Documentation de Active IQ Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/index.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Documentation de Active IQ Unified Manager . . . 1
Notes de version pour Active IQ Unified Manager . . . 2
Commencer . . . 3
Commencez avec Active IQ Unified Manager sur VMware vSphere . . . 3
Configuration système requise . . . 3
Installer Active IQ Unified Manager . . . 3
Commencez avec Active IQ Unified Manager sous Linux . . . 4
Configuration système requise . . . 4
Installer Active IQ Unified Manager . . . 4
Commencez avec Active IQ Unified Manager sur Windows . . . 5
Configuration système requise . . . 5
Installer Active IQ Unified Manager . . . 6
Installer Unified Manager sur les systèmes VMware vSphere . . . 7
Découvrez Active IQ Unified Manager . . . 7
Découvrez Active IQ Unified Manager . . . 7
Découvrez ce que fait le serveur Active IQ Unified Manager . . . 7
Découvrez la séquence d'installation de Active IQ Unified Manager . . . 7
Configuration requise pour l'installation d'Unified Manager . . . 8
Assurez-vous que le serveur répond aux exigences d'installation d'Active IQ Unified Manager . . . 8
Découvrez les exigences en matière d'infrastructure virtuelle et de matériel pour Active IQ Unified Manager . . . 8
Découvrez les logiciels VMware et les exigences d'installation d'Active IQ Unified Manager . . . 10
Utilisez les navigateurs compatibles dans Active IQ Unified Manager . . . 10
Découvrez les exigences en matière de protocole et de port pour Active IQ Unified Manager . . . 11
Remplissez la feuille de calcul dans Active IQ Unified Manager . . . 14
Installation, mise à niveau et suppression d'Unified Manager sur VMware vSphere . . . 16
Découvrez le processus de déploiement d'Active IQ Unified Manager . . . 16
Flux de travail de déploiement de l'appliance virtuelle Unified Manager . . . 16
Flux de travail de mise à niveau de l'appliance virtuelle Unified Manager . . . 20
Redémarrez la machine virtuelle Active IQ Unified Manager . . . 23
Supprimer Active IQ Unified Manager . . . 24
Installer Unified Manager sur les systèmes Linux . . . 25
Introduction à Active IQ Unified Manager . . . 25
Découvrez Active IQ Unified Manager . . . 25
Comprendre le rôle du serveur Active IQ Unified Manager . . . 25
Consultez la séquence d'installation de Active IQ Unified Manager . . . 25
Configuration requise pour l'installation d'Unified Manager . . . 26
Comprendre les exigences d'installation d'Active IQ Unified Manager . . . 26
Comprendre les exigences en matière d'infrastructure virtuelle et de matériel pour Active IQ Unified Manager . . . 26
Découvrez les logiciels Linux et les exigences d'installation dans Active IQ Unified Manager . . . 28
Utilisez les navigateurs compatibles avec Active IQ Unified Manager . . . 31
Découvrez les exigences en matière de protocole et de port dans Active IQ Unified Manager . . . 31

Remplissez la feuille de calcul dans Active IQ Unified Manager . . . 34
Installer, mettre à niveau et supprimer le logiciel Unified Manager . . . 35
Installer, mettre à niveau et supprimer le logiciel Active IQ Unified Manager . . . 35
Comprendre la séquence d'installation d'Active IQ Unified Manager sur Red Hat Enterprise Linux . . . 36
Configurer le logiciel requis . . . 36
Configurez SELinux pour les partages NFS et CIFS dans Active IQ Unified Manager . . . 39
Installer Unified Manager sur les systèmes Linux . . . 42
Mise à niveau d'Unified Manager sur Red Hat Enterprise Linux . . . 49
Mettez à niveau les produits tiers après l'installation d'Unified Manager . . . 54
Redémarrer Active IQ Unified Manager . . . 55
Supprimer Active IQ Unified Manager . . . 55
Supprimez l'utilisateur umadmin personnalisé et le groupe de maintenance pour Active IQ Unified Manager . . . 56
Installer Unified Manager sur les systèmes Windows . . . 57
Introduction à Active IQ Unified Manager . . . 57
Découvrez Active IQ Unified Manager . . . 57
Découvrez ce que fait le serveur Active IQ Unified Manager . . . 57
Découvrez la séquence d'installation d'Active IQ Unified Manager . . . 57
Configuration requise pour l'installation d'Unified Manager . . . 58
Assurez-vous que le serveur répond aux exigences d'installation d'Active IQ Unified Manager . . . 58
Comprendre les exigences en matière d'infrastructure virtuelle et de matériel pour Active IQ Unified Manager . . . 58
Comprendre les exigences logicielles et d'installation de Windows pour Active IQ Unified Manager . . . 60
Utilisez les navigateurs compatibles dans Active IQ Unified Manager . . . 61
Comprendre les exigences en matière de protocole et de port pour Active IQ Unified Manager . . . 62
Remplissez la feuille de calcul dans Active IQ Unified Manager . . . 65
Installer, mettre à niveau et supprimer le logiciel Unified Manager . . . 66
Découvrez le processus d'installation d'Active IQ Unified Manager sous Windows . . . 66
Installer Unified Manager sur Windows . . . 67
Modifier le mot de passe JBoss sous Windows dans Active IQ Unified Manager . . . 70
Utilisez la voie de mise à niveau prise en charge pour les versions de Active IQ Unified Manager . . . 71
Mettez à niveau Active IQ Unified Manager sous Windows . . . 72
Mettre à niveau les produits tiers . . . 73
Désinstallez les produits tiers dans Active IQ Unified Manager . . . 74
Redémarrez Active IQ Unified Manager sous Windows . . . 75
Désinstaller Active IQ Unified Manager . . . 75
Effectuer des tâches de configuration et d'administration . . . 77
Configurer Active IQ Unified Manager . . . 77
Découvrez comment configurer Active IQ Unified Manager . . . 77
Découvrez la séquence de configuration dans Active IQ Unified Manager . . . 77
Accédez à l'interface utilisateur Web dans Active IQ Unified Manager . . . 77
Effectuez la configuration initiale de l'interface utilisateur Web Active IQ Unified Manager . . . 78
Ajouter des clusters à Active IQ Unified Manager . . . 80
Configurer les notifications . . . 82
Modifiez le mot de passe de l'utilisateur local dans Active IQ Unified Manager . . . 91

Définissez le délai d'inactivité de la session dans Active IQ Unified Manager . . . 91
Définissez le délai d'expiration de la session à l'aide de la CLI dans Active IQ Unified Manager . . . 92
Modifier le nom de l'hôte de Unified Manager . . . 92
Activer et désactiver la gestion du stockage basée sur des stratégies dans Active IQ Unified Manager . . . 97
Configurer la sauvegarde Active IQ Unified Manager . . . 98
Gérer les paramètres des fonctionnalités . . . 98
Découvrez les paramètres des fonctionnalités dans Active IQ Unified Manager . . . 98
Activez la gestion du stockage basée sur des politiques dans Active IQ Unified Manager . . . 99
Découvrez la fonctionnalité API Gateway dans Active IQ Unified Manager . . . 99
Spécifiez le délai d'inactivité dans Active IQ Unified Manager . . . 100
Activer les événements du portail Active IQ dans Active IQ Unified Manager . . . 100
Activez et désactivez les paramètres de sécurité pour la conformité dans Active IQ Unified Manager . . . 101
Activer et désactiver le chargement de scripts dans Active IQ Unified Manager . . . 102
Ajouter une bannière de connexion dans Active IQ Unified Manager . . . 102
Utilisez la console de maintenance . . . 102
Découvrez la console de maintenance dans Active IQ Unified Manager . . . 102
Découvrez l'utilisateur de maintenance dans Active IQ Unified Manager . . . 103
Fonctionnalités de diagnostic utilisateur dans Active IQ Unified Manager . . . 103
Accédez à la console de maintenance dans Active IQ Unified Manager . . . 103
Accédez à la console de maintenance via la console VM vSphere dans Active IQ Unified Manager . . . 104
Menus de la console de maintenance . . . 105
Modifiez le mot de passe de l'utilisateur de maintenance sous Windows dans Active IQ Unified Manager . . . 110
Modifiez le mot de passe umadmin d'Active IQ Unified Manager sur les systèmes Linux . . . 110
Modifier les ports qu'Active IQ Unified Manager utilise pour les protocoles HTTP et HTTPS . . . 111
Ajouter des interfaces réseau à Active IQ Unified Manager . . . 112
Régénérez le certificat client dans Active IQ Unified Manager . . . 112
Ajouter de l'espace disque . . . 113
Gérer l'accès des utilisateurs . . . 116
Ajouter des utilisateurs . . . 116
Modifier les paramètres utilisateur dans Active IQ Unified Manager . . . 118
Afficher les utilisateurs dans Active IQ Unified Manager . . . 118
Supprimer des utilisateurs ou des groupes dans Active IQ Unified Manager . . . 119
Découvrez le contrôle d'accès basé sur les rôles dans Active IQ Unified Manager . . . 119
Découvrez les types d'utilisateurs dans Active IQ Unified Manager . . . 119
Découvrez les rôles des utilisateurs dans Active IQ Unified Manager . . . 120
Découvrez les rôles et les capacités des utilisateurs dans Active IQ Unified Manager . . . 121
Gérer les paramètres d'authentification SAML . . . 123
Activer l'authentification SAML dans Active IQ Unified Manager . . . 123
Utilisez un fournisseur d'identité dans Active IQ Unified Manager . . . 123
Activer l'authentification SAML dans Active IQ Unified Manager . . . 124
Modifier le fournisseur d'identité d'authentification SAML dans Active IQ Unified Manager . . . 126
Mettez à jour les paramètres d'authentification SAML après une modification du certificat de sécurité d'Active IQ Unified Manager. . . . 126
Désactiver l'authentification SAML dans Active IQ Unified Manager . . . 128

Désactivez l'authentification SAML depuis la console de maintenance Active IQ Unified Manager 128
Utilisez la page d'authentification SAML dans Active IQ Unified Manager 129
Gérer l'authentification 130
Modifier les serveurs d'authentification dans Active IQ Unified Manager 130
Supprimer les serveurs d'authentification dans Active IQ Unified Manager 130
Authentifiez-vous avec Active Directory ou OpenLDAP dans Active IQ Unified Manager 131
Journalisation d'audit 131
Utilisez la page d'authentification à distance dans Active IQ Unified Manager 134
Gérer les certificats de sécurité 137
Consultez le certificat de sécurité HTTPS dans Active IQ Unified Manager 137
Téléchargez une demande de signature de certificat HTTPS dans Active IQ Unified Manager 138
Installez un certificat HTTPS signé par une autorité de certification dans Active IQ Unified Manager 138
Découvrez les certificats HTTPS générés à l'aide d'outils externes dans Active IQ Unified Manager Unified Manager 139
Descriptions des pages pour la gestion des certificats 141
Surveiller et gérer le stockage 144
Introduction à Active IQ Unified Manager 144
Découvrez Active IQ Unified Manager 144
Découvrez la surveillance de l'état de santé dans Active IQ Unified Manager 144
Découvrez la surveillance des performances dans Active IQ Unified Manager 145
Utilisez les API REST d'Active IQ Unified Manager 146
Que fait le serveur Unified Manager 146
Comprendre l'interface utilisateur 147
Découvrez l'interface utilisateur de Active IQ Unified Manager 147
Agencements de fenêtres typiques dans Active IQ Unified Manager 147
Personnalisation de la disposition des fenêtres dans Active IQ Unified Manager 148
Utilisez l'aide d'Active IQ Unified Manager 149
Ajoutez vos rubriques d'aide favorites à vos favoris dans Active IQ Unified Manager 150
Rechercher des objets de stockage dans Active IQ Unified Manager 150
Exportez les données de stockage sous forme de rapports dans Active IQ Unified Manager 152
Filtrer le contenu de la page d'inventaire dans Active IQ Unified Manager 153
Consultez les événements actifs à partir de la cloche de notification dans Active IQ Unified Manager 154
Surveillez et gérez les clusters depuis le tableau de bord 154
Surveillez et gérez les clusters depuis le tableau de bord dans Active IQ Unified Manager 154
Découvrez la page du tableau de bord Active IQ Unified Manager 155
Résolvez ou gérez directement les problèmes ONTAP depuis Unified Manager 158
Gérer les clusters 165
Découvrez comment fonctionne le processus de découverte de clusters dans Active IQ Unified Manager 165
Consultez la liste des clusters surveillés par Active IQ Unified Manager 166
Ajouter des clusters à Active IQ Unified Manager 167
Modifier les paramètres du cluster dans Active IQ Unified Manager 169
Supprimez les clusters d'Active IQ Unified Manager 170
Redécouvrez les clusters dans Active IQ Unified Manager 171
Surveiller l'infrastructure virtuelle VMware 171

Comprenez comment Active IQ Unified Manager surveille l'infrastructure virtuelle VMware . . . 171
Afficher et ajouter des serveurs vCenter dans Active IQ Unified Manager . . . 175
Supprimer un serveur vCenter d'Active IQ Unified Manager . . . 177
Comprendre comment Active IQ Unified Manager surveille les machines virtuelles . . . 177
Affichez la visibilité de l'infrastructure virtuelle dans un environnement de reprise après sinistre avec Active IQ Unified Manager . . . 179
Provisionner et gérer les charges de travail . . . 181
Provisionnez et gérez les charges de travail dans Active IQ Unified Manager . . . 181
Aperçu des workloads . . . 182
Gérer les niveaux de service de performance . . . 189
Gérer les stratégies d'efficacité du stockage . . . 196
Gérer et surveiller les configurations MetroCluster . . . 198
Découvrez le comportement du volume lors des basculements et des retours en arrière dans Active IQ Unified Manager . . . 198
Comprendre la connectivité des clusters dans une configuration MetroCluster sur FC dans Active IQ Unified Manager . . . 200
Découvrez la mise en miroir des données MetroCluster sur FC dans Active IQ Unified Manager . . . 201
Surveillez les configurations MetroCluster dans Active IQ Unified Manager . . . 202
Surveillez la réplication MetroCluster dans Active IQ Unified Manager . . . 205
Gérer les quotas . . . 206
Découvrez les limites de quota dans Active IQ Unified Manager . . . 206
Consultez les quotas des utilisateurs et des groupes d'utilisateurs dans Active IQ Unified Manager . . . 206
Créez des règles pour générer des adresses e-mail dans Active IQ Unified Manager . . . 206
Créez un format de notification par e-mail pour les quotas d'utilisateurs et de groupes d'utilisateurs dans Active IQ Unified Manager . . . 207
Modifier les adresses e-mail des quotas d'utilisateurs et de groupes dans Active IQ Unified Manager . . . 208
En savoir plus sur les quotas . . . 208
Description des boîtes de dialogue de quotas . . . 209
Dépannage . . . 213
Ajouter de l'espace disque au répertoire de la base de données Unified Manager . . . 213
Modifiez l'intervalle de collecte des statistiques de performance dans Active IQ Unified Manager . . . 216
Modifiez la durée pendant laquelle Active IQ Unified Manager conserve les données d'événements et de performances . . . 217
Résoudre une erreur d'authentification inconnue dans Active IQ Unified Manager . . . 218
Résoudre l'erreur « Utilisateur introuvable » dans Active IQ Unified Manager . . . 218
Résolvez le problème causé par l'ajout de LDAP à l'aide d'Other authentication service dans Active IQ Unified Manager . . . 219
Résolvez un problème de rotation des journaux du SDK de gestion NetApp dans Active IQ Unified Manager . . . 220
Gérer les événements et les alertes . . . 221
Gérer les événements . . . 221
Découvrez les événements de la plateforme Active IQ dans Active IQ Unified Manager . . . 221
Que sont les événements de l'Event Management System . . . 221
Comprendre comment Active IQ Unified Manager gère un événement reçu . . . 227
Consultez les détails de l'événement dans Active IQ Unified Manager . . . 228

Consultez les événements non attribués dans Active IQ Unified Manager . . . 229
Accuser réception et résoudre les événements dans Active IQ Unified Manager . . . 229
Attribuer des événements à des utilisateurs spécifiques dans Active IQ Unified Manager . . . 230
Désactivez les événements indésirables dans Active IQ Unified Manager . . . 231
Résolvez les problèmes à l'aide de la correction automatique dans Active IQ Unified Manager . . . 232
Activer et désactiver la génération de rapports d'événements Active IQ dans Active IQ Unified Manager . . . 233
Téléversez un nouveau fichier de règles Active IQ dans Active IQ Unified Manager . . . 234
Comment Active IQ Unified Manager génère des événements de la plateforme Active IQ . . . 235
Résoudre les événements de la plateforme Active IQ dans Active IQ Unified Manager . . . 235
Configurez les paramètres de conservation des événements dans Active IQ Unified Manager . . . 236
Qu'est-ce qu'une fenêtre de maintenance Unified Manager . . . 236
Gérer les événements liés aux ressources du système hôte dans Active IQ Unified Manager . . . 239
Apprenez-en davantage sur les événements . . . 239
Liste des événements et des types de gravité . . . 245
Description des fenêtres d'événements et des boîtes de dialogue . . . 298
Gérer les alertes . . . 311
Découvrez les alertes dans Active IQ Unified Manager . . . 311
Informations contenues dans un e-mail d'alerte Active IQ Unified Manager . . . 311
Ajouter des alertes . . . 312
Ajoutez des alertes pour les événements de performance dans Active IQ Unified Manager . . . 315
Tester les alertes dans Active IQ Unified Manager . . . 316
Désactiver les alertes pour les événements résolus et obsolètes dans Active IQ Unified Manager . . . 316
Exclure les volumes de destination de reprise après sinistre de la génération d'alertes dans Active IQ Unified Manager . . . 317
Consultez les alertes dans Active IQ Unified Manager . . . 318
Modifier les alertes dans Active IQ Unified Manager . . . 318
Supprimer les alertes dans Active IQ Unified Manager . . . 318
Description des fenêtres d'alerte et des boîtes de dialogue . . . 319
Gérer les scripts . . . 325
Gérer les scripts dans Active IQ Unified Manager . . . 325
Fonctionnement des scripts avec les alertes dans Active IQ Unified Manager . . . 325
Ajouter des scripts dans Active IQ Unified Manager . . . 326
Supprimer les scripts dans Active IQ Unified Manager . . . 327
Exécution du script de test dans Active IQ Unified Manager . . . 327
Découvrez les commandes CLI prises en charge par Active IQ Unified Manager . . . 328
Description des fenêtres de script et des boîtes de dialogue . . . 334
Surveiller et gérer les performances du cluster . . . 336
Introduction à la surveillance des performances d'Active IQ Unified Manager . . . 336
Découvrez la surveillance des performances dans Active IQ Unified Manager . . . 336
Explorez les fonctionnalités de surveillance des performances d'Active IQ Unified Manager . . . 336
Utilisez les interfaces d'Active IQ Unified Manager pour gérer les performances du système de stockage . . . 337
Consultez la configuration du cluster et les données de performance dans Active IQ Unified Manager . . . 337
Comprendre les cycles de collecte de continuité des données dans Active IQ Unified Manager . . . 339

