du cluster de destination.

Informations connexes

- Pour plus d'informations sur la vue **relation : toutes les relations**, voir "Relation : vue de toutes les relations".
- Pour plus d'informations sur la vue **Relationship:MetroCluster**, voir "Contrôle des configurations MetroCluster".
- Pour plus d'informations sur la vue **relation : toutes les relations**, voir "Relation : vue du taux de transfert du dernier mois".

Relation : vue du 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 qui est transférée au quotidien pour les volumes dans des relations asynchrones. Cette page fournit également des informations détaillées sur les transferts quotidiens et le temps requis pour 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, créer et appliquer des filtres pour limiter la liste des données affichées, ajouter/supprimer/réorganiser des colonnes de la page et 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 régulièrement un rapport de ces données à générer et à envoyer par e-mail. Par exemple, si vous souhaitez afficher les relations de volume, vous pouvez accéder au menu **Storage** > **volumes** > **relationship: 1 dernier mois transfert Rate** ou accéder au menu **protection** > **relations** > **relations:dernier 1 mois transfert Rate** et utiliser **Filter** 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 lancé.

- **Heure de fin**

  Affiche l'heure de fin du transfert de volume avec date.

Informations connexes

- Pour plus d'informations sur la vue **Relationship:MetroCluster**, voir "Contrôle des configurations MetroCluster".
- Pour plus d'informations sur la vue **Relationship: Last 1 Month Transfer Status**, voir "Relation : vue État transfert du dernier mois".
- Pour plus d'informations sur la vue **relation : toutes les relations**, voir "Relation : vue du taux de transfert du dernier mois"

Générer des rapports personnalisés

Création de rapports Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) permet d'afficher, de personnaliser, de télécharger et de planifier des rapports pour vos systèmes de stockage ONTAP. Ces rapports peuvent fournir des informations détaillées sur la capacité du système de stockage, l'état, les performances, la sécurité et les relations de protection.

La nouvelle fonctionnalité de création de rapports et de planification de Unified Manager, introduite dans Active IQ Unified Manager 9.6, remplace le moteur de création de rapports précédent retiré dans Unified Manager version 9.5.

Les rapports fournissent différentes vues de votre réseau et fournissent des informations exploitables sur la capacité, l'état, les performances, la sécurité et la protection des données. Vous pouvez personnaliser vos vues en affichant, en masquant et en réorganisant les colonnes, en filtrant les données, en triant des données, et la recherche dans les résultats. Vous pouvez enregistrer des vues personnalisées pour les réutiliser, les télécharger en tant que rapports et les planifier en tant que rapports récurrents à distribuer par e-mail.

Vous pouvez télécharger des vues au format Microsoft® Excel et les personnaliser. Vous pouvez utiliser des fonctions Excel avancées, telles que des tri complexes, des filtres superposés, des tableaux croisés dynamiques et des graphiques. Lorsque vous êtes satisfait du rapport Excel obtenu, vous pouvez télécharger le fichier Excel à utiliser chaque fois que le rapport est planifié et partagé.

Outre la génération de rapports depuis l'interface utilisateur, vous pouvez extraire des données de santé, de sécurité et de performances à partir d'Unified Manager en utilisant les méthodes suivantes :

- Utilisation des outils ODBC (Open Database Connectivity) et ODBC pour accéder directement à la base de données pour les informations de cluster
- Exécution d'API REST Unified Manager pour renvoyer les informations que vous souhaitez consulter

À partir de cette version de Active IQ Unified Manager, les rapports ont apporté les améliorations suivantes :

- Un e-mail est envoyé pour un rapport conformément à l'horaire configuré. Même si vous générez un rapport à la demande, vous recevrez un e-mail.
- Le nom du fichier du rapport et les métadonnées du rapport incluent le nom d'hôte à partir duquel le rapport a été généré. Même si un changement de nom de fichier change, vous pouvez toujours identifier le nom d'hôte à partir duquel le rapport a été généré en raison de cette amélioration.

Points d'accès pour générer des rapports

Vous pouvez regrouper dans Unified Manager des informations sur les 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 méthodes pour accéder aux fonctions de reporting proposées par Unified Manager :

- Extraction de données directement à partir des pages d'inventaire dans l'interface utilisateur.
- Utilisation des outils ODBC (Open Database Connectivity) et 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.

Les bases de données Unified Manager sont accessibles pour le reporting personnalisé

Unified Manager utilise une base de données MySQL pour stocker les données depuis les clusters où celles-ci surveillent. Les données sont conservées dans différents schémas de la base de données MySQL.

Toutes les données de table des bases de données suivantes sont disponibles :

Base de données	Description
modèle_netapp	Données relatives aux objets des contrôleurs ONTAP.
vue_modèle_netapp	Données sur les objets des contrôleurs ONTAP, adaptées à la consommation des outils de rapport.
performances_netapp	Compteurs de performances spécifiques au cluster.
ocum	Informations et données d'application Unified Manager pour la prise en charge du filtrage, du tri et du calcul de certains champs dérivés
rapport_ocum	Données pour la configuration de l'inventaire et des informations relatives à la capacité.
ocum_report_birt	Vues pour la configuration d'inventaire et les données relatives à la capacité, adaptées à la consommation des outils de rapport.
opm	Paramètres de configuration des performances et informations sur les seuils
scatemonitor	Informations sur les problèmes de performances et d'état de l'application Unified Manager.
modèle_vmware	Données d'objet VMware pour les datastores hébergés sur un système de stockage NetApp.
vue_modèle_vmware	Vues des données d'objets VMware pour les datastores hébergés sur un système de stockage NetApp, adaptés à la consommation des outils de reporting.

Base de données	Description
performances_vmware	Données de compteur de performances VMware pour les datastores hébergés sur un système de stockage NetApp.

Un utilisateur de création de rapports — 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 au reporting et à d'autres vues de base de données directement depuis la base de données Unified Manager. Notez que cet utilisateur n'est pas autorisé à accéder aux tables contenant des données utilisateur ou des informations d'identification du cluster.

API REST Unified Manager pouvant être utilisées pour le reporting

Vous pouvez utiliser des API REST pour gérer les clusters en visualisant les informations relatives à l'état, la capacité, les performances et la sécurité collectées par Unified Manager.

Les API REST sont exposées via la page Web de swagger. Vous pouvez accéder à la page Web swagger pour afficher la documentation de l'API REST de Unified Manager et lancer manuellement un appel d'API. Dans l'interface utilisateur 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, reportez-vous à "Mise en route des API REST de Active IQ Unified Manager"la section .

Pour accéder aux API REST, vous devez disposer du rôle opérateur, administrateur de stockage ou administrateur d'applications.

Présentation des rapports

Des rapports affichent des informations détaillées sur le stockage, le réseau, la qualité de service et les relations de protection, vous permettant d'identifier et de résoudre les problèmes potentiels avant qu'ils ne se produisent.

Lorsque vous personnalisez une vue, vous pouvez l'enregistrer avec un nom unique pour une utilisation ultérieure. Vous pouvez planifier un rapport en fonction de 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 fonctions Excel avancées, puis la télécharger de nouveau dans Unified Manager . Si vous planifiez un rapport à l'aide de cette vue, il utilisera le fichier Excel que vous avez chargé pour créer des rapports fiables que vous pouvez partager.

Vous pouvez gérer tous les rapports qui ont été planifiés à partir de la page programmes de rapports.

> Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage pour gérer les rapports.

Vous pouvez télécharger des rapports sous forme de fichiers CSV (valeurs séparées par des virgules), Excel ou PDF.

Comprendre la relation de vue et de rapport

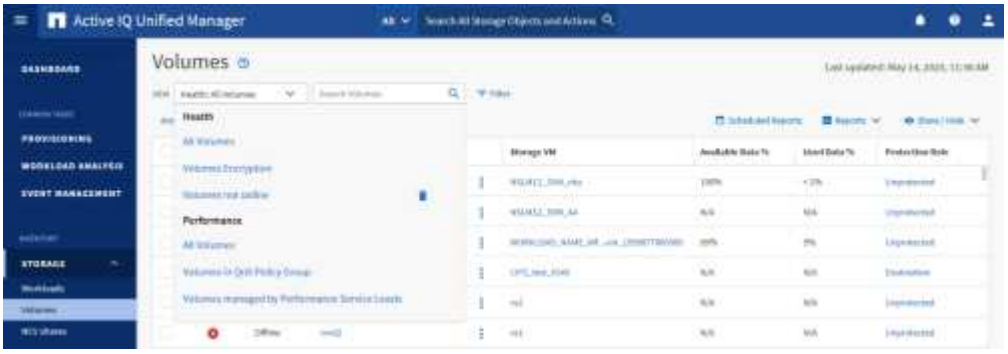
Les pages d'affichage et d'inventaire deviennent des rapports lorsque vous les

téléchargez ou les planifiez.

Vous pouvez personnaliser et enregistrer les vues et les pages d'inventaire pour les réutiliser. La quasi-totalité des informations qu'il est possible d'afficher dans Unified Manager peuvent être enregistrées, réutilisées, personnalisées, planifiées et partagées sous la forme d'un 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 représentent les vues par défaut fournies par Unified Manager. Les vues par défaut ne peuvent pas être modifiées ni supprimées.

- Si vous supprimez une vue personnalisée de la liste, elle 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 reflèteront la modification lors de la prochaine génération et envoi du rapport par e-mail, conformément à la planification du rapport. Lors de la modification des vues, assurez-vous que vos modifications fonctionnent avec les personnalisations Excel associées utilisées pour les rapports. Si nécessaire, vous pouvez mettre à jour le fichier Excel en le téléchargeant, en effectuant les modifications requises et en le téléchargeant comme une nouvelle personnalisation Excel pour la vue.



Seuls les utilisateurs disposant du rôle Administrateur d'applications 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 Active IQ Unified Manager

Type	Objet réseau ou de stockage
Capacité	Clusters 64 bits Volumes Qtrees

Type	Objet réseau ou de stockage
Santé	Clusters Nœuds 64 bits Machines virtuelles de stockage Volumes Partages SMB/CIFS Partages NFS
Performances	Clusters Nœuds 64 bits Machines virtuelles de stockage Volumes LUN Espaces de noms NVMe Interfaces réseau (LIFS) Ports
Qualité de service	Groupes de règles de QoS classiques Groupes de règles de QoS adaptative Groupes de règles de niveau de service de performance
Relations de protection des volumes (disponibles à partir de la page volumes)	Toutes les relations État du transfert du dernier mois Taux de transfert du dernier mois
Sécurité	Machines virtuelles de stockage Clusters

Limites de la création de rapports

La nouvelle fonctionnalité de reporting Active IQ Unified Manager est limitée.

Rapports existants issus des versions précédentes de Unified Manager

Vous pouvez uniquement modifier le planning et les destinataires des rapports existants créés et importés (en tant que fichiers .rptdesign) dans Unified Manager 9.5 et versions antérieures. Si vous avez personnalisé les 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 rapport.

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 (préférée)
- Placez le pointeur de 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 qu'aucune personnalisation ne soit nécessaire. Vous pouvez utiliser la nouvelle solution de création de rapports pour recréer tous les rapports personnalisés.

Planification et rapport

Vous pouvez créer plusieurs planifications différentes avec n'importe quelle combinaison de destinataires pour chaque rapport enregistré. Cependant, vous ne pouvez pas réutiliser le planning 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 d'événements et télécharger le rapport résultant au format CSV, vous ne pouvez pas planifier de rapports d'événements récurrents pour la génération et la distribution.

Pièces jointes du rapport

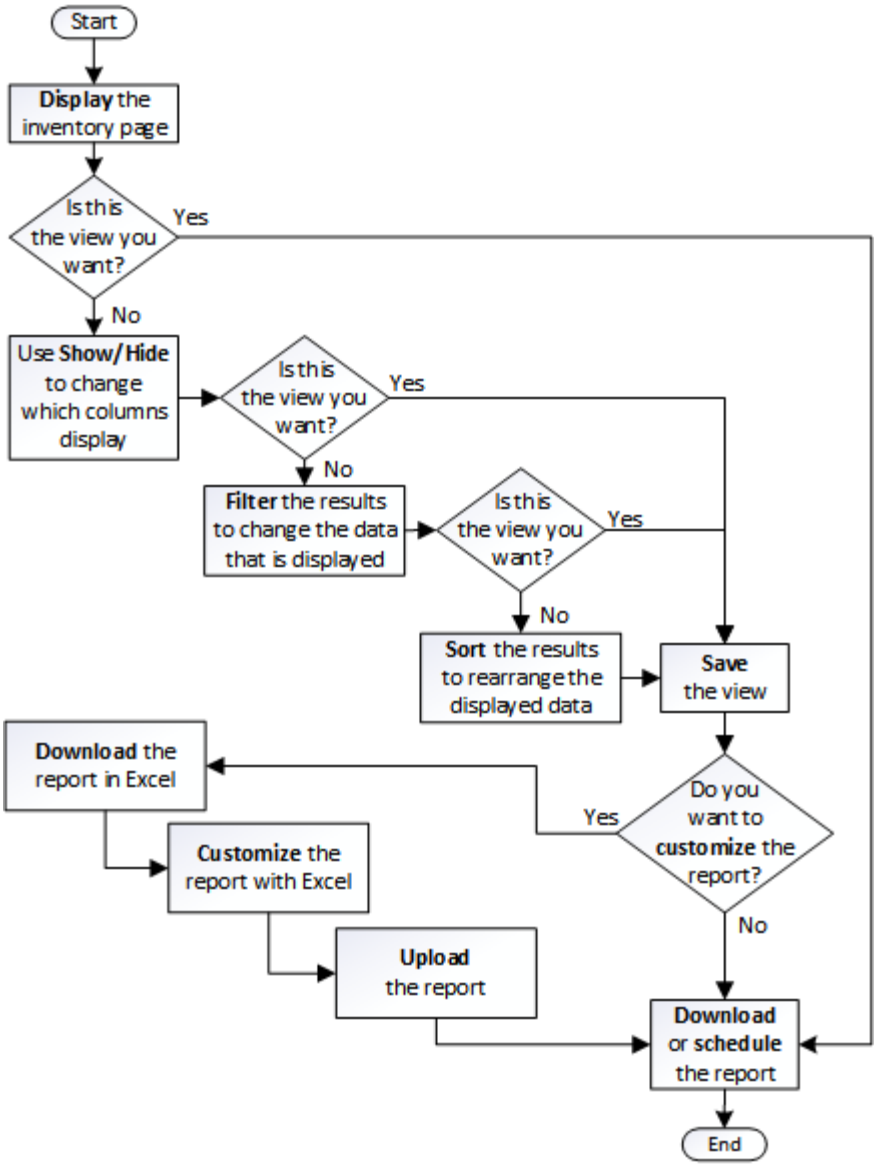
Les rapports ne peuvent pas être envoyés dans le corps d'un e-mail. Au lieu de cela, les rapports sont envoyés uniquement sous forme de pièces jointes PDF, Excel ou CSV.

Utilisation des rapports

Découvrez comment rechercher et personnaliser les vues de pages d'inventaire dans des rapports planifiés partageables.

Flux de travail des rapports

Arbre de décision décrivant le flux de travail du rapport.



Création rapide de rapports

Créez un modèle de rapport personnalisé afin de découvrir les vues et les rapports de planification. Ce rapport de démarrage rapide trouve une liste de volumes que vous pouvez déplacer vers le Tier cloud, car il existe une quantité équitable de données inactives. Vous ouvrez la vue Performance: Tous les volumes, personnalisez la vue à l'aide de filtres et de colonnes, enregistrez la vue personnalisée en tant que rapport et planifiez le partage du rapport une fois par semaine.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré des agrégats FabricPool et certains volumes sur ces agrégats.

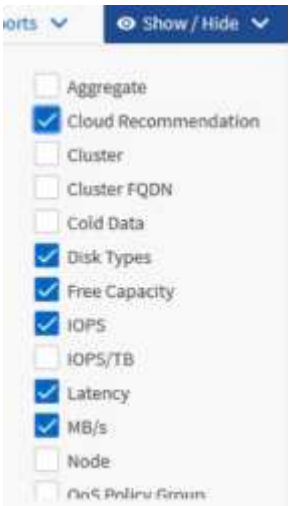
Procédez comme suit pour :

- Ouvrez la vue par défaut

- Personnalisez les colonnes en filtrant et en triant les données
- Enregistrez la vue
- Planifier la génération d'un rapport pour la vue personnalisée

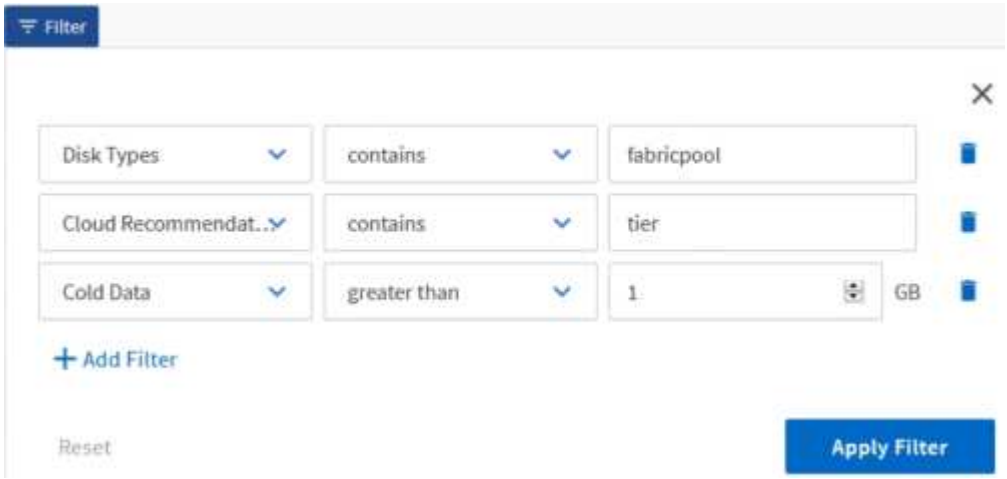
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **Performance** > **tous les volumes**.
3. Cliquez sur **Afficher/Masquer** pour vous assurer que la colonne "types de disque" s'affiche dans la vue.



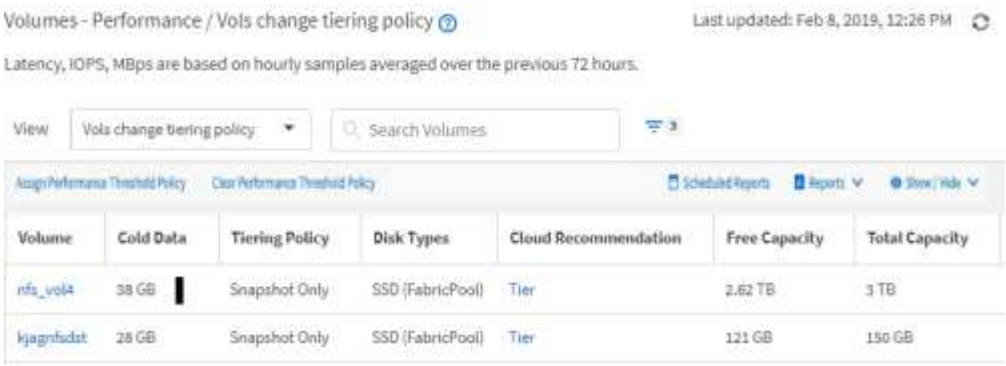
Ajoutez ou supprimez d'autres colonnes pour créer une vue contenant les champs importants pour votre rapport.

4. Faites glisser la colonne "types de disque" à côté de la colonne "recommandations sur le 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 la FabricPool
   - La recommandation cloud contient le Tier
   - Données inactives supérieures à 10 Go



Notez que chaque filtre est associé à une logique et que tous les volumes renvoyés doivent répondre à tous les critères. Vous pouvez ajouter jusqu'à cinq filtres.

6. Cliquez sur la partie supérieure de la colonne données froides pour trier les résultats afin que les volumes avec les données les plus 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 que la vue montre, par exemple « vols change Tiering policy ». Lorsque vous avez terminé, cliquez sur la coche ou appuyez sur **entrée** pour enregistrer la vue avec le nouveau nom.



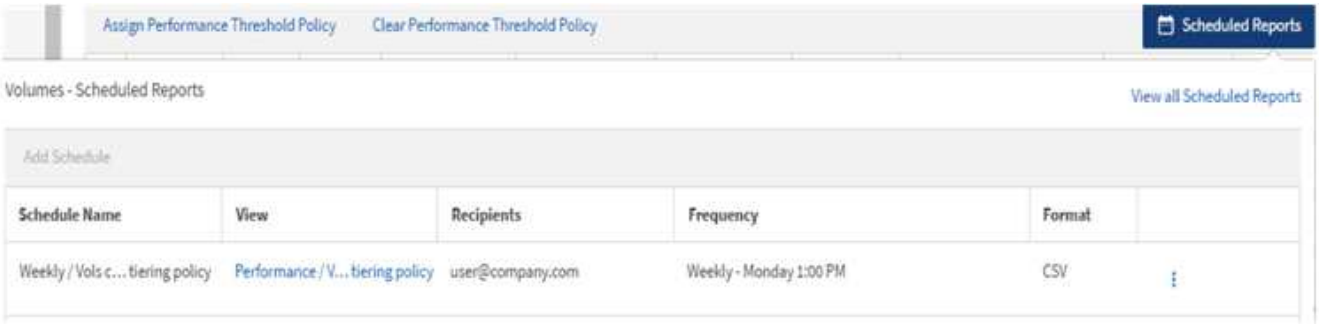
8. Téléchargez le rapport sous forme de fichier **CSV**, **Excel** ou **PDF** pour voir le résultat avant de le planifier ou de le partager.

   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, de tri, de tableaux croisés dynamiques ou de graphiques complexes en téléchargeant la vue sous forme de fichier Excel. Une fois le fichier ouvert dans Excel, utilisez les fonctions avancées pour personnaliser votre rapport. Lorsque vous êtes satisfait, chargez le fichier Excel. Ce fichier, avec ses personnalisations, est appliqué à la vue lorsque le rapport est exécuté.

   Pour plus d'informations sur la personnalisation des rapports à l'aide d'Excel, reportez-vous à la section *Sample Microsoft Excel Reports*.

9. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire. Tous les rapports programmés relatifs à l'objet, dans ce cas, les volumes, apparaissent dans la liste.



10. Cliquez sur **Ajouter un programme** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
11. Entrez un nom pour le rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

L'exemple de rapport suivant est au format CSV :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capi	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

performance-volumes-28-Mar-2019

L'exemple de rapport suivant est au format PDF :

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok	[illegible]	Snapshot Only	28.01	121.32	150	[illegible]	[illegible]	[illegible]
Ok	[illegible]	Snapshot Only	379.64	2676.57	3072	[illegible]	[illegible]	[illegible]

En fonction des résultats présentés dans ce rapport, vous pouvez utiliser ONTAP System Manager ou l'interface de ligne de commande de ONTAP pour modifier la règle de Tiering en « automatique » ou « toutes » pour certains volumes, afin de décharger des données plus inactives vers le Tier cloud.

Recherche d'un rapport planifié

Vous pouvez rechercher des rapports programmés par nom, nom d'affichage, type d'objet ou destinataires.

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Report Schedules**.
2. Utilisez le champ de texte **Rechercher les rapports programmés**.

Pour trouver des rapports par …	Essayer …
Nom du programme	Saisissez une partie du nom du programme de rapport.
Nom de la vue	Saisissez une partie du nom de la vue de rapport. Les vues par défaut et les vues personnalisées apparaissent dans la liste des vues.
Destinataire	Saisissez 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 dans l'ordre croissant ou décroissant en fonction de cette colonne, par exemple le nom ou le format du programme.

Personnalisation des rapports

Vous pouvez personnaliser les vues de différentes manières afin de créer un rapport contenant toutes les informations nécessaires à la gestion de vos clusters ONTAP.

Commencez par 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 sur une colonne spécifique par ordre croissant ou décroissant.

Depuis Unified Manager 9.8, vous pouvez également télécharger la vue dans Excel pour la personnaliser à l'aide de fonctions avancées. Lorsque vous avez terminé, chargez 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 fiables que vous pouvez partager.

Pour plus d'informations sur la personnalisation des rapports à l'aide d'Excel, reportez-vous à la section *Sample Microsoft Excel Reports*.

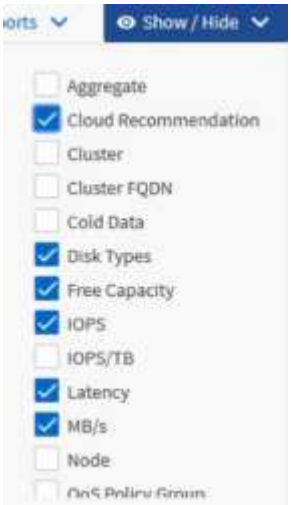
> Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage pour gérer les rapports.

Personnalisation des colonnes

Utilisez **Afficher/Masquer** pour choisir les colonnes que vous souhaitez utiliser dans votre rapport. Faites glisser les colonnes de la page d'inventaire pour les réorganiser.