Découvrez les horodatages des données collectées et des événements dans Active IQ Unified Manager . . . 340
Navigation dans les flux de travail de performance de l'interface graphique d'Unified Manager . . . 340
Naviguez dans les flux de travail de performance dans l'interface graphique Active IQ Unified Manager . . . 340
Connectez-vous à l'interface utilisateur Active IQ Unified Manager . . . 341
Interface graphique et chemins de navigation . . . 341
Rechercher des objets de stockage dans Active IQ Unified Manager . . . 347
Filtrer le contenu de la page d'inventaire dans Active IQ Unified Manager . . . 348
Surveillez les performances du cluster depuis le tableau de bord . . . 350
Surveillez les performances du cluster depuis le tableau de bord dans Active IQ Unified Manager . . . 350
Consultez les panneaux de performance sur le tableau de bord Active IQ Unified Manager . . . 350
Interpréter les messages de bannière de performance dans Active IQ Unified Manager . . . 351
Modifiez l'intervalle de collecte des statistiques de performance dans Active IQ Unified Manager . . . 352
Dépanner les workloads à l'aide de l'analyseur de workload . . . 352
Dépannez les charges de travail avec l'analyseur de charge de travail dans Active IQ Unified Manager . . . 353
Comprendre les données de l'analyseur de charge de travail dans Active IQ Unified Manager . . . 353
Comprendre quand utiliser l'analyseur de charge de travail dans Active IQ Unified Manager . . . 355
Utilisez l'analyseur de charge de travail dans Active IQ Unified Manager . . . 355
Surveillez les performances du cluster depuis la page de destination du cluster de performances . . . 356
Surveillez les performances du cluster depuis la page d'accueil « Performances du cluster » dans Active IQ Unified Manager . . . 356
Comprendre la page d'accueil du cluster de performance dans Active IQ Unified Manager . . . 356
Page d'accueil du cluster de performance . . . 357
Surveillez les performances à l'aide des pages d'inventaire des performances . . . 361
Surveillez les performances des objets à l'aide des pages d'inventaire des performances dans Active IQ Unified Manager . . . 361
Consultez les pages d'inventaire des performances pour tous les objets de stockage dans Active IQ Unified Manager . . . 362
Affiner le contenu de la page d'inventaire des performances . . . 368
Consultez les recommandations d'Active IQ Unified Manager concernant la hiérarchisation des données vers le cloud . . . 371
Surveillez les performances à l'aide des pages Performance Explorer . . . 372
Surveillez les performances à l'aide des pages Performance Explorer dans Active IQ Unified Manager 372
Utilisez les objets racine pour la surveillance des performances dans Active IQ Unified Manager . . . 372
Filtrer les objets corrélés dans la grille Active IQ Unified Manager . . . 373
Spécifiez une plage horaire pour les objets corrélés . . . 373
Définissez des objets corrélés pour la création de graphiques de comparaison dans Active IQ Unified Manager . . . 375
Comprendre les graphiques de compteurs dans Active IQ Unified Manager . . . 376
Comprendre les types de graphiques de compteurs de performance dans Active IQ Unified Manager . 377
Sélectionnez les graphiques de performance à afficher dans Active IQ Unified Manager . . . 379
Développez le volet Graphiques de compteurs dans Active IQ Unified Manager . . . 380
Modifiez la période des graphiques de compteurs pour une période plus courte dans Active IQ Unified

Manager . . . 380
Consultez les détails de l'événement dans la chronologie des événements d'Active IQ Unified Manager. . . . 381
Vue agrandie des graphiques de compteur . . . 382
Afficher la latence du volume par composant de cluster dans Active IQ Unified Manager . . . 384
Affichez le trafic IOPS SVM par protocole dans Active IQ Unified Manager . . . 385
Consultez les graphiques de volume et de latence LUN pour vérifier la garantie de performance dans Active IQ Unified Manager . . . 386
Consultez les performances de tous les clusters SAN Array dans Active IQ Unified Manager . . . 386
Afficher les IOPS des nœuds en fonction des charges de travail locales dans Active IQ Unified Manager . . . 387
Composants des pages de destination des objets . . . 387
Gérer les performances à l'aide des informations du groupe de règles QoS . . . 393
Gérez les performances à l'aide des informations des groupes de stratégies QoS dans Active IQ Unified Manager . . . 393
Contrôlez le débit des charges de travail grâce à la QoS de stockage dans Active IQ Unified Manager 394
Consultez les groupes de règles QoS disponibles sur tous les clusters dans Active IQ Unified Manager . . . 395
Afficher les volumes ou les LUN appartenant au même groupe de stratégie QoS dans Active IQ Unified Manager . . . 395
Affichez les paramètres des groupes de règles QoS pour les volumes ou les LUN dans Active IQ Unified Manager . . . 396
Comparez les volumes ou les LUN au sein du même groupe de règles QoS dans Active IQ Unified Manager . . . 397
Affichez les politiques QoS dans les graphiques de débit avec Active IQ Unified Manager . . . 397
Affichez les paramètres QoS minimum et maximum de la charge de travail dans Active IQ Unified Manager . . . 399
Gérez les performances à l'aide de la capacité de performance et des informations sur les IOPS disponibles . . . 400
Gérez la capacité de performance et les IOPS disponibles dans Active IQ Unified Manager . . . 400
Comprendre le compteur de capacité de performance utilisée dans Active IQ Unified Manager . . . 400
Utilisez la valeur de capacité de performance utilisée dans Active IQ Unified Manager . . . 401
Comprendre les IOPS disponibles dans Active IQ Unified Manager . . . 402
Afficher les valeurs de capacité de performance utilisées des nœuds et des agrégats dans Active IQ Unified Manager . . . 403
Consultez les valeurs IOPS disponibles pour les nœuds et les agrégats dans Active IQ Unified Manager . . . 404
Consultez les graphiques des compteurs de capacité de performance dans Active IQ Unified Manager 405
Configurez les seuils de capacité de performance utilisés dans Active IQ Unified Manager . . . 407
Utilisez le compteur de capacité de performance utilisée dans Active IQ Unified Manager . . . 407
Comprendre et utiliser la page de planification du basculement de nœud . . . 408
Utilisez la page Node Failover Planning dans Active IQ Unified Manager . . . 408
Déterminez les actions correctives à partir de la page Performance/Node Failover Planning dans Active IQ Unified Manager . . . 408
Examinez les composants de la page Planification du basculement des performances/nœuds dans

Active IQ Unified Manager . . . 408
Créez des politiques de seuil pour la planification du basculement des nœuds dans Active IQ Unified Manager . . . 410
Utilisez le graphique de répartition de la capacité de performance utilisée pour la planification du basculement dans Active IQ Unified Manager . . . 411
Collecter des données et surveiller les performances du workload . . . 412
Collectez des données et surveillez les performances de la charge de travail dans Active IQ Unified Manager . . . 412
Surveillez les types de charges de travail avec Active IQ Unified Manager . . . 413
Comprendre les valeurs de mesure des performances de la charge de travail dans Active IQ Unified Manager . . . 414
Comprendre comment Active IQ Unified Manager calcule la plage de performances attendue . . . 416
Utilisez les prévisions de latence pour l'analyse des performances dans Active IQ Unified Manager . . . 417
Utilisez la latence de la charge de travail pour identifier les problèmes de performance dans Active IQ Unified Manager . . . 418
Évaluez comment les opérations de cluster peuvent affecter la latence des charges de travail dans Active IQ Unified Manager . . . 419
Surveillez les performances de MetroCluster avec Active IQ Unified Manager . . . 420
Comprendre les événements et alertes de performance . . . 421
Comprendre les événements et alertes de performance dans Active IQ Unified Manager . . . 421
Identifier les sources des événements de performance dans Active IQ Unified Manager . . . 421
Priorisez les événements de performance par niveau de gravité dans Active IQ Unified Manager . . . 422
Surveillez les modifications de configuration détectées par Active IQ Unified Manager . . . 422
Comprendre les politiques de seuil de performance définies par le système dans Active IQ Unified Manager . . . 423
Analysez les événements et notifications de performance dans Active IQ Unified Manager . . . 426
Comprendre comment Active IQ Unified Manager détermine l'impact sur les performances d'un événement . . . 428
Comprendre les composants du cluster et la contention dans Active IQ Unified Manager . . . 429
Identifier les rôles de la charge de travail dans les événements de performance dans Active IQ Unified Manager . . . 431
Gérer les seuils de performance . . . 432
Gérez les seuils de performance dans Active IQ Unified Manager . . . 432
Utilisez des politiques de seuil de performance définies par l'utilisateur dans Active IQ Unified Manager . . . 432
Répondez aux politiques de seuils de performance dépassés dans Active IQ Unified Manager . . . 434
Comprendre les compteurs de performance suivis à l'aide de seuils dans Active IQ Unified Manager . . . 435
Comprendre les objets de stratégie de seuil combinés et les compteurs dans Active IQ Unified Manager . . . 436
Créez des politiques de seuil de performance définies par l'utilisateur dans Active IQ Unified Manager 437
Attribuez des politiques de seuil de performance aux objets de stockage dans Active IQ Unified Manager . . . 438
Consultez les règles de seuil de performance dans Active IQ Unified Manager . . . 439
Modifiez les règles de seuil de performance définies par l'utilisateur dans Active IQ Unified Manager . . . 440
Supprimez les stratégies de seuil de performance des objets de stockage dans Active IQ Unified

Manager . . . 440
Comprendre les modifications apportées aux politiques de seuil de performance dans Active IQ Unified Manager . . . 441
Gérez les politiques de seuil lors du déplacement d'objets dans Active IQ Unified Manager . . . 442
Analyser les événements de performance . . . 443
Analysez les événements de performance dans Active IQ Unified Manager . . . 443
Afficher les informations relatives aux événements de performance dans Active IQ Unified Manager . . . 443
Analyser les événements à partir de seuils de performance définis par l'utilisateur . . . 444
Analyser les événements à partir des seuils de performance définis par le système . . . 445
Analyser les événements à partir de seuils de performance dynamiques . . . 451
Résoudre les événements de performance . . . 459
Résolvez les événements de performance dans Active IQ Unified Manager . . . 459
Vérifiez que la latence se situe dans la plage attendue dans Active IQ Unified Manager . . . 459
Évaluez comment les modifications de configuration affectent les performances de la charge de travail dans Active IQ Unified Manager . . . 459
Améliorez les performances de la charge de travail en ajustant les paramètres côté client dans Active IQ Unified Manager . . . 459
Comprendre comment les problèmes liés aux clients ou au réseau affectent les performances d'Active IQ Unified Manager . . . 460
Analysez les volumes à forte activité au sein d'un groupe de politiques QoS dans Active IQ Unified Manager . . . 460
Déplacez les LIF pour améliorer les performances dans Active IQ Unified Manager . . . 461
Effectuez les opérations d'efficacité du stockage aux heures creuses . . . 461
Comprendre comment l'ajout de disques affecte la réallocation des données dans Active IQ Unified Manager . . . 462
Améliorez les performances des charges de travail en activant Flash Cache sur un nœud dans Active IQ Unified Manager . . . 463
Améliorez les performances des charges de travail en activant Flash Pool sur un agrégat de stockage dans Active IQ Unified Manager . . . 463
Vérifiez l'état de la configuration MetroCluster dans Active IQ Unified Manager . . . 464
Vérifiez les configurations MetroCluster dans Active IQ Unified Manager . . . 464
Déplacez les charges de travail vers un autre agrégat dans Active IQ Unified Manager . . . 465
Déplacez les charges de travail vers un autre nœud dans Active IQ Unified Manager . . . 466
Déplacez les charges de travail vers un agrégat sur un autre nœud dans Active IQ Unified Manager . . . 468
Déplacez les charges de travail vers un nœud d'une autre paire haute disponibilité dans Active IQ Unified Manager . . . 469
Déplacez les charges de travail vers un autre nœud d'une paire haute disponibilité dans Active IQ Unified Manager . . . 471
Utilisez les paramètres de stratégie QoS pour prioriser les charges de travail des nœuds dans Active IQ Unified Manager . . . 473
Supprimez les volumes et les LUN inactifs dans Active IQ Unified Manager . . . 473
Comprendre comment l'ajout de disques affecte la disposition des agrégats dans Active IQ Unified Manager . . . 474
Établissez une connexion entre un serveur Unified Manager et un fournisseur de données externe . . . 474
Établissez une connexion entre Active IQ Unified Manager et un fournisseur de données externe . . . 474

Envoyez les données de performance d'Active IQ Unified Manager à un serveur externe . . . 474
Configurez Graphite pour recevoir les données de performance de Active IQ Unified Manager . . . 476
Configurez une connexion entre Active IQ Unified Manager et un fournisseur de données externe . . . 477
Surveiller et gérer l'état du cluster . . . 479
Introduction à la surveillance de l'état de santé d'Active IQ Unified Manager . . . 479
Découvrez la surveillance de l'état de santé avec Active IQ Unified Manager . . . 479
Comprendre les fonctionnalités de surveillance de l'état de santé d'Active IQ Unified Manager . . . 480
Utilisez les interfaces d'Active IQ Unified Manager pour gérer l'état du système de stockage . . . 481
Gérer et surveiller les clusters et l'état des objets de cluster . . . 482
Comprendre la surveillance des clusters . . . 482
Consultez la liste et les détails des clusters dans Active IQ Unified Manager . . . 484
Vérifiez l'état des clusters dans une configuration MetroCluster dans Active IQ Unified Manager . . . 484
Consultez l'état de santé et la capacité de tous les clusters All SAN Array dans Active IQ Unified Manager . . . 486
Consultez la liste des nœuds et les détails dans Active IQ Unified Manager . . . 487
Générez un rapport d'inventaire matériel pour le renouvellement du contrat dans Active IQ Unified Manager . . . 488
Consultez la liste et les détails des machines virtuelles de stockage dans Active IQ Unified Manager . . . 488
Affichez la liste des agrégats et les détails dans Active IQ Unified Manager . . . 489
Consultez les informations de capacité de FabricPool dans Active IQ Unified Manager . . . 489
Consultez les détails du pool de stockage dans Active IQ Unified Manager . . . 491
Consultez la liste des volumes et les détails dans Active IQ Unified Manager . . . 491
Consultez les détails relatifs aux partages NFS dans Active IQ Unified Manager . . . 492
Affichez les détails concernant les partages SMB/CIFS dans Active IQ Unified Manager . . . 493
Consultez la liste des copies Snapshot dans Active IQ Unified Manager . . . 494
Supprimer les copies d'instantané dans Active IQ Unified Manager . . . 494
Calculer l'espace récupérable pour les copies Snapshot dans Active IQ Unified Manager . . . 495
Comprendre les fenêtres et boîtes de dialogue des objets de cluster dans Active IQ Unified Manager . . . 496
Flux de travail et tâches courants de surveillance de l'état dans Unified Manager . . . 496
Comprendre les flux de travail et les tâches de santé courants d'Active IQ Unified Manager . . . 496
Surveiller et résoudre les problèmes de disponibilité des données . . . 497
Résoudre les problèmes de capacité . . . 504
Gérer les seuils de santé . . . 506
Gérer les objectifs de sécurité du cluster . . . 511
Gérer les opérations de sauvegarde et de restauration . . . 524
Gérer les scripts . . . 541
Gérer et surveiller les groupes . . . 544
Prioriser les événements des objets de stockage à l'aide d'annotations . . . 552
Envoyer un bundle de support via l'interface utilisateur web et la console de maintenance . . . 561
Tâches et informations relatives à plusieurs flux de travail . . . 568
Protéger et restaurer les données . . . 626
Créer et dépanner les relations de protection . . . 626
Types de protection SnapMirror dans Active IQ Unified Manager . . . 626
Configurez les relations de protection dans Unified Manager . . . 628
Effectuer un basculement et un rétablissement de la relation de protection . . . 630

Résoudre l'échec d'une tâche de protection . . . 634
Résoudre les problèmes de latence dans Active IQ Unified Manager . . . 638
Gérer et surveiller les relations de protection . . . 639
Découvrez comment gérer et surveiller les relations de protection dans Active IQ Unified Manager . . . 639
Consultez l'état de la protection des volumes dans Active IQ Unified Manager . . . 640
Afficher les relations de protection des volumes dans Active IQ Unified Manager . . . 642
Surveillez les relations LUN du groupe de cohérence dans Active IQ Unified Manager . . . 642
Créez une relation SnapVault à partir de la vue Health: All Volumes dans Active IQ Unified Manager . . . 643
Créez une relation de protection SnapVault à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager . . . 644
Créez une relation SnapMirror à partir de la vue Health : All Volumes dans Active IQ Unified Manager 645
Créez une relation SnapMirror à partir de la page de détails de l'état du volume dans Active IQ Unified Manager . . . 647
Créez une relation SnapMirror avec la réplication flexible des versions dans Active IQ Unified Manager . . . 648
Créez des relations SnapMirror avec la réplication flexible des versions et la fonctionnalité de retour en arrière dans Active IQ Unified Manager . . . 649
Configurez les paramètres d'efficacité de la destination dans Active IQ Unified Manager . . . 650
Créer des plannings SnapMirror et SnapVault dans Active IQ Unified Manager . . . 651
Étendez la protection à l'aide de relations en cascade ou en éventail dans Active IQ Unified Manager . . . 651
Modifiez les relations de protection à partir de la page Relations de volumes dans Active IQ Unified Manager . . . 652
Modifiez les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager . . . 653
Créez une politique SnapMirror pour optimiser l'efficacité des transferts dans Active IQ Unified Manager . . . 653
Créez une politique SnapVault pour optimiser l'efficacité des transferts dans Active IQ Unified Manager . . . 654
Annuler un transfert depuis la page Relations de volumes dans Active IQ Unified Manager . . . 654
Annuler un transfert depuis la page Détails du volume/de l'état dans Active IQ Unified Manager . . . 655
Mettre en veille une relation de protection depuis la page Relations de volume dans Active IQ Unified Manager . . . 656
Mettre en veille une relation de protection depuis la page Détails du volume/de la santé dans Active IQ Unified Manager . . . 657
Rompre une relation SnapMirror depuis la page Relations de volumes d'Active IQ Unified Manager . . . 658
Supprimez une relation de protection depuis la page Volume Relationships dans Active IQ Unified Manager . . . 658
Reprenez les transferts planifiés sur une relation mise en veille depuis la page Relations de volume dans Active IQ Unified Manager . . . 659
Reprenez les transferts sur une relation mise en veille depuis la page Détails du volume/de la santé dans Active IQ Unified Manager . . . 659
Initialisez ou mettez à jour les relations de protection à partir de la page Relations de volumes dans Active IQ Unified Manager . . . 660
Initialisez ou mettez à jour les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager . . . 661

Resynchronisez les relations de protection à partir de la page Relations de volumes dans Active IQ Unified Manager . . . 662
Inverser les relations de protection à partir de la page Relations de volume dans Active IQ Unified Manager . . . 663
Restaurez les données à l'aide des pages de détails Volume et Volume/Santé dans Active IQ Unified Manager . . . 664
Découvrez les pools de ressources dans Active IQ Unified Manager . . . 665
Créez des pools de ressources dans Active IQ Unified Manager . . . 666
Modifier les pools de ressources dans Active IQ Unified Manager . . . 666
Afficher l'inventaire du pool de ressources dans Active IQ Unified Manager . . . 667
Ajouter des membres au pool de ressources dans Active IQ Unified Manager . . . 667
Supprimez les agrégats des pools de ressources dans Active IQ Unified Manager . . . 668
Supprimer les pools de ressources dans Active IQ Unified Manager . . . 668
Surveillez les relations de protection de reprise après sinistre des machines virtuelles de stockage . . . 669
Gérer les associations de machines virtuelles de stockage dans Active IQ Unified Manager . . . 671
Exigences relatives aux SVM et aux pools de ressources pour la prise en charge des services de stockage dans Active IQ Unified Manager . . . 673
Découvrez les tâches dans Active IQ Unified Manager . . . 674
Surveillez les tâches dans Active IQ Unified Manager . . . 674
Affichez les détails du travail dans Active IQ Unified Manager . . . 675
Annuler les tâches dans Active IQ Unified Manager . . . 675
Réessayez une tâche de protection ayant échoué dans Active IQ Unified Manager . . . 675
Description des fenêtres et boîtes de dialogue relatives aux relations de protection . . . 676
Générer des rapports personnalisés . . . 719
Rapports Unified Manager . . . 719
Découvrez les rapports d'Active IQ Unified Manager . . . 719
Points d'accès pour générer des rapports . . . 719
Comprendre les rapports dans Active IQ Unified Manager . . . 721
Comprendre la relation entre la vue et le rapport dans Active IQ Unified Manager . . . 721
Découvrez les différents types de rapports dans Active IQ Unified Manager . . . 722
Comprendre les limitations de reporting dans Active IQ Unified Manager . . . 723
Travailler avec des rapports . . . 724
Comprendre les flux de travail des rapports dans Active IQ Unified Manager . . . 724
Commencez à créer des rapports dans Active IQ Unified Manager . . . 725
Recherchez un rapport planifié dans Active IQ Unified Manager . . . 728
Personnaliser les rapports . . . 728
Téléchargez les rapports dans Active IQ Unified Manager . . . 732
Programmer des rapports . . . 732
Planifiez des rapports dans Active IQ Unified Manager . . . 732
Planifier un rapport . . . 733
Gérer les planifications de rapports . . . 735
Exemples de rapports personnalisés . . . 737
Comprendre des exemples de rapports personnalisés dans Active IQ Unified Manager . . . 737
Personnaliser les rapports de stockage du cluster . . . 738
Personnaliser les rapports de capacité des agrégats . . . 741

Personnaliser les rapports de capacité des volumes . . . 743
Personnaliser les rapports de capacité Qtree . . . 746
Personnaliser les rapports de partage NFS . . . 747
Personnaliser les rapports de VM de stockage . . . 748
Personnaliser les rapports de relation de volume . . . 750
Personnaliser les rapports de performance des volumes . . . 754
Exemples de rapports Microsoft Excel . . . 755
Comprendre des exemples de rapports Microsoft Excel dans Active IQ Unified Manager . . . 755
Créez un rapport pour afficher un tableau et un graphique de capacité agrégée dans Active IQ Unified Manager . . . 755
Afficher les graphiques comparant la capacité totale agrégée à la capacité disponible dans Active IQ Unified Manager . . . 758
Créez un rapport pour afficher les graphiques de capacité de volume disponibles dans Active IQ Unified Manager . . . 761
Créez un rapport pour afficher les agrégats présentant le plus grand nombre d'IOPS disponibles dans Active IQ Unified Manager . . . 764
Gérer le stockage à l'aide des API REST . . . 767
Premiers pas avec Active IQ Unified Manager . . . 767
Démarrer avec les API REST d'Active IQ Unified Manager . . . 767
Identifier les utilisateurs prévus des API REST d'Active IQ Unified Manager . . . 767
Gérez l'accès à l'API et les catégories d'Active IQ Unified Manager . . . 767
Comprendre les services REST proposés dans Active IQ Unified Manager . . . 769
Comprendre les numéros de version de l'API dans Active IQ Unified Manager . . . 770
Comprendre le modèle de ressources de stockage ONTAP dans Active IQ Unified Manager . . . 770
Accès à l'API REST et authentification dans Active IQ Unified Manager . . . 771
Accédez et authentifiez les API REST dans Active IQ Unified Manager . . . 771
Découvrez les codes d'état HTTP d'Active IQ Unified Manager . . . 774
Suivez les pratiques recommandées pour l'utilisation des API Active IQ Unified Manager . . . 775
Dépannez à l'aide des journaux système dans Active IQ Unified Manager . . . 776
Comprenez comment Active IQ Unified Manager utilise les objets Job pour le traitement asynchrone . . . 776
Découvrez l'exemple de programme serveur Hello API dans Active IQ Unified Manager . . . 777
API REST de Unified Manager . . . 781
Comprendre les catégories des API REST d'Active IQ Unified Manager . . . 781
Gérez les objets de stockage dans un centre de données à l'aide des API dans Active IQ Unified Manager . . . 782
Accédez aux API ONTAP via un accès proxy dans Active IQ Unified Manager . . . 789
Effectuez des tâches administratives à l'aide des API dans Active IQ Unified Manager . . . 791
Gérer les utilisateurs dans Active IQ Unified Manager à l'aide des API . . . 793
Consultez les indicateurs de performance à l'aide des API dans Active IQ Unified Manager . . . 794
Affichez les tâches et les détails du système à l'aide des API dans Active IQ Unified Manager . . . 804
Gérez les événements et les alertes à l'aide des API dans Active IQ Unified Manager . . . 805
Gérer les workloads . . . 808
Flux de travail courants pour la gestion du stockage . . . 816
Comprendre les flux de travail API courants pour la gestion du stockage dans Active IQ Unified Manager . . . 816

Déterminez les problèmes d'espace dans les agrégats à l'aide des API Active IQ Unified Manager . . . 817
Déterminez les problèmes liés aux objets de stockage à l'aide des API d'événements d'Active IQ Unified Manager . . . 819
Dépannez les volumes ONTAP à l'aide des API de passerelle Active IQ Unified Manager . . . 820
Flux de travail pour la gestion des workloads . . . 823
Mentions légales . . . 848
Copyright . . . 848
Marques déposées . . . 848
Brevets . . . 848
Politique de confidentialité . . . 848
Open source . . . 848

Documentation de Active IQ Unified Manager

Notes de version pour Active IQ Unified Manager

Présente un résumé des nouvelles fonctionnalités, des limitations et des problèmes connus pour Active IQ Unified Manager 9.18.

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

Commencer

Commencez avec Active IQ Unified Manager sur VMware vSphere

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

Configuration système requise

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

Pour connaître les exigences système détaillées, consultez "Configuration requise pour l'installation d'Unified Manager" et "Matrice d'interopérabilité".

Installer Active IQ Unified Manager

Téléchargez le programme d'installation

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

Vérifier l'intégrité

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

Installer Unified Manager

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

    - Pour configurer le DHCP en IPv6, cochez la case « Activer l'adressage automatique IPv6 ». Ne renseignez aucun autre champ.
5. Mettez la machine virtuelle sous tension.
6. Cliquez sur l'onglet Console pour afficher le processus de démarrage initial.
7. Configurez le fuseau horaire.
8. Saisissez un nom d'utilisateur et un mot de passe de maintenance pour Unified Manager.

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

Commencez avec Active IQ Unified Manager sous Linux

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

Configuration système requise

- Système d'exploitation : Red Hat Enterprise Linux versions 8.x et 9.4, basé sur l'architecture x86_64, installé à l'aide de l'environnement de base « Server with GUI » via 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 montés séparément `/opt` et `/var/log`, assurez-vous que `/opt` dispose de 15 Go, `/var/log` dispose de 16 Go et `/tmp` dispose de 10 Go d'espace libre.

Pour connaître les exigences système détaillées et obtenir des informations sur l'installation du produit dans un environnement sécurisé, consultez le "Configuration requise pour l'installation d'Unified Manager" et le "Matrice d'interopérabilité".

Installer Active IQ Unified Manager

Téléchargez le programme d'installation

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

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

Vérifier l'intégrité

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

- Exécutez `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` pour créer un fichier contenant la clé publique 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 du

package d'installation.

Vérifier la configuration du dépôt

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

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

Installer Unified Manager

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

Pour installer Unified Manager, exécutez la commande suivante, soit en tant qu'utilisateur root, soit en utilisant `sudo`, depuis 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 permettant de se connecter à l'interface utilisateur web de Unified Manager s'affichent. Si vous ne parvenez pas à vous connecter à l'interface utilisateur web, consultez le fichier `README` fourni avec le logiciel pour plus d'informations sur les restrictions du port 443.

Commencez avec Active IQ Unified Manager sur Windows

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

Configuration système requise

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

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

  - English
  - japonais
  - Chinois simplifié

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

Pour connaître les exigences système détaillées, consultez "Configuration requise pour l'installation d'Unified Manager" et "Matrice d'interopérabilité".

Installer Active IQ Unified Manager

Téléchargez le programme d'installation

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

Installer Unified Manager

Pour installer Unified Manager, assurez-vous d'avoir installé Microsoft .NET 4.5.2 ou une version ultérieure. Dans le cadre du processus d'installation, Unified Manager installe également d'autres packages tiers si nécessaire. Pour plus d'informations sur les packages logiciels dépendants, consultez la "Logiciels Windows et exigences d'installation".

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

Installer Unified Manager sur les systèmes VMware vSphere

Découvrez Active IQ Unified Manager

Découvrez Active IQ Unified Manager

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

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

Informations connexes

"Outil NetApp Interoperability Matrix Tool"

Découvrez ce que fait le serveur Active IQ Unified Manager

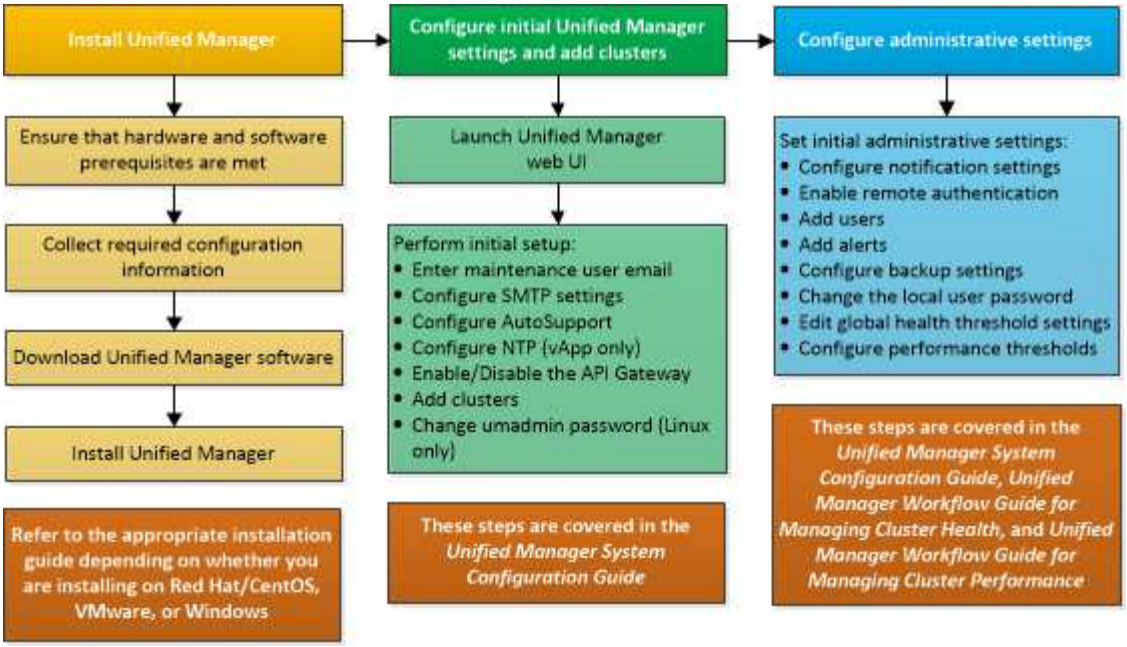
L'infrastructure serveur d'Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur applicatif. Elle fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations du cluster, stocke les données dans la base de données et les analyse pour détecter d'éventuels problèmes au niveau du cluster.

Découvrez la séquence d'installation de Active IQ Unified Manager

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

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



Configuration requise pour l'installation d'Unified Manager

Assurez-vous que le serveur répond aux exigences d'installation d'Active IQ 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 toute modification du code de l'application Unified Manager. Si vous devez appliquer des mesures de sécurité au serveur Unified Manager, vous devez effectuer ces modifications au niveau du système d'exploitation sur lequel Unified Manager est installé.

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

"Prise en charge des mesures de sécurité appliquées à Active IQ Unified Manager pour Clustered Data ONTAP"

Informations connexes

Pour plus d'informations, voir "Outil NetApp Interoperability Matrix Tool"

Découvrez les exigences en matière d'infrastructure virtuelle et de matériel pour Active IQ Unified Manager

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

Le tableau suivant présente les valeurs recommandées pour la mémoire, le processeur et l'espace disque. Ces valeurs ont été validées afin que Unified Manager offre des performances acceptables.

Configuration matérielle	Paramètres recommandés
RAM	12 Go
Processeurs	4 processeurs
capacité en cycles CPU	9572 MHz au total (exigence minimale 9572 MHz)
Espace disque libre	• 5 Go (provisionnement fin) • 152 Go (provisionnement épais)

Unified Manager peut être installé sur des systèmes disposant de peu de mémoire, mais les 12 Go de RAM recommandés garantissent qu'une quantité de mémoire suffisante est disponible pour des performances optimales et permettent au système d'accueillir des clusters et des objets de stockage supplémentaires à mesure que votre configuration évolue. Vous ne devez définir aucune limite de mémoire sur la machine virtuelle sur laquelle Unified Manager est déployé et ne devez activer aucune fonctionnalité (par exemple, le ballooning) qui empêcherait le logiciel d'utiliser la mémoire allouée sur le système.

De plus, il existe une limite au nombre de nœuds qu'une seule instance d'Unified Manager peut surveiller avant que vous n'installiez une seconde instance d'Unified Manager. Pour connaître les limites de nœuds, ainsi que les recommandations concernant le CPU et la mémoire, consultez "le guide des bonnes pratiques de Unified Manager".

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

Exigence d'utilisation dédiée

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

Besoins en espace pour les sauvegardes

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

Exigences en matière de connectivité hôte

Le système physique ou le système virtuel sur lequel vous installez Unified Manager doit être configuré de telle sorte que vous puissiez `ping` résoudre correctement le nom de l'hôte à partir de l'hôte lui-même. En cas de configuration IPv6, vous devez vérifier que `ping6` la résolution du nom de l'hôte aboutit afin de garantir la réussite de l'installation d'Unified Manager.