Étapes

1. Cliquez sur **Afficher/Masquer** pour ajouter ou supprimer des colonnes.



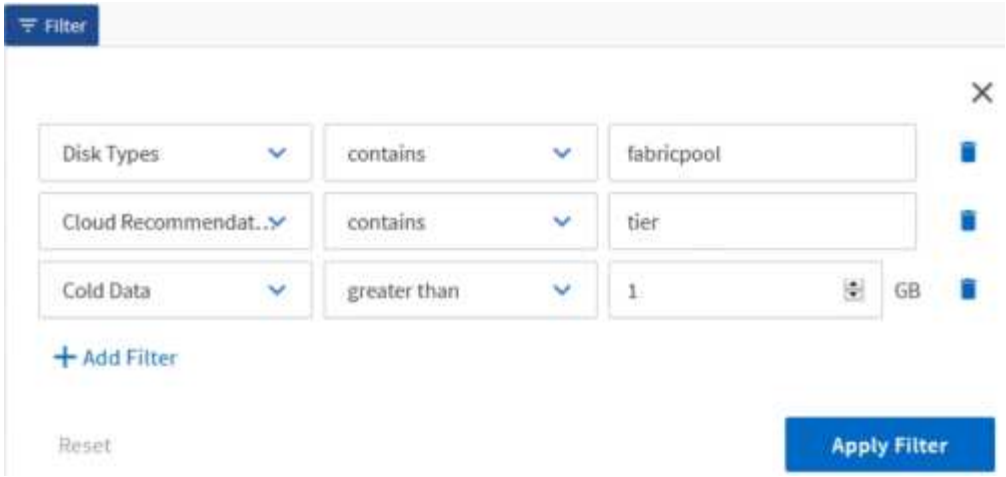
2. Sur la page d'inventaire, faites glisser les colonnes pour les réorganiser selon l'ordre de votre choix dans votre rapport.
3. Nommez la vue non enregistrée pour enregistrer vos modifications.

Filtrage des 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 cibler les résultats que vous souhaitez afficher, puis cliquez sur **appliquer le filtre**.



2. Nommez la vue non enregistrée pour enregistrer vos modifications.

Tri des données

Pour trier les résultats, cliquez sur une colonne et indiquez l'ordre croissant ou décroissant. Le tri des données classe les informations dont vous avez besoin pour le rapport.

Étapes

1. Cliquez sur le 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.

Utilisation de la fonction de recherche pour affiner votre vue

Une fois la vue souhaitée disponible, vous pouvez affiner les résultats à l'aide du champ de recherche pour mettre l'accent 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. Saisissez le champ Rechercher pour affiner les données répertoriées dans la vue. Vous pouvez entrer des données partielles dans l'une des colonnes affichées. Par exemple, si vous souhaitez rechercher des nœuds qui incluent "US_East" dans le nom, 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.

Utilisation d'Excel pour personnaliser votre rapport

Une fois la vue enregistrée, vous pouvez la télécharger au format classeur Excel (.xlsx). Lorsque vous ouvrez le fichier Excel, vous pouvez utiliser des fonctions Excel avancées pour personnaliser votre rapport.

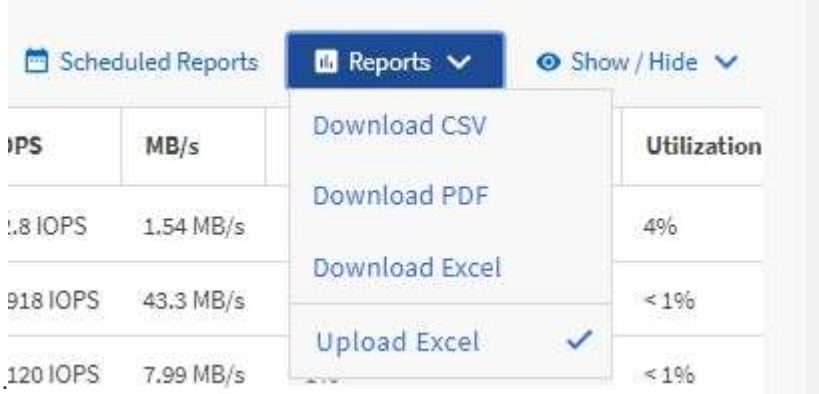
Ce dont vous aurez besoin

Vous ne pouvez charger qu'un fichier classeur Excel avec l'extension .xlsx.

Par exemple, certaines fonctions Excel avancées que vous pouvez utiliser dans votre rapport sont les suivantes :

- Tri multi-colonne
- Filtrage complexe
- Barres de coupe pivotantes
- 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 enregistrée personnalisée nommée `Volumes-not online` a un nom de fichier `health-volumes-05-May-2020-19-18-00.xlsx` si elle est enregistrée à ce jour et à cette heure.
- Vous pouvez ajouter des feuilles au fichier Excel, mais ne modifiez pas 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 "`data". Utilisez les formules de page de données pour créer des graphiques sur de nouvelles pages.
  - Ne nommez pas de nouvelles données ou informations de feuille.
- Si un fichier Excel personnalisé existe, une coche apparaît à côté de l'élément de menu **Rapports** > **Upload Excel**. Lorsque vous téléchargez le fichier Excel, la version avec les personnalisations est utilisée.



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 à un autre emplacement, enregistrez-le à l'emplacement d'origine à l'aide du nom de fichier d'origine avant de charger le fichier.
5. Personnalisez le fichier à l'aide des fonctions Excel, telles que les tri complexes, les filtres superposés, les tables de pivot ou les graphiques. Pour plus d'informations, consultez la documentation Microsoft® Excel.
6. Sélectionnez **Rapports** > **Upload Excel** et sélectionnez le fichier que vous avez modifié. Le fichier téléchargé le plus récemment est téléchargé à partir du même emplacement de fichier.
7. Envoyez-vous un rapport de test à l'aide de la fonction **Rapports programmés**.

Téléchargement de rapports

Vous pouvez télécharger des rapports et enregistrer les données sur un lecteur local ou réseau sous la forme d'un fichier CSV (valeurs séparées par des virgules), d'un fichier Microsoft Excel (.XLSX) ou d'un fichier PDF. Vous pouvez ouvrir des fichiers CSV et XLSX avec des applications de tableur, telles que Microsoft Excel, et des fichiers PDF avec des lecteurs comme Adobe Acrobat.

Étapes

1. Cliquez sur le bouton **Rapports** pour télécharger le rapport comme suit :

Choisissez	Pour…
Télécharger le CSV	Enregistrez le rapport sous la forme d'un fichier CSV (valeurs séparées par des virgules).
Télécharger le PDF	Enregistrez le rapport en tant que fichier .PDF.
Téléchargez Excel	Enregistrez le rapport sous forme de fichier Microsoft Excel (XLSX).

Planification des rapports

Après avoir une vue que vous souhaitez réutiliser et partager comme rapport, vous pouvez la planifier à l'aide de Active IQ Unified Manager. Vous pouvez gérer les rapports programmés, modifier les destinataires et la fréquence de distribution de chaque planning 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 ni planifier les tableaux de bord, les favoris ou les pages de configuration.

À partir de Active IQ Unified Manager 9.8, vous pouvez télécharger des vues au format Microsoft® Excel et les personnaliser. Vous pouvez utiliser des fonctions Excel avancées telles que des tri complexes, des filtres superposés, des tableaux croisés dynamiques et des graphiques. Lorsque vous êtes satisfait du rapport Excel obtenu, vous pouvez télécharger le fichier Excel à utiliser chaque fois que le rapport est planifié et partagé.

Vous pouvez programmer 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 attribuer en tant que seul destinataire à voir le rapport, car vos destinataires le verront.

Planification d'un rapport

Une fois que vous avez une vue ou un fichier Excel que vous souhaitez planifier pour la génération et la distribution régulières, vous pouvez planifier le rapport.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré les paramètres du serveur SMTP dans la page **général** > **Notifications** pour que le moteur de génération de rapports puisse envoyer des rapports sous forme de pièces jointes d'e-mail 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.

Procédez comme suit 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 affichant les performances de vos interfaces réseau, mais vous pouvez utiliser n'importe quelle vue que vous souhaitez.

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 en fonction des besoins à l'aide des fonctionnalités intégrées de Unified Manager.
3. Après avoir personnalisé la vue, vous pouvez fournir un nom unique dans le champ **View** 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 "Utilisation d'Excel pour personnaliser votre rapport".
5. Pour afficher 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 sous forme de fichier **CSV**, **PDF** ou **XLSX**.

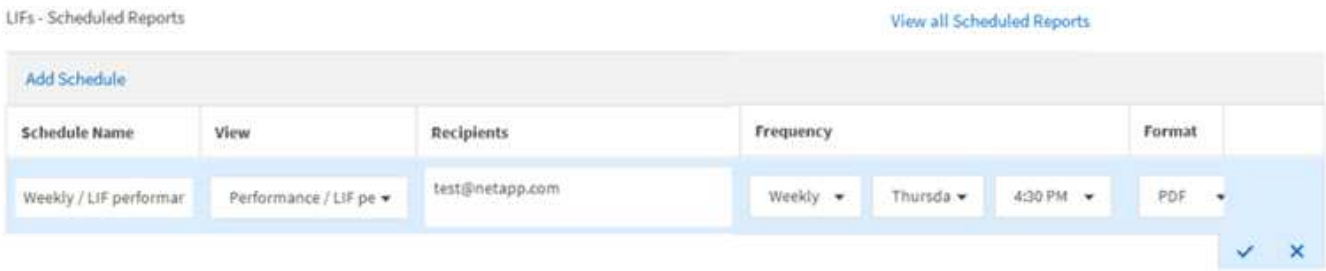
   Ouvrez le fichier avec une application installée, telle que Microsoft Excel (CSV/XSLX) ou Adobe Acrobat (PDF).

6. Si vous êtes satisfait du rapport, cliquez sur **Rapports planifiés**.
7. Dans la page programmes 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 comme **destinataire**. Lorsque vous êtes 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 **Daily**, **Weekly** ou **Monthly**.
11. Sélectionnez le format : **PDF**, **CSV** ou **XSLX**.

> Pour les rapports dans lesquels vous avez utilisé Excel pour personnaliser le contenu, sélectionnez toujours **XSLX**.

12. Cliquez sur la coche (✓) pour enregistrer le planning de rapport.



Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence programmée.

Planification des rapports .rptdesign importés

Vous pouvez planifier les rapports existants qui ont été créés et importés dans une version antérieure d'Unified Manager.

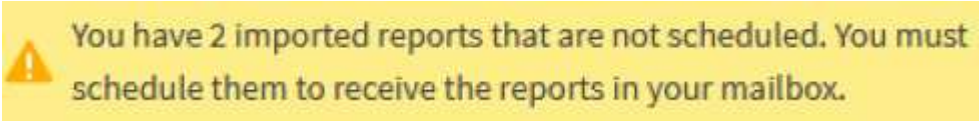
La planification des rapports importés nécessite les éléments suivants :

- Rapports de fichiers .rptdesign importés dans une version antérieure d'Unified Manager
- Applicable lors de la mise à niveau vers Unified Manager 9.6 GA ou version ultérieure

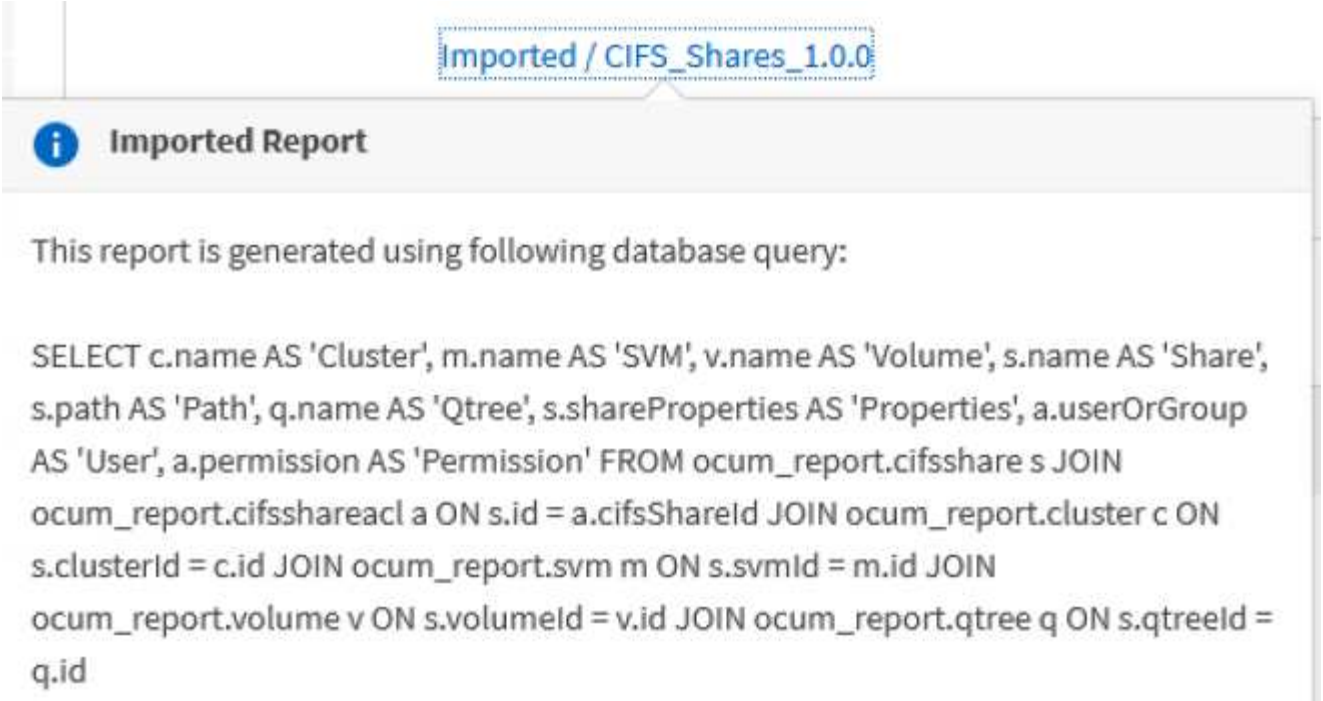
Après la mise à niveau vers Unified Manager 9.6 GA ou version ultérieure, la page Report Schedules répertorie les rapports importés. Vous pouvez modifier le planning de ces rapports pour spécifier les adresses e-mail, la fréquence et le format du destinataire (PDF ou CSV). Sinon, ces rapports ne peuvent pas être modifiés ou affichés dans l'interface utilisateur d'Unified Manager.

Étapes

1. Ouvrez la page programmes de rapport. Si vous avez importé des rapports, un message s'affiche.



2. Cliquez sur le nom **View** pour afficher la requête SQL utilisée pour générer le rapport.



3. Cliquez sur l'icône plus ⋮, cliquez sur **Modifier**, définissez les détails de la planification du rapport et enregistrez le rapport.

> Vous pouvez également supprimer tous les rapports indésirables de l'icône plus ⋮.

Gestion des planifications de rapports

Vous pouvez gérer vos planifications de rapports à partir de la page programmes de rapports. Vous pouvez afficher, modifier ou supprimer des planifications existantes.

Ce dont vous aurez besoin

> Vous ne pouvez pas programmer de nouveaux rapports à partir de la page Rapports horaires. Vous pouvez uniquement ajouter des rapports planifiés à partir des pages de stock d'objets.

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Report Schedules**.
2. Sur la page Rapports horaires :

Les fonctions que vous recherchez…	Alors…
Afficher un planning existant	Faites défiler la liste des rapports existants à l'aide des barres de défilement et des commandes de page.

Les fonctions que vous recherchez…	Alors…
Modifier une planification existante	a. Cliquez sur l'icône plus ⋮ correspondant à l'horaire que vous souhaitez utiliser. b. Cliquez sur **Modifier**. c. Apportez les modifications nécessaires. d. Cliquez sur la coche pour enregistrer vos modifications.
Supprimer une planification existante	a. Cliquez sur l'icône plus ⋮ correspondant à l'horaire que vous souhaitez utiliser. b. Cliquez sur **Supprimer**. c. Confirmez votre décision.

Modification des rapports planifiés

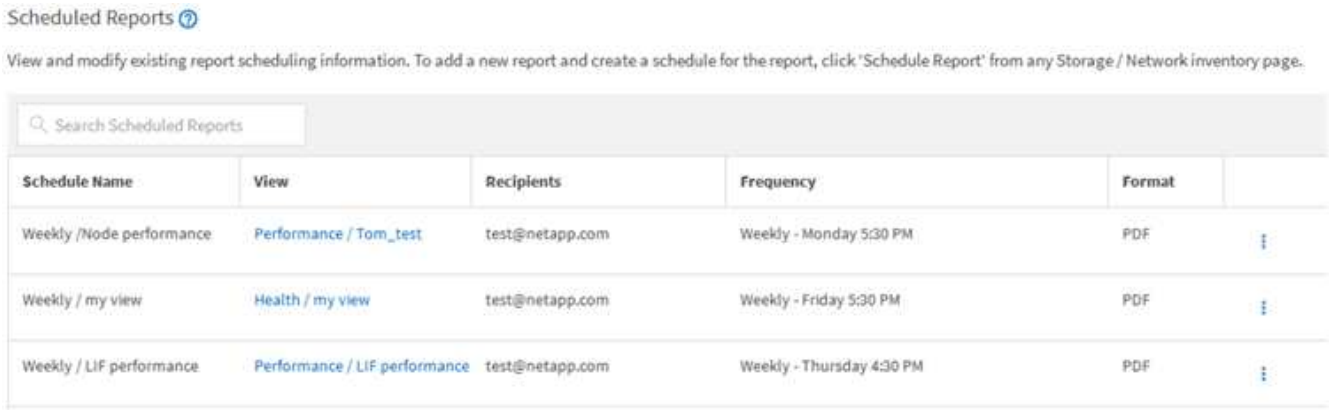
Une fois les rapports planifiés, vous pouvez les modifier sur la page Rapports programmes.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Report Schedules**.



> Si vous disposez des autorisations appropriées, vous pouvez modifier n'importe quel rapport et son planning dans le système.

2. Cliquez sur l'icône plus ⋮ correspondant à l'horaire que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Vous pouvez modifier le **Nom de l'annexe**, **liste des destinataires**, **fréquence** et **format** pour le calendrier des rapports.

5. Lorsque vous avez terminé, cliquez sur la coche pour enregistrer vos modifications.

Suppression de rapports planifiés

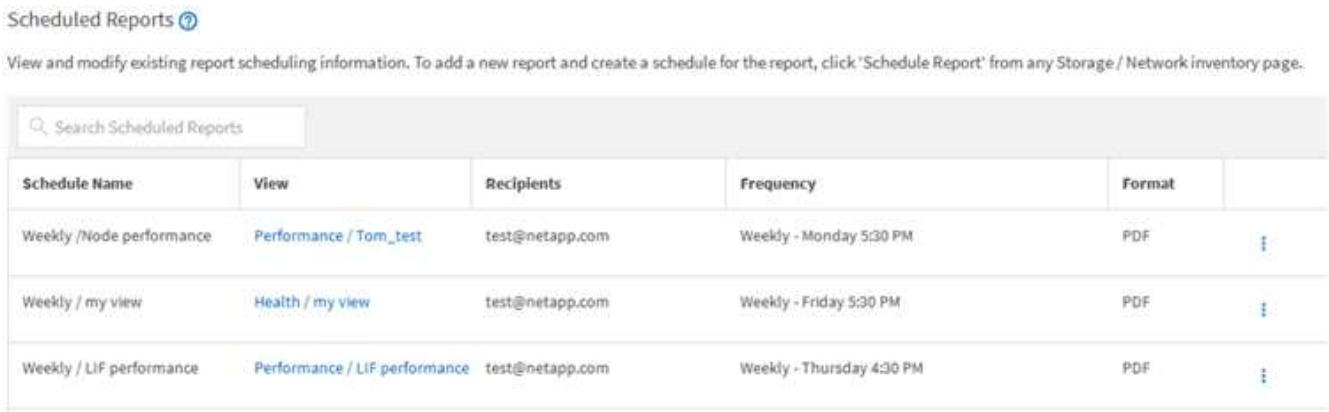
Une fois les rapports programmés, vous pouvez les supprimer de la page Rapports programmes.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Report Schedules**.



> Si vous disposez des autorisations appropriées, vous pouvez supprimer tout rapport et son planning dans le système.

2. Cliquez sur l'icône plus ⋮ correspondant à la planification 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 et distribué sur le planning 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 généralement utilisés pour vous aider à identifier les problèmes potentiels et à résoudre les problèmes potentiels avant qu'ils ne surviennent.

La liste des rapports de cette section n'est pas exhaustive et va s'accroître au fil du temps. Vous pouvez suggérer des rapports personnalisés à ajouter à cette section en fournissant des commentaires sur la documentation.

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage pour gérer les rapports.

Personnalisation des rapports de stockage de cluster

Les exemples de rapports sur le stockage en cluster présentés dans cette section ne sont que des exemples pour vous aider à comprendre comment créer des rapports sur la capacité du cluster afin de vous aider à surveiller les ressources du système de stockage.

Création d'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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant la capacité par modèle de cluster, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes, telles que « FQDN du cluster » et « version du système d'exploitation », que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser les colonnes ""Total Raw Capacity"", "Model/Family" et les trois colonnes agrégées près de la colonne "Cluster".
5. Cliquez sur le haut de la colonne "Model/famille" pour trier les résultats par type de cluster.
6. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple, « Capacity by Cluster Model » (capacité par modèle de cluster).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Add Schedule** pour ajouter une nouvelle ligne à la page **Report Schedules** afin que vous puissiez définir les caractéristiques du planning pour le nouveau rapport.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez vouloir ajouter de la capacité à certains clusters ou mettre à niveau les anciens modèles de cluster.

Créez un rapport pour identifier les clusters dont la capacité LUN est la plus non allouée

Vous pouvez créer un rapport pour trouver les clusters dont la capacité LUN n'est pas allouée est la plus élevée et où 5 To, afin de faciliter l'identification des emplacements où

ajouter des workloads supplémentaires.

Ce dont vous avez besoin * vous devez avoir le rôle d'administrateur d'applications ou d'administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les clusters dont la capacité de LUN est la plus non allouée, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **clusters**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « Unallocated LUN Capacity » près de la colonne « HA pair » (paire HA).
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **appliquer le filtre** :
   - Capacité de LUN non allouée supérieure à 0.5 To
6. Cliquez sur la partie supérieure de la colonne « capacité LUN non allouée » pour trier les résultats par 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 non allouée la plus' » et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
10. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

D'après les résultats affichés dans le rapport, il est possible que vous souhaitiez utiliser la capacité de LUN non allouée du cluster.

Création d'un rapport pour afficher les paires haute disponibilité avec la capacité la plus disponible

Vous pouvez créer un rapport pour trouver les paires haute disponibilité avec la plus grande capacité de provisionnement de nouveaux volumes et de nouvelles LUN.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les paires haute disponibilité 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 **Storage** > **clusters**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les clusters**.

3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « capacité inutilisée agrégée » près de la colonne « paire HA ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **appliquer le filtre** :
   - Capacité non utilisée de l'agrégat supérieure à 0.5 To
6. Cliquez sur la partie supérieure de la colonne « capacité non utilisée totale » pour trier les résultats par la plus grande quantité de capacité totale inutilisée.
7. Enregistrer la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « capacité agrégée la moins utilisée », et cliquer sur la coche (✓).
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
10. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez équilibrer les paires haute disponibilité en fonction de la capacité des agrégats.

Création d'un rapport pour afficher les nœuds exécutant d'anciennes versions de ONTAP

Vous pouvez créer un rapport pour afficher la version du logiciel ONTAP installée sur tous les nœuds du cluster. Ainsi, vous pouvez voir les nœuds à mettre à niveau.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les nœuds exécutant d'anciennes versions de ONTAP, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Nodes**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
3. Faites glisser la colonne « version OS » près de la colonne « nœud ».
4. Cliquez sur le haut de la colonne « version OS » pour trier les résultats par la version la plus ancienne de ONTAP.
5. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple, « noeuds par version ONTAP ».
6. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
7. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
8. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

Basé sur les résultats présentés dans ce rapport, vous pouvez mettre à niveau les nœuds exécutant d'anciennes versions de ONTAP.

Personnalisation des rapports de capacité d'agrégats

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier les problèmes potentiels liés à la capacité de stockage des agrégats et à y répondre.

Les rapports de cette section ne sont que des exemples pour vous aider à comprendre comment créer des rapports sur la capacité globale afin de vous aider à surveiller les ressources du système de stockage.

Création d'un rapport pour afficher les agrégats dont la capacité est maximale

Vous pouvez créer un rapport pour localiser les agrégats arrivant à pleine capacité, afin de pouvoir ajouter de la capacité ou déplacer les charges de travail vers d'autres agrégats.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les agrégats qui atteignent leur pleine capacité, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **appliquer le filtre** :
   - Jours complets à moins de 45 jours
5. Cliquez sur la partie supérieure de la colonne "Days to Full" pour trier les résultats par le moins 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, « `Days to full aggregate Capacity` », et cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Add Schedule** pour ajouter une nouvelle ligne à la page **Report Schedules** afin que vous puissiez définir les caractéristiques du planning pour le nouveau rapport.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez augmenter le stockage sur les agrégats pour

atteindre pleinement leur capacité. Par ailleurs, vous pouvez vouloir augmenter le nombre de jours jusqu'à ce que la capacité totale soit supérieure à la valeur par défaut de 7 jours. Ainsi, vous recevez des événements qui donnent plus de temps à réagir en cas de faible quantité d'espace disponible sur les agrégats.

Création d'un rapport pour afficher les agrégats complets d'au moins 80 %

Vous pouvez créer un rapport pour mettre en évidence les agrégats remplis à 80 % ou plus.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant des agrégats complets d'au moins 80 %, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser les colonnes « % de données disponibles » et « % de données utilisées » près de la colonne « agrégat ».
5. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **appliquer le filtre** :
   - Données utilisées % supérieur à 80 %
6. Cliquez sur le 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 affiche, par exemple, « agrégats approchant le plein », puis cliquez sur la coche (✓) .
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
10. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez vouloir déplacer des données depuis certains agrégats.

Création d'un rapport pour afficher les agrégats qui sont surengagés

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des agrégats, et pour afficher les agrégats dont la surallocation est de l'exploitation.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les agrégats dépassant le seuil dépassé, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « % de capacité excédentaire » 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 excédentaire est supérieur à 100 %
6. Cliquez sur le haut de la colonne « % de capacité excédentaire » 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 sur-validés », puis cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
10. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez ajouter de la capacité aux agrégats ou déplacer des données depuis certains agrégats.

Personnalisation des rapports de capacité de volume

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier et à résoudre les problèmes potentiels liés à la capacité de volume et aux performances.

Création d'un rapport pour identifier les volumes dont la suppression automatique de l'instantané est désactivée sur la capacité maximale

Vous pouvez créer un rapport contenant la liste des volumes dont la capacité est proche de celle maximale avec la fonction de suppression automatique de l'instantané désactivée. Les résultats peuvent vous aider à identifier les volumes dans lesquels vous souhaitez configurer la suppression automatique des snapshots.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les colonnes requises dans l'ordre correct, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser et déposez les colonnes "`napshot Autodelete'" et "Days to Full" près de la colonne "Available Data Capacity".
5. Cliquez sur l'icône de filtre, ajoutez les deux filtres suivants, puis cliquez sur **appliquer le filtre** :
   - Jours complets à moins de 30 jours
   - La suppression automatique de l'instantané est désactivée
6. Cliquez sur le haut de la colonne **jours à plein** 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 montre, par exemple « vols proches capacité ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans le rapport, vous pouvez activer la suppression automatique des snapshots sur les volumes ou trouver un moyen d'augmenter l'espace disponible.

Création d'un rapport permettant d'identifier l'espace utilisé par les volumes dont l'allocation dynamique est désactivée

Lorsqu'un volume n'est pas à provisionnement fin, il occupe la totalité de l'espace sur le disque, comme défini lors de la création du volume. L'identification des volumes dont le provisionnement fin est désactivé vous permet de décider si vous souhaitez activer le provisionnement fin sur certains volumes.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les colonnes requises dans l'ordre correct, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **capacité** > **tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Glissez-déposez les colonnes « % de données utilisées » et « provisionnement fin » près de la colonne « capacité de données disponible ».

5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, **Thin Provisioned** est **No**, puis cliquez sur **Apply Filter**.
6. Cliquez sur le haut de la colonne « % de données utilisées » pour trier les résultats de sorte que les volumes dont le pourcentage est le plus élevé apparaissent en haut de la liste.
7. Enregistrez la vue avec un nom pour refléter ce que la vue est affichée, par exemple « vols no thin provisioning ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page **Rapports horaires** afin de définir les caractéristiques du nouveau rapport.
10. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez activer le provisionnement fin sur certains volumes.

Création d'un rapport pour identifier les volumes de données stockées dans les agrégats FabricPool qui doivent être déplacées vers le Tier cloud

Vous pouvez créer un rapport contenant la liste des volumes résidant sur des agrégats FabricPool, dont les recommandations pour le cloud sont nombreuses et dont les données inactives sont importantes. Ce rapport vous aidera à décider si vous devez modifier la règle de Tiering de certains volumes en « auto » ou « toutes » pour décharger des données plus inactives vers le Tier cloud.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez avoir configuré des agrégats FabricPool et certains volumes sur ces agrégats.

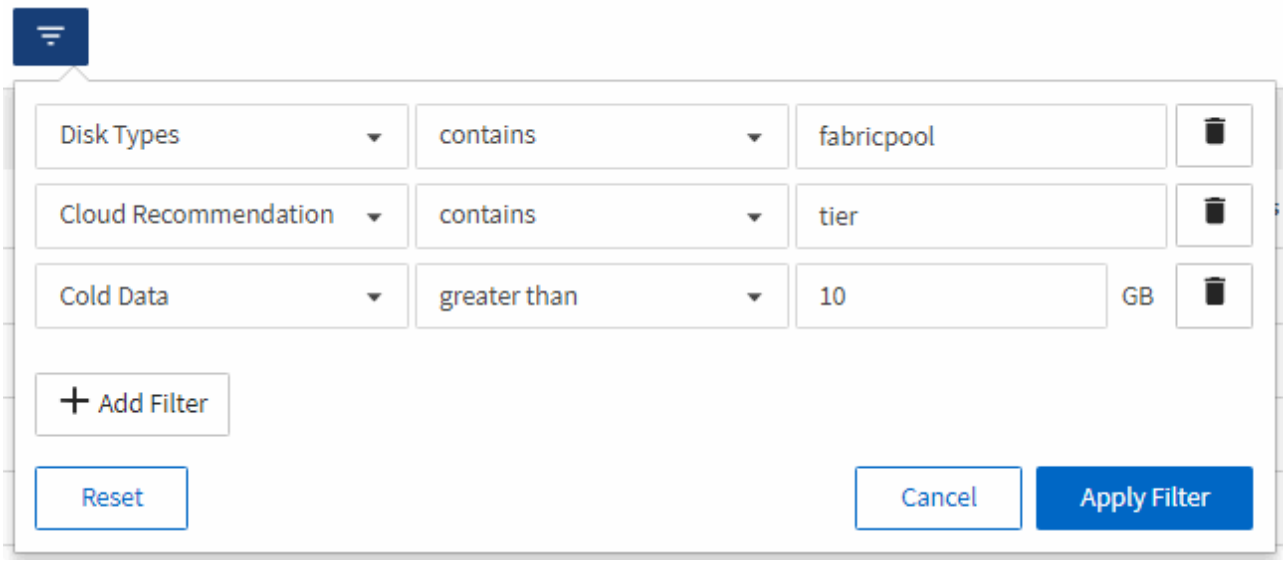
Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les colonnes requises dans l'ordre correct, puis planifiez la génération d'un rapport pour cette vue.

Étapes

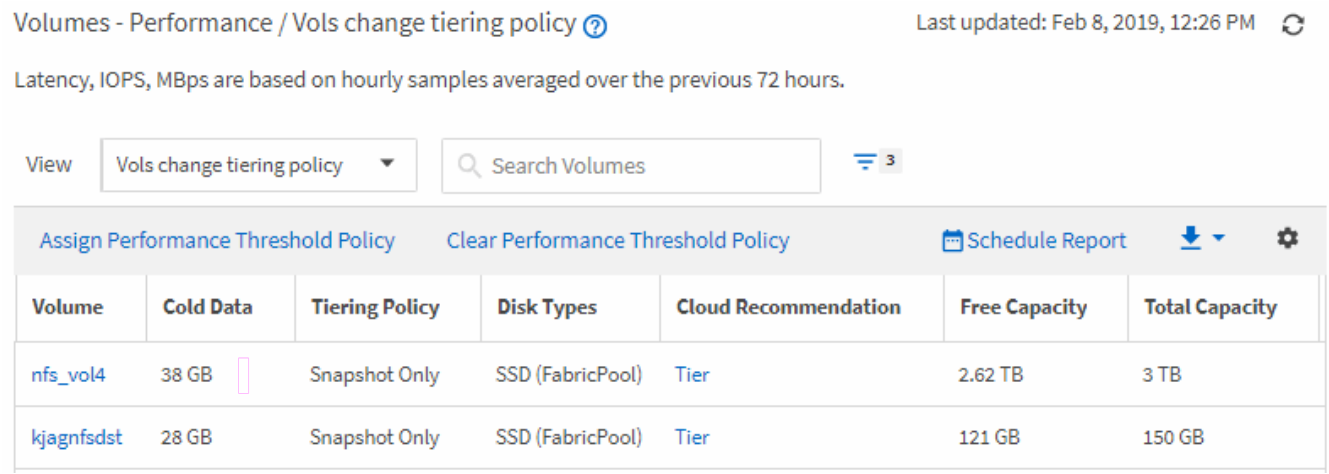
1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **Performance** > **tous les volumes**.
3. Dans le sélecteur de colonne, assurez-vous que la colonne "Type de disque" apparaît dans la vue.

   Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Glissez-déposez la colonne "Type de disque" près de la colonne "Recommandation du Cloud".
5. Cliquez sur l'icône de filtre, ajoutez les trois filtres suivants, puis cliquez sur **appliquer le filtre** :
   - Le type de disque contient la FabricPool
   - La recommandation cloud contient le Tier
   - Données inactives supérieures à 10 Go



6. Cliquez sur la partie supérieure de la colonne données froides pour que les volumes avec les données les plus froides apparaissent en haut de la vue.
7. Sauvegardez la vue avec un nom qui reflète la vue, par exemple « les volumes changent la politique de Tiering
».



8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
10. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez utiliser System Manager ou l'interface de ligne de commande d'ONTAP pour modifier la règle de Tiering en « automatique » ou « toutes » pour certains volumes, afin de décharger davantage de données inactives vers le Tier cloud.

Personnalisation des rapports de capacité qtree

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier les

problèmes potentiels liés à la capacité de qtree et à y répondre.

Création d'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 afficher les qtrees presque pleins.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les qtrees presque pleins, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Qtrees**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure 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 % utilisé du disque est supérieur à 75 %
5. Cliquez sur le haut de la colonne "disque utilisé %" pour trier les résultats par pourcentage de capacité.
6. Enregistrez la vue avec un nom spécifique qui reflète l'affichage de la vue, par exemple « Qtrees Nearing full » », puis cochez la case (✓).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page **Rapports horaires** afin de définir les caractéristiques du nouveau rapport.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, il est possible de modifier les limites matérielles et logicielles du disque (si elles sont définies) ou d'équilibrer les données sur l'ensemble des qtrees.

Personnalisation des rapports de partage NFS

Vous pouvez personnaliser des rapports de partage NFS pour analyser des informations sur les règles d'exportation NFS et les volumes de vos systèmes de stockage. Vous pouvez par exemple personnaliser les rapports pour afficher les volumes dont les volumes et les chemins de montage sont inaccessibles avec l'export policy par défaut.

Création d'un rapport pour afficher les volumes dont le chemin de montage est inaccessible

Vous pouvez créer un rapport pour rechercher des volumes dont le chemin de montage est inaccessible.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée pour les volumes ayant un chemin de montage inaccessible, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **NFS Shares**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure 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 un programme** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
7. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous pouvez corriger les chemins de montage inaccessibles.

Création d'un rapport pour afficher les volumes qui utilisent l'export policy par défaut

Vous pouvez créer un rapport pour rechercher les volumes qui utilisent la stratégie d'exportation par défaut.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée pour les volumes qui utilisent la règle d'exportation par défaut, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **NFS Shares**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure 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** :
   - Export policy contient la valeur par défaut
5. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « « volumes avec une export policy par défaut » et cliquez sur la coche (✓).

6. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
7. Cliquez sur **Ajouter un programme** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
8. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous pouvez vouloir configurer une règle d'exportation personnalisée.

Personnalisation des rapports sur les machines virtuelles de stockage

Vous pouvez créer des rapports sur les VM de stockage afin d'analyser les informations sur les volumes et de consulter l'état global et la disponibilité du stockage. Par exemple, vous pouvez créer des rapports pour afficher les SVM atteignant le nombre maximal de volumes et pour analyser les SVM arrêtés.

Création d'un rapport pour afficher les VM de stockage dont le volume maximal est atteint

Vous pouvez créer un rapport pour trouver des SVM atteignant la limite du volume maximal.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les VM de stockage qui atteignent la limite maximale du volume, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Storage VM**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
3. Faites glisser les colonnes ""Volume Count"" et "Maimum allowed volumes" près de la colonne "Storage VM".
4. Cliquez sur la partie supérieure de la colonne "Volume autorisé au maximum" pour trier les résultats par le plus grand nombre de volumes.
5. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple "machines virtuelles atteignant max volumes" et cliquez sur la coche (✓).
6. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
7. Cliquez sur **Add Schedule** pour ajouter une nouvelle ligne à la page **Report Schedules** afin que vous puissiez définir les caractéristiques du planning pour le nouveau rapport.
8. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-

mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez équilibrer les volumes affectés aux machines virtuelles de stockage ou, si possible, utiliser ONTAP System Manager pour modifier le nombre maximal de volumes autorisés.

Création d'un rapport pour afficher les machines virtuelles de stockage arrêtées

Vous pouvez créer un rapport pour afficher la liste de tous les SVM arrêtés.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée affichant les machines virtuelles de stockage arrêtées, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Storage VM**.
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 inclure dans le rapport.
4. Faites glisser la colonne "Enregistrer`" près de la colonne "Storage VM".
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **appliquer le filtre** :
   - L'état est arrêté
6. Enregistrer la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « `SVMs en tête " » et cocher la case (✓).
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Cliquez sur **Add Schedule** pour ajouter une nouvelle ligne à la page **Report Schedules** afin que vous puissiez définir les caractéristiques du planning pour le nouveau rapport.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pourriez chercher à déterminer pourquoi le SVM est arrêté pour voir si vous devez redémarrer les SVM arrêtés.

Personnalisation des rapports de relation de volume

Le rapport Volume Relationships Inventory vous permet d'analyser les détails de l'inventaire du 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.

Création d’un rapport pour regrouper les relations de volume par source d’échec

Vous pouvez créer un rapport qui regroupe des volumes en raison de la mauvaise santé de la relation.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée qui regroupe les volumes par source d’échec, puis planifier la génération d’un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **relation** > **toutes les relations**.
3. Sélectionnez **Afficher/Masquer** pour vous assurer que les colonnes « Santé des relations » 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 « relation Health » et « mauvaise raison » près de la colonne « Enregistrer ».
5. Cliquez sur l’icône de filtre, ajoutez le filtre suivant, puis cliquez sur **appliquer le filtre** :
   - La santé de la relation est mauvaise
6. Cliquez sur le haut de la colonne « raison malsaine » pour regrouper les relations de volume par source d’échec.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple, « vol relations par échec ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d’inventaire.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l’aide de la fréquence spécifiée.

En fonction des résultats présentés dans le rapport, vous pouvez étudier la source et l’impact de chaque type de défaillance.

Création d’un rapport pour regrouper les relations de volume par problème

Vous pouvez créer un rapport qui regroupe les relations de volume par problème.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée qui regroupe les relations de volume par problème, puis planifier la génération d’un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.

2. Dans le menu Affichage, sélectionnez **relation** > **toutes les relations**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « motif malsain » près de la colonne « Enregistrer ».
5. Cliquez sur le haut de la colonne « raison malsaine » pour regrouper les volumes par numéro.
6. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue montre, par exemple, « vol relations par numéro ».
7. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
8. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans le rapport, vous pouvez étudier la source et l'impact de chaque type de problème.

Création d'un rapport pour visualiser 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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée des volumes à des intervalles de temps spécifiques, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **relation** > **État transfert du dernier mois**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure 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 sur la partie supérieure de la colonne « durée du 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. Entrez un nom pour la planification du rapport, définissez la fréquence sur **hebdomadaire** et renseignez les autres champs de rapport, puis cliquez sur la coche () à la✓ fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-

mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous pouvez étudier les intervalles de temps de transfert.

Création d'un rapport pour afficher le transfert de volume ayant échoué ou réussi

Vous pouvez créer un rapport qui affiche l'état des transferts de volume. Vous pouvez afficher les transferts de volumes ayant échoué et ayant réussi dans ce rapport.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée pour afficher les transferts ayant échoué et les transferts réussis, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **relation** > **État transfert du dernier mois**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « résultat d'opération » près de la colonne « Enregistrer ».
5. Cliquez sur le haut de la colonne « résultat d'opération » pour trier les volumes selon l'état.
6. Enregistrez la vue avec 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. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous pouvez étudier l'état du transfert.

Création d'un rapport pour afficher les transferts de volumes en fonction de la taille du transfert

Vous pouvez créer un rapport pour afficher les transferts de volumes en fonction de la taille du transfert.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée des transferts de volume en fonction de la taille du transfert, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **relation** > **taux de transfert du dernier mois**.

3. Cliquez sur le haut de la colonne « taille totale de transfert » pour trier les transferts de volume par taille.
4. Enregistrez la vue avec 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. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans le rapport, vous pouvez étudier les relations de volume en fonction de la taille du transfert.

Création d'un rapport pour afficher les transferts de volumes regroupés par jour

Vous pouvez créer un rapport pour afficher les transferts de volumes regroupés par jour.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Utilisez 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 **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **relation** > **taux de transfert du dernier mois**.
3. Cliquez sur le haut de la colonne "Day" 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. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans ce rapport, vous pouvez étudier les transferts de volume au quotidien.

Personnalisation des rapports de performances des volumes

Ces exemples de rapports personnalisés sont utilisés pour vous aider à identifier les problèmes potentiels liés aux performances des volumes et à y répondre.

Création d'un rapport permettant d'afficher les volumes dont le volume de données inactives est élevé sur un agrégat non compatible FabricPool

Vous pouvez créer un rapport pour afficher les volumes contenant une quantité importante de données inactives sur un agrégat non FabricPool. Cela peut vous aider à

identifier les volumes à transférer vers un agrégat FabricPool.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour créer une vue personnalisée pour les volumes contenant une quantité importante de données inactives sur un agrégat non compatible avec FabricPool, puis planifier la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **Performance** > **tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour vous assurer que la colonne "Type de disque" s'affiche 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 inactives supérieures à 100 Go
   - Le type de disque contient un disque SSD
6. Cliquez sur le haut de la colonne "Type de disque" pour trier les volumes par type de disque de sorte 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 « les volumes de données inactives pas FabricPool ».
8. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire.
9. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats affichés dans ce rapport, vous pouvez trouver des volumes qui présentent de bons candidats à déplacer vers des agrégats FabricPool.

Exemples de rapports Microsoft Excel

Ces exemples de rapports Microsoft Excel sont destinés à présenter les options de reporting disponibles à l'aide des fonctions avancées d'Excel.

La fonctionnalité avancée d'Excel peut créer un large éventail de rapports spécifiques à vos besoins. Pour obtenir des informations complètes sur l'utilisation d'Excel, reportez-vous à la documentation du produit.

> Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage pour gérer les rapports.

Création d’un rapport pour afficher une table et un graphique de capacité d’agrégat

Vous pouvez créer un rapport pour analyser la capacité dans un fichier Excel en utilisant les totaux additionnés et le format de graphique de colonnes en cluster.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d’applications ou Administrateur de stockage.

Procédez comme suit pour ouvrir une vue Santé : tous les agrégats, télécharger la vue dans Excel, créer un graphique des capacités disponibles, télécharger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Sélectionnez **Rapports** > **Télécharger Excel**.

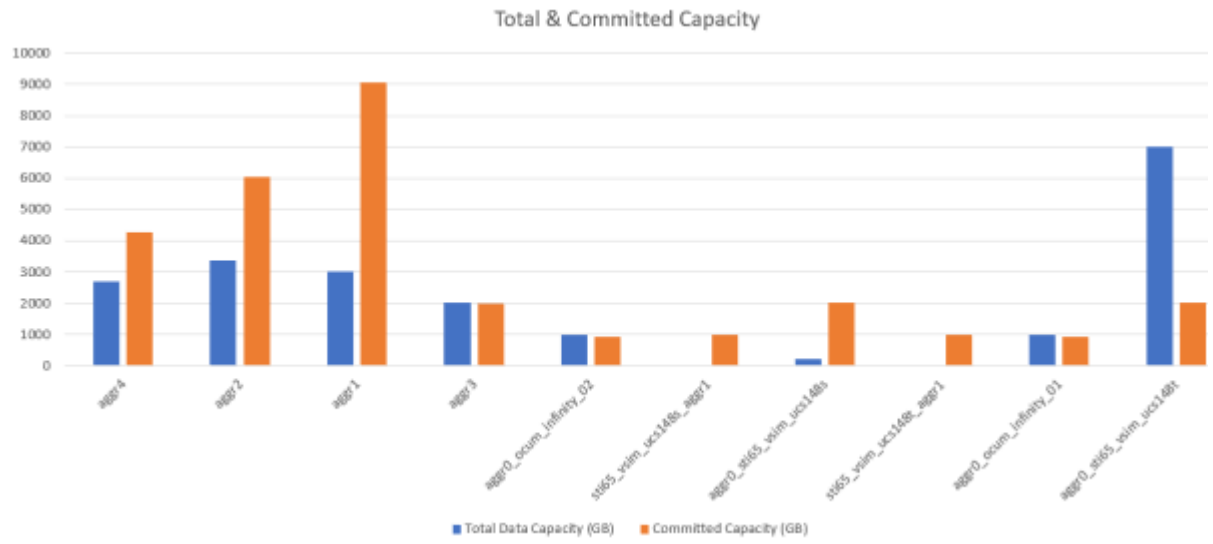
   Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

3. Si nécessaire, cliquez sur **Activer la modification**.
4. Dans Excel, ouvrez le fichier téléchargé.
5. Créez une nouvelle feuille (⊕) après la `data` feuille et nommez-la **capacité totale de données**.
6. Ajoutez les colonnes suivantes dans la nouvelle feuille capacité totale des données :
   a. Capacité totale des 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, entrez la formule suivante, en vous assurant qu’elle référence la feuille de données (data!) et référence les spécificateurs de colonne et de ligne corrects pour les données capturées (Total Data Capacity extrait les données de la colonne E, des lignes 2 à 20).
   a. =SUM(data!E$2:data!E$20)
   b. =SUM(data!F$2:data!F$50)
   c. =SUM(data!G$2:data!G$50)
   d. =SUM(data!H$2:data!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 fiche de données, sélectionnez les colonnes **capacité totale de données (Go)** et **capacité engagée (Go)**.
2. Sélectionnez **tableaux recommandés** dans le menu **Insert** et sélectionnez le graphique **clustered Column**.
3. Cliquez avec le bouton droit de la souris sur le graphique et sélectionnez **déplacer le graphique** pour le déplacer vers la `Total Data Capacity` feuille.
4. Les menus **Design** 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 ou l'emplacement du fichier.

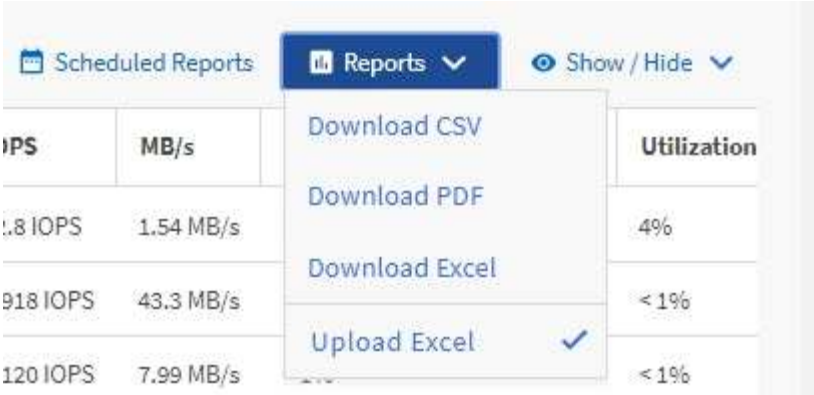


6. Dans Unified Manager, sélectionnez **Rapports** > **Upload Excel**.

> Assurez-vous que vous vous trouvez dans la même vue que celle 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 en regard de l'option de menu **Rapports** > **Télécharger Excel**.



10. Cliquez sur **Rapports planifiés**.
11. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.

    Sélectionnez le format **XLSX** pour le rapport.

12. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

Sur la base des résultats présentés dans ce rapport, vous voudrez peut-être étudier la meilleure façon d'utiliser la capacité disponible sur votre réseau.