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

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

Découvrez les logiciels VMware et les exigences d'installation d'Active IQ Unified Manager

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

Logiciel du système d'exploitation

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

> L'OVA Unified Manager sur les systèmes VMware vSphere exécute Debian OS 13 (Trixie) en interne. Pour des informations sur les versions du matériel de la machine virtuelle que les versions prises en charge des serveurs ESXi peuvent supporter, consultez la documentation VMware.

Les versions suivantes de vSphere sont prises en charge :

- VMware vCenter Server 7.0 et 8.0

Consultez l'Interoperability Matrix pour obtenir la liste complète et la plus récente des versions d'ESXi prises en charge.

"mysupport.netapp.com/matrix"

Pour que l'appliance virtuelle fonctionne correctement, l'heure du serveur VMware ESXi doit correspondre à celle du serveur NTP. La synchronisation de l'heure du serveur VMware ESXi avec celle du serveur NTP permet d'éviter une défaillance liée à l'heure.

exigences d'installation

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

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

Si le déploiement échoue dans votre environnement avec High Availability en raison de ressources insuffisantes, vous devrez peut-être modifier les Cluster Features Virtual Machine Options en désactivant VM Restart Priority et en laissant Host Isolation Response activé.

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

Utilisez les navigateurs compatibles dans Active IQ Unified Manager

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

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

"mysupport.netapp.com/matrix"

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit un affichage correct des fonctionnalités du logiciel.

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

Découvrez les exigences en matière de protocole et de port pour Active IQ Unified Manager

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

Connexions au serveur Unified Manager

Dans la plupart des installations, il n'est pas nécessaire de spécifier les numéros de port lors de la connexion à l'interface 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 saisir `https://<host>` au lieu de `https://<host>:443`.

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

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

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

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

Connexions depuis le serveur Unified Manager

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

En fonction de votre environnement, vous pouvez choisir de modifier les ports et les protocoles utilisés par le

serveur Unified Manager pour se connecter à des destinations spécifiques.

Le serveur Unified Manager se connecte aux systèmes de stockage gérés, aux serveurs et aux autres composants via les protocoles et ports suivants :

Destination	Protocole	Port	Description
Système de stockage	HTTPS	443/TCP	Utilisé pour surveiller et gérer les systèmes de stockage. Si vous utilisez ce port, ou tout autre port, pour vous connecter au serveur VMware vCenter ou au serveur ESXi, assurez-vous que le port est disponible et qu'il est possible de s'y connecter à partir d'un site sécurisé.
Système de stockage	NDMP	10000/TCP	Utilisé pour certaines opérations de restauration Snapshot.
AutoSupport serveur	HTTPS	443	Utilisé pour envoyer des informations AutoSupport. Nécessite un accès à Internet pour exécuter cette fonction.
Serveur d'authentification	LDAP	389	Utilisé pour effectuer des requêtes d'authentification, ainsi que des requêtes de recherche d'utilisateurs et de groupes.
LDAPS	636	Utilisé pour les communications LDAP sécurisées.	Serveur de messagerie

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

Remplissez la feuille de calcul dans Active IQ Unified Manager

Avant d'installer et de configurer Unified Manager, assurez-vous d'avoir à portée de main des informations spécifiques sur votre environnement. Vous pouvez les consigner dans une feuille de calcul.

Informations d'installation d'Unified Manager

Les informations nécessaires à l'installation d'Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Adresse IP du serveur ESXi	
Nom de domaine pleinement qualifié de l'hôte	
Adresse IP de l'hôte	
Masque de réseau	
Adresse IP de la passerelle	

Système sur lequel le logiciel est déployé	Votre valeur
Adresse DNS principale	
Adresse DNS secondaire	
Domaines de recherche	
Nom d'utilisateur de maintenance	
Mot de passe utilisateur de maintenance	

Informations de configuration d'Unified Manager

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

Paramètre	Votre valeur
adresse e-mail de l'utilisateur de maintenance	
Serveur NTP	
nom de l'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
port SMTP	25 (Valeur par défaut)
Adresse électronique utilisée pour envoyer les notifications d'alerte	
Nom de l'hôte ou adresse IP du serveur d'authentification	
Nom de l'administrateur Active Directory ou nom unique de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom unique de base du serveur d'authentification	
URL du fournisseur d'identité (IdP)	
Métadonnées du fournisseur d'identité (IdP)	
Adresses IP des hôtes de destination des traps SNMP	
port SNMP	

Informations sur le cluster

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

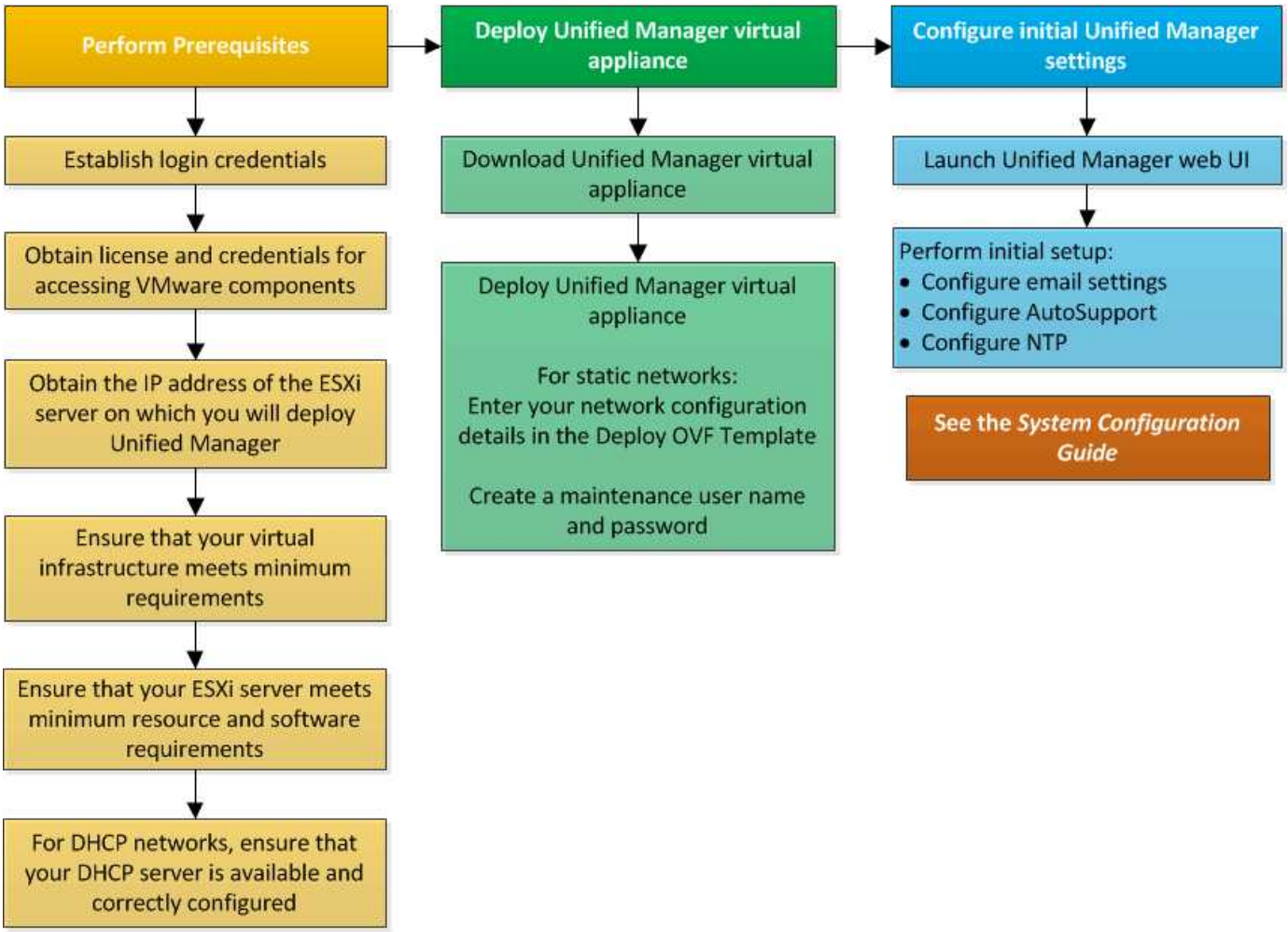
Cluster 1 sur N	Votre valeur
Nom de l'hôte ou adresse IP de gestion du cluster	

Cluster 1 sur N	Votre valeur
Nom d'utilisateur de l'administrateur ONTAP L'administrateur doit avoir reçu le rôle « `admin` ».	
Mot de passe de l'administrateur ONTAP	
Protocole	HTTPS

Installation, mise à niveau et suppression d'Unified Manager sur VMware vSphere

Découvrez le processus de déploiement d'Active IQ Unified Manager

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



Flux de travail de déploiement de l'appliance virtuelle Unified Manager

Déployer Active IQ Unified Manager

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

Avant de commencer

- Vous devez vérifier et compléter les exigences système pour le déploiement.

  Voir "Configuration système requise".

- Assurez-vous de disposer des informations suivantes :
  - Identifiants de connexion pour le site d'assistance NetApp
  - Identifiants pour accéder au serveur VMware vCenter et au client Web vSphere
  - Adresse IP du serveur ESXi sur lequel vous déployez l'appliance virtuelle Unified Manager
  - Détails concernant le centre de données, tels que l'espace de stockage dans le datastore et les besoins en mémoire
  - Le protocole 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 à l'aide de la console VMware, et non via SSH.

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

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

Étapes

1. Suivez les étapes dans "Télécharger Unified Manager".
2. De plus, suivez les étapes dans "Déployer l'appliance virtuelle Unified Manager".

Téléchargez le fichier d'installation Active IQ Unified Manager

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

Avant de commencer

Vous devez disposer des identifiants de connexion pour le site de 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 d'Unified Manager :

"Site de support NetApp"

2. Sélectionnez la version requise de Unified Manager et acceptez le contrat de licence de l'utilisateur final (EULA).
3. Téléchargez et enregistrez le `.tar` fichier d'installation VMware vSphere dans un répertoire local ou un répertoire réseau accessible à votre vSphere Client.
4. Vérifiez la somme de contrôle pour vous assurer que le logiciel a été téléchargé correctement.
5. Accédez au répertoire dans lequel vous avez téléchargé le `.tar` fichier et saisissez la commande suivante dans votre 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 indiquées dans le `README` fichier.

Déployez l'appliance virtuelle Active IQ Unified Manager

Après avoir téléchargé le fichier d'installation, déployez Unified Manager en tant qu'appliance virtuelle. Utilisez le vSphere Web Client pour déployer l'appliance virtuelle sur un serveur ESXi. Lors du déploiement de l'appliance virtuelle, une machine virtuelle est créée.

Avant de commencer

Vous devez consulter la configuration système requise. Apportez les modifications nécessaires avant de déployer l'appliance virtuelle Unified Manager.

Voir "Exigences en matière d'infrastructure virtuelle".

Voir "Exigences relatives aux logiciels et à l'installation de VMware".

Si vous utilisez le protocole DHCP (Dynamic Host Configuration Protocol), assurez-vous que le serveur DHCP est disponible et que les configurations DHCP et de la carte réseau de la machine virtuelle sont correctes. Le protocole 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 du serveur DNS appropriées ont été configurées.

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

- Identifiants pour accéder au serveur VMware vCenter 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 la disponibilité de l'espace de stockage
- Si vous n'utilisez pas DHCP, obtenez les adresses IPv4 ou IPv6 des périphériques réseau auxquels vous prévoyez de vous connecter :
  - Nom de domaine complet (FQDN) de l'hôte
  - Adresse IP de l'hôte

- Masque de réseau
- Adresse IP de la passerelle par défaut
- Adresses DNS primaires et secondaires
- Domaines de recherche

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

Lors du déploiement de l'appliance virtuelle, un certificat auto-signé unique est généré pour l'accès HTTPS. Lors de l'accès à l'interface web de Unified Manager, un avertissement concernant les certificats non approuvés peut s'afficher dans votre navigateur.

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

Étapes

1. Dans le vSphere Client, cliquez sur **Fichier** > **Déployer le modèle OVF**.
2. Terminez l'assistant Deploy OVF Template pour déployer l'appliance virtuelle Unified Manager.

   Sur la page Détails de l'avis :

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

     Sur la page Personnaliser le modèle :

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

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

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

   Le processus de démarrage initial prend quelques minutes.

5. Pour configurer votre fuseau horaire, saisissez votre zone géographique ainsi que votre ville ou région comme indiqué dans la fenêtre VM Console.

   Toutes les informations de date affichées utilisent le fuseau horaire configuré pour Unified Manager, indépendamment du 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, même si leur

affichage peut différer. Par exemple, si vous créez une copie Snapshot à l'aide d'un périphérique configuré dans un fuseau horaire différent de celui du serveur de gestion, l'horodatage sera celui 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 réseau statique, sélectionnez l'une des options suivantes :

Si vous utilisez…	Ensuite, faites ceci…
DHCP	Sélectionnez **Réessayer DHCP**. Si vous prévoyez d'utiliser DHCP, assurez-vous qu'il est correctement configuré. Si vous utilisez un réseau compatible DHCP, le nom de domaine complet (FQDN) et les entrées du serveur DNS sont automatiquement attribués à l'appliance virtuelle. Si DHCP n'est pas correctement configuré avec DNS, le nom de l'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 réseau statique	a. Sélectionnez **Entrez les détails de la configuration réseau statique**. Le processus de configuration prend quelques minutes. b. Confirmez les valeurs que vous avez saisies et sélectionnez **Y**.

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

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

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

   La console de la VM affiche l'URL de l'interface utilisateur Web de 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".

Flux de travail de mise à niveau de l'appliance virtuelle Unified Manager

Mise à niveau d'Active IQ Unified Manager

Vous pouvez mettre à niveau Active IQ Unified Manager vers la version 9.18 uniquement à partir des versions 9.14 ou 9.16.

Pendant la mise à niveau, Unified Manager est indisponible. Veuillez terminer toutes les opérations en cours avant de mettre à niveau Unified Manager.

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

Si votre système a été mis à niveau depuis Unified Manager 9.7, vous ne pouvez pas effectuer une mise à niveau directe de la version 9.14 à la version 9.18 en raison de modifications du système de fichiers dans les versions Debian. Suivez plutôt la procédure de mise à niveau recommandée : 9.14 → 9.16P2 → 9.18.

Étapes

1. Suivez les étapes dans "Téléchargez l'image ISO de Unified Manager".
2. De plus, suivez les étapes décrites dans "Mettez à niveau Unified Manager".

Utilisez la voie de mise à niveau prise en charge pour les versions de Active IQ Unified Manager

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

Toutes les versions d'Unified Manager ne permettent pas d'effectuer une mise à niveau sur place vers des versions ultérieures. Les mises à niveau d'Unified Manager sont limitées à un modèle N-2. Cela signifie que vous ne pouvez effectuer une mise à niveau que vers les deux versions suivantes sur toutes les plateformes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.18 uniquement à partir d'Unified Manager 9.14 et 9.16.

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

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

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.11 → 9.13
2. Mise à niveau 9.13 → 9.14
3. Mise à niveau 9.13 → 9.16
4. Mise à niveau 9.14 ou 9.16 → 9.18

Pour plus d'informations sur la matrice des chemins de mise à niveau, consultez ceci "article de la base de connaissances (KB)".

Téléchargez le fichier de mise à niveau Active IQ Unified Manager

Avant de mettre à niveau Unified Manager, téléchargez le fichier de mise à niveau de Unified Manager depuis le NetApp Support Site.

Avant de commencer

Vous devriez disposer d'identifiants de connexion pour le site d'assistance NetApp.

Étapes

1. Connectez-vous au site d'assistance NetApp :

   "Site de support NetApp"

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

Mettez à niveau l'appliance virtuelle Active IQ Unified Manager

Vous pouvez mettre à niveau l'appliance virtuelle Active IQ Unified Manager des versions 9.14 ou 9.16 vers la version 9.18.

Avant de commencer

Assurez-vous de ce qui suit :

- 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 aux exigences système et logicielles.

  Voir "Exigences en matière d'infrastructure virtuelle".

  Voir "Exigences relatives aux logiciels et à l'installation de VMware".

- Pour les utilisateurs de vSphere 6.5 et versions ultérieures, vous avez installé VMware Remote Console (VMRC).
- Lors de la mise à niveau, il vous sera peut-être demandé de confirmer si vous souhaitez conserver les paramètres par défaut précédents de conservation des données de performance pendant 13 mois ou les modifier à 6 mois. Après confirmation, l'historique des données de performance est supprimé au bout de 6 mois.
- Vous disposez des informations suivantes :
  - Identifiants de connexion pour le site d'assistance NetApp
  - Identifiants pour accéder au serveur VMware vCenter et au client Web vSphere
  - Identifiants de l'utilisateur de maintenance d'Unified Manager

Pendant la mise à niveau, Unified Manager est indisponible. Veuillez terminer toutes les opérations en cours avant de mettre à niveau Unified Manager.

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

Étapes

1. Dans le 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 **Summary** > **Commands** > **Shut Down Guest**.
4. Créez une copie de sauvegarde, telle qu'un instantané ou un clone, de la machine virtuelle Unified Manager afin de créer une sauvegarde cohérente au niveau des applications.

5. Depuis le client vSphere, mettez sous tension la machine virtuelle Unified Manager.
6. Lancez VMware Remote Console.
7. Cliquez sur l'icône **CDROM** et sélectionnez **Connect to Disk Image File (.iso)**.
8. Sélectionnez le `ActiveIQUnifiedManager-<version>-virtual-update.iso` fichier, puis 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 sera indisponible pendant le processus de mise à niveau et sera de nouveau disponible une fois celui-ci terminé.

12. Saisissez `y` pour continuer.

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

13. Saisissez `y` pour continuer.

    La 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 de Unified Manager.

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

Redémarrez la machine virtuelle Active IQ Unified Manager

Vous pouvez redémarrer la machine virtuelle (VM) Unified Manager à partir de la console de maintenance. Il est recommandé de redémarrer la VM après avoir généré un nouveau certificat de sécurité, ou en cas de problème avec la VM.

Avant de commencer

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

Vous pouvez également redémarrer la machine virtuelle depuis vSphere à l'aide de l'option VMware **Restart Guest**. Consultez "la cmdlet Restart-VMGuest dans la référence CMDLET VMware vSphere PowerCLI de Broadcom."

Étapes

1. Dans la console de maintenance, sélectionnez **Configuration système** > **Redémarrer la machine virtuelle**.

2. Lancez l’interface utilisateur web Unified Manager depuis votre navigateur et connectez-vous.

Supprimer Active IQ Unified Manager

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

Avant de commencer

- Vous devez disposer des identifiants nécessaires pour accéder à VMware vCenter Server et au client Web vSphere.
- Toute connexion active entre le serveur Unified Manager et 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 n’a pas de connexion active à un fournisseur de données externe.
2. Dans le vSphere Client, cliquez sur **Accueil** > **Inventaire** > **VM et modèles**.
3. Sélectionnez la machine virtuelle que vous souhaitez supprimer, puis cliquez sur l’onglet **Summary**.
4. Si la machine virtuelle est en cours d’exécution, cliquez sur **Alimentation** > **Arrêter le système invité**.
5. Faites un clic droit sur la machine virtuelle que vous souhaitez supprimer, puis cliquez sur **Supprimer du disque**.

Installer Unified Manager sur les systèmes Linux

Introduction à Active IQ Unified Manager

Découvrez Active IQ Unified Manager

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

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

Informations connexes

"Outil NetApp Interoperability Matrix Tool"

Comprendre le rôle du serveur Active IQ Unified Manager

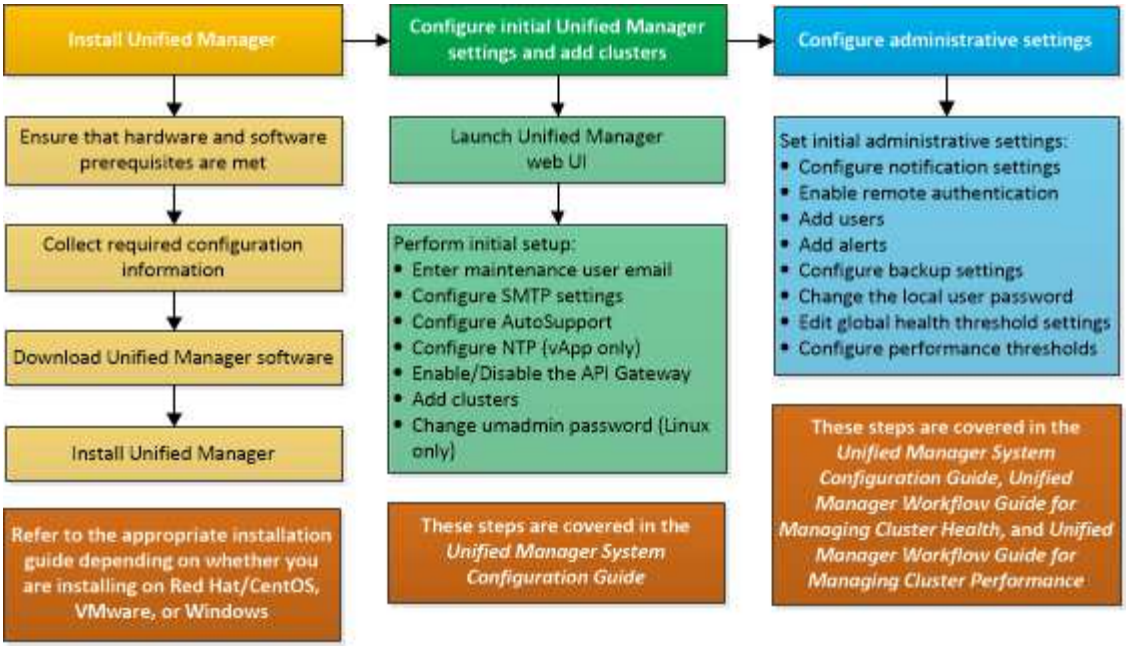
L'infrastructure serveur d'Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur applicatif. Elle fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations du cluster, stocke les données dans la base de données et les analyse pour détecter d'éventuels problèmes au niveau du cluster.

Consultez la séquence d'installation de Active IQ Unified Manager

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

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



Configuration requise pour l'installation d'Unified Manager

Comprendre les exigences d'installation d'Active IQ 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 toute modification du code de l'application Unified Manager. Si vous devez appliquer des mesures de sécurité au serveur Unified Manager, vous devez effectuer ces modifications au niveau du système d'exploitation sur lequel Unified Manager est installé.

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

"Prise en charge des mesures de sécurité appliquées à Active IQ Unified Manager pour Clustered Data ONTAP"

Informations connexes

"Outil NetApp Interoperability Matrix Tool"

Comprendre les exigences en matière d'infrastructure virtuelle et de matériel pour Active IQ Unified Manager

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

Le tableau suivant présente les valeurs recommandées pour la mémoire, le processeur et l'espace disque. Ces valeurs ont été validées afin que Unified Manager offre des performances acceptables.

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

Unified Manager peut être installé sur des systèmes disposant de peu de mémoire, mais les 12 Go de RAM recommandés garantissent qu'une quantité de mémoire suffisante est disponible pour des performances optimales et permettent au système d'accueillir des clusters et des objets de stockage supplémentaires à mesure que votre configuration évolue. Vous ne devez définir aucune limite de mémoire sur la machine virtuelle sur laquelle Unified Manager est déployé et ne devez activer aucune fonctionnalité (par exemple, le ballooning) qui empêcherait le logiciel d'utiliser la mémoire allouée sur le système.

De plus, il existe une limite au nombre de nœuds qu'une seule instance d'Unified Manager peut surveiller avant que vous n'installiez une seconde instance d'Unified Manager. Pour connaître les limites de nœuds, les recommandations concernant le processeur et la mémoire, consultez la "guide des bonnes pratiques Unified Manager".

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

Exigence d'utilisation dédiée

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

Besoins en espace pour les sauvegardes

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

Exigences en matière de connectivité hôte

Le système physique ou le système virtuel sur lequel vous installez Unified Manager doit être configuré de telle sorte que vous puissiez `ping` résoudre correctement le nom de l'hôte à partir de l'hôte lui-même. En cas de configuration IPv6, vous devez vérifier que `ping6` la résolution du nom de l'hôte aboutit afin de garantir la réussite de l'installation d'Unified Manager.

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

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

Découvrez les logiciels Linux et les exigences d'installation dans Active IQ Unified Manager

Le système Linux sur lequel vous installez Unified Manager requiert des versions spécifiques du système d'exploitation et des logiciels associés. Pour les installations Linux, Unified Manager ne peut être installé que sur un système d'exploitation Red Hat Enterprise Linux. Il ne peut pas être installé sur un autre système d'exploitation.

Logiciel du système d'exploitation

Le système Linux doit avoir installé les versions suivantes du système d'exploitation et des logiciels de prise en charge :

- Red Hat Enterprise Linux versions 8.x et 9.6, basées sur l'architecture x86_64

Consultez l'Interoperability Matrix pour obtenir la liste complète et la plus récente des versions de Red Hat Enterprise Linux prises en charge.

"NetApp Matrice d'interopérabilité"

Le serveur doit être dédié à l'exécution d'Unified Manager. Aucune autre application ne doit être installée sur le serveur. Dans certains environnements, un scanner de vulnérabilités tel que Qualys est installé sur le système Linux en raison de la politique de l'entreprise. Vous devez désactiver le scanner de vulnérabilités avant d'installer Unified Manager afin d'éviter tout échec de l'installation.

> Les outils d'analyse de vulnérabilités (tels que Qualys) peuvent entraîner une utilisation élevée du processeur lors de l'analyse de la machine virtuelle (VM), que ce soit en interne (lorsque Unified Manager et l'outil d'analyse de vulnérabilités sont installés sur la même VM) ou en externe (lorsque Unified Manager et l'outil d'analyse de vulnérabilités sont installés sur deux serveurs différents et que l'outil d'analyse de vulnérabilités analyse la VM sur laquelle Unified Manager est installé). Ce problème rend souvent la VM indisponible et affecte les services Unified Manager. Par conséquent, NetApp recommande de désactiver l'outil d'analyse de vulnérabilités sur la VM sur laquelle Unified Manager est installé. S'il n'est pas possible de désactiver l'outil d'analyse, analysez alors la VM en dehors des heures ouvrables et redémarrez les services une fois l'analyse terminée.

Logiciels tiers

Unified Manager est déployé sur un serveur web WildFly. WildFly 27.0.1.Final est intégré et configuré avec Unified Manager.

Les packages tiers suivants sont requis, mais ne sont pas inclus dans Unified Manager. Ces packages sont automatiquement installés par le `yum`programme d'installation, à condition que vous ayez configuré les dépôts comme indiqué dans les sections suivantes.

- MySQL Community Edition version 8.4.10 (provenant du dépôt MySQL)
- OpenJDK version 17.0.14+6 (provenant du dépôt Red Hat Extra Enterprise Linux Server)
- Python 3.13.3 (provenant du dépôt Red Hat Extra Enterprise Linux Server)
- Version 7zip 7z2301-linux-x64. Pour plus d'informations, consultez "Configurer le package logiciel 7-zip".

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

Exigences d'autorisation de l'utilisateur

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

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

exigences d'installation

Les bonnes pratiques d'installation de Red Hat Enterprise Linux et des dépôts associés sur votre système sont décrites ci-dessous. Les systèmes installés ou configurés différemment, ou déployés hors site (dans le cloud), peuvent nécessiter des étapes supplémentaires, et Unified Manager risque de ne pas fonctionner correctement dans ces déploiements.

- Vous devez installer Red Hat Enterprise Linux conformément aux bonnes pratiques de Red Hat et sélectionner les options par défaut suivantes, ce qui nécessite de choisir l'environnement de base "Server with GUI".
- Lors de l'installation d'Unified Manager sur Red Hat Enterprise Linux, le système doit avoir accès au dépôt approprié afin que le programme d'installation puisse accéder et installer toutes les dépendances logicielles requises.
- Pour que le `yum` programme d'installation puisse trouver les logiciels dépendants dans les dépôts Red Hat Enterprise Linux, vous devez avoir enregistré le système lors de l'installation de Red Hat Enterprise Linux ou ultérieurement à l'aide d'un abonnement Red Hat valide.

  Consultez la documentation Red Hat pour obtenir des informations sur Red Hat Subscription Manager.

- Vous devez activer le dépôt Extra Packages for 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 le télécharger et le configurer

manuellement.

Voir "Configuration manuelle du référentiel EPEL".

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

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

  Voir "Configuration manuelle du dépôt MySQL".

- Vous ne devez installer qu'une seule version de Java sur votre hôte Unified Manager ; sinon, le système risque de ne pas pouvoir déterminer la version à 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 dépôts ne sont pas répliqués d'un système connecté à Internet vers le système non connecté, vous devez suivre les instructions d'installation pour déterminer les dépendances logicielles externes de votre système. Vous pouvez ensuite télécharger les logiciels 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 artefacts et les packages, vous devez utiliser la `yum install` commande. Vous devez vous assurer que les deux systèmes exécutent la même version du système d'exploitation et que la licence d'abonnement correspond à la version appropriée de Red Hat Enterprise Linux.

> Vous ne devez pas installer les logiciels tiers requis à partir de dépôts autres que ceux listés ici. Les logiciels installés depuis les dépôts Red Hat sont conçus spécifiquement pour Red Hat Enterprise Linux et respectent les bonnes pratiques Red Hat (organisation des répertoires, permissions, etc.). Les logiciels provenant d'autres sources peuvent ne pas respecter ces recommandations, ce qui peut entraîner l'échec de l'installation d'Unified Manager ou des problèmes lors des mises à jour ultérieures.

Exigence du port 443

Les images génériques de Red Hat Enterprise Linux peuvent bloquer l'accès externe au port 443. De ce fait, il se peut que vous ne puissiez pas vous connecter à l'interface web de l'administrateur après l'installation de Unified Manager. L'exécution de la commande suivante autorise l'accès au port 443 pour tous les utilisateurs et applications externes sur une image générique de Red Hat Enterprise Linux.