Création d'un rapport pour afficher le total des agrégats par rapport aux graphiques de capacité disponible

Vous pouvez créer un rapport pour analyser le total du stockage et la capacité engagée au format Excel.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

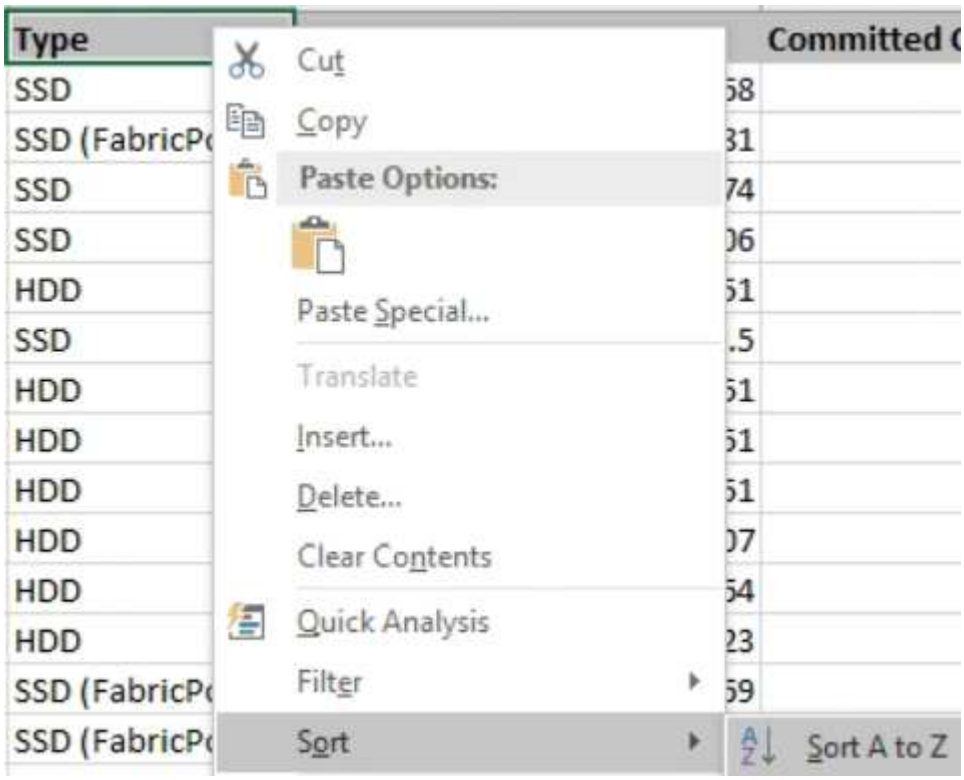
Procédez comme suit pour ouvrir une vue Santé : tous les agrégats, télécharger la vue dans Excel, créer un graphique des capacités totales et allouées, charger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
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 de la souris sur la colonne Type et sélectionnez **Trier** > **Trier A à Z**.



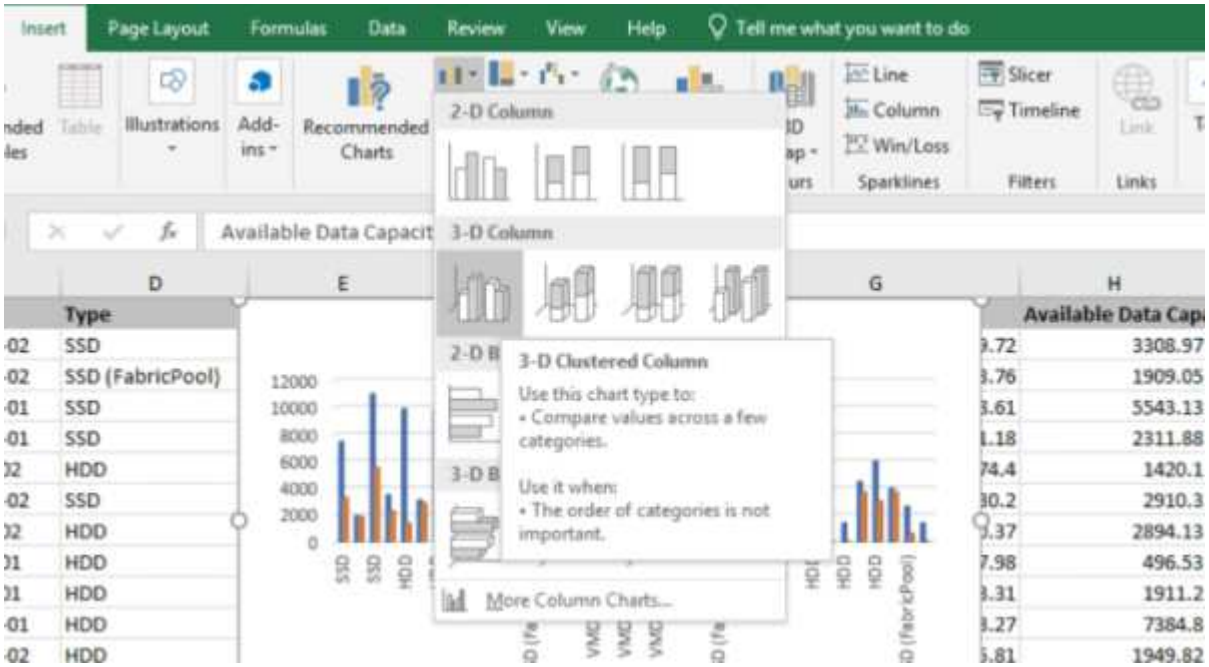
Cette action organisera vos données en fonction du type de stockage :

- DISQUES DURS
- Hybride
- SSD
- SSD (FabricPool)

6. Sélectionnez les `Type`, `Total Data Capacity`, colonnes et `Available Data Capacity`.

7. Dans le menu **Insérer**, sélectionnez un `3-D column` graphique.

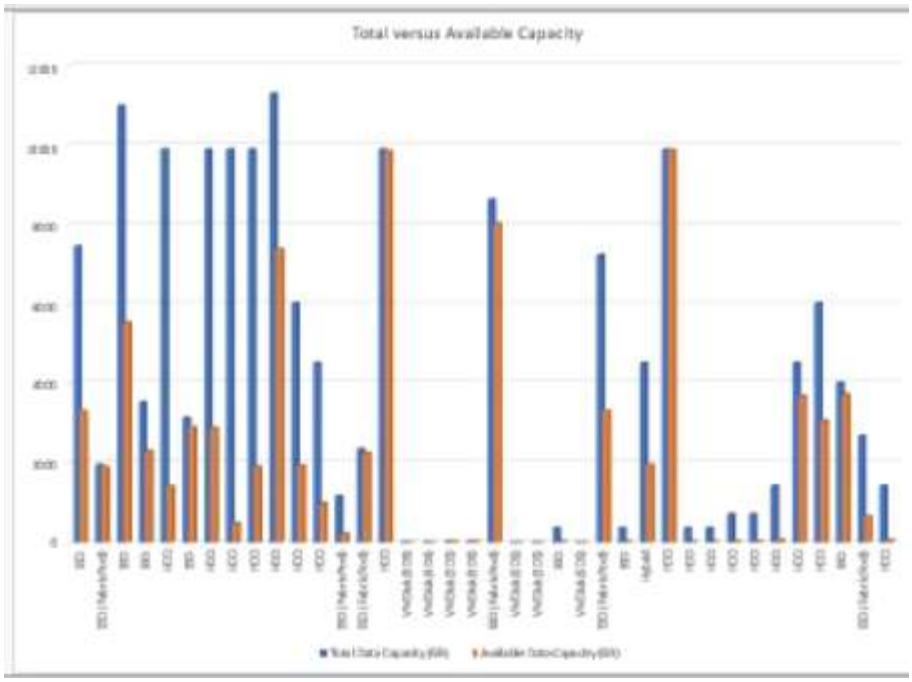
   Le graphique apparaît sur la feuille de données.



8. Cliquez avec le bouton droit de la souris sur le graphique et sélectionnez **déplacer le graphique**.
9. Sélectionnez **Nouvelle feuille** et nommez la feuille **cartes de stockage totales**.

   Assurez-vous que la nouvelle feuille apparaît après les fiches d'informations et de données.

10. Nommez le titre du graphique **Total par rapport à la capacité disponible**.
11. Les menus **Design** 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 ou l'emplacement du fichier.

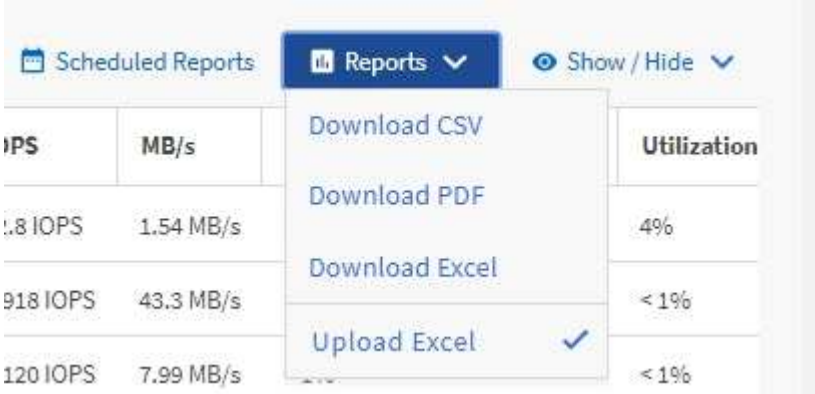


13. Dans Unified Manager, sélectionnez **Rapports** > **Upload Excel**.

> Assurez-vous que vous vous trouvez dans la même vue que celle 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 en regard de l'option de menu **Rapports** > **Télécharger Excel**.



17. Cliquez sur **Rapports planifiés**.
18. Cliquez sur **Add Schedule** pour ajouter une nouvelle ligne à la page **Report Schedules** afin que vous puissiez définir les caractéristiques du planning pour le nouveau rapport.

> Sélectionnez le format **XLSX** pour le rapport.

19. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez équilibrer la charge sur vos agrégats.

Création d'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.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour ouvrir une vue Santé : tous les volumes, télécharger la vue dans Excel, créer un graphique des capacités disponibles, télécharger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Sélectionnez **Rapports** > **Télécharger Excel**.

   Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

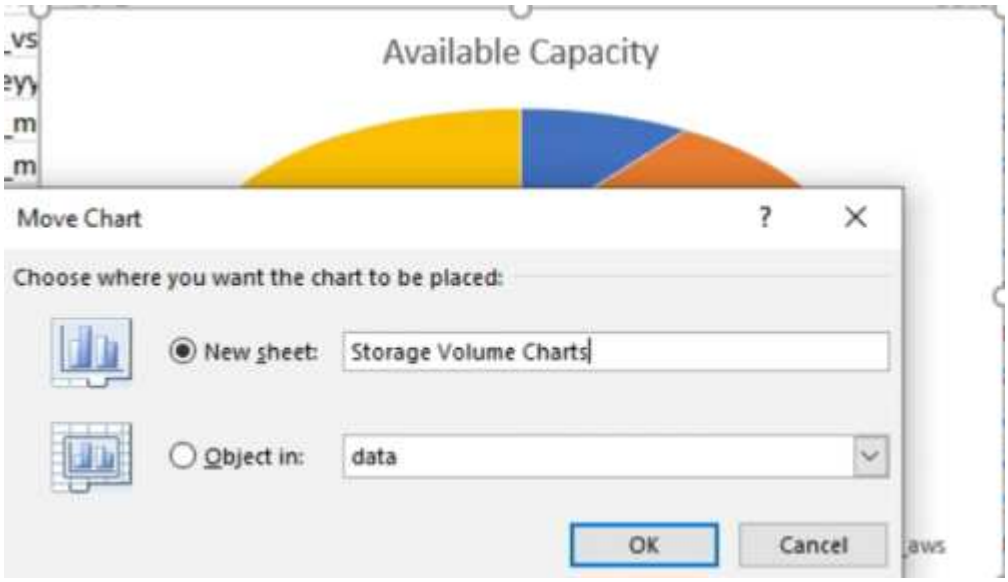
3. Si nécessaire, cliquez sur **Activer la modification**.
4. Dans Excel, ouvrez le fichier téléchargé.
5. Sur la `data` feuille, sélectionnez les données à utiliser dans les `Volume` colonnes et `Available Data` %.
6. Dans le menu **Insérer**, sélectionnez un `3-D piechart`.

   Le graphique indique quels volumes disposent du plus grand espace disponible. Le graphique apparaît sur la feuille de données.

> Selon la configuration de votre réseau, la sélection de colonnes entières ou de lignes de données trop nombreuses peut rendre votre graphique circulaire illisible. Cet exemple utilise le graphique à secteurs 3-D, 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 de la souris sur le graphique et sélectionnez **déplacer le graphique**.
9. Sélectionnez **Nouvelle feuille** et nommez la feuille **cartes du volume de stockage**.

> Assurez-vous que la nouvelle feuille apparaît après les fiches d'informations et de données.

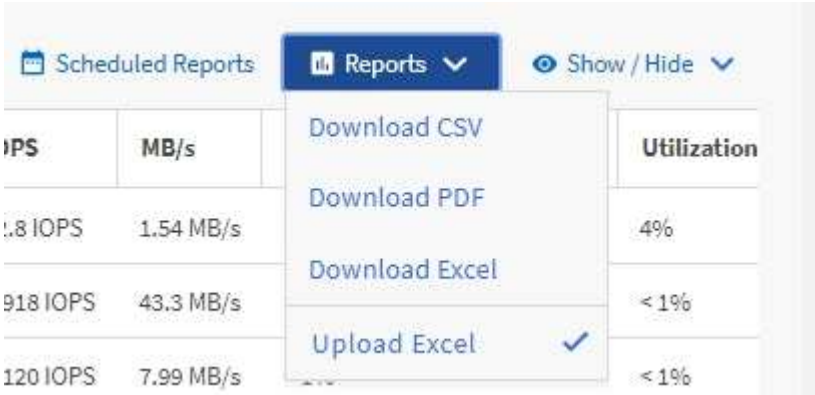


10. Les menus **Design** et **format**, disponibles lorsque le graphique est sélectionné, vous pouvez personnaliser l'apparence du graphique.
11. Lorsque vous êtes satisfait, enregistrez le fichier avec vos modifications.
12. Dans Unified Manager, sélectionnez **Rapports** > **Upload Excel**.

> Assurez-vous que vous vous trouvez dans la même vue que celle 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 en regard de l'option de menu **Rapports** > **Télécharger Excel**.



16. Cliquez sur **Rapports planifiés**.

17. Cliquez sur **Add Schedule** pour ajouter une nouvelle ligne à la page **Report Schedules** afin que vous puissiez définir les caractéristiques du planning pour le nouveau rapport.
18. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    > Sélectionnez le format **XLSX** pour le rapport.

    Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, il est possible que vous souhaitiez équilibrer la charge sur vos volumes.

Créez un rapport pour afficher les agrégats dont les IOPS sont les plus disponibles

Ce rapport indique les agrégats qui disposent des IOPS par type d'agrégat les plus disponibles, sur lesquels vous pouvez provisionner de nouvelles charges de travail.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Procédez comme suit pour ouvrir une vue Santé : tous les volumes, télécharger la vue dans Excel, créer un graphique des capacités disponibles, télécharger le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Aggregates**.
2. Sélectionnez **Performance : tous les agrégats** dans la liste déroulante **View**.
3. Sélectionnez **Afficher/Masquer** pour afficher la `Available IOPS` colonne et masquer les `Cluster FQDN, Inactive Data Reporting,` colonnes et `Threshold Policy`.
4. Faites glisser et déposez les `Available IOPS` colonnes et `Free Capacity` en regard de la `Type` colonne.
5. Nommer et enregistrer la vue personnalisée `Available IOPS Per Aggr.`
6. Sélectionnez **Rapports** > **Télécharger Excel**.

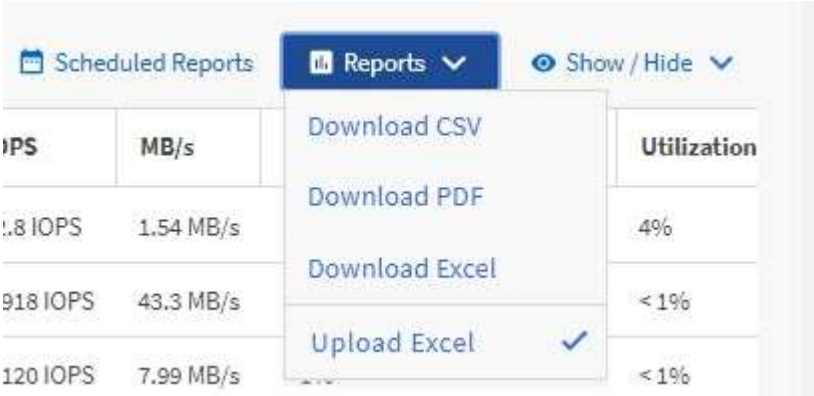
Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

7. Si nécessaire, cliquez sur **Activer la modification**.
8. Dans Excel, ouvrez le fichier téléchargé.
9. Dans la feuille de données, cliquez sur le petit triangle situé en haut à gauche de la feuille pour sélectionner la feuille entière.
10. Sur le ruban **Data**, sélectionnez **Trier** dans le `Sort & Filter area.`
11. Définissez les niveaux de tri suivants :
    a. Spécifiez les options **Trier par** en tant que (IOPS), **Trier par** en tant que et **Trier par `Available IOPS`** en tant `Cell Values,` que `Largest to Smallest.`
    b. Cliquez sur **Ajouter niveau**.
    c. Spécifiez le **Trier par** comme, le **Trier par** `Type` comme et le **ordre** `Cell Values,` comme `Z to A.`
    d. Cliquez sur **Ajouter niveau**.
    e. Spécifiez le **Trier par** comme **Trier par** et le * `Largest to Smallest.`Trier par `Free Capacity (GB),`* comme `Cell Values,`
    f. Cliquez sur **OK**.
12. Enregistrez et fermez le fichier Excel.
13. Dans Unified Manager, sélectionnez **Rapports** > **Upload Excel**.

    Assurez-vous que vous vous trouvez dans la même vue que celle 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 en regard de l'option de menu **Rapports** > **Télécharger Excel**.



17. Cliquez sur **Rapports planifiés**.
18. Cliquez sur **Ajouter un calendrier** pour ajouter une nouvelle ligne à la page programmes de rapports afin de définir les caractéristiques de planification du nouveau rapport.
19. Entrez un nom pour le planning de rapport et renseignez les autres champs de rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

Sélectionnez le format **XLSX** pour le rapport.

Le rapport est envoyé immédiatement sous forme de test. Ensuite, le rapport génère et est envoyé par e-mail aux destinataires répertoriés à l'aide de la fréquence spécifiée.

En fonction des résultats présentés dans ce rapport, vous pouvez provisionner de nouveaux workloads sur les agrégats disposant des valeurs d'IOPS les plus élevées.

Gérer le stockage à l'aide des API REST

Mise en route des API REST de Active IQ Unified Manager

Active IQ Unified Manager fournit un ensemble d'API afin de gérer vos ressources de stockage sur les systèmes de stockage pris en charge par le biais d'une interface de service web RESTful pour toute intégration tierce.

Dans ces sections, vous trouverez des informations sur les API Unified Manager, des exemples de flux de travail pour résoudre des problèmes spécifiques et des exemples de codes. Grâce à ces informations, vous pouvez créer des clients RESTful de solutions logicielles de gestion NetApp pour la gestion des systèmes NetApp. Les API sont basées sur le style architectural de Representational State Transfer (REST). Les quatre opérations REST Create, Read, Update et Delete (également appelées CRUD) sont prises en charge.

Voir "Active IQ Unified Manager" pour consulter des ressources supplémentaires et des informations sur les avantages de l'API REST Active IQ Unified Manager.

Public visé par ce contenu

Les rubriques ici sont destinées aux développeurs qui créent des applications interfactrices avec le logiciel Active IQ Unified Manager via des API REST.

Les administrateurs et architectes du stockage peuvent consulter ces informations pour découvrir comment utiliser les API REST Unified Manager pour créer des applications client pour gérer et surveiller les systèmes de stockage NetApp.

Vous devez utiliser ces informations pour gérer votre stockage et les API du fournisseur de stockage, du cluster ONTAP et de gestion.

> Vous devez avoir l'un des rôles suivants : opérateur, administrateur de stockage ou administrateur d'applications. 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 à l'API Active IQ Unified Manager

Avec les API Active IQ Unified Manager, vous pouvez gérer et provisionner les objets de stockage dans votre environnement. Vous pouvez également accéder à l'interface utilisateur Web de Unified Manager pour effectuer certaines de ces fonctions.

Construire une URL pour accéder directement aux API REST

Vous pouvez accéder directement aux API REST via un langage de programmation comme Python, C#, C++, JavaScript, et ainsi de suite. Entrez le nom d'hôte ou l'adresse IP et l'URL pour accéder aux API REST au format

https://<hostname>/api

> Le port par défaut est 443. Vous pouvez configurer le port selon les besoins de votre environnement.

Accès à la page de documentation en ligne de l'API

Vous pouvez accéder à la page de contenu *API Documentation* Reference fournie avec le produit pour afficher la documentation de l'API, ainsi que pour émettre manuellement un appel d'API (sur l'interface, par exemple, swagger). Vous pouvez accéder à cette documentation en cliquant sur **barre de menus** > **bouton aide** > **Documentation API**

Vous pouvez également entrer le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page API REST au format

https://<hostname>/docs/api/

Catégories

Les appels API sont organisés en fonction des domaines ou des catégories. Pour localiser une API spécifique, cliquez sur la catégorie API applicable.

Les API REST fournies avec Unified Manager vous permettent d'effectuer des fonctions d'administration, de surveillance et de provisionnement. Les API sont regroupées sous les catégories suivantes.

- **datacenter**

  Cette catégorie contient les API qui vous aident dans la gestion du stockage de data Center et l'analytique à l'aide des 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, partages de fichiers, espaces de noms et autres éléments de votre data center.

- **serveur-gestion**

  Les API de la catégorie **management-Server** contiennent les `jobs, system,` API et `events`. Les tâches sont planifiées pour une exécution asynchrone liée à la gestion des objets ou des charges de travail de stockage dans Unified Manager. L' `events`API renvoie les événements de votre data Center, tandis que l' `system`API renvoie les détails sur 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 performance et des règles d'efficacité du stockage. Les API vous permettent également de configurer des points d'accès, des répertoires actifs, ainsi que d'attribuer des niveaux de service de performance et des règles d'efficacité du stockage aux charges de travail de stockage.

- **administration**

  Cette catégorie contient les API utilisées pour exécuter des tâches administratives, telles que la gestion des paramètres de sauvegarde, l'affichage des certificats de stockage de confiance pour les sources de données Unified Manager et la gestion des clusters ONTAP comme sources de données pour Unified Manager.

- **passerelle**

  Unified Manager vous permet d'appeler des API REST ONTAP via les API dans la catégorie passerelle et de gérer les objets de stockage dans votre data Center.

- **sécurité**

Cette catégorie contient des API pour la gestion des utilisateurs de Unified Manager.

Services REST proposés en Active IQ Unified Manager

Avant d'utiliser les API Active IQ Unified Manager, vous devez connaître les services ET les opérations REST proposés.

Les API de provisionnement et d'administration utilisées pour configurer le serveur d'API prennent en charge les opérations de lecture (GET) ou d'écriture (POST, CORRECTIF, SUPPRESSION). Voici quelques exemples d'opérations GET, CORRECTIF, POST et DE SUPPRESSION prises en charge par les API :

- Exemple pour OBTENIR : `GET /datacenter/cluster/clusters` récupère les détails de cluster dans votre data Center. Le nombre maximum d'enregistrements renvoyés par `GET` l'opération est de 1000.

> Les API vous permettent de filtrer, trier et trier les enregistrements par attributs pris en charge.

- Exemple de POST : `POST /datacenter/svm/svms` crée une machine virtuelle de stockage (SVM) personnalisée.
- Exemple de PATCH : `PATCH /datacenter/svm/svms/{key}` modifie les propriétés d'un SVM en utilisant sa clé unique.
- Exemple de SUPPRESSION : `DELETE /storage-provider/access-endpoints/{key}` supprime un terminal d'accès d'une LUN, d'un SVM ou d'un partage de fichiers à l'aide de sa clé unique.

Les opérations REST pouvant être effectuées à l'aide des API dépendent du rôle de l'utilisateur de l'opérateur, de l'administrateur du stockage ou de l'administrateur d'applications.

Rôle utilisateur	Méthode REST prise en charge
Opérateur	Accès en lecture seule aux données. Les utilisateurs disposant de ce rôle peuvent exécuter toutes les demandes GET.
Administrateur du stockage	Accès en lecture à toutes les données. Les utilisateurs disposant de ce rôle peuvent exécuter toutes les demandes GET. En outre, ils ont un accès en écriture (pour exécuter DES DEMANDES DE CORRECTIF, D'POST-TRAITEMENT et DE SUPPRESSION) afin d'effectuer certaines activités, telles que la gestion, les objets de service de stockage et les options de gestion du stockage.
Administrateur d'applications	Accès en lecture et en écriture à toutes les données. Les utilisateurs disposant de ce rôle peuvent exécuter des demandes D'OBTENTION, DE CORRECTION, DE PUBLICATION et DE SUPPRESSION pour toutes les fonctions.

Pour plus d'informations sur toutes les opérations DE REPOS, reportez-vous à la documentation *Online API*.

Version de l'API dans Active IQ Unified Manager

Les URI de l'API REST dans Active IQ Unified Manager spécifie 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 d'API sur le logiciel client en envoyant une réponse que le client peut traiter.

La partie numérique de ce numéro de version est incrémentielle par rapport aux rejets. Les URI avec un numéro de version fournissent une interface cohérente qui maintient la rétrocompatibilité dans les versions futures. Vous trouvez 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 version la plus récente 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 au nombre entier incrémentiel) disponible dans votre instance Unified Manager.

Pour toutes les demandes, vous devez demander explicitement la version de l'API que vous souhaitez utiliser. Lorsque le numéro de version est spécifié, le service ne renvoie pas les éléments de réponse que votre application n'est pas conçue pour gérer. Dans les demandes REST, vous devez inclure le paramètre de version. Les versions précédentes des API sont finalement obsolètes après quelques versions. Dans cette version, la `v1` version des API est obsolète.

Ressources de stockage dans ONTAP

Les ressources de stockage de ONTAP peuvent être classées dans *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**

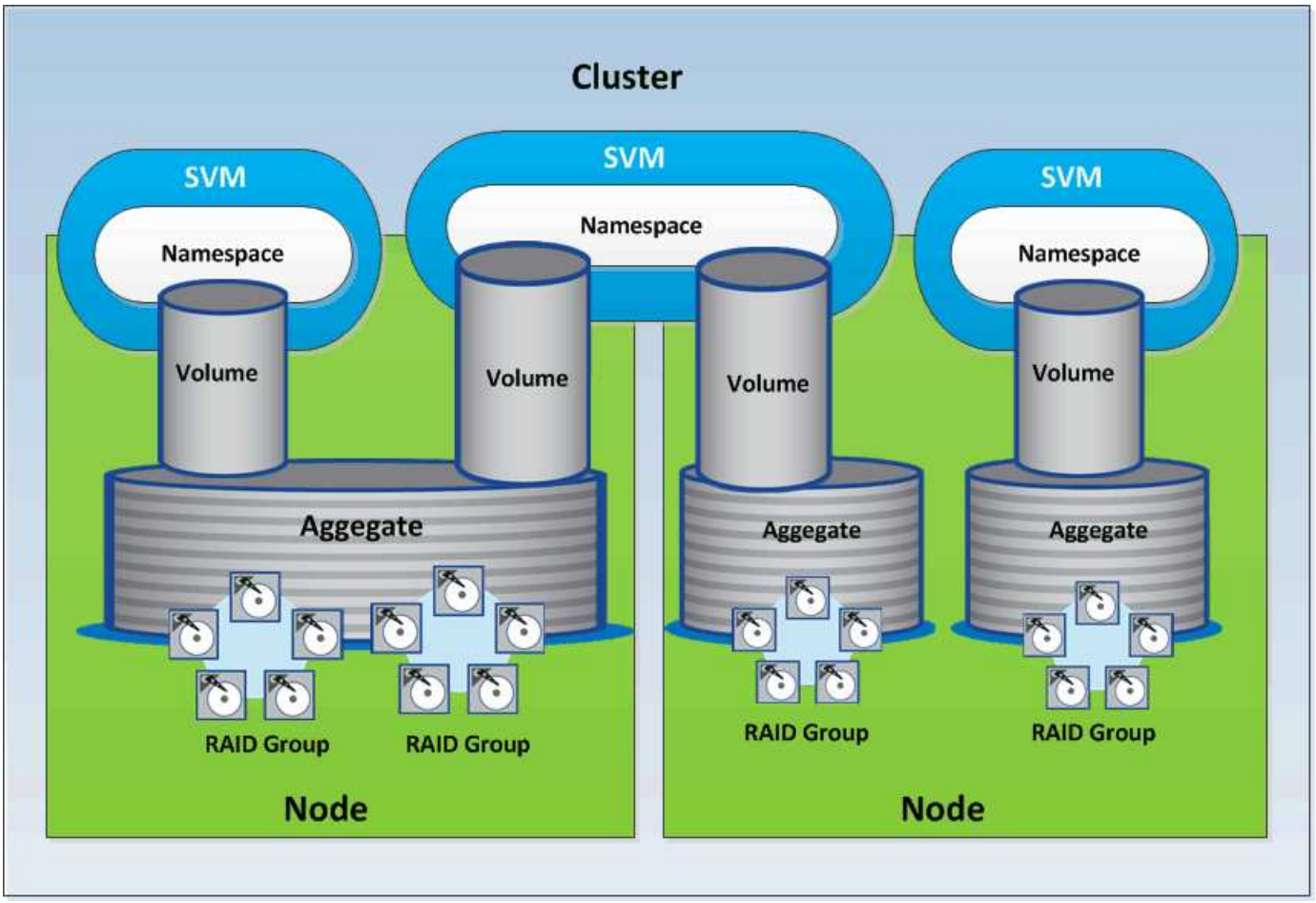
  Désigne les objets de stockage physique fournis par ONTAP. Les ressources de stockage physique sont les disques, les clusters, les contrôleurs de stockage, les nœuds et les agrégats.

- **Ressources de stockage logiques**

  Désigne les 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 elles existent indépendamment de toute ressource de stockage physique spécifique, telle qu'un agrégat, une LUN de baie ou un disque.

  Les ressources de stockage logique comprennent des volumes de tous les types et qtrees, ainsi que des fonctionnalités et des configurations que vous pouvez utiliser avec ces ressources, comme les copies Snapshot, la déduplication, la compression et les quotas.

L'illustration suivante présente les ressources de stockage dans un cluster à deux nœuds :



Accès à l'API REST et authentification dans Active IQ Unified Manager

L'API REST Active IQ Unified Manager est accessible depuis n'importe quel client REST ou plateforme de programmation pouvant émettre des requêtes HTTP avec un mécanisme d'authentification HTTP de base.

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 d'API.
- Orifice 443

  Le port HTTPS par défaut est défini sur 443. Vous pouvez personnaliser le port HTTPS si nécessaire.

Pour émettre des requêtes HTTP à partir d'un navigateur Web, vous devez utiliser des plug-ins de navigateur d'API REST. Vous pouvez également accéder à l'API REST à l'aide de 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 sécuriser les flux d'informations (demande et réponse), les API REST sont accessibles uniquement via HTTPS. Le serveur d'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 un certificat CA).

Vous devez configurer l'accès utilisateur au serveur d'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 d'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 de Unified Manager.

Codes d'état HTTP utilisés dans Active IQ Unified Manager

Lors de l'exécution des API ou de la résolution des problèmes, vous devez connaître les divers codes d'état et codes d'erreur HTTP 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 d'API synchrone.
201	Créé	Création de nouvelles ressources par des appels synchrones, tels que 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 non valide	Indique un échec de validation de l'entrée. L'utilisateur doit corriger les entrées, par exemple les clés valides dans un corps de demande.
401	Demande non autorisée	Vous n'êtes pas autorisé à afficher la ressource/non autorisé.
403	Demande interdite	Il est interdit d'accéder à la ressource que vous tentez d'atteindre.
404	Ressource introuvable	La ressource que vous avez essayé de joindre est introuvable.
405	Méthode non autorisée	Méthode non autorisée.
429	Nombre de demandes trop important	Renvoyé lorsque l'utilisateur envoie trop de demandes 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 une `GET` opération ou `GET ALL` 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 continue à être 500. Si l'opération réussit, le code d'état renvoyé est 200.

Recommandations pour l'utilisation des API pour Active IQ Unified Manager

Lorsque vous utilisez des API dans Active IQ Unified Manager, vous devez respecter 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. Nous vous recommandons d'utiliser la dernière version de l'API disponible pour votre instance Unified Manager. Pour plus d'informations sur les versions de l'API Unified Manager, reportez-vous à la section « GESTION des versions de l'API DE ST dans Active IQ Unified Manager ».
- Lors de la mise à jour des valeurs d'une baie à l'aide d'une API Unified Manager, vous devez mettre à jour l'ensemble de la chaîne de valeurs. Vous ne pouvez pas ajouter de valeurs à un tableau. Vous ne pouvez remplacer qu'une baie existante.
- Vous pouvez utiliser des opérateurs de filtre, tels que pipe (|) et Wild card (*) pour tous les paramètres de requête, à l'exception des valeurs doubles, par exemple, IOPS et performances dans les API de metrics.
- Évitez d'interroger les objets en utilisant une combinaison de caractères génériques (*) et de tuyaux (|) des opérateurs de filtre. Il est possible que le nombre d'objets soit incorrect.
- Lorsque vous utilisez des valeurs pour le filtre, assurez-vous que la valeur ne contient aucun `?` caractère. Ceci est pour atténuer les risques de l'injection SQL.
- Notez que la `GET` demande (All) pour toute API renvoie un maximum de 1000 enregistrements. Même si vous exécutez la requête en définissant le `max_records` paramètre sur une valeur supérieure à 1000, seuls 1000 enregistrements sont renvoyés.
- Pour effectuer des fonctions administratives, il est recommandé d'utiliser l'interface utilisateur de Unified Manager.

Journaux pour le dépannage

Les journaux système vous permettent d'analyser les causes des défaillances et de résoudre les problèmes susceptibles de survenir lors de l'exécution des API.

Récupérez les journaux à partir de l'emplacement suivant pour résoudre les problèmes liés aux appels API.

Emplacement du journal	Utiliser
`/var/log/ocie/access_log.log`	Contient tous les détails d'appel API, tels que le nom d'utilisateur de l'utilisateur appelant 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 pour dépanner n'importe quel workflow de l'interface graphique. Vous pouvez également l'utiliser pour mettre l'analyse à l'échelle, en fonction du temps d'exécution.
`/var/log/ocum/ocumserver.log`	Contient tous les journaux d'exécution de l'API. Vous pouvez utiliser ce fichier journal pour dépanner et déboguer les appels API.
`/var/log/ocie/server.log`	Contient tous les déploiements de serveur Wildfly et journaux relatifs au service de démarrage/arrêt. Vous pouvez utiliser ce fichier journal pour trouver la cause principale de tout problème survenant au cours du démarrage, de l'arrêt ou du déploiement du serveur Wildfly.
`/var/log/ocie/au.log`	Contient les journaux relatifs à l'unité d'acquisition. Vous pouvez utiliser ce fichier journal lors de la création, de la modification ou de la suppression d'objets dans ONTAP, mais ils ne sont pas répercutés pour les API REST de Active IQ Unified Manager.

Processus asynchrones des objets de travail

Active IQ Unified Manager fournit l' `jobs`API qui récupère les informations sur les travaux effectués lors de l'exécution d'autres API. Vous devez savoir comment le traitement asynchrone fonctionne à l'aide de l'objet travail.

Certains appels API, en particulier ceux utilisés pour ajouter ou modifier des ressources, peuvent prendre plus de temps que d'autres appels. Unified Manager traite ces requêtes à long terme de manière asynchrone.

Demandes asynchrones décrites à l'aide de l'objet travail

Après avoir effectué un appel API qui s'exécute de manière asynchrone, le code de réponse HTTP 202 indique

que la demande a été validée et acceptée avec succès, mais pas encore terminée. La requête est traitée comme une tâche d'arrière-plan qui continue à s'exécuter après la réponse HTTP initiale au client. La réponse inclut l'objet Job qui fixe la requête, y compris son identifiant unique.

Interrogation de l'objet travail associé à une requête API

L'objet travail renvoyé dans la réponse HTTP contient plusieurs propriétés. Vous pouvez interroger la propriété d'état pour déterminer si la demande a bien été effectuée. Un objet travail 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 travail pour détecter un état de terminal pour la tâche, succès ou 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 demande asynchrone

Vous pouvez utiliser la procédure de haut niveau suivante pour effectuer un appel d'API asynchrone :

1. Lancez l'appel d'API asynchrone.
2. Recevoir une réponse HTTP 202 indiquant que la demande a été acceptée avec succès.
3. Extraire l'identifiant de l'objet travail du corps de réponse.
4. Dans une boucle, attendez que l'objet Job atteigne l'état du terminal `NORMAL, ERROR,` ou `PARTIAL_FAILURES.`
5. Vérifiez l'état du terminal du travail et récupérez le résultat du travail.

Bonjour serveur API

Le *Hello API Server* est un exemple de programme qui montre comment appeler une API REST dans Active IQ Unified Manager à l'aide d'un simple client REST. L'exemple de programme fournit des informations de base sur le serveur d'API au format JSON (le serveur prend uniquement en charge le `application/json` format).

L'URI utilisé est : `https://<hostname>/api/datacenter/svm/svms.` cet exemple de code prend les paramètres d'entrée suivants :

- Adresse IP ou FQDN du serveur d'API
- Facultatif : numéro de port (par défaut : 443)
- Nom d'utilisateur
- Mot de passe

- Format de réponse (`application/json`)

Pour appeler des API REST, vous pouvez aussi utiliser d'autres scripts comme Jersey et RESTEasy pour écrire un client JAVA REST pour Active IQ Unified Manager. Vous devez tenir compte des considérations suivantes concernant le code d'échantillon :

- Utilise une connexion HTTPS vers Active IQ Unified Manager pour appeler l'URI REST spécifiée
- Ignore le certificat fourni par Active IQ Unified Manager
- Ignore la vérification du nom de l'hôte lors de l'établissement de la liaison
- Utilise `javax.net.ssl.HttpsURLConnection` pour une connexion URI
- Utilise une bibliothèque tierce (`org.apache.commons.codec.binary.Base64`) pour construire la chaîne codée 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 ultérieur.

```
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.HttpsURLConnection;
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 {
            HttpsURLConnection 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 HttpsURLConnection
getAllTrustingHttpsUrlConnection()    {        HttpsURLConnection conn =
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 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 comprend les détails de chaque appel d'API REST. Ce document ne répète pas les détails de la documentation en ligne. Chaque appel d'API répertorié ou décrit dans ce document comprend uniquement les informations dont vous avez besoin pour localiser l'appel sur la page de documentation. Après avoir localisé un appel API spécifique, vous pouvez vérifier 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 au sein d'un flux de travail afin de localiser l'appel sur la page de documentation :

- Catégorie

  Les appels API sont organisés sur la page de documentation en zones ou catégories liées à la fonctionnalité. Pour localiser un appel API spécifique, faites défiler la page jusqu'en bas, puis cliquez sur la

catégorie 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 à laquelle l'action utilise comme partie de l'appel. La chaîne de chemin d'accès est ajoutée à l'URL principale pour former l'URL complète identifiant la ressource.

Gestion des objets de stockage dans un data Center à l'aide d'API

Les API REST de la `datacenter` catégorie vous permettent de gérer les objets de stockage de votre data Center, 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 QUI fournissent une agrégation intercluster avec filtrage, tri et prise en charge de pagination. Lors de l'exécution de ces API, ils renvoient les données à partir de la base de données. Par conséquent, les objets nouvellement créés doivent être découverts par le cycle d'acquisition suivant pour apparaître dans la réponse.

Si vous souhaitez interroger les détails d'un objet spécifique, vous devez entrer l'ID unique de cet objet pour afficher ses détails. Par exemple, pour les mesures et les informations analytiques des objets de stockage, reportez-vous à la section "Affichage des metrics de performances".

```
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, exemples, requêtes et réponses aux API sont disponibles sur votre interface API swagger. Vous pouvez filtrer et trier les résultats par paramètres spécifiques comme indiqué sur le swagger. Ces API vous permettent de filtrer les résultats d'objets de stockage spécifiques, par exemple, cluster, volume ou VM de stockage.

Des API pour les objets de stockage dans votre data Center

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 data Center. L'API renvoie des informations, telles que l'adresse IPv4 ou IPv6 du cluster, des informations sur le nœud, telles que l'état de santé du nœud, la capacité de performances et la paire haute disponibilité (HA), et indique si le cluster est une baie SAN.
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Affiche le détail des licences installées sur les clusters de votre data Center. 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 entrer 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 data Center. Vous pouvez afficher des informations sur le cluster, l'état de santé des nœuds, la capacité en termes de performances et la paire haute disponibilité 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 data Center. Outre les détails du cluster, du SVM et du volume, les informations relatives à 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 le détail des export policies pour les services NFS pris en charge. Vous pouvez interroger les export policy pour un cluster ou une VM de stockage et réutiliser la clé export policy pour le provisionnement des partages de fichiers NFS. Pour plus d'informations sur l'attribution et la réutilisation de règles d'exportation sur les charges de travail, reportez-vous à la section « provisionnement de partages de fichiers CIFS et NFS ».
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Vous pouvez utiliser cette méthode pour afficher le regroupement des agrégats dans le data Center ou un agrégat spécifique pour le provisionnement des charges de travail sur ceux-ci ou pour la surveillance. Des informations telles que les détails du cluster et du nœud, la capacité en termes de performances 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 des LUN dans l'intégralité du data Center. Vous pouvez afficher des informations sur les LUN, notamment les détails sur le cluster et SVM, les règles de QoS et les igroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Vous pouvez l'utiliser pour en savoir plus sur toutes les règles de QoS applicables aux objets de stockage du data Center. 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 renvoyés.

Verbe HTTP	Chemin	Description
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des qtrees dans le data Center pour tous les volumes FlexVol ou FlexGroup. Les informations telles que les détails du cluster et du SVM, le volume FlexVol et l'export policy sont renvoyées.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Vous pouvez utiliser cette méthode pour afficher la collection de volumes dans le data Center. Les informations relatives aux volumes, telles que les SVM et le cluster, les règles de qualité de services et d'export, que le volume soit de type read-write, protection des données ou load-sharing, sont renvoyées. Pour les volumes FlexVol et FlexClone, vous pouvez afficher les informations relatives aux agrégats respectifs. Pour un volume FlexGroup, la requête renvoie la liste des agrégats constitutifs.

Verbe HTTP	Chemin	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Vous pouvez affecter des groupes initiateurs autorisés à accéder à des cibles de LUN spécifiques. Si un groupe initiateur existe, vous pouvez l'attribuer. Vous pouvez également créer des igroups et les affecter avec des LUN.
		
		Vous pouvez utiliser ces méthodes pour interroger, créer, supprimer et modifier respectivement les igroups.
		
		Points à prendre en compte :
		
		• `POST`: Lors de la création d'un groupe initiateur, vous pouvez désigner la VM de stockage sur laquelle vous souhaitez attribuer l'accès.
		• `DELETE`: Pour supprimer un groupe initiateur, vous devez fournir la clé du groupe initiateur en tant que paramètre d'entrée. Si vous avez déjà attribué un groupe initiateur à une LUN, vous ne pouvez pas supprimer ce groupe initiateur.
		• `PATCH`: Pour modifier un groupe initiateur, vous devez fournir une clé de groupe initiateur en tant que paramètre d'entrée. Vous devez également saisir la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.

Verbe HTTP	Chemin	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		Ces méthodes permettent d'afficher, de créer, de supprimer et de modifier les machines virtuelles de stockage (VM de stockage).
		
		• `POST`: Vous devez entrer l'objet VM de stockage que vous souhaitez créer en tant que 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 la machine virtuelle de stockage pour supprimer une machine virtuelle de stockage particulière.
		• `PATCH`: Vous devez fournir la clé de la VM de stockage pour modifier une VM de stockage particulière. Vous devez également saisir les propriétés que vous souhaitez mettre à jour, ainsi que leurs valeurs.

Points à prendre en compte :

Si vous avez activé le provisionnement des charges de travail basées sur les objectifs de niveau de service dans votre environnement, lors de la création de la machine virtuelle de stockage, assurez-vous qu'elle prend en charge tous les protocoles requis pour le provisionnement des LUN et des partages de fichiers, par exemple, CIFS ou SMB, NFS, FCP, Et iSCSI. Les workflows de provisionnement peuvent échouer si la VM 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 des charges de travail basées sur les objectifs SLO sur votre environnement, vous ne pouvez pas supprimer cette 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, en plus de la configuration Active Directory locale. Cependant, le nom du serveur CIFS ou SMB reste dans la configuration Active Directory que vous devez supprimer manuellement du serveur Active Directory.

Des API pour les éléments réseau de votre data Center

Les API suivantes de la catégorie Datacenter récupèrent les 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 l'environnement de votre datacenter. Une touche de port étant un paramètre d'entrée, vous pouvez afficher les informations de ce port spécifique. Les informations telles que les détails sur le cluster, le domaine de diffusion, les détails du port, tels que son état, sa vitesse, et le type, et si le port est activé, est récupéré.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des interfaces FC dans l'environnement de votre data Center. Une clé d'interface étant un paramètre d'entrée, vous pouvez afficher les informations de cette interface spécifique. Les informations telles que les détails du cluster, les détails du nœud de rattachement et les détails du port de rattachement 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 l'environnement de votre data Center. Une touche de port étant un paramètre d'entrée, vous pouvez afficher les informations de ce port spécifique. Les informations telles que les détails de cluster, la description de 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 l'environnement de votre data Center. Une clé d'interface étant un paramètre d'entrée, vous pouvez afficher les informations de cette interface spécifique. Les informations telles que les détails du cluster, les détails de l'IPspace, les détails du nœud domestique, si le basculement est activé, sont récupérées.

Accès aux API ONTAP via un accès proxy

Les API de passerelle permettent d'utiliser les identifiants Active IQ Unified Manager pour exécuter les API REST ONTAP et gérer les objets de stockage. Ces API sont disponibles lorsque la fonctionnalité de passerelle d'API est activée depuis l'interface utilisateur Web d'Unified Manager.

Les API REST Unified Manager prennent en charge uniquement un ensemble d'actions à effectuer sur les données Unified Manager, c'est-à-dire les clusters ONTAP. Vous pouvez utiliser les autres fonctions au moyen des API ONTAP. Les API de passerelle permettent à Unified Manager de constituer une interface pass-through pour tunneling de toutes les demandes d'API sur les clusters ONTAP qu'il gère, sans se connecter individuellement à chaque cluster de data Center. Il s'agit d'un point unique de gestion pour l'exécution des API dans les clusters ONTAP gérés par votre instance Unified Manager. La fonctionnalité de passerelle d'API permet à Unified Manager de devenir un plan de contrôle unique depuis lequel vous pouvez gérer plusieurs clusters ONTAP sans vous connecter individuellement. Les API de passerelle vous permettent de rester connecté à Unified Manager et de gérer les clusters ONTAP en exécutant des opérations de l'API REST ONTAP.

> Tous les utilisateurs peuvent exécuter une requête à l'aide de l'opération OBTENIR. Les administrateurs d'applications peuvent exécuter toutes les opérations REST de ONTAP.

La passerelle agit comme un proxy pour le tunnel des requêtes API en maintenant les demandes d'en-tête et de corps dans le même format que dans les API ONTAP. Vous pouvez utiliser vos identifiants Unified Manager et exécuter les opérations spécifiques pour accéder aux clusters ONTAP et les gérer sans passer par les identifiants individuels du cluster. Il continue de gérer l'authentification de cluster et la gestion de cluster, mais redirige les requêtes d'API afin de s'exécuter directement sur le cluster spécifique. La réponse renvoyée par les API est la même que la réponse renvoyée par les API REST respectives ONTAP 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 REST ONTAP. Vous pouvez vérifier les détails du cluster et choisir d'exécuter d'autres méthodes basées sur l'UUID ou l'identifiant universel unique (UUID) du cluster. Les API de la passerelle ne récupèrent que les clusters pris en charge par ONTAP 9.5 ou version ultérieure, et sont ajoutés à Unified Manager sur HTTPS.

Verbe HTTP	Chemin (URL)	Description
GET POST DELETE PATCH OPTIONS (Non disponible sur l'andaineur) HEAD (Non disponible sur l'andaineur)	/gateways/{uuid}/{path} La valeur de {UUID} doit être remplacée par l'UUID de cluster sur lequel l'opération DE REPOS est à effectuer. Assurez-vous également que l'UUID est bien 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 de ONTAP. Vous devez supprimer /api/ de l'URL.	Il s'agit d'une API proxy à point unique prenant en charge LES opérations POST, DE SUPPRESSION, DE CORRECTIFS et D'OBTENTION pour toutes les API REST de ONTAP. Aucune restriction ne s'applique à l'API tant qu'elle est prise en charge par ONTAP. La fonctionnalité de tunneling ou proxy ne peut pas être désactivée. La OPTIONS méthode renvoie toutes les opérations prises en charge par une API REST ONTAP. Par exemple, si une API ONTAP prend uniquement en charge GET l'opération, l'exécution de OPTIONS la méthode à l'aide de 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. La OPTIONS méthode détermine si une ressource est disponible. Cette opération peut être utilisée pour afficher les métadonnées relatives à 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.

Présentation du tunneling de la passerelle d'API

Les API de passerelle 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 terminal REST de ONTAP. L'API de passerelle transforme l'URL et l'Hypermedia en tant que liens Engine of application State (HATEOEA) dans l'en-tête et le corps de réponse avec l'URL de base de la passerelle API. L'API de passerelle agit comme l'URL de base du proxy auquel vous ajoutez l'URL REST ONTAP et exécutez le noeud final REST ONTAP requis.

> Pour qu'une API ONTAP s'exécute correctement via la passerelle d'API, elle doit être prise en charge par cette version du cluster ONTAP sur lequel elle est exécutée. Les résultats ne sont pas obtenus lors de l'exécution d'une API qui n'est pas prise en charge sur le cluster ONTAP.