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

Vous devez installer Red Hat Enterprise Linux avec l'environnement de base « `Server with GUI` ». Il fournit les commandes utilisées par les instructions d'installation de Unified Manager. D'autres environnements de base peuvent vous obliger à installer des 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
```

Avant d'exécuter les commandes, veuillez contacter votre service informatique pour vérifier si vos politiques de sécurité exigent une procédure différente.

> La fonctionnalité THP (Transparent Huge Pages) doit être désactivée sur les systèmes Red Hat. Lorsqu'elle est activée, elle peut, dans certains cas, entraîner l'arrêt d'Unified Manager si

certains processus consomment trop de mémoire et sont interrompus.

Utilisez les navigateurs compatibles avec Active IQ Unified Manager

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

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

"mysupport.netapp.com/matrix"

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit un affichage correct des fonctionnalités du logiciel.

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

Découvrez les exigences en matière de protocole et de port dans Active IQ Unified Manager

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

Connexions au serveur Unified Manager

Dans la plupart des installations, il n'est pas nécessaire de spécifier les numéros de port lors de la connexion à l'interface 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 saisir `https://<host>` au lieu de `https://<host>:443`.

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

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

Interface	Protocole	Port	Description
ligne de commandes Linux	SSH/SFTP	22	Utilisé pour accéder à la ligne de commandes de Red Hat Enterprise Linux et récupérer les bundles de support.
base de données MySQL	MySQL	3306	Utilisé pour activer l'accès à Unified Manager par OnCommand Workflow Automation et OnCommand API Services.
Syslog	UDP	514	Permet d'accéder aux messages EMS par abonnement des systèmes ONTAP et de créer des événements à partir de ces messages.
REST	HTTPS	9443	Permet d'accéder en temps réel aux événements EMS basés sur l'API REST à partir de systèmes ONTAP authentifiés.
base de données MySQL	MySQL	3306	Utilisé pour activer l'accès à Unified Manager par OnCommand Workflow Automation et OnCommand API Services.
Courtier AMQP QPID	TCP/IP	56072	Utilisé pour la communication des messages internes.
Courtier AMQP QPID	WebSocket via TCP	56080	Utilisé pour écouter sur ce port les messages reçus de ONTAP (agent cloud).
Courtier AMQP QPID	WebSocket via TCP	56443	Ce port est utilisé pour écouter les messages reçus d'ONTAP (cloud agent). La communication via ce port prend en charge le chiffrement fourni par TLS ou SSL.

Le port par défaut de MySQL, 3306, est limité à l'hôte local lors de l'installation d'Unified Manager sur les systèmes Linux. Cela n'a aucune incidence sur les scénarios de mise à niveau, pour lesquels la configuration précédente est conservée. Cette configuration peut être modifiée, et la connexion peut être rendue disponible pour d'autres hôtes à l'aide de l'option `Control access to MySQL port 3306` dans la console de maintenance. Pour plus d'informations, voir "Options de menu supplémentaires". Les ports utilisés pour la communication HTTP et

HTTPS (ports 80 et 443) peuvent être modifiés à l'aide de la console de maintenance Unified Manager. Pour plus d'informations, voir "Menus de la console de maintenance".

Connexions depuis le serveur Unified Manager

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

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

Le serveur Unified Manager se connecte aux systèmes de stockage gérés, aux serveurs et aux autres composants via les protocoles et ports suivants :

Destination	Protocole	Port	Description
Système de stockage	HTTPS	443/TCP	Utilisé pour surveiller et gérer les systèmes de stockage.
Système de stockage	NDMP	10000/TCP	Utilisé pour certaines opérations de restauration Snapshot.
AutoSupport serveur	HTTPS	443	Utilisé pour envoyer des informations AutoSupport. Nécessite un accès à Internet pour exécuter cette fonction.
Serveur d'authentification	LDAP	389	Utilisé pour effectuer des requêtes d'authentification, ainsi que des requêtes de recherche d'utilisateurs et de groupes.
LDAPS	636	Utilisé pour les communications LDAP sécurisées.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	émetteur de pièges SNMP
SNMPv1 ou SNMPv3	162/UDP	Utilisé pour envoyer des traps SNMP de notification d'alerte.	Serveur du fournisseur de données externe
TCP	2003	Utilisé pour envoyer des données de performance à un fournisseur de données externe, tel que Graphite.	Serveur NTP

Destination	Protocole	Port	Description
NTP	123/UDP	Utilisé pour synchroniser l'heure du serveur Unified Manager avec un serveur NTP externe. (Systèmes VMware uniquement)	Syslog
UDP	514	Utilisé par Unified Manager pour envoyer les journaux d'audit à un serveur syslog distant.	Courtier AMQP QPID
TCP/IP	56072	Utilisé pour la communication des messages internes.	Courtier AMQP QPID
WebSocket via TCP	56080	Utilisé pour écouter sur ce port les messages reçus de ONTAP (agent cloud).	Courtier AMQP QPID

Remplissez la feuille de calcul dans Active IQ Unified Manager

Avant d'installer et de configurer Unified Manager, assurez-vous d'avoir à portée de main des informations spécifiques sur votre environnement. Vous pouvez les consigner dans une feuille de calcul.

Informations d'installation d'Unified Manager

Les informations nécessaires à l'installation d'Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Nom de domaine pleinement qualifié 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 de configuration d'Unified Manager

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

Paramètre	Votre valeur
adresse e-mail de l'utilisateur de maintenance	

Paramètre	Votre valeur
nom de l'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
port SMTP	25 (Valeur par défaut)
Adresse électronique utilisée pour envoyer les notifications d'alerte	
Nom de l'hôte ou adresse IP du serveur d'authentification	
Nom de l'administrateur Active Directory ou nom unique de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom unique de base du serveur d'authentification	
URL du fournisseur d'identité (IdP)	
Métadonnées du fournisseur d'identité (IdP)	
Adresses IP des hôtes de destination des traps SNMP	
port SNMP	

Informations sur le cluster

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

Cluster 1 sur N	Votre valeur
Nom de l'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 de l'administrateur ONTAP	
Protocole	HTTPS

Installer, mettre à niveau et supprimer le logiciel Unified Manager

Installer, mettre à niveau et supprimer le logiciel Active IQ Unified Manager

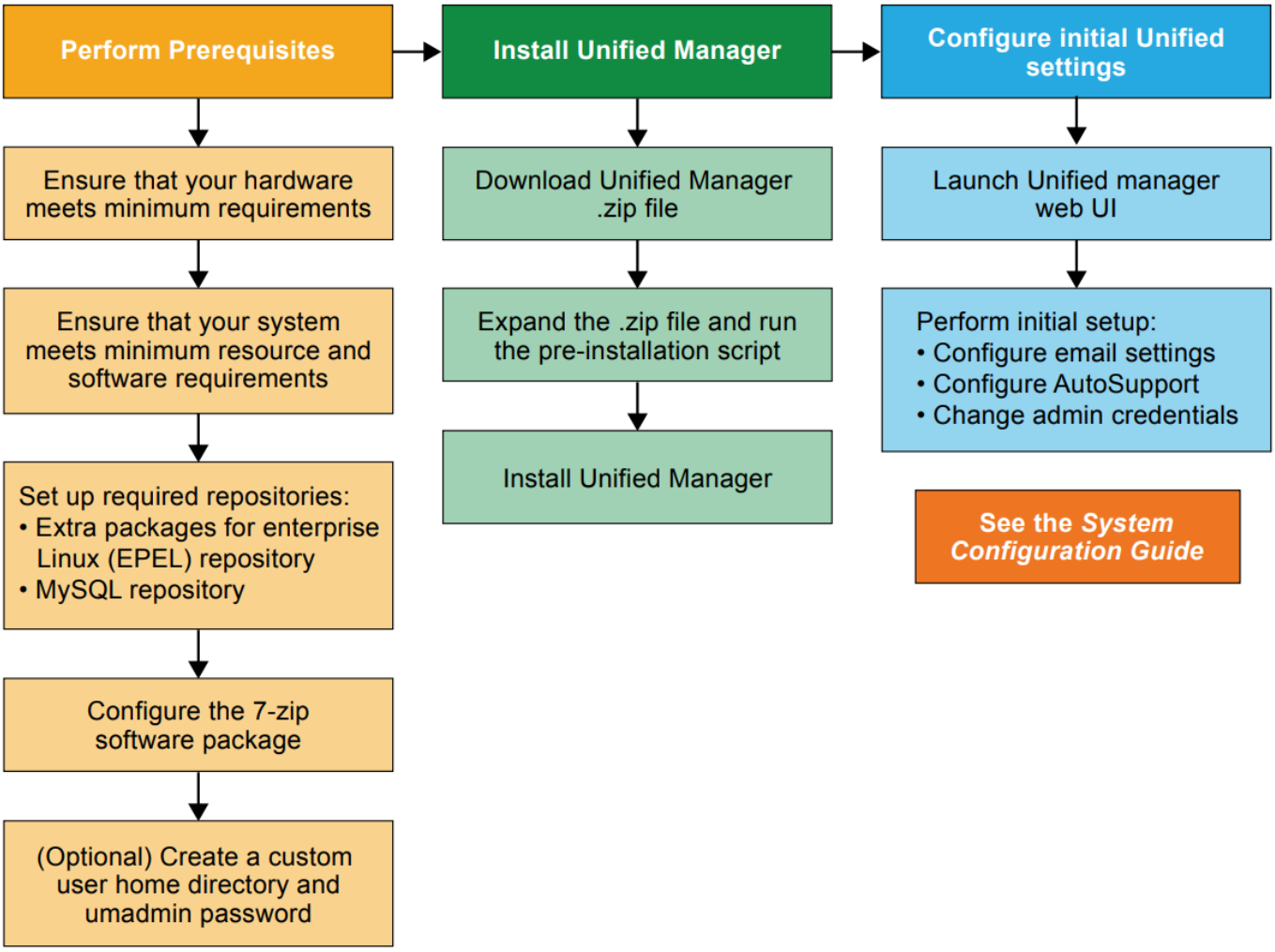
Sur les systèmes Linux, vous pouvez installer le logiciel Unified Manager, le mettre à niveau vers une version plus récente ou le supprimer.

Unified Manager peut être installé sur des serveurs Red Hat Enterprise Linux. Le serveur Linux sur lequel vous installez Unified Manager peut être exécuté soit sur une machine physique, soit sur une machine virtuelle

exécutée sur VMware ESXi, Microsoft Hyper-V ou Citrix XenServer.

Comprendre la séquence d'installation d'Active IQ Unified Manager sur Red Hat Enterprise Linux

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



Configurer le logiciel requis

Configurer le référentiel EPEL pour Active IQ Unified Manager

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

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

Étapes

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

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

Pour la version 9, téléchargez-la depuis :

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

2. Configurer le référentiel EPEL:

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

Pour les systèmes Red Hat Enterprise Linux 8, si vous disposez de dépôts internes avec des paquets RPM modulaires, par exemple, *javapackages-filesystem-<version>.module.rpm*, assurez-vous que les métadonnées des paquets modulaires sont également disponibles dans le même dépôt.

Configurez le référentiel MySQL pour Active IQ Unified Manager

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

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

Cette tâche peut échouer si le système n'est pas connecté à Internet. Consultez la documentation MySQL si le système sur lequel vous installez Unified Manager n'a pas accès à Internet.

Étapes

1. Téléchargez le dépôt MySQL correspondant à votre installation. Pour la version 8, téléchargez-le depuis :

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

Pour la version 9, téléchargez-la depuis :

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

2. Configurer le dépôt MySQL :

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

Pour un système Red Hat Enterprise Linux 8, si vous utilisez des dépôts internes contenant java-17-openjdk, 7-zip et d'autres progiciels fournis par le dépôt AppStream, vous devez désactiver votre dépôt 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 un message d'erreur concernant une clé manquante ou une incompatibilité de clé, et que votre installation échoue, essayez les étapes suivantes :

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

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

for example:

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

- Sur un système sans connexion Internet, mettez à jour votre fichier de dépôt MySQL et désactivez `gpgcheck` en marquant `gpgcheck=0`.

Configurez le logiciel 7-zip dans Active IQ Unified Manager

Pour installer correctement Unified Manager sur un système Red Hat Enterprise Linux, votre système doit être configuré avec un accès au package logiciel 7-zip. Si l'accès réseau est disponible et que l'URL 7-zip n'est pas bloquée par un pare-feu, 7-zip est téléchargé automatiquement sur votre système pendant le processus d'installation ou de mise à niveau. NetApp recommande la méthode de téléchargement automatique.

Assurez-vous que l'URL suivante n'est pas bloquée dans votre pare-feu pour permettre à Unified Manager de télécharger automatiquement le package logiciel 7-zip:
https://7-zip.org/a/7z2301-linux-x64.tar.xz

Vous pouvez également préinstaller 7-zip.

Préinstallez le package 7-zip

Vous pouvez préinstaller 7-zip en le téléchargeant manuellement ou à l'aide d'un script fourni. Choisissez l'une des deux méthodes suivantes :

Téléchargement à l'aide d'un script fourni

Étape

1. Exécutez le `install7zip.sh` script inclus dans le fichier zip Unified Manager.

Télécharger manuellement

Assurez-vous de télécharger le package 7-zip uniquement depuis le site officiel.

Étapes

1. Téléchargez le package 7-zip (version 23.01) depuis le site officiel:

   https://7-zip.org/a/7z2301-linux-x64.tar.xz

2. Copiez le fichier sur votre machine virtuelle RHEL :

   ```
   7z2301-linux-x64.tar.xz
   ```

3. Extraire l'archive:

```
sudo tar -xf 7z2301-linux-x64.tar.xz
```

4. Déplacez le `7zz` fichier vers le `/usr/bin/` répertoire:

```
sudo cp 7zz /usr/bin/
```

5. Définissez les autorisations d'exécution :

```
sudo chmod 755 /usr/bin/7zz
```

Vérifiez l'installation

Vérifiez que le paquet 7-zip a bien été installé sur votre système :

```
7zz -version
```

Configurez SELinux pour les partages NFS et CIFS dans Active IQ Unified Manager

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 éléments.

Si vous prévoyez de monter `/opt/netapp` ou `/opt/netapp/data` depuis un emplacement autre que le système de fichiers racine, et que SELinux est activé dans votre environnement, vous devez définir le contexte approprié pour les répertoires montés. Pour le scénario applicable dans votre environnement, suivez ces étapes pour définir et confirmer le contexte SELinux correct.

Configurez le 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 la base de données.

1. Exécutez cette commande pour vérifier le contexte :

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

   Exemple de résultat :

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

Dans ce résultat, le contexte est `default_t`. Vous devriez remplacer ce contexte par `mysqld_db_t`.

2. Suivez ces étapes pour définir le contexte en fonction de la manière dont vous avez effectué le montage `/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 l' `/opt/netapp/data/`option de montage, ajoutez l'étiquette MySQL comme suit :

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

   ```
   mount <nfsshare>:/<mountpoint> /opt/netapp/data -o
   context=system_u:object_r:mysqld_db_t:s0
   ```
3. Vérifiez si le contexte est correctement défini :

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

Exemple de résultat :

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

Configurez le contexte SELinux lorsque `/opt/netapp` est monté, et lorsque `/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 correctement défini le contexte pour `/opt/netapp/data/`, assurez-vous que le répertoire parent `/opt/netapp` n'a pas le contexte SELinux défini sur `file_t`.

Étapes

1. Exécutez cette commande pour vérifier le contexte :

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

   Exemple de résultat :

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

   Dans ce résultat, le contexte est `file_t` et doit être modifié. Les commandes suivantes définissent le contexte sur `usr_t`. Vous pouvez définir le contexte sur toute valeur autre que `file_t` en fonction de vos

exigences de sécurité.

2. Suivez ces étapes pour définir le contexte, en fonction de la manière dont vous avez effectué le montage `/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 l' `/opt/netapp`option de montage, ajoutez l'étiquette MySQL comme suit :

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

2. Démontez, puis remontez `/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
   ```

Exemple de sortie

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

Configurez le contexte SELinux lorsque `/opt/netapp` est monté, et que `/opt/netapp/data/` n'est pas monté 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 la base de données.

Étapes

1. Exécutez cette commande pour vérifier le contexte :

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

   Exemple de résultat :

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

   Dans ce résultat, le contexte est `default_t`. Vous devriez remplacer ce contexte par `mysqld_db_t`.

2. Suivez les étapes suivantes pour définir le contexte en fonction de la manière dont vous avez effectué le montage `/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 l `/opt/netapp/` option de montage, ajoutez l'étiquette MySQL comme suit
   `context=system_u:object_r:mysqld_db_t:s0`

   c. Démontez, puis remontez `/opt/netapp/` pour activer le contexte.

   d. Si vous disposez d'un montage NFS direct, exécutez la commande suivante pour définir le contexte sur `mysqld_db_t`:
   ```
   mount <nfsshare>:/<mountpoint> /opt/netapp -o
   context=system_u:object_r:mysqld_db_t:s0
   ```

3. Vérifiez si le contexte est correctement défini :

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

Exemple de résultat :

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

Installer Unified Manager sur les systèmes Linux

Créez un répertoire local utilisateur personnalisé et un mot de passe umadmin avant d'installer Active IQ Unified Manager

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

Avant de commencer

- Le système doit satisfaire aux exigences décrites dans "Configuration matérielle requise du système".
- Vous devez pouvoir vous connecter en tant qu'utilisateur root au système Red Hat Enterprise Linux.

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

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

Comme certains environnements d'installation restreignent l'accès à `/home`, l'installation échoue. Vous devez créer le répertoire local à un autre emplacement. Par ailleurs, certains sites peuvent imposer des règles de complexité des mots de passe ou exiger que ceux-ci soient définis par les administrateurs locaux plutôt que par le programme d'installation.

Si votre environnement d'installation nécessite que vous modifiiez ces paramètres d'installation par défaut, suivez ces étapes pour créer un répertoire local 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 des paramètres par défaut de l'installation.

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

Les politiques de sécurité de votre environnement ne doivent pas restreindre les privilèges sudo de l'utilisateur de maintenance d'Unified Manager. Certaines opérations d'Unified Manager pourraient échouer si ces privilèges sont restreints. Après une installation réussie, vérifiez que vous pouvez exécuter la commande sudo suivante lorsque vous êtes connecté en tant qu'utilisateur umadmin.

```
sudo systemctl status ocie
```

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

Étapes

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

   ```
   groupadd maintenance
   ```

3. Créez le compte utilisateur "umadmin" dans le groupe de maintenance sous un répertoire local de votre choix :

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

4. Définissez le mot de passe umadmin :

   ```
   passwd umadmin
   ```

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

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

Télécharger Active IQ Unified Manager

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

Avant de commencer

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

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

Étapes

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

"Site de support NetApp"

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



- Assurez-vous de télécharger la version correcte du fichier d'installation pour votre système Red Hat Enterprise Linux. Selon que Red Hat Enterprise Linux 8 ou 9 soit installé, veillez à 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 fichier `.zip`.

4. Vérifiez la somme de contrôle pour vous assurer de l'intégrité du logiciel téléchargé.
5. Si vous avez téléchargé le certificat de signature de code et la signature numérique, vous pouvez vérifier l'intégrité du fichier d'installation. Vous pouvez utiliser les commandes suivantes pour vérifier l'intégrité du fichier d'installation :
   - Cette commande crée un fichier contenant la clé publique du certificat de signature de code :

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

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

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

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

Installez Active IQ Unified Manager sur Red Hat Enterprise Linux

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

Avant de commencer

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

  Voir "Configuration matérielle requise du système".

  Voir "Logiciels Linux et exigences d'installation".

- Vous devez avoir téléchargé le fichier Unified Manager `.zip` depuis le site de support NetApp vers le système cible.

- Vous auriez dû vérifier l'intégrité du fichier `.zip` téléchargé.
- Vous devez disposer d'un navigateur Web compatible.
- Votre logiciel d'émulation doit avoir le défilement arrière activé.

Le système Red Hat Enterprise Linux peut disposer de toutes les versions requises des logiciels de prise en charge nécessaires (Java, MySQL, utilitaires supplémentaires), de seulement certains des logiciels requis, ou il peut s'agir d'un système nouvellement installé ne disposant d'aucun des logiciels requis.

Étapes

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

Logiciels requis et version minimale	Commande permettant de vérifier le logiciel et sa version
OpenJDK version 17.0.14+6	`java -version`
MySQL 8.4.10 Community Edition	`rpm -qa`
grep -i mysql`	7-zip

3. Si la version de MySQL installée est antérieure à MySQL 8.4.10 Community Edition, saisissez la commande suivante pour la désinstaller :

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

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

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

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

   Les modules `.rpm` requis 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'il n'existe aucun paramètre de configuration système ni aucun logiciel installé susceptible d'entrer en conflit avec l'installation d'Unified Manager :

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

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

   Pour un système Red Hat Enterprise Linux 8, si vous disposez de dépôts internes avec JDK 17 -

OpenJDK, 7-zip et d'autres packages logiciels fournis par le dépôt AppStream, vous devez désactiver votre dépôt 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 devez effectuer l'étape 7 uniquement si votre système n'est pas connecté à Internet et que vous devez télécharger manuellement les paquets nécessaires à votre installation. Si votre système a accès à Internet et que tous les paquets requis sont disponibles, passez à l'étape 8. Pour les systèmes non connectés à Internet ou n'utilisant pas les dépôts Red Hat Enterprise Linux, procédez comme suit pour déterminer si des paquets requis sont manquants, puis téléchargez-les :

   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 « `Installing:` » correspondent aux paquets disponibles dans le répertoire actuel, et les éléments de la section « `Installing for dependencies:` » correspondent aux paquets manquants sur votre système.

   b. Sur un système disposant d'un accès à Internet, téléchargez les paquets manquants :

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

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

   a. Copiez les paquets manquants depuis le système connecté à Internet vers votre système d'installation.

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

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

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

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

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

   > N'essayez pas d'installer à l'aide de commandes alternatives (telles que `rpm -ivh`). Pour qu'Unified Manager soit correctement installé sur un système Red Hat Enterprise Linux, tous les fichiers Unified Manager et les fichiers associés doivent être installés dans un ordre précis et dans une structure de répertoires spécifique, imposée automatiquement par la commande `yum install netapp-um<version>.x86_64.rpm`.

9. Ignorez la notification par courriel qui s'affiche immédiatement après les messages d'installation.

Le courriel informe l'utilisateur racine d'un échec initial de la tâche cron, ce qui n'a aucun effet néfaste sur l'installation.

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

    Le message est similaire au suivant :

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

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

11. Notez 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 local personnalisé avant d'installer Unified Manager, vous devez spécifier le shell de connexion de l'utilisateur umadmin :

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

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

Découvrez les utilisateurs créés lors de l'installation d'Active IQ Unified Manager

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

- **umadmin**

  Utilisé pour vous connecter à Unified Manager pour la première fois. Cet utilisateur se voit attribuer le rôle d'utilisateur "Application Administrator" et est configuré avec le type "Maintenance User". Cet utilisateur est créé par Unified Manager.

- **jboss**

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

- **mysql**

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

Outre ces utilisateurs, Unified Manager crée également des groupes correspondants : maintenance, jboss et mysql. Les groupes 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 local 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.

Modifier le mot de passe JBoss dans Active IQ Unified Manager

Vous pouvez réinitialiser le mot de passe JBoss spécifique à votre instance, défini lors de l'installation. Vous pouvez réinitialiser le mot de passe de façon facultative si votre site exige cette fonction de sécurité pour remplacer le paramètre d'installation de Unified Manager. Cette opération modifie également le mot de passe utilisé par JBoss pour accéder à MySQL.

- Vous devez disposer d'un accès utilisateur root au système Red Hat Enterprise Linux sur lequel Unified Manager est installé.
- Vous devez pouvoir accéder au 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. Arrêtez les services Unified Manager en saisissant les commandes suivantes dans l'ordre indiqué :

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   N'arrêtez pas le logiciel MySQL associé.

3. Saisissez la commande suivante pour démarrer le processus de changement de mot de passe :

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

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

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

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

5. Une fois le script terminé, démarrez les services de Unified Manager en saisissant 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'UI de Unified Manager.

Mise à niveau d'Unified Manager sur Red Hat Enterprise Linux

Mise à niveau d'Active IQ Unified Manager sur Red Hat Enterprise Linux

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

Les correctifs du logiciel Unified Manager, lorsqu'ils sont fournis par NetApp, sont installés 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 logicielles sont disponibles pour les deux produits, vous devez déconnecter les deux produits, puis configurer une nouvelle connexion Workflow Automation après avoir effectué les mises à niveau. Si vous effectuez une mise à niveau d'un seul des produits, vous devez alors vous connecter à Workflow Automation après la mise à niveau et vérifier qu'il continue à acquérir des données depuis Unified Manager.

Utilisez la voie de mise à niveau prise en charge pour les versions de Active IQ Unified Manager

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

Toutes les versions d'Unified Manager ne permettent pas d'effectuer une mise à niveau sur place vers des versions ultérieures. Les mises à niveau d'Unified Manager sont limitées à un modèle N-2. Cela signifie que vous ne pouvez effectuer une mise à niveau que vers les deux versions suivantes sur toutes les plateformes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.18 uniquement à partir d'Unified Manager 9.14 et 9.16.

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

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

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.11 → 9.13
2. Mise à niveau 9.13 → 9.14
3. Mise à niveau 9.13 → 9.16
4. Mise à niveau 9.14 ou 9.16 → 9.18

Pour plus d'informations sur la matrice des chemins de mise à niveau, consultez ceci "article de la base de connaissances (KB)".

Mise à niveau d'Active IQ Unified Manager

Vous pouvez mettre à niveau Unified Manager 9.14 ou 9.16 vers la version 9.18 en téléchargeant et en exécutant le fichier d'installation sur la plateforme Linux.

Avant de commencer

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

  Voir "Configuration matérielle requise du système".

Voir "Logiciels Linux et exigences d'installation".

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

  Voir "Mise à jour de JRE sous Linux".

- Vous devez installer ou mettre à niveau 7-zip vers la version appropriée avant de mettre à niveau Unified Manager. Voir "Configurer le package logiciel 7-zip".
- Pour éviter toute perte de données, vous devez avoir créé une sauvegarde de la base de données Unified Manager au cas où un problème surviendrait pendant la mise à niveau. NetApp recommande de déplacer le fichier de sauvegarde du `/opt/netapp/data` répertoire vers un emplacement externe.
- Lors de la mise à niveau, il vous sera peut-être demandé de confirmer si vous souhaitez conserver les paramètres par défaut précédents pour la conservation des données de performance pendant 13 mois ou les modifier pour une durée de 6 mois. Après confirmation, l'historique des données de performance est supprimé au bout de 6 mois.
- Vous devez avoir terminé toutes les opérations en cours, car Unified Manager n'est pas disponible pendant le processus de mise à niveau.
- MySQL Community Edition est automatiquement mis à niveau lors de la mise à niveau de Unified Manager. Si la version de MySQL installée sur votre système est antérieure à 8.4.10, le processus de mise à niveau de Unified Manager met automatiquement MySQL à niveau vers 8.4.10.

Étapes

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

   Voir "Téléchargement d'Unified Manager pour Linux".

3. Accédez au répertoire cible et décompressez le package Unified Manager :

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

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

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

   ```
   ls *.rpm
   ```

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

5. Exécutez le script de pré-installation pour vous assurer qu'aucun paramètre de configuration système ni aucun logiciel installé ne risque d'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 dépôts logiciels requis. Si le script détecte des problèmes, vous devez les résoudre et poursuivre la mise à niveau.

   Si des paquets manquants sont détectés, suivez les étapes mentionnées dans "Étapes supplémentaires à effectuer pour les paquets manquants". S'il n'y a pas de paquets manquants, poursuivez avec les étapes

suivantes.

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

   `upgrade.sh`

   Ce script exécute automatiquement les modules RPM, en mettant à niveau les logiciels de prise en charge nécessaires et les modules Unified Manager qui s'exécutent sur ceux-ci. De plus, le script de mise à niveau vérifie s'il existe des paramètres de configuration système ou des logiciels installés susceptibles d'entrer en conflit avec la mise à niveau. Si le script détecte des problèmes, vous devez les résoudre avant de mettre à niveau Unified Manager. Si vous avez précédemment installé des packages, tels que *net-snmp*, avant de mettre à niveau Unified Manager, la dépendance MySQL peut désinstaller le package pendant la mise à niveau. Vous devez réinstaller manuellement le package pour continuer à l'utiliser.

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

   Le message est similaire au suivant :

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

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

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

Étapes supplémentaires à effectuer pour les paquets manquants

Si des paquets 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 dépôts Red Hat Enterprise Linux, suivez les étapes suivantes pour déterminer si des paquets requis vous manquent et téléchargez ces paquets.

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

1. Consultez la liste des paquets disponibles et indisponibles :

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

   Les éléments de la section « `Installing:` » correspondent aux paquets disponibles dans le répertoire actuel, et les éléments de la section « `Installing for dependencies:` » correspondent aux paquets manquants sur votre système.

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

les paquets manquants.

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

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

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

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

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

```
yum install *.rpm
```

5. Démarrez le serveur Unified Manager. Exécutez les commandes suivantes :

```
systemctl start ocie

systemctl start ocieau
```

Cette procédure termine le processus de mise à niveau d'Unified Manager. Saisissez l'adresse IP ou l'URL indiquée dans une nouvelle fenêtre d'un navigateur web compatible pour démarrer l'interface utilisateur web d'Unified Manager, puis connectez-vous à l'aide du même nom d'utilisateur de maintenance (umadmin) et du mot de passe que vous avez définis précédemment.

Mettez à niveau le système d'exploitation hôte Red Hat Enterprise Linux pour Active IQ Unified Manager

Si vous avez 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 décrites dans cette rubrique. Dans les deux cas, vous devez créer une sauvegarde d'Unified Manager sur le système Red Hat Enterprise Linux 7.x, puis restaurer cette sauvegarde sur un système Red Hat Enterprise Linux 8.x. Notez que les versions de Red Hat Enterprise Linux prises en charge vont de 8.0 à 8.10.

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

Cette tâche nécessitant la création d'une sauvegarde d'Unified Manager sur le système Red Hat Enterprise Linux 7.x, il est recommandé de la réaliser uniquement lorsque vous êtes prêt à effectuer l'intégralité de la mise à niveau, afin qu'Unified Manager soit hors ligne le moins longtemps possible. Des lacunes dans les données collectées apparaissent dans l'interface utilisateur d'Unified Manager pendant la période d'arrêt du système Red Hat Enterprise Linux 7.x et avant le démarrage du nouveau système Red Hat Enterprise Linux 8.x.

Consultez "Gestion des opérations de sauvegarde et de restauration" si vous devez examiner les instructions

détaillées relatives aux processus de sauvegarde et de restauration.

Suivez ces étapes 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 de Unified Manager sur ce système pendant que le système Red Hat Enterprise Linux 7.x est encore disponible.

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

   Voir "Logiciels Linux et exigences d'installation".

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

   Voir "Installation de Unified Manager sous Linux".

   Une fois l'installation terminée, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification. Le fichier de sauvegarde renseignera ces informations lors de la restauration.

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

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

7. Saisissez l'adresse IP ou l'URL dans votre navigateur web pour ouvrir l'interface utilisateur web de Unified Manager, puis connectez-vous au système.

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

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

Suivez ces étapes si vous ne disposez pas d'un système de 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` fichier) ainsi que le contenu du répertoire du référentiel de la base de données (`/database-dumps-repo` sous-répertoire) vers un emplacement externe.
2. Supprimez l'image Red Hat Enterprise Linux 7.x du système et effacez complètement le système.
3. Installez et configurez le logiciel Red Hat Enterprise Linux 8.x sur le même système.

   Voir "Logiciels Linux et exigences d'installation".

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

celle que vous aviez sur le système Red Hat Enterprise Linux 7.x.

Voir "Installation de Unified Manager sous Linux".

Une fois l'installation terminée, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification. Le fichier de sauvegarde renseignera ces informations lors de la restauration.

5. Copiez le fichier de sauvegarde (`.7z` file) depuis l'emplacement externe vers `/opt/netapp/data/ocum-backup/` et les fichiers du référentiel de base de données vers le sous-répertoire `/database-dumps-repo` sous le répertoire `/ocum-backup`.
6. Saisissez la commande suivante pour restaurer la base de données Unified Manager à partir du fichier de sauvegarde :

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

7. Saisissez l'adresse IP ou l'URL dans votre navigateur web pour ouvrir l'interface utilisateur web de Unified Manager, puis connectez-vous au système.

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

Mettez à niveau les produits tiers après avoir installé Active IQ Unified Manager