Dans cet exemple, l'API de la passerelle (URL de base du proxy) est : `/gateways/{uuid}/`

L'API ONTAP prise est : `/storage/volumes`. Vous devez ajouter l'URL REST de l'API ONTAP comme valeur

pour le paramètre path.

> Lors de l'ajout du chemin, assurez-vous d'avoir supprimé l'ajout `storage/volumes. «»/" symbol at the beginning of the URL. For the API `/storage/volumes,`

L'URL ajoutée est : `/gateways/{uuid}/storage/volumes`

Lors de l'exécution de l' `GET`opération, l'URL générée est la suivante : `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

La `/api` balise de l'URL REST ONTAP est supprimée de l'URL ajoutée et celle de l'API de passerelle est conservée.

Commande Curl exemple

```
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 de 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 REST ONTAP.

Définition de la portée de l'API

Toutes les API disposent d'un contexte défini dans le cadre du cluster. Les API qui s'exécutent sur la base des VM de stockage également que le cluster fait partie du périmètre, c'est-à-dire que les opérations des API sont effectuées sur une VM de stockage particulière dans un cluster géré. Lorsque vous exécutez l' `/gateways/{uuid}/{path}`API, assurez-vous de saisir l'UUID de cluster (UUID de source de données Unified Manager) pour le cluster sur lequel vous exécutez l'opération. Pour définir le contexte sur 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 VM de stockage au sein de ce cluster.

Commande Curl exemple

```
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, reportez-vous à la section "AUTOMATISATION DES API REST ONTAP"

Exécution des tâches administratives à l'aide d'API

Vous pouvez utiliser les API de la `administration` catégorie pour modifier les paramètres de sauvegarde, vérifier les informations sur le fichier de sauvegarde et les

certificats de cluster, et également gérer les clusters ONTAP en tant que sources de données Active IQ Unified Manager.

> Vous devez avoir le rôle Administrateur d'applications pour exécuter ces opérations. Vous pouvez également configurer ces paramètres à l'aide de l'interface utilisateur Web Unified Manager.

Verbe HTTP	Chemin	Description

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Vous pouvez utiliser la `GET` méthode pour afficher les paramètres du planning de sauvegarde configuré dans Unified Manager par défaut. Vous pouvez vérifier les éléments suivants :
		
		• Indique si la planification est activée ou désactivée
		• Fréquence de la sauvegarde planifiée (quotidienne ou hebdomadaire)
		• Heure de la sauvegarde
		• Nombre maximal de fichiers de sauvegarde à conserver 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 programme de sauvegarde. Toutefois, vous pouvez utiliser la `PATCH` méthode pour modifier les paramètres par défaut.

`GET`	`/admin/backup-file-info`	Un fichier de dump de sauvegarde est généré chaque fois que la planification des sauvegardes est modifiée pour Unified Manager. Vous pouvez utiliser cette méthode pour vérifier si le fichier de sauvegarde est généré en fonction des 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 l'ajout d'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 la 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 en tant que source de données par Unified Manager, utilisez la clé de cluster ONTAP.

Gestion des utilisateurs à l'aide d'API

Vous pouvez utiliser les API de la `security` catégorie pour contrôler l'accès utilisateur à certains objets de cluster 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 avoir le rôle Administrateur d'applications pour exécuter ces opérations. Vous pouvez également configurer ces paramètres à l'aide de l'interface utilisateur Web Unified Manager.

Les API sous la `security` catégorie utilisent le paramètre Users, c'est-à-dire le nom d'utilisateur, et non le paramètre key comme identifiant unique pour l'entité utilisateur.

Verbe HTTP	Chemin	Description
GET POST	/security/users /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 base de données.
GET PATCH DELETE	/security/users/{name}	La méthode OBTENIR vous permet de récupérer tous les détails d'un utilisateur, tels que le nom, l'adresse e-mail, le rôle et le type d'autorisation. La méthode PATCH vous permet de mettre à jour les détails. La méthode DE SUPPRESSION vous permet de supprimer l'utilisateur.

Affichage des metrics de performances à l'aide d'API

Active IQ Unified Manager propose un ensemble d'API sous la catégorie vous `/datacenter` permettant de consulter les données de performances de vos clusters et objets de stockage dans un data Center. Ces API récupère les données de performance des différents objets de stockage tels que les clusters, les nœuds, les LUN, les volumes, les agrégats, Machines virtuelles de stockage, interfaces FC, ports FC, ports Ethernet et interfaces IP.

Les API et `/analytics` offrent différentes vues des metrics de performance. Elles `/metrics` vous permettent d'accéder à différents niveaux de détail pour les objets de stockage suivants dans votre data Center :

- clusters
- nœuds
- Machines virtuelles de stockage
- 64 bits
- volumes
- LUN
- Interfaces FC
- Ports FC

- Ports Ethernet
- Interfaces IP

Le tableau suivant établit une comparaison entre `/metrics` les API et `/analytics` en ce qui concerne les détails des données de performances récupérées.

Métriques	Analytique
Détails de performance pour un seul objet. Par exemple, l' `/datacenter/cluster/clusters/{key}/metrics`API requiert la saisie de la clé de cluster comme paramètre path pour récupérer les metrics de ce cluster spécifique.	Détails de performance pour plusieurs objets du même type dans un data Center. Par exemple, l' `/datacenter/cluster/clusters/analytics`API extrait les metrics collectifs de tous les clusters d'un data Center.
Des exemples de metrics de performances d'un objet de stockage basés sur le paramètre d'intervalle de temps pour la récupération.	Valeur agrégée générale de performance pour un certain type d'objet de stockage pendant une certaine période (au-dessus de 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'a été récupéré.
Les compteurs cumulés, tels que minimum, maximum, 95e percentile et les valeurs de performances moyennes sur une période de temps, sont récupérés pour un seul objet, tel que lecture, écriture, total et autres compteurs.	Une valeur agrégée unique s'affiche pour tous les objets du même type.

Métriques	Analytique
La plage horaire et les données d'échantillon sont basées sur le calendrier suivant : la plage horaire des données. Les exemples peuvent être 1h, 12h, 1d, 2d, 3d, 15d, 1 w, 1 m, 2 m, 3 m, 6 m. Vous obtenez des échantillons d'1 heure si la plage est supérieure à 3 jours (72 h) sinon il s'agit de 5 minutes d'échantillons. La période pour chaque plage horaire est la suivante : • 1h: Mesures au cours de la dernière heure échantillonnée sur 5 minutes. • 12h : mesures sur les 12 dernières heures échantillonnées sur 5 minutes. • 1d : mesures effectuées au cours de la journée la plus récente échantillonnées sur 5 minutes. • 2d : mesures sur les 2 derniers jours échantillonnées en 5 minutes. • 3d : mesures sur les 3 derniers jours échantillonnées en 5 minutes. • 15d : mesures sur les 15 derniers jours échantillonnés sur une heure. • 1w : mesures sur la semaine la plus récente échantillonnées sur 1 heure. • 1m : indicateurs sur le mois le plus récent échantillonnés sur une heure. • 2m : mesures effectuées au cours des 2 derniers mois échantillonnés sur une heure. • 3m : mesures effectuées au cours des 3 derniers mois échantillonnés sur une heure. • 6m : mesures effectuées au cours des 6 derniers mois échantillonnés sur une heure. Valeurs disponibles : 1h, 12h, 1d, 2d, 3d, 15d, 1 w, 1 m, 2 m, 3 m, 6 m. Valeur par défaut : 1h	Au-dessus de 72 heures. La durée de calcul de cet échantillon est représentée au format standard ISO-8601.

Exemple de résultat pour les API de metrics

Par exemple, l' `/datacenter/cluster/nodes/{key}/metrics`API extrait les détails suivants (entre autres) pour un nœud :

> Les 95 percentiles de la valeur sommaire indiquent que 95 % des échantillons prélevés pour la période ont une valeur de compteur inférieure à la valeur indiquée comme percentile 95.

```
{
```

```
      "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 résultat pour les API d’analytique

Par exemple, l' `/datacenter/cluster/nodes/analytics`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 `/metrics` en détail les API et `/analytics`.

> Les mesures d'IOPS et 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 joker (*) n'est pas pris en charge.

Verb. HTTP	Chemin	Description
GET	/datacenter/cluster/clusters/{key}/metrics	Récupère les données de performances (échantillon et récapitulatif) d'un cluster spécifié par le paramètre d'entrée de la clé de cluster. Les informations telles que la clé de 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 performance de haut niveau pour tous les clusters d'un data Center. 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 récapitulatif) d'un nœud spécifié par le paramètre d'entrée de la clé de nœud. Les informations telles que l'UUID du nœud, la plage de temps, l'aperçu des IOPS, le débit, la latence et les performances, le nombre d'échantillons collectés et le pourcentage utilisés sont renvoyées.
GET	/datacenter/cluster/nodes/analytics	Récupère les mesures de performance de haut niveau pour tous les nœuds d'un data Center. Vous pouvez filtrer vos résultats en fonction des critères requis. Les informations telles que les clés de nœud et de cluster, ainsi que les valeurs telles que les IOPS agrégées, le débit et la période de collecte (en heures) sont renvoyées.

Verb. HTTP	Chemin	Description
GET	/datacenter/storage/aggregates/{key}/metrics	Récupère les données de performances (échantillon et récapitulatif) d'un agrégat spécifié par le paramètre d'entrée de la clé d'agrégat. Les informations telles que la plage de temps, un récapitulatif des IOPS, de la latence, du débit et de la capacité des performances, le nombre d'échantillons collectés pour chaque compteur et le pourcentage utilisés sont renvoyées.
GET	/datacenter/storage/aggregates/analytics	Récupère les mesures de performances de haut niveau pour tous les agrégats du data Center. Vous pouvez filtrer vos résultats en fonction des critères requis. Les informations, telles que les clés d'agrégat et de cluster, ainsi que les 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 récapitulatif) d'une LUN ou d'un partage de fichiers (volume) spécifié par le paramètre d'entrée de la clé de volume ou de la LUN. Des informations telles que un récapitulatif des valeurs minimale, maximale et moyenne des valeurs totales d'IOPS, de latence et de débit, et le nombre d'échantillons prélevés pour chaque compteur est renvoyé.

Verb. HTTP	Chemin	Description
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	Récupère les mesures de performances de haut niveau pour toutes les LUN ou volumes d'un data Center. Vous pouvez filtrer vos résultats en fonction des critères requis. Les informations, telles que les machines virtuelles de stockage et les clés de cluster, ainsi que des valeurs telles que les IOPS agrégées, le débit et la période de collecte (en heures) sont renvoyées.
GET	/datacenter/svm/svms/{key}/metrics	Récupère les données de performances (échantillon et récapitulatif) d'une machine virtuelle de stockage spécifiée par le paramètre d'entrée de la clé de la machine virtuelle de stockage. Résumé des IOPS en fonction de chaque protocole pris en charge, tel que `nvmf, fcp, iscsi,` et `nfs`, 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 data Center. Vous pouvez filtrer vos résultats en fonction des critères requis. Les informations telles que l'UUID (UUID) du serveur virtuel de stockage, les IOPS agrégées, la latence, le débit et la période de collecte sont renvoyées (en heures).
GET	/datacenter/network/ethernet/ports/{key}/metrics	Récupère les mesures de performances d'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 minimum, maximum et les valeurs de performances moyennes sur la période de temps.

Verb. HTTP	Chemin	Description
GET	/datacenter/network/ethernet/ports/analytics	Récupère les mesures de performances de haut niveau de tous les ports ethernet de l'environnement de votre datacenter. Les informations telles que la clé du cluster et des nœuds, ainsi que l'UUID, le débit, la période de collecte et le pourcentage d'utilisation des ports sont renvoyées. Vous pouvez filtrer le résultat par exemple en fonction des paramètres disponibles, par exemple la clé de port, le pourcentage d'utilisation, le nom du cluster, du nœud et son UUID, etc.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Récupère les mesures de performances d'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 minimum, maximum et les valeurs de performances moyennes sur la période de temps.
GET	/datacenter/network/fc/interfaces/analytics	Récupère les mesures de performances de haut niveau de tous les ports ethernet de l'environnement de votre datacenter. Des informations telles que la clé du cluster et de l'interface FC, ainsi que l'UUID, le débit, les IOPS, la latence et la machine virtuelle de stockage sont renvoyés. Vous pouvez filtrer le résultat en fonction des paramètres disponibles, par exemple le nom du cluster et de l'interface FC, l'UUID, la machine virtuelle de stockage, le débit, etc.

Verb. HTTP	Chemin	Description
GET	/datacenter/network/fc/ports/{key}/metrics	Récupère les metrics de performances d'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 minimum, maximum et les valeurs de performances moyennes sur la période de temps.
GET	/datacenter/network/fc/ports/analytics	Récupère les metrics de performance de haut niveau pour tous les ports FC de votre environnement de data Center. Les informations telles que la clé du cluster et des nœuds, ainsi que l'UUID, le débit, la période de collecte et le pourcentage d'utilisation des ports sont renvoyées. Vous pouvez filtrer le résultat par exemple en fonction des paramètres disponibles, par exemple la clé de port, le pourcentage d'utilisation, le nom du cluster, du nœud et son UUID, etc.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Récupère les mesures de performances d'une interface IP réseau comme spécifié 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.

Verb. HTTP	Chemin	Description
GET	/datacenter/network/ip/interfaces/analytics	Récupère les mesures de performances de haut niveau pour toutes les interfaces IP réseau de l'environnement de votre centre de données. Des informations telles que le cluster et l'interface IP, ainsi que l'UUID, le débit, les IOPS et la latence sont renvoyés. Vous pouvez filtrer le résultat par les paramètres disponibles, par exemple le nom du cluster et de l'interface IP, ainsi que l'UUID, les IOPS, la latence, le débit, etc.

Affichage des travaux et des détails du système

Vous pouvez utiliser l' `jobs`API sous la `management-server` catégorie pour afficher les détails d'exécution des opérations asynchrones. L' `system`API sous la `management-server` catégorie vous permet d'afficher les détails des instances dans votre environnement Active IQ Unified Manager.

Affichage des travaux

Dans Active IQ Unified Manager, des opérations, telles que l'ajout et la modification de ressources sont réalisées par des invocations API synchrones et asynchrones. Les invocations planifiées pour une exécution asynchrone peuvent être suivies par un objet Job créé pour cette invocation. Chaque objet Job possède une clé unique d'identification. Chaque objet travail renvoie l'URI de l'objet travail pour vous permettre d'accéder à et de suivre la progression du travail. Vous pouvez utiliser cette API pour récupérer les détails de chaque exécution.

Cette API vous permet d'interroger tous les objets Job pour votre datacenter, 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 travaux spécifiques. Vous pouvez également utiliser la touche travail pour interroger les détails d'un travail spécifique et exécuter l'ensemble d'opérations suivant sur les ressources.

Catégorie	Verbe HTTP	Chemin	Description
serveur-gestion	OBTENEZ	/management-server/jobs	Affiche les détails du travail de tous les travaux. Sans ordre de tri, le dernier objet travail soumis est retourné en haut.

Catégorie	Verbe HTTP	Chemin	Description
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}` Saisissez la clé de travail de l'objet travail pour afficher les détails spécifiques de ce travail.	Affiche les détails de l'objet Job spécifique.

Affichage des détails du système

L'utilisation de l' `/management-server/system`API vous permet d'interroger les détails spécifiques aux instances de votre environnement Unified Manager. L'API renvoie des informations sur le produit et les services, telles que la version de Unified Manager installée sur votre système, votre UUID, le nom du fournisseur, le système d'exploitation hôte et le nom, Description et état des services exécutés sur l'instance Unified Manager.

Catégorie	Verbe HTTP	Chemin	Description
serveur-gestion	OBTENEZ	`/management-server/system`	Aucun paramètre d'entrée n'est requis pour l'exécution de cette API. Les détails système de l'instance Unified Manager actuelle sont renvoyés par défaut.

Gestion des événements et des alertes à l'aide d'API

Les `events` API , `alerts` et `scripts` de la `management-server` catégorie vous permettent de gérer les événements, les alertes et les scripts associés aux alertes dans votre environnement Active IQ Unified Manager.

Affichage et modification des événements

Unified Manager reçoit les événements générés sur ONTAP pour les clusters contrôlés et gérés par Unified Manager. Grâce à ces API, vous pouvez afficher les événements générés pour les clusters, puis les résoudre et les mettre à jour.

En exécutant la `GET` méthode de l' `/management-server/events`API, vous pouvez interroger les événements de votre data Center, y compris les données historiques. Utilisez les filtres intégrés, tels que le nom, le niveau d'impact, la zone d'impact, la gravité, état, nom de ressource et 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 soulevé, telles que la disponibilité, la capacité, la configuration, la sécurité, et de performances.

En exécutant l'opération DE CORRECTIF pour cette API, vous pouvez activer le workflow de résolution pour l'événement. Vous pouvez attribuer un événement à vous-même ou à un autre utilisateur et accuser réception de l'événement. Lors de l'exécution des 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, reportez-vous "Gestion des événements"à la section .

Catégorie	Verbe HTTP	Chemin	Description
serveur-gestion	OBTENEZ	`/management-server/events` `/management-server/events/{key}`	Lorsque vous exécutez la méthode obtenir TOUT, le corps de réponse comprend les détails de l'événement 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 la série suivante d'opérations sur les ressources. Le corps de réponse comprend les détails de cet événement.
serveur-gestion	CORRECTIF	`management-server/events/{key}`	Exécutez cette API pour attribuer un événement ou modifier l'état sur validé ou résolu. Vous pouvez également utiliser cette méthode pour attribuer l'événement à vous-même ou à un autre utilisateur. Il s'agit d'une opération synchrone.

Gestion des 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 l' `/management-server/alerts`API, vous pouvez configurer des alertes pour qu'elles envoient automatiquement des notifications lorsque des événements ou événements spécifiques de certains types de gravité se produisent.

Pour plus d'informations sur les alertes, reportez-vous "Gestion des alertes"à la section .

Catégorie	Verbe HTTP	Chemin	Description
serveur-gestion	OBTENEZ	`/management-server/alerts` `/management-server/alerts/{key}`	Recherchez toutes les alertes existantes dans votre environnement ou une alerte spécifique à l'aide de la clé d'alerte. Vous pouvez afficher les informations relatives aux alertes générées dans votre environnement : description des alertes, action, ID d'e-mail à destination duquel la notification est envoyée, événement et gravité.
serveur-gestion	POST	`/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 s'applique, si l'alerte est activée et si vous émettez des interruptions SNMP. Vous pouvez ajouter des informations supplémentaires pour lesquelles vous souhaitez générer l'alerte, telles que l'action, l'ID e-mail de notification, les détails du script, si vous ajoutez un script d'alerte, etc.
serveur-gestion	PATCH et SUPPRESSION	`management-server/events/{key}`	Ces méthodes permettent de modifier et de supprimer des alertes spécifiques. Vous pouvez modifier différents attributs, tels que la description, le nom, ainsi que l'activation et la désactivation de l'alerte. Vous pouvez supprimer une alerte lorsque celle-ci n'est plus requise.

Lors de la sélection d'une ressource pour l'ajout d'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 recevez des alertes uniquement pour les événements critiques du cluster. Vous ne recevez pas d'alertes concernant les événements critiques sur les nœuds, les agrégats, etc.

Gestion des scripts

En utilisant l' `/management-server/scripts`API, vous pouvez également associer une alerte à un script 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 générée pour un événement dans Unified Manager.

Pour plus d'informations sur les scripts, reportez-vous "Gestion des scripts"à la section .

Catégorie	Verbe HTTP	Chemin	Description
serveur-gestion	OBTENEZ	`/management-server/scripts`	Utilisez cette API pour interroger tous les scripts existants de votre environnement. Utilisez le filtre standard et commandez par opération pour afficher uniquement des scripts spécifiques.
serveur-gestion	POST	`/management-server/scripts`	Utilisez cette API pour ajouter une description pour le script et télécharger le fichier script associé à une alerte.

Gestion des workloads à l'aide d'API

Les API décrites ici couvrent les différentes fonctions de l'administration du stockage, notamment l'affichage des charges de travail du stockage, la création de LUN et de partages de fichiers, la gestion des niveaux de service de performance et des règles d'efficacité du stockage, ainsi que l'attribution des règles aux charges de travail du stockage.

Affichage des charges de travail de stockage à l'aide d'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 data Center. Ces API fournissent également une vue synthétique du nombre de charges de travail de stockage provisionnées dans votre environnement Active IQ Unified Manager et de leurs statistiques de capacité et de performance (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 data Center. Pour plus d'informations sur le filtrage de la réponse en fonction de colonnes spécifiques, reportez-vous à la documentation de référence sur les API disponible dans votre instance Unified Manager.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/workloads`

Affichez le récapitulatif 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 Performance. Les charges de travail de stockage qui s'affichent peuvent être pour tout partage de fichiers NFS, LUN ou CIFS. L'API offre une présentation des charges de travail de stockage, une vue d'ensemble des charges de travail de stockage provisionnées par Unified Manager, une présentation du data Center, un aperçu de l'espace total, utilisé et disponible et des IOPS dans le data Center, 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	OBTENEZ	`/storage-provider/workloads-summary`

Gestion des terminaux d'accès à l'aide d'API

Vous devez créer des terminaux d'accès ou des interfaces logiques (LIF) nécessaires pour le provisionnement des SVM, des LUN et des partages de fichiers. Vous pouvez afficher, créer, modifier et supprimer les terminaux d'accès des SVM, des LUN ou des partages de fichiers dans votre environnement Active IQ Unified Manager.

Affichez les terminaux d'accès

Vous pouvez afficher la liste des terminaux d'accès dans votre environnement Unified Manager à l'aide de la méthode suivante. Pour interroger une liste de terminaux d'accès d'un SVM, d'une LUN ou d'un partage de fichiers spécifique, vous devez entrer l'identifiant unique pour le SVM, la LUN ou le partage de fichiers. Vous pouvez également saisir la clé unique de point final d'accès pour récupérer les détails du point final d'accès particulier.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	OBTENEZ	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Ajoutez des terminaux d'accès

Vous pouvez créer des points finaux d'accès personnalisés et lui affecter les propriétés requises. Vous devez entrer les détails du point final d'accès que vous souhaitez créer en tant que paramètres d'entrée. Vous pouvez utiliser cette API, ou l'interface de ligne de commandes System Manager ou ONTAP pour créer un terminal 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 minimal de terminaux d'accès par nœud pour assurer le provisionnement efficace des LUN et des partages de fichiers. Vous devez configurer votre SVM avec au moins deux terminaux d'accès par nœud, un prenant en charge le protocole CIFS et/ou NFS, un autre prenant en charge le protocole iSCSI ou FCP.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

Supprime les points de terminaison d'accès

Vous pouvez supprimer un point final d'accès spécifique à l'aide de la méthode suivante. Vous devez fournir la clé de point final d'accès comme paramètre d'entrée pour supprimer un point final d'accès particulier.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	`/storage-provider/access-endpoints/{key}`

Modifier les points de terminaison d'accès

Vous pouvez modifier un point final d'accès et mettre à jour ses propriétés à l'aide de la méthode suivante. Vous devez fournir la clé de point final d'accès pour modifier un point final 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}`

Gestion du mappage Active Directory à l'aide d'API

Vous pouvez utiliser les API répertoriées ici pour gérer les mappages Active Directory sur le SVM requis pour le provisionnement des partages CIFS sur les SVM. Les mappages de Active Directory doivent être configurés pour le mappage des SVM avec ONTAP.

Afficher les mappages d'Active Directory

Vous pouvez afficher les détails de configuration des mappages Active Directory d'un SVM en utilisant la méthode suivante. Pour afficher les mappages d'Active Directory sur un SVM, vous devez saisir la clé SVM. Pour interroger les détails d'un mappage particulier, vous devez entrer la clé de mappage.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	OBTENEZ	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Ajouter un mappage Active Directory

Vous pouvez créer des mappages Active Directory sur un SVM en utilisant la méthode suivante. Vous devez entrer les détails de mappage comme paramètres d'entrée.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/active-directories-mappings`

Gestion des partages de fichiers à l'aide d'API

Vous pouvez utiliser l' `/storage-provider/file-shares`API pour afficher, ajouter, modifier et supprimer les volumes de partage de fichiers CIFS et NFS dans votre environnement de data Center.

Avant de provisionner les volumes des partages de fichiers, assurez-vous que le SVM a été créé et provisionné avec les protocoles pris en charge. Si vous affectez des niveaux de service de performances (PSLs) ou des politiques d'efficacité du stockage (PPE), pendant le provisioning, les PSLs ou PPE 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 les partages de fichiers automatiquement et ajoutés manuellement 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	OBTENEZ	`/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 à votre SVM. Vous devez entrer les détails du partage de fichiers que vous souhaitez créer, en tant que paramètres

d'entrée. Vous ne pouvez pas utiliser cette API pour ajouter des volumes FlexGroup.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/file-shares`

> Selon que les paramètres de la liste de contrôle d'accès (ACL) ou des paramètres de export policy sont fournis, les partages CIFS ou les 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, fournissant ainsi un accès à tous.

Création de volumes de protection des données : lorsque vous ajoutez des partages de fichiers à votre SVM, le type du volume qui est monté, par défaut, est `rw` (lecture-écriture). Pour la création de volumes de protection des données (DP), spécifiez `dp` comme valeur du `type` paramètre.

Supprimer des 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. En outre, vous devez entrer la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.

> Notez que vous ne pouvez mettre à jour qu'une seule propriété à une seule invocation de cette API. Pour plusieurs mises à jour, vous devez exécuter cette API autant de fois.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares/{key}`

Gestion des LUN à l'aide d'API

Vous pouvez utiliser l' `/storage-provider/luns`API pour afficher, ajouter, modifier et supprimer les LUN de l'environnement de data Center.

Avant de provisionner les LUN, assurez-vous que le SVM a été créé et provisionné avec les protocoles pris en charge. Si vous affectez des niveaux de service de performances (PSLs) ou des politiques d'efficacité du stockage (PPE) pendant le provisionnement, les PSLs ou PPE doivent être créés avant de créer le LUN.

Afficher les LUN

Pour afficher les LUN dans votre environnement Unified Manager, vous pouvez utiliser la méthode suivante. 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 toutes les LUN automatiquement et manuellement ajoutées à votre instance Unified Manager. Vous pouvez afficher les détails d'une LUN spécifique en exécutant cette API avec la clé LUN.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	OBTENEZ	`/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	POST	`/storage-provider/luns`

> Dans votre requête curl, si vous fournissez une valeur pour le paramètre facultatif nom_volume_tag dans l'entrée, cette valeur est utilisée lors de la dénomination du volume lors de la création de la LUN. Cette balise permet de rechercher facilement le volume. Si vous fournissez la clé de volume dans la demande, le marquage est ignoré.

Supprimer les LUN

Vous pouvez utiliser la méthode suivante pour supprimer une LUN spécifique. Vous devez fournir la clé de LUN pour supprimer une LUN particulière.

> Si vous avez créé un volume dans ONTAP, puis provisionné des LUN via Unified Manager sur ce volume, lorsque vous supprimez toutes 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 une LUN et mettre à jour ses propriétés. Vous devez fournir la clé de LUN pour modifier une LUN particulière. Vous devez également entrer la propriété de LUN à mettre à jour avec sa valeur. Pour mettre à jour des baies LUN à l'aide de cette API, vous devez consulter les recommandations de la section « recommandations d'utilisation des API ».

Vous ne pouvez mettre à jour qu'une seule propriété à une seule invocation de cette API. Pour plusieurs mises à jour, vous devez exécuter cette API autant de fois.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/luns/{key}`

Gestion des niveaux de service en matière de performances à l'aide d'API

Vous pouvez afficher, créer, modifier et supprimer les niveaux de services de performances à l'aide des API du fournisseur de stockage pour votre Active IQ Unified Manager.

Afficher les niveaux de services de performances

Utilisez la méthode suivante pour afficher les niveaux de services de performances à 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 performances spécifique, vous devez saisir l'ID unique du niveau de service de performance pour récupérer ses détails.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	OBTENEZ	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Ajouter des niveaux de service de performance

Utilisez la méthode suivante pour créer des niveaux de service 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 requis pour les charges de travail de stockage. Entrez 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	POST	`/storage-provider/performance-service-levels`

Supprimez les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour supprimer un niveau de service de performance spécifique. Vous ne pouvez pas supprimer un niveau de service de performances s'il est affecté 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 Performance comme paramètre d'entrée pour supprimer un niveau de service Performance spécifique.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	`/storage-provider/performance-service-levels/{key}`

Modifier les niveaux de services de performances

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 affecté à une charge de travail. Vous devez fournir l'ID unique de l' pour modifier un niveau de service de performances particulier. Vous devez également entrer 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}`

Affichage des fonctionnalités d'agrégats en fonction des niveaux de service de performances

Vous pouvez utiliser la méthode suivante pour interroger les capacités d'agrégat en fonction des niveaux de service de performances. Cette API renvoie la liste des agrégats disponibles dans votre data Center et indique les fonctionnalités en termes de niveaux de service de performances que ces agrégats peuvent prendre en charge. Lors du provisionnement des charges de travail sur un volume, il est possible de voir la capacité d'un agrégat pour prendre en charge un niveau de Service Performance spécifique et de provisionner les charges de travail selon cette fonctionnalité. 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 dans l'interface utilisateur Web de Unified Manager.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	OBTENEZ	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Gestion des règles d'efficacité du stockage à l'aide d'API

Vous pouvez afficher, créer, modifier et supprimer les règles d'efficacité du stockage en utilisant les API du fournisseur de stockage.

Notez les points suivants :

- Il n'est pas obligatoire d'attribuer une règle d'efficacité du stockage lors de la création d'une charge de travail sur Unified Manager.
- Vous ne pouvez pas annuler l'affectation d'une stratégie d'efficacité du stockage à une charge de travail après son affectation.
- Si une charge de travail dispose de certains 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 applicable lorsque vous ajoutez les charges de travail de stockage sur Unified Manager.

Consultez les règles d'efficacité du stockage

Utilisez la méthode suivante pour afficher les règles d'efficacité du stockage avant de les attribuer aux charges de travail de stockage. Cette API répertorie l'ensemble des règles 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 règle Storage Efficiency spécifique, vous devez entrer l'ID unique de la règle pour en récupérer les détails.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	OBTENEZ	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Ajoutez des règles relatives à l'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour créer des règles personnalisées d'efficacité du stockage et les attribuer à vos charges de travail de stockage si les règles définies par le système ne répondent pas aux besoins de provisionnement de vos charges de travail de stockage. Entrez les détails de la règle d'efficacité du stockage que vous souhaitez créer, en tant que paramètres d'entrée.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/storage-efficiency-policies`

Supprimez les règles d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour supprimer une stratégie d'efficacité du stockage spécifique. Vous ne pouvez pas supprimer une stratégie d'efficacité du stockage s'il est affecté 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 règle d'efficacité du stockage sous forme de paramètre d'entrée pour supprimer une règle d'efficacité du stockage en particulier.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	`/storage-provider/storage-efficiency-policies/{key}`

Modification des stratégies d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour modifier une stratégie d'efficacité du stockage et mettre à jour ses propriétés. Vous ne pouvez pas modifier une règle d'efficacité du stockage définie par le système ou affectée à une charge de travail. Vous devez fournir l'ID unique de la politique d'efficacité du stockage pour modifier une politique d'efficacité de stockage en particulier. En outre, vous devez fournir la propriété que vous voulez mettre à jour, ainsi que sa valeur.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/storage-efficiency-policies/{key}`

Workflows API communs pour la gestion du stockage

Les workflows courants fournissent aux développeurs d'applications client des exemples de la façon dont une application client peut appeler les API Active IQ Unified Manager pour exécuter des fonctions courantes de gestion du stockage. Cette section contient certains de ces exemples de flux de travail.

Les flux de travail décrivent les quelques cas d'utilisation courants de gestion du stockage ainsi que des exemples de codes à utiliser. Chacune des tâches est décrite à l'aide d'un processus de workflow composé d'un ou de plusieurs appels API.

Présentation des appels API utilisés dans les workflows

Vous pouvez consulter la page de documentation en ligne de votre instance Unified Manager qui comprend les détails de chaque appel d'API REST. Ce document ne répète pas les détails de la documentation en ligne. Chaque appel API utilisé dans les exemples de flux de travail de ce document comprend uniquement les informations dont vous avez besoin pour localiser l'appel sur la page de documentation. Après avoir localisé un appel API spécifique, vous pouvez vérifier les détails complets de l'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 au sein d'un flux de travail afin de localiser l'appel sur la page de documentation :

- Catégorie : les appels API sont organisés sur la page de documentation en zones ou catégories liées aux fonctions. Pour localiser un appel API spécifique, faites défiler la page jusqu'en bas et cliquez sur la catégorie 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 à laquelle l'action s'applique dans le cadre d'un appel. La chaîne de chemin d'accès est ajoutée à l'URL principale pour former l'URL complète identifiant la ressource.

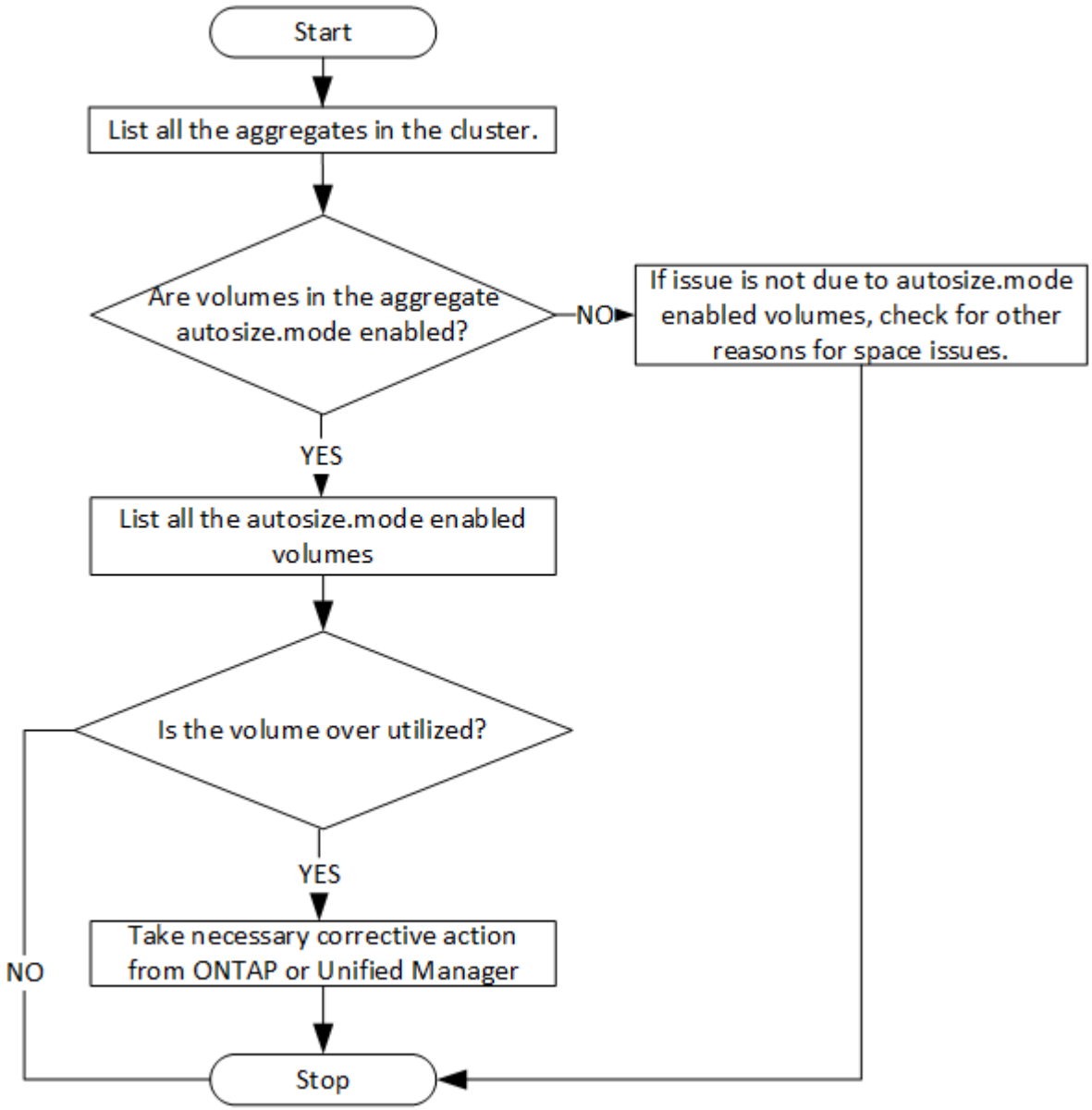
Détermination des problèmes d'espace dans les agrégats à l'aide d'API

Vous pouvez utiliser les API de data Center de Active IQ Unified Manager pour surveiller la disponibilité et l'utilisation de l'espace dans vos volumes. Vous pouvez identifier les problèmes d'espace de votre volume et les ressources de stockage sur-exploitées ou sous-utilisées,

Les API de data Center pour les agrégats récupère les informations pertinentes sur l'espace disponible et utilisé, et les paramètres d'efficacité pour le gain d'espace. Vous pouvez également filtrer les informations récupérées en fonction des attributs spécifiés.

L'une des méthodes permettant de déterminer le manque d'espace de vos agrégats consiste à vérifier si il existe des volumes dans votre environnement où le mode de taille automatique est activé. Vous devez ensuite identifier les volumes sur-utilisés et effectuer les actions correctives nécessaires.

L'organigramme suivant illustre le processus de récupération des informations sur les volumes dont le mode autotaille est activé :



Ce flux suppose que les clusters ont déjà été créés dans ONTAP et ajoutés à Unified Manager.

1. Obtenir la clé de cluster, sauf si vous en connaissez la valeur :

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/cluster/clusters`

2. En utilisant la clé de cluster comme paramètre de filtre, interrogez les agrégats sur ce cluster.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/storage/aggregates`

3. Depuis le délai de réponse, analysez l'utilisation de l'espace par les agrégats et déterminez quels agrégats ont des problèmes d'espace. Pour chaque agrégat ayant un problème d'espace, procurez-vous la clé d'agrégat à partir de la même sortie JSON.
4. À l'aide de chaque clé d'agrégat, filtrez tous les volumes dont la valeur du paramètre autosize.mode est définie sur `grow`.

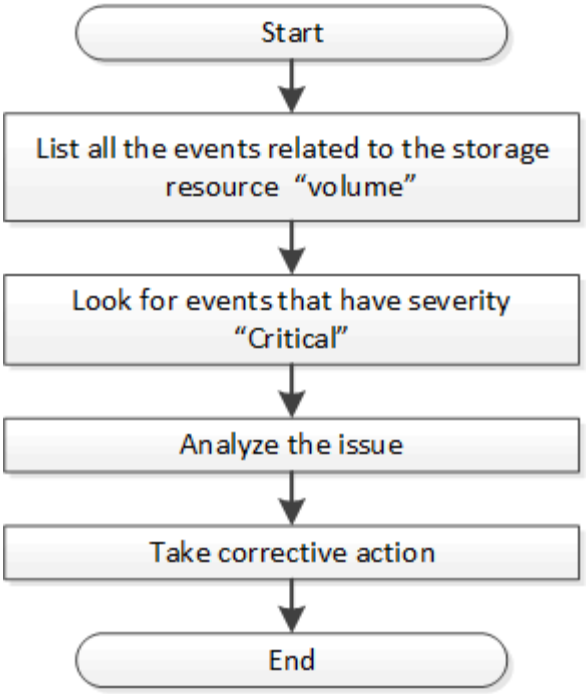
Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/storage/volumes`

5. Analysez les volumes sur-utilisés.
6. Effectuez les actions correctives nécessaires, telles que le déplacement du volume dans les agrégats, pour résoudre les problèmes d'espace de votre volume. Vous pouvez effectuer ces actions à partir de l'interface Web de ONTAP ou de Unified Manager.

Détermination des problèmes dans les objets de stockage à l'aide des API d'événements

Lorsqu'un objet de stockage de votre data Center franchit un seuil, vous obtenez une notification à propos de cet événement. Grâce à cette notification, vous pouvez analyser le problème et appliquer les actions correctives nécessaires à l'aide des `events` API.

Ce flux de travail utilise l'exemple d'un volume en tant qu'objet de ressource. Vous pouvez utiliser les `events` API pour récupérer la liste des événements liés à un volume, analyser les problèmes critiques pour ce volume, puis prendre des mesures correctives pour corriger le problème.



Procédez comme suit afin de déterminer les problèmes rencontrés sur votre volume avant de prendre les mesures correctives qui s'imposent.

Étapes

1. Analysez les notifications d'événements Active IQ Unified Manager critiques pour les volumes de votre data Center.
2. Interroger tous les événements pour les volumes à l'aide des paramètres suivants de l'API /management-Server/events :
   ```
   "resource_type": "volume"
   "severity": "critical"
   ```

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	/serveur-gestion/événements

3. Affichez la sortie et analysez les problèmes des volumes spécifiques.
4. Effectuez les actions nécessaires en utilisant l'API REST ou l'interface utilisateur Web de Unified Manager pour résoudre les problèmes.

Dépannage des volumes ONTAP à l'aide d'API de passerelle

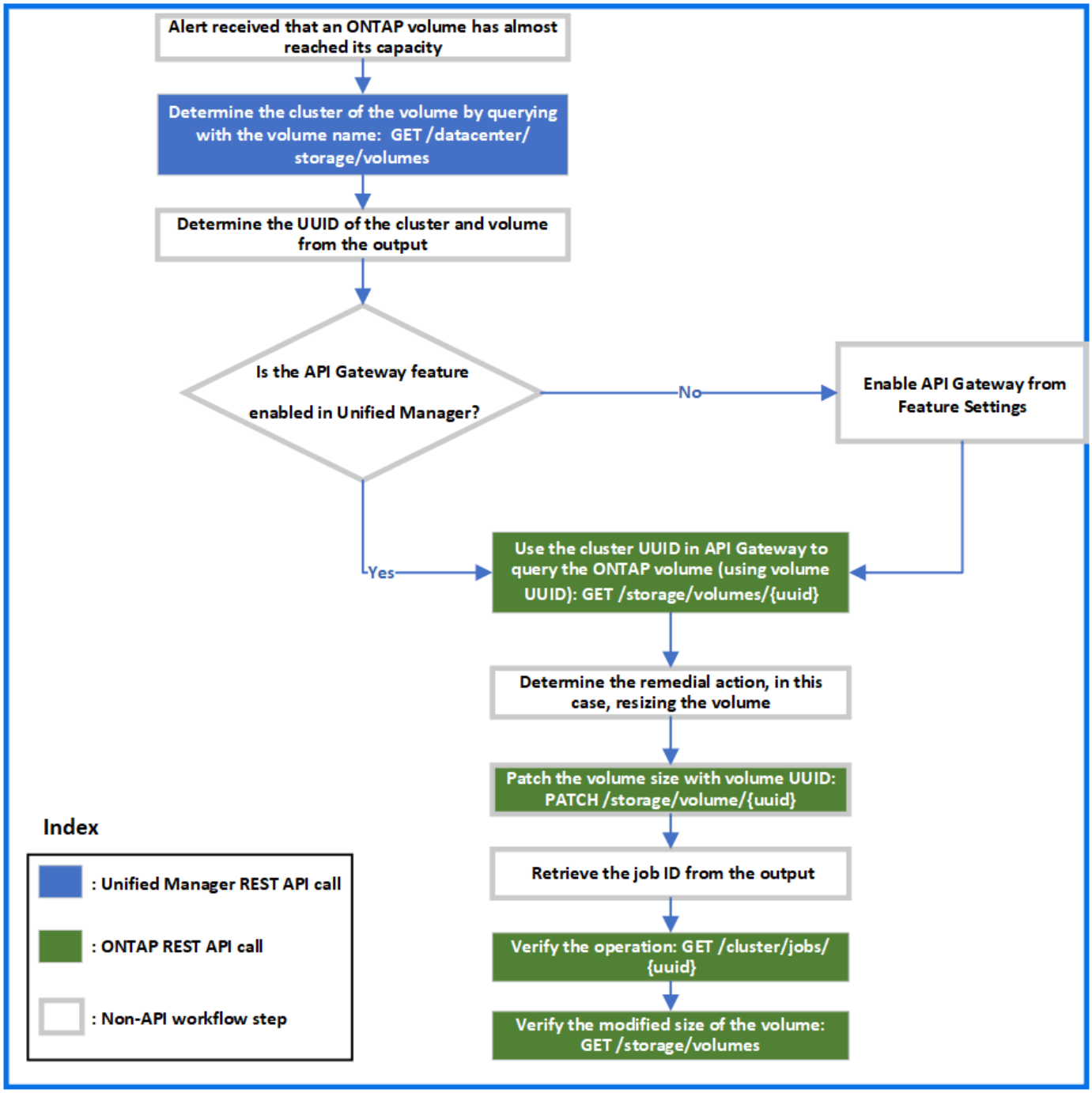
Les API de passerelle servent de passerelle pour appeler les API ONTAP pour interroger les informations sur vos objets de stockage ONTAP et prendre les mesures correctives nécessaires pour résoudre les problèmes signalés.

Ce flux de travail prend un exemple d'utilisation dans lequel un événement est déclenché lorsqu'un volume ONTAP atteint presque sa capacité. Ce workflow explique 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 que :

- Vous connaissez les API de passerelle et leur utilisation. Pour plus d’informations, voir "Accès aux API ONTAP via un accès proxy".
- Vous connaissez l’utilisation des API REST de ONTAP. Pour plus d’informations sur l’utilisation des API REST ONTAP, reportez-vous à la section "Documentation sur l’automatisation ONTAP".
- Vous êtes administrateur d’applications.
- Le cluster sur lequel vous souhaitez exécuter les opérations d’API REST est pris en charge par ONTAP 9.5 ou version ultérieure et le cluster est ajouté à Unified Manager via HTTPS.

Le schéma suivant illustre chaque étape du workflow pour le dépannage des problèmes liés à l’utilisation de la capacité des volumes ONTAP.



Ce workflow couvre les points d'invocation des API REST Unified Manager et ONTAP.

1. Noter le nom du volume provenant de l'événement afin de prévenir l'utilisation de la capacité du volume.
2. En utilisant le nom du volume comme valeur dans le paramètre name, interrogez le volume en exécutant l'API Unified Manager suivante.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/storage/volumes`

3. Récupère l'UUID et l'UUID de volume du cluster à partir du résultat.

4. Dans l'interface utilisateur Web d'Unified Manager, accédez à **général** > **Paramètres de fonctionnalité** > **passerelle API** pour vérifier si la fonctionnalité passerelle API est activée. Sauf si elle est activée, les API de la catégorie passerelle ne sont pas disponibles pour que vous puissiez appeler. Activez la fonction si elle est désactivée.
5. Utilisez l'UUID de cluster pour exécuter l'API ONTAP /`storage/volumes/{uuid}`via une passerelle d'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 d'API, les identifiants Unified Manager sont transférés en interne à des fins d'authentification, et vous n'avez pas besoin d'exécuter une étape d'authentification supplémentaire pour l'accès individuel au cluster.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : stockage	OBTENEZ	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

> Dans /gateways/{UUID}/{path}, la valeur de {UUID} doit être remplacée par l'UUID de cluster sur lequel l'opération DE REPOS doit être effectuée. {path} doit être remplacé par l'URL REST ONTAP /stockage/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}`

Commande Curl exemple

```
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>"
```

6. À partir des résultats, déterminez la taille, l'utilisation et la mesure corrective à prendre. Dans ce flux de travail, la mesure corrective prise consiste à redimensionner le volume.
7. Utilisez l'UUID de cluster et exécutez l'API ONTAP suivante via la passerelle d'API pour redimensionner le volume. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, reportez-vous à l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : stockage	CORRECTIF	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

> En plus de l'UUID et de l'UUID de volume du cluster, vous devez saisir une valeur pour le paramètre size permettant le redimensionnement du volume. Assurez-vous de saisir la valeur *dans octets*. Par exemple, si vous souhaitez augmenter la taille d'un volume de 100 Go à 120 Go, entrez la valeur de la taille du paramètre à la fin de la requête : `-d {\"size\": 128849018880}"`

Commande Curl exemple

```
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.

8. Vérifiez si le travail a bien été exécuté à l'aide de l'UUID du travail. Utilisez l'UUID et l'UUID de cluster pour exécuter l'API ONTAP suivante via la passerelle d'API. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, reportez-vous à l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : cluster	OBTENEZ	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.

9. Exécutez l'API ONTAP suivante pour interroger les détails du volume redimensionné. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, reportez-vous à l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : stockage	OBTENEZ	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

La sortie affiche une taille de volume accrue de 120 Go.

Des workflows API pour la gestion des workloads

Active IQ Unified Manager permet de provisionner et de modifier les charges de travail de stockage (LUN, partages de fichiers NFS et partages CIFS). Le provisionnement s'effectue en plusieurs étapes, de la création des SVM (Storage Virtual machine) à l'application des règles de niveau de service en matière de performances et d'efficacité du stockage aux charges de travail du stockage. La modification des charges de travail consiste en des étapes de modification de paramètres spécifiques et d'activation de fonctionnalités supplémentaires.

Les flux de production suivants sont décrits :

- Flux de production pour le provisionnement des SVM (Storage Virtual machines) sur Unified Manager.

> Ce flux de travail est requis avant de provisionner des LUN ou des partages de fichiers sur Unified Manager.

- Provisionnement des partages de fichiers.
- Provisionner les LUN.
- Modification des LUN et des partages de fichiers (à l'aide de l'exemple de mise à jour du paramètre Performance Service Level pour les charges de travail du stockage).
- Modification d'un partage de fichiers NFS pour prendre en charge le protocole CIFS
- Modification des charges de travail pour mettre à niveau QoS vers AQoS

> Pour chaque workflow de provisionnement (partages de LUN et de fichiers), veillez à avoir terminé le workflow de vérification des SVM sur les clusters.

Vous devez également lire les recommandations et limites avant d'utiliser chaque API dans les workflows. Les détails pertinents des API sont disponibles dans leurs différentes sections répertoriées dans les concepts et références associés.

Vérification des SVM sur les clusters à l'aide d'API

Avant de provisionner des partages de fichiers ou des LUN, vous devez vérifier si les clusters disposent de SVM (Storage Virtual machines) créés.

> Le flux de travail suppose que des clusters ONTAP doivent avoir été ajoutés à Unified Manager et que la clé de cluster a été obtenue. Les clusters doivent disposer des licences requises pour provisionner les LUN et les partages de fichiers sur eux.

1. Vérifier si le cluster a un SVM créé ou non.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

CURL d'échantillon

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si la clé SVM n'est pas renvoyée, créer la SVM. Pour la création des SVM, il faut la clé de cluster sur laquelle vous provisionnez la SVM. Vous devez également spécifier le nom du SVM. Effectuez la procédure suivante.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Obtenir la clé de cluster.

CURL d'échantillon

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. Depuis le résultat, obtenir la clé du cluster, puis l'utiliser comme entrée pour la création de la SVM.

> Lors de la création du SVM, s'assurer qu'il prend en charge tous les protocoles requis pour le provisionnement des LUN et des partages de fichiers sur eux, par exemple, CIFS, NFS, FCP, Et iSCSI. Les workflows 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 le SVM.

Catégorie	Verbe HTTP	Chemin
data center	POST	`/datacenter/svm/svms`

CURL d'échantillon

Entrer les détails de l'objet SVM en tant que 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,uuid=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,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcp\": { \"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 la SVM que vous avez créée.

4. Vérifier la création du SVM à l'aide de la clé d'objet de travail pour la requête. Si la SVM est correctement créée, la clé de SVM est renvoyée dans la réponse.

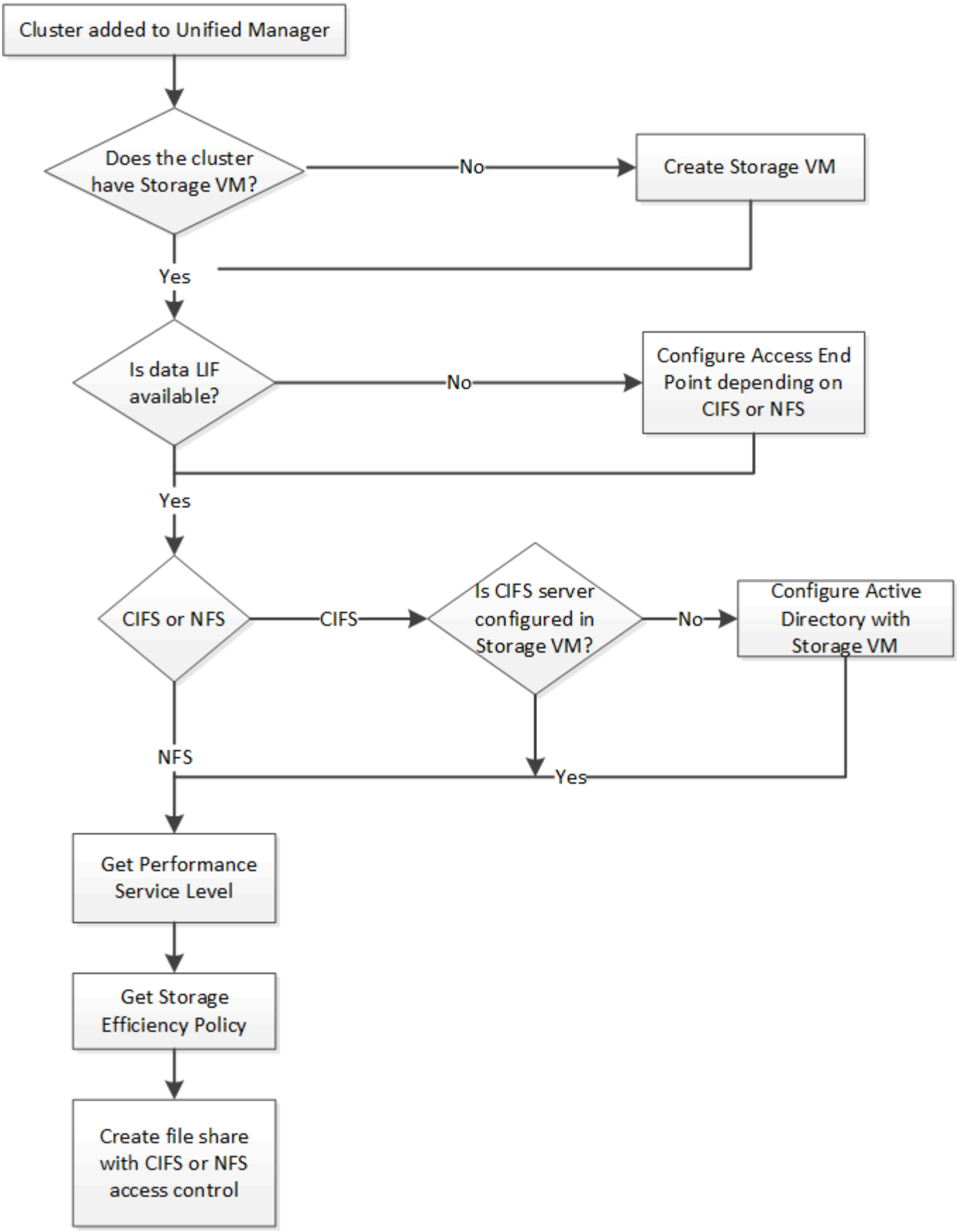
Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

Provisionnement des partages de fichiers CIFS et NFS à l'aide d'API

Vous pouvez provisionner les partages CIFS et les partages de fichiers NFS sur vos SVM

(Storage Virtual machines) en utilisant les API de provisionnement fournies dans Active IQ Unified Manager. Ce workflow de provisionnement détaille les étapes à suivre pour récupérer les clés des SVM, Performance Service Levels et Storage Efficiency Policies avant de créer les partages de fichiers.

Le schéma suivant illustre chaque étape d’un workflow de provisionnement de partage de fichiers. Il inclut le provisionnement des partages CIFS et des partages de fichiers NFS.


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

Vérifiez les points suivants :

- Les clusters ONTAP ont été ajoutés à Unified Manager et la clé de cluster a été obtenue.
- Les 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 terminaux d'accès sont disponibles sur le SVM sur lequel vous souhaitez créer le partage CIFS. Obtenez la liste des terminaux d'accès disponibles sur le SVM :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

CURL d'échantillon

```
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, procurez-vous la clé du point de terminaison d'accès, sinon créez le point de terminaison d'accès.

Veillez à 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 terminal d'accès avec le protocole CIFS activé sur celui-ci.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

CURL d'échantillon

Vous devez entrer les détails du point final 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 travail que vous pouvez utiliser pour vérifier le noeud final d'accès que vous avez créé.

3. Vérifiez le point d'accès :

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

4. Déterminez si vous devez créer un partage CIFS ou NFS. Pour créer des partages CIFS, suivez ces sous-étapes :

   a. Déterminer si le serveur CIFS est configuré sur votre SVM, il s'agit de déterminer si un mappage Active Directory est créé sur le SVM.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/active-directories-mappings`

   b. Si le mappage Active Directory est créé, prendre la clé, sinon créer le mappage Active Directory sur la SVM.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/active-directories-mappings`

CURL d'échantillon

Vous devez entrer les détails de 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 dépanner et de relancer la demande.

5. Obtenir la clé SVM pour le SVM sur lequel vous souhaitez créer le partage CIFS ou le partage de fichiers NFS, comme décrit dans la rubrique *vérification des SVM sur clusters* workflow.
6. Obtenir la clé pour le niveau de service des performances en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/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 sur `true`. À partir de la sortie, procurez-vous la clé du niveau de service de performances que vous souhaitez appliquer sur le partage de fichiers.

7. Si vous le souhaitez, vous pouvez également obtenir la clé de stratégie d'efficacité du stockage pour la stratégie d'efficacité du stockage que vous souhaitez appliquer au partage de fichiers en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/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 les règles d'exportation. Les sous-étapes suivantes fournissent des informations si vous souhaitez créer un partage de fichiers pour la prise en charge d'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, reportez-vous à la rubrique *modification des charges de travail du stockage*.

a. Pour la création uniquement d'un partage CIFS, collectez les informations de la liste de contrôle d'accès (ACL). Pour créer le partage CIFS, indiquez des valeurs valides pour les paramètres d'entrée suivants. Pour chaque groupe d'utilisateurs que vous attribuez, une liste de contrôle d'accès est créée lorsqu'un partage CIFS/SMB est provisionné. En fonction des valeurs que vous saisissez 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 valeurs d'échantillon

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. Pour la création uniquement d'un partage de fichiers NFS, collectez les informations de l'export policy. Pour créer le partage de fichiers NFS, indiquez des valeurs valides pour les paramètres d'entrée suivants. En fonction de vos valeurs, l'export policy est jointe au partage de fichiers NFS lors de sa création.

   > Lors du provisionnement du partage NFS, vous pouvez créer une export policy en fournissant toutes les valeurs requises ou fournir la clé export policy et réutiliser une export policy existante. Si vous souhaitez réutiliser une export policy pour la machine virtuelle de stockage, vous devez ajouter la clé export policy. À moins que vous ne connaissiez la clé, vous pouvez récupérer la clé de la règle d'export à l'aide de `/datacenter/protocols/nfs/export-policies` l'API. Pour créer une nouvelle règle, vous devez entrer les règles comme indiqué dans l'exemple suivant. Pour les règles saisies, l'API tente de rechercher une export policy existante en faisant correspondre l'hôte, la VM de stockage et les règles. S'il existe une export policy existante, elle est utilisée. Dans le cas contraire, une nouvelle export-policy est créée.

   Une commande curl avec des valeurs d'échantillon

```
"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 stratégie d'exportation, fournissez les valeurs valides des paramètres d'entrée obligatoires pour les partages de fichiers CIFS et NFS :

Storage Efficiency Policy est un paramètre facultatif pour la création de partages de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/file-shares`

La sortie JSON affiche une clé d'objet travail 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 objet travail renvoyée dans l'interrogation du travail :

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/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	OBTENEZ	`/storage-provider/file-shares/{key}`

Sortie JSON échantillon

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 appelle l' `/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",
```

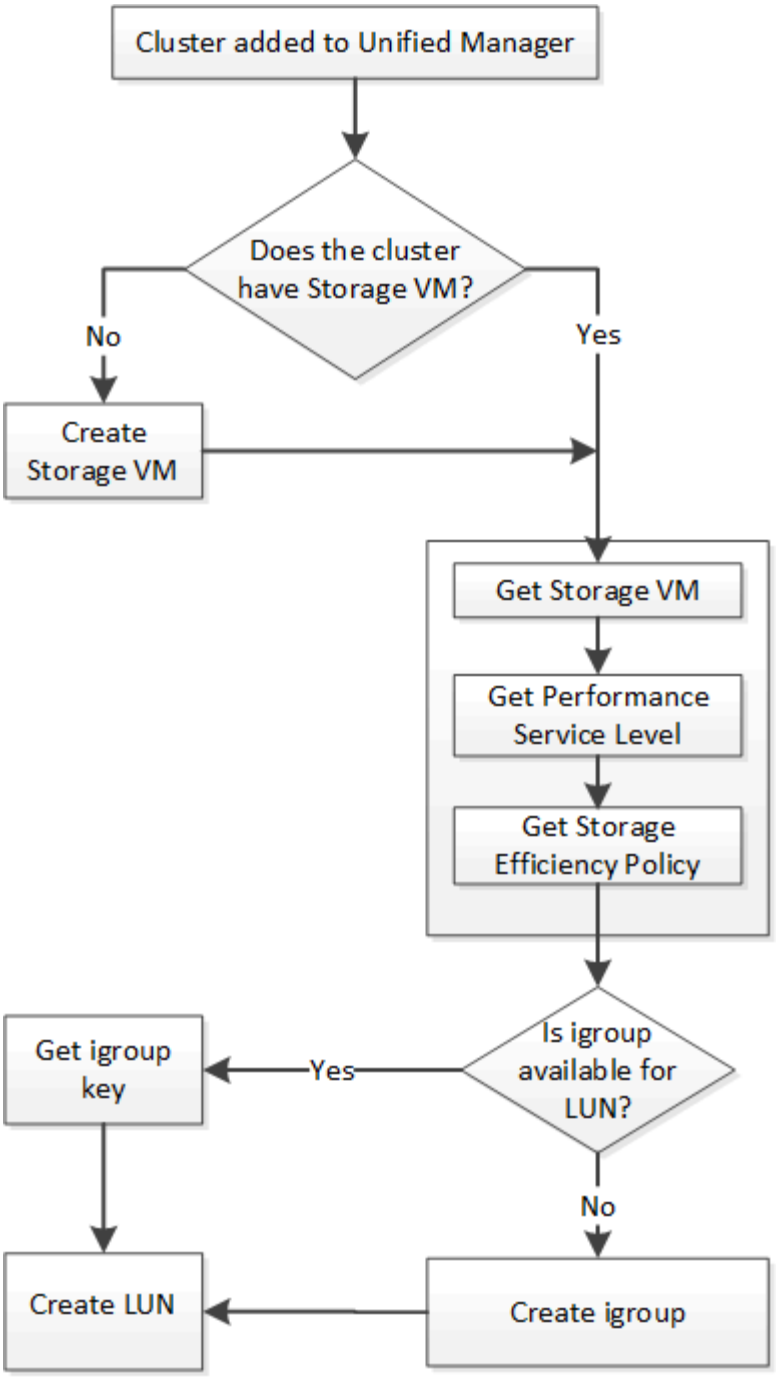
```
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "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"
        }
    }
}
```


Provisionnement des LUN à l’aide d’API

Vous pouvez provisionner des LUN sur vos SVM (Storage Virtual machines) en utilisant les API de provisionnement fournies par Active IQ Unified Manager. Ce workflow de provisionnement détaille les étapes à suivre pour récupérer les clés des SVM, les niveaux de service performances et les règles d’efficacité du stockage avant de créer la LUN.

Le schéma suivant illustre les étapes d’un workflow de provisionnement de LUN.



Ce flux de travail 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. Obtenir la clé SVM pour le SVM sur lequel vous souhaitez créer la LUN, comme décrit dans la rubrique *Vérification des SVM sur les clusters* workflow.
2. Obtenir la clé pour le niveau de service des performances en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/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 sur `true`. Dans le résultat de cette commande, vous devez obtenir la clé du niveau de service de performances que vous souhaitez appliquer sur le LUN.

3. Si vous le souhaitez, vous pouvez également obtenir la clé de la politique d'efficacité du stockage que vous souhaitez appliquer sur la LUN en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/storage-efficiency-policies`

4. Déterminez si des groupes initiateurs (igroups) ont été créés pour autoriser l'accès à la cible de LUN que vous souhaitez créer.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Vous devez saisir la valeur de paramètre pour indiquer la SVM pour laquelle le groupe initiateur a autorisé l'accès. En outre, pour effectuer une requête sur un groupe initiateur spécifique, entrez le nom de ce groupe initiateur (clé) comme paramètre d'entrée.

5. Dans le résultat de cette commande, si vous trouvez le groupe initiateur auquel vous souhaitez accorder l'accès, obtenez la clé. Sinon, créez le groupe initiateur.

Catégorie	Verbe HTTP	Chemin
data center	POST	`/datacenter/protocols/san/igroups`

Vous devez entrer les détails du groupe initiateur que vous souhaitez créer en tant que paramètres d'entrée. Il s'agit d'un appel synchrone pour vérifier la création du groupe initiateur dans la sortie. En cas d'erreur, un message s'affiche pour vous permettre de dépanner et de relancer l'API.

6. Créer la LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/luns`

Pour créer la LUN, assurez-vous d'avoir ajouté les valeurs récupérées en tant que paramètres d'entrée obligatoires.

> La stratégie d'efficacité du stockage est un paramètre facultatif pour la création des LUN.

CURL d'échantillon

Vous devez entrer tous les détails de la LUN que vous souhaitez créer en tant que paramètres d'entrée.

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier la LUN que vous avez créée.

7. Vérifiez la création de la LUN à l'aide de la clé de l'objet travail renvoyée dans l'interrogation du travail :

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

À la fin de la réponse, vous voyez la clé de la LUN créée.

8. Vérifiez la création de la LUN en exécutant l'API suivante avec la clé renvoyée :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Sortie JSON échantillon

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 appelle `/storage-provider/performance-service-levels/` l'API pour attribuer le niveau de services de performance à la LUN.

== étapes de dépannage en cas d'échec de la création ou du mappage de LUN

À l'issue de ce workflow, il se peut que la création de LUN ait échoué. Même si la LUN est correctement créée, le mappage de LUN avec le groupe initiateur peut échouer en raison d'une indisponibilité d'une LIF SAN ou d'un point de terminaison d'accès sur le nœud sur lequel vous créez la LUN. En cas de défaillance, le message suivant s'affiche :

```
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 ce problème.

1. Créer un point d'accès prenant en charge le protocole ISCSI/FCP sur le SVM sur lequel vous avez essayé de créer la LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

CURL d'échantillon

Vous devez entrer les détails du point final d'accès que vous souhaitez créer, en tant que paramètres d'entrée.

> Assurez-vous que dans le paramètre d'entrée vous avez ajouté l'adresse pour indiquer le nœud d'origine de la LUN et l'adresse ha pour indiquer le nœud partenaire du nœud de départ. Lorsque vous exécutez cette opération, des terminaux d'accès sont créés sur le nœud de rattachement et le nœud partenaire.

2. Interroger le travail avec la clé objet Job renvoyée dans la sortie JSON pour vérifier qu'elle s'exécute correctement pour ajouter les terminaux d'accès sur la SVM et que les services iSCSI/FCP ont été activés sur la SVM.

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

Sortie JSON échantillon

À la fin de la sortie, vous pouvez voir la clé des points d'extrémité d'accès créés. Dans le résultat suivant, la valeur "nom": "AccessEndpointKey" indique le noeud final d'accès créé sur le noeud d'origine du LUN, pour lequel la clé est 9c964258-14ef-11ea-95e2-00a098e32c28. La valeur "name": "AccessEndpointHADKey" indique le noeud final d'accès créé sur le noeud partenaire du noeud d'origine, pour lequel la clé est 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modifiez la LUN pour mettre à jour le mappage de groupe initiateur. Pour plus d'informations sur la modification des flux de travail, reportez-vous à la section « Modifier les charges de travail de stockage ».

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/lun/{key}`

Dans le champ d'entrée, spécifiez la clé igroup avec laquelle vous souhaitez mettre à jour le mappage de LUN, ainsi que la clé de LUN.

CURL d'échantillon

La sortie JSON affiche une clé d'objet travail que vous pouvez utiliser pour vérifier si le mappage a réussi.

4. Vérifiez le mappage de LUN en interrogeant la clé de LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Sortie JSON échantillon

Dans le résultat, vous voyez que la LUN a été correctement mappée avec le groupe initiateur (clé d19ec2fa-fec7-11e8-b23d-00a098e32c28) avec lequel elle a été initialement mise en service.

Modification des 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 dont les paramètres sont manquants ou à modifier les paramètres existants.

Ce flux de travail utilise un exemple de mise à jour des niveaux de service de performance pour les LUN et les partages de fichiers.

> Le flux de travail suppose que le partage de fichiers ou de LUN a été provisionné avec des niveaux de service de performance.

Modification des 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.
- Règles d'efficacité du stockage.
- Niveau de service de performances.
- Les paramètres de la liste de contrôle d'accès (ACL).
- Paramètres des export-policy. Vous pouvez également supprimer des paramètres d'export policy et rétablir les règles d'export policy par défaut (vides) sur le partage de fichiers.

> Lors d'une exécution d'API unique, vous ne pouvez mettre à jour qu'un 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. Procurez-vous la clé de partage de fichiers CIFS ou NFS du partage de fichiers à mettre à jour. Elle interroge tous les partages de fichiers sur votre data Center. Ignorez cette étape si vous connaissez déjà la

clé de partage de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares`

2. Affichez les détails du partage de fichiers en exécutant l'API suivante avec la clé de partage de fichiers obtenue.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/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": {}
      },
```

3. Obtenez la clé du niveau de service de performances que vous souhaitez attribuer à ce partage de fichiers. Aucune stratégie n'est actuellement attribuée à cette règle.

Catégorie	Verbe HTTP	Chemin
Niveaux de services de performances	OBTENEZ	`/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 sur `true`. À partir de la sortie, procurez-vous la clé du niveau de service de performances que vous souhaitez appliquer au partage de fichiers.

4. Appliquez le niveau de service 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, avec la clé

de partage de fichiers. Dans ce cas, c'est la clé du niveau de service de performance.

CURL d'échantillon

```
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 terminaux d'accès des nœuds home et Partner ont été créés correctement.

5. Vérifiez si le niveau de service de performances a été ajouté au partage de fichiers à l'aide de la clé d'objet travail affichée dans votre sortie.

Catégorie	Verbe HTTP	Chemin
Serveur de gestion	OBTENEZ	`/management-server/jobs/{key}`

Si vous effectuez une requête en fonction de l'ID de l'objet travail, vous voyez si le partage de fichiers a été mis à jour avec succès. En cas de défaillance, dépannez la panne et exécutez de nouveau l'API. Lors de la création réussie, interroger le partage de fichiers pour voir l'objet modifié :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/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"
            }
        }
```

Mise à jour des LUN

Lors de la mise à jour d'une LUN, vous pouvez modifier les paramètres suivants :

- Capacité ou taille
- Paramètre en ligne ou hors ligne
- Règles d'efficacité du stockage
- Niveau de service de performances
- Mappage de LUN

> Lors d'une exécution d'API unique, vous ne pouvez mettre à jour qu'un paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performances à une LUN. Vous pouvez utiliser la même procédure pour mettre à jour toute autre propriété de LUN.

1. Procurez-vous la clé LUN du LUN que vous souhaitez mettre à jour. Cette API renvoie les détails de toutes LES LUN de votre data Center. Ignorez cette étape si vous connaissez déjà la clé LUN.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	OBTENEZ	`/storage-provider/luns`

2. Afficher les détails de la LUN en exécutant l'API suivante avec la clé de LUN obtenue.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

   Pour afficher les détails de la LUN dans le résultat de la commande. Vous pouvez voir qu'aucun niveau de service de performances n'est attribué à cette LUN.

   Sortie JSON échantillon

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Obtenez la clé du niveau de service de performances que vous souhaitez attribuer à la LUN.

Catégorie	Verbe HTTP	Chemin
Niveaux de services de performances	OBTENEZ	`/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 sur `true`. Dans le résultat de cette commande, vous devez obtenir la clé du niveau de service de performances que vous souhaitez appliquer sur le LUN.

4. Appliquez le niveau de service de performances sur la LUN.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	`/storage-provider/lun/{key}`

Dans l'entrée, vous devez spécifier uniquement le paramètre à mettre à jour et la clé LUN. Dans ce cas, c'est la clé du niveau de service de performances.

CURL d'échantillon

```
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 tâche que vous pouvez utiliser pour vérifier la LUN que vous avez mise à jour.

5. Afficher les détails de la LUN en exécutant l'API suivante avec la clé de LUN obtenue.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Pour afficher les détails de la LUN dans le résultat de la commande. Vous pouvez voir que le niveau de service performances est attribué à cette LUN.

Sortie JSON échantillon

```
     "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"
            }
```

Modification d'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 de partages de fichiers, il est possible de spécifier à la fois les paramètres de listes de contrôle d'accès (ACL) et les règles d'export policy pour le même partage de fichiers. Toutefois, si vous souhaitez activer CIFS sur le même volume que celui 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.

Ce dont vous aurez besoin

1. Un partage de fichiers NFS doit avoir été créé avec uniquement les détails de la export policy. Pour plus d'informations, reportez-vous aux sections *gestion des partages de fichiers* et *modification des charges de travail du 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 *Provisioning des partages de fichiers CIFS et NFS*.

Cette fonctionnalité s'applique à un partage de fichiers NFS que vous avez créé en ajoutant uniquement des règles d'export policy 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 de la liste de contrôle d'accès pour autoriser l'accès CIFS.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares`

CURL d'échantillon

En fonction des privilèges d'accès que vous attribuez au groupe d'utilisateurs, comme indiqué dans l'exemple suivant, une liste de contrôle d'accès 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"
    }
```

Sortie JSON échantillon

L'opération renvoie l'ID du travail qui exécute la mise à jour.

2. Vérifiez si les paramètres ont été correctement ajoutés en interrogeant les détails du partage de fichiers pour le même partage de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares/{key}`

Sortie JSON échantillon

```
"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 la liste de contrôle d’accès attribuée ainsi que l’export policy vers le même partage de fichiers.

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Informations sur les droits d’auteur tiers et les licences utilisées dans ce produit.

"Avis pour Active IQ Unified Manager 9.14"

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 DÉLICTUELLE (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.