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

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

Mise à niveau d'OpenJDK sous Linux pour Active IQ Unified Manager

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

Avant de commencer

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

Vous pouvez mettre à jour les versions d'OpenJDK au sein d'une même famille de versions. Par exemple, vous pouvez passer d'OpenJDK 11.0.14 à OpenJDK 11.0.17, mais vous ne pouvez pas passer directement d'OpenJDK 11 à 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
```

Redémarrer Active IQ Unified Manager

Il se peut que vous deviez redémarrer Unified Manager après avoir effectué des modifications de configuration.

Avant de commencer

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

Étapes

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

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

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

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

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

Supprimer Active IQ Unified Manager

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

Avant de commencer

- Vous devez disposer d'un accès utilisateur root au serveur depuis lequel vous souhaitez supprimer Unified Manager.
- Security-Enhanced Linux (SELinux) doit être désactivé sur le système Linux. Remplacez le mode d'exécution de SELinux par « Permissive » à l'aide de la commande `setenforce 0`.
- 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 3306 de MySQL. 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. Arrêtez et supprimez Unified Manager du serveur :

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

   Cette étape supprime tous les paquets RPM NetApp associés. Elle ne supprime pas les modules logiciels requis, tels que Java, MySQL et 7zip.

3. **Facultatif:** Le cas échéant, supprimez les modules logiciels de support, tels que Java, MySQL et 7zip:

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

Une fois cette opération terminée, le logiciel est désinstallé. 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 packages Java et MySQL, sauf si ces packages sont requis et utilisés par une autre application du système. Cependant, les données MySQL ne sont pas supprimées.

Supprimez l'utilisateur umadmin personnalisé et le groupe de maintenance pour Active IQ Unified Manager

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

La désinstallation standard d'Unified Manager ne supprime pas l'utilisateur umadmin et le compte de maintenance personnalisés. Vous devez les supprimer manuellement.

Étapes

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

   ```
   userdel umadmin
   ```

3. Supprimer le groupe de maintenance :

   ```
   groupdel maintenance
   ```

Installer Unified Manager sur les systèmes Windows

Introduction à Active IQ Unified Manager

Découvrez Active IQ Unified Manager

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

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

Informations connexes

"Outil NetApp Interoperability Matrix Tool"

Découvrez ce que fait le serveur Active IQ Unified Manager

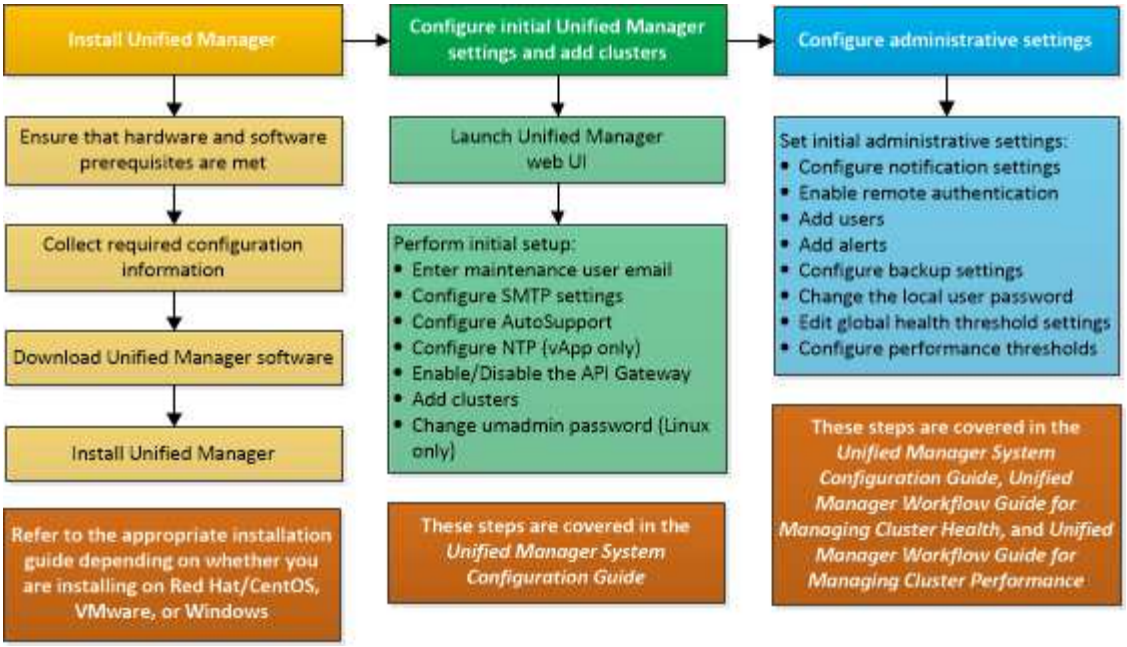
L'infrastructure serveur d'Unified Manager se compose d'une unité de collecte de données, d'une base de données et d'un serveur applicatif. Elle fournit des services d'infrastructure tels que la découverte, la surveillance, le contrôle d'accès basé sur les rôles (RBAC), l'audit et la journalisation.

Unified Manager collecte les informations du cluster, stocke les données dans la base de données et les analyse pour détecter d'éventuels problèmes au niveau du cluster.

Découvrez la séquence d'installation d'Active IQ Unified Manager

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

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



Configuration requise pour l'installation d'Unified Manager

Assurez-vous que le serveur répond aux exigences d'installation d'Active IQ 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 toute modification du code de l'application Unified Manager. Si vous devez appliquer des mesures de sécurité au serveur Unified Manager, vous devez effectuer ces modifications au niveau du système d'exploitation sur lequel Unified Manager est installé.

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

"Prise en charge des mesures de sécurité appliquées à Active IQ Unified Manager pour Clustered Data ONTAP"

Informations connexes

"Outil NetApp Interoperability Matrix Tool"

Comprendre les exigences en matière d'infrastructure virtuelle et de matériel pour Active IQ Unified Manager

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

Le tableau suivant présente les valeurs recommandées pour la mémoire, le processeur et l'espace disque. Ces valeurs ont été validées afin que Unified Manager offre des performances acceptables.

Configuration matérielle	Paramètres recommandés
RAM	12 Go
Processeurs	4 processeurs
capacité en cycles CPU	9572 MHz au total (exigence minimale 9572 MHz)
Espace disque libre	150 Go, dont la capacité est répartie comme suit : • 100 Go d'espace disque pour le répertoire d'installation • 50 Go d'espace disque pour le répertoire de données MySQL

Unified Manager peut être installé sur des systèmes disposant de peu de mémoire, mais les 12 Go de RAM recommandés garantissent qu'une quantité de mémoire suffisante est disponible pour des performances optimales et permettent au système d'accueillir des clusters et des objets de stockage supplémentaires à mesure que votre configuration évolue. Vous ne devez définir aucune limite de mémoire sur la machine virtuelle sur laquelle Unified Manager est déployé et ne devez activer aucune fonctionnalité (par exemple, le ballooning) qui empêcherait le logiciel d'utiliser la mémoire allouée sur le système.

De plus, il existe une limite au nombre de nœuds qu'une seule instance d'Unified Manager peut surveiller avant que vous n'installiez une seconde instance d'Unified Manager. Pour connaître les limites de nœuds, les recommandations concernant le processeur et la mémoire, consultez "le guide des bonnes pratiques de Unified Manager".

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

Exigence d'utilisation dédiée

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

Besoins en espace pour les sauvegardes

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

Exigences en matière de connectivité hôte

Le système physique ou le système virtuel sur lequel vous installez Unified Manager doit être configuré de telle sorte que vous puissiez `ping` résoudre correctement le nom de l'hôte à partir de l'hôte lui-même. En cas de configuration IPv6, vous devez vérifier que `ping6` la résolution du nom de l'hôte aboutit afin de garantir la réussite de l'installation d'Unified Manager.

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

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

Comprendre les exigences logicielles et d'installation de Windows pour Active IQ Unified Manager

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

Logiciel du système d'exploitation

Vous pouvez installer Unified Manager sur les éditions Windows suivantes :

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

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

- English
- japonais
- Chinois simplifié

Consultez l'Interoperability Matrix 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 d'Unified Manager. Aucune autre application ne doit être installée sur le serveur. Il est possible qu'un logiciel anti-virus actif soit installé sur votre système Windows en raison de la réglementation de votre entreprise. Vous devez désactiver le logiciel anti-virus avant d'installer Unified Manager pour éviter l'échec de l'installation.

Logiciels tiers

Les modules 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.

- Packages redistribuables Microsoft Visual C++ pour Visual Studio 2015 version 14.29.30133.0
- MySQL Community Edition version 8.4.10
- Python 3.13.3
- OpenJDK version 17.0.15+6
- 7-zip version 25.01 ou ultérieure

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

Manager 9.5.

Si MySQL est préinstallé, vous devez vous assurer que :

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

Unified Manager est déployé sur un serveur web WildFly. WildFly 27.0.1.Final est intégré et configuré avec Unified Manager.

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

exigences d'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 a été créé, exécutez la commande suivante dans l'interface de ligne de commandes `echo %temp%` :
- Vous devez réserver 2 Go d'espace disque sur le lecteur Windows pour la mise en cache des fichiers MSI d'Unified Manager.
- Le serveur Microsoft Windows sur lequel vous souhaitez installer Unified Manager doit être configuré avec un domaine complet (FQDN) afin que `ping` les réponses au nom de l'hôte et au FQDN aboutissent.
- Vous devez désactiver le service Microsoft IIS worldwide web publishing et vous assurer que les ports 80 et 443 sont libres.
- Vous devez vous assurer que le paramètre de l'hôte de session Bureau à distance pour « `Windows Installer RDS Compatibility` » est désactivé pendant l'installation.
- Le port UDP 514 doit être libre et aucun autre service ne doit l'utiliser.
- 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 d'Unified Manager, par exemple, `C:\ProgramData\NetApp\OnCommandAppData\`
  - le répertoire d'installation d'Unified Manager, par exemple, `\C:\Program Files\NetApp\`
  - répertoire de données MySQL, par exemple, `C:\ProgramData\MySQL\MySQLServerData`

Utilisez les navigateurs compatibles dans Active IQ Unified Manager

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

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

"mysupport.netapp.com/matrix"

Pour tous les navigateurs, la désactivation des bloqueurs de fenêtres contextuelles garantit un affichage

correct des fonctionnalités du logiciel.

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

Comprendre les exigences en matière de protocole et de port pour Active IQ Unified Manager

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

Connexions au serveur Unified Manager

Dans la plupart des installations, il n'est pas nécessaire de spécifier les numéros de port lors de la connexion à l'interface 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 saisir `https://<host>` au lieu de `https://<host>:443`.

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

Interface	Protocole	Port	Description
interface utilisateur Web de Unified Manager	HTTP	80	Utilisé pour accéder à l'interface utilisateur web de Unified Manager; redirige automatiquement vers le port sécurisé 443.
Interface utilisateur Web de Unified Manager et programmes utilisant des API	HTTPS	443	Utilisé pour accéder en toute sécurité à l'interface utilisateur Web Unified Manager ou pour effectuer des appels API ; les appels API ne peuvent être effectués qu'en utilisant HTTPS.
Console de maintenance	SSH/SFTP	22	Utilisé pour accéder à la console de maintenance et récupérer les bundles de support.
ligne de commandes Linux	SSH/SFTP	22	Utilisé pour accéder à la ligne de commandes de Red Hat Enterprise Linux et récupérer les bundles de support.
Syslog	UDP	514	Permet d'accéder aux messages EMS par abonnement des systèmes ONTAP et de créer des événements à partir de ces messages.

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

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

Connexions depuis le serveur Unified Manager

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

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

Le serveur Unified Manager se connecte aux systèmes de stockage gérés, aux serveurs et aux autres composants via les protocoles et ports suivants :

Destination	Protocole	Port	Description
Système de stockage	HTTPS	443/TCP	Utilisé pour surveiller et gérer les systèmes de stockage.
Système de stockage	NDMP	10000/TCP	Utilisé pour certaines opérations de restauration Snapshot.
AutoSupport serveur	HTTPS	443	Utilisé pour envoyer des informations AutoSupport. Nécessite un accès à Internet pour exécuter cette fonction.
Serveur d'authentification	LDAP	389	Utilisé pour effectuer des requêtes d'authentification, ainsi que des requêtes de recherche d'utilisateurs et de groupes.
LDAPS	636	Utilisé pour les communications LDAP sécurisées.	Serveur de messagerie
SMTP	25	Utilisé pour envoyer des e-mails de notification d'alerte.	émetteur de pièges SNMP
SNMPv1 ou SNMPv3	162/UDP	Utilisé pour envoyer des traps SNMP de notification d'alerte.	Serveur du fournisseur de données externe
TCP	2003	Utilisé pour envoyer des données de performance à un fournisseur de données externe, tel que Graphite.	Serveur NTP
NTP	123/UDP	Utilisé pour synchroniser l'heure du serveur Unified Manager avec un serveur NTP externe. (Systèmes VMware uniquement)	Courtier AMQP QPID
TCP/IP	56072	Utilisé pour la communication des messages internes.	Courtier AMQP QPID
WebSocket via TCP	56080	Utilisé pour écouter sur ce port les messages reçus de ONTAP (agent cloud).	Courtier AMQP QPID

Destination	Protocole	Port	Description
WebSocket via TCP	56443	Utilisé pour écouter sur ce port les messages reçus d'ONTAP (cloud agent). La communication via ce port prend en charge le chiffrement fourni par TLS ou SSL.	Syslog

Remplissez la feuille de calcul dans Active IQ Unified Manager

Avant d'installer et de configurer Unified Manager, assurez-vous d'avoir à portée de main des informations spécifiques sur votre environnement. Vous pouvez les consigner dans une feuille de calcul.

Informations d'installation d'Unified Manager

Les informations nécessaires à l'installation d'Unified Manager.

Système sur lequel le logiciel est déployé	Votre valeur
Nom de domaine pleinement qualifié 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 de configuration d'Unified Manager

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

Paramètre	Votre valeur
adresse e-mail de l'utilisateur de maintenance	
nom de l'hôte ou adresse IP du serveur SMTP	
Nom d'utilisateur SMTP	
Mot de passe SMTP	
port SMTP	25 (Valeur par défaut)
Adresse électronique utilisée pour envoyer les notifications d'alerte	

Paramètre	Votre valeur
Nom de l'hôte ou adresse IP du serveur d'authentification	
Nom de l'administrateur Active Directory ou nom unique de liaison LDAP	
Mot de passe Active Directory ou mot de passe de liaison LDAP	
Nom unique de base du serveur d'authentification	
URL du fournisseur d'identité (IdP)	
Métadonnées du fournisseur d'identité (IdP)	
Adresses IP des hôtes de destination des traps SNMP	
port SNMP	

Informations sur le cluster

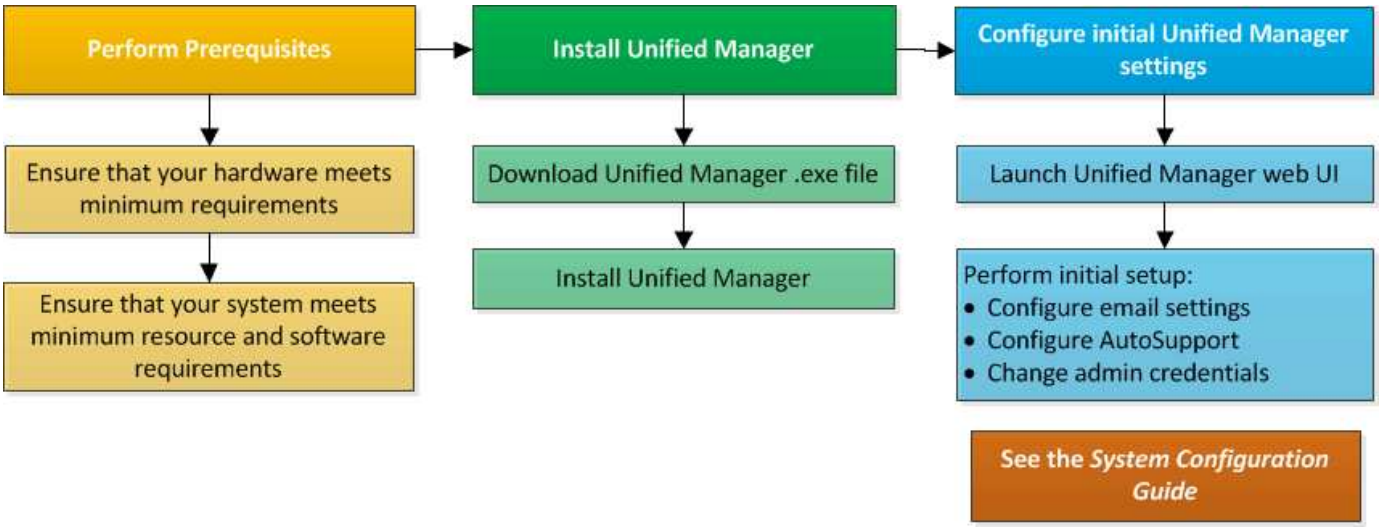
Les détails des systèmes de stockage que vous gérez à l'aide d'Unified Manager.

Cluster 1 sur N	Votre valeur
Nom de l'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 de l'administrateur ONTAP	
Protocole	HTTPS

Installer, mettre à niveau et supprimer le logiciel Unified Manager

Découvrez le processus d'installation d'Active IQ Unified Manager sous Windows

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



Installer Unified Manager sur Windows

Installer Active IQ Unified Manager sous Windows

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

Avant de commencer

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

  Voir "Configuration matérielle requise du système".

  Voir "Logiciels Windows et exigences d'installation".

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

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

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

Étapes

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

   "Site de support NetApp"

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

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

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

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

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

L'installation crée plusieurs répertoires :

- Répertoire d'installation

  Il s'agit du répertoire racine 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 où sont stockées les bases de données MySQL, que vous avez spécifié lors de l'installation. Exemple : `C:\ProgramData\MySQL\MySQLServerData\`

- Répertoire Java

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

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

  Il s'agit du répertoire où sont stockées toutes les données générées par l'application. Cela inclut les journaux, les packages de support, les sauvegardes et toutes les autres données supplémentaires.

Exemple : `C:\ProgramData\NetApp\OnCommandAppData\`

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

Effectuez une installation sans assistance d'Active IQ Unified Manager

Vous pouvez installer Unified Manager sans 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 sous forme de paires clé-valeur.

Étapes

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

Option	Instructions

Si des packages tiers sont préinstallés	`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 les 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'option `/qr` active le mode silencieux avec une interface utilisateur réduite. Une interface utilisateur de base s'affiche et montre la progression de l'installation. Aucune saisie ne vous est demandée. Si des packages tiers tels que JRE, MySQL et 7zip ne sont pas préinstallés, vous devez utiliser l'option `/qr`. L'installation échoue si l'option `/qn` est utilisée sur un serveur sur lequel des packages 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 l' `/qn`option lorsque des packages tiers ne sont pas installés.

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

   `https://IP address`

Modifier le mot de passe JBoss sous Windows dans Active IQ Unified Manager

Vous pouvez réinitialiser le mot de passe JBoss spécifique à votre instance, défini lors de l'installation. Vous pouvez réinitialiser le mot de passe de façon facultative si votre site exige cette fonction de sécurité pour remplacer le paramètre d'installation de Unified Manager. Cette opération modifie également le mot de passe utilisé par JBoss pour accéder à MySQL.

Avant de commencer

- Vous devez disposer des privilèges d'administrateur Windows pour le système sur lequel Unified Manager est installé.
- Vous devriez avoir le mot de passe de l'utilisateur root de 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 de Unified Manager.
2. Utilisez la console des services Windows pour arrêter les services Unified Manager suivants :
   - Service d'acquisition NetApp Active IQ (Ocie-au)
   - NetApp Service du serveur de gestion Active IQ (Oncommandsvc)
3. Lancez le `password.bat` script pour démarrer le processus de changement de mot de passe :

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

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

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

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

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

Utilisez la voie de mise à niveau prise en charge pour les versions de Active IQ Unified Manager

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

Toutes les versions d'Unified Manager ne permettent pas d'effectuer une mise à niveau sur place vers des versions ultérieures. Les mises à niveau d'Unified Manager sont limitées à un modèle N-2. Cela signifie que vous ne pouvez effectuer une mise à niveau que vers les deux versions suivantes sur toutes les plateformes. Par exemple, vous pouvez effectuer une mise à niveau vers Unified Manager 9.18 uniquement à partir d'Unified Manager 9.14 et 9.16.

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

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

Exemple de chemin de mise à niveau :

1. Mise à niveau 9.11 → 9.13
2. Mise à niveau 9.13 → 9.14
3. Mise à niveau 9.13 → 9.16
4. Mise à niveau 9.14 ou 9.16 → 9.18

Pour plus d'informations sur la matrice des chemins de mise à niveau, consultez ceci "article de la base de connaissances (KB)".

Mettez à niveau Active IQ Unified Manager sous Windows

Vous pouvez mettre à niveau Unified Manager 9.14 ou 9.16 vers la version 9.18 en téléchargeant et en exécutant le fichier d'installation sur la plateforme Windows.

Avant de commencer

- Le système sur lequel vous effectuez la mise à niveau d'Unified Manager doit répondre aux exigences système et logicielles.

  Voir "Configuration matérielle requise du système".

  Voir "Logiciels Windows et exigences d'installation".

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

  Assurez-vous que Microsoft .NET 4.5.2 ou une version supérieure est installée sur votre système avant de commencer la mise à niveau.

- MySQL Community Edition est automatiquement mis à niveau lors de la mise à niveau de Unified Manager. Si la version de MySQL installée sur votre système est antérieure à 8.4.10, le processus de mise à niveau de Unified Manager met automatiquement MySQL à niveau vers 8.4.10. Vous ne devez pas effectuer de mise à niveau autonome d'une version antérieure de MySQL vers 8.4.10.
- Tous les clusters sont pris en charge, à l'exception des systèmes ASA r2.
- Vous devez disposer des privilèges d'administrateur Windows. Assurez-vous que votre nom d'utilisateur ne commence pas par un point d'exclamation "!". Installation of Unified Manager might fail if the user name of user running the installation begins with "!".
- Vous devez disposer d'identifiants valides pour vous connecter au site d'assistance NetApp.
- Pour éviter la perte de données, vous auriez dû créer une sauvegarde de la machine Unified Manager au cas où un problème surviendrait lors de la mise à niveau.
- Vous devez disposer de suffisamment d'espace disque pour effectuer la mise à niveau.

  L'espace disponible sur le disque d'installation doit être supérieur de 2,5 Go à la taille du répertoire de données. Si l'espace libre est insuffisant, la mise à niveau s'interrompt et un message d'erreur s'affiche, indiquant l'espace à ajouter.

- Lors de la mise à niveau, il vous sera peut-être demandé de confirmer si vous souhaitez conserver les paramètres par défaut précédents pour la conservation des données de performance pendant 13 mois ou les remplacer par 6 mois. Après confirmation, les données historiques de performance datant de plus de 6 mois sont supprimées.
- Avant la mise à niveau, vous devez fermer tous les fichiers ou dossiers ouverts dans *<InstallDir>\JDK* et *MySQL Data Directory*.
- Si un logiciel antivirus est actif sur votre système Windows, la mise à niveau d'Unified Manager risque d'échouer. Il est recommandé de désactiver tout logiciel antivirus avant de procéder à la mise à niveau d'Unified Manager.

Pendant la mise à niveau, Unified Manager est indisponible. Veuillez terminer toutes les opérations en cours

avant de mettre à niveau Unified Manager.

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

Étapes

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

   "Site de support NetApp".

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

   Unified Manager vous affiche le message suivant :

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

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

> Pour effectuer une mise à niveau silencieuse d'Unified Manager, exécutez la commande suivante :
> `ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

Mettre à niveau les produits tiers

Mettez à niveau les produits tiers dans Active IQ Unified Manager sous Windows

Vous pouvez mettre à niveau des produits tiers, tels que JRE, dans Unified Manager lorsqu'il est installé sur des systèmes Windows.

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

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

Mettez à niveau OpenJDK sous Windows pour Active IQ Unified Manager

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

Avant de commencer

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

Vous pouvez mettre à jour les versions d'OpenJDK au sein d'une même famille de versions. Par exemple, vous pouvez passer d'OpenJDK 11.0.16 à OpenJDK 11.0.18, mais vous ne pouvez pas passer directement d'OpenJDK 11 à OpenJDK 12.

Étapes

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

   Par exemple, téléchargez le `jdk-17.0.15_windows-x64_bin.zip` fichier depuis "la page de téléchargement des archives d'Oracle Java SE 17".

   > Un compte Oracle est requis pour télécharger le fichier. Si vous n'avez pas de compte Oracle, accédez à "la page de connexion au compte Oracle" 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)
   - NetApp Service du serveur de gestion 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` vers l'emplacement où Java est installé. Exemple : `C:\Program Files\NetApp\JDK\`
6. Démarrez les services Unified Manager à l'aide de la console Windows Services :
   - NetApp Service du serveur de gestion Active IQ (Oncommandsvc)
   - Service d'acquisition NetApp Active IQ (Ocie-au)

Désinstallez les produits tiers dans Active IQ Unified Manager

Après la mise à niveau d'Unified Manager, vous pouvez désinstaller les produits tiers, tels que Python ou Microsoft Visual C++ 2013. Cette opération est facultative.

Désinstaller Python

Étapes

1. Dans le **Panneau de configuration**, sélectionnez **Programmes** > **Programmes et fonctionnalités**.
2. Sélectionnez Python dans la liste des programmes.
3. Sélectionnez **Désinstaller ce programme**. Désinstallez toute version de Python à l'exception de 3.13.3. Assurez-vous de conserver la version 3.13.3 de Python.

Désinstaller Microsoft Visual C++ 2013

Étapes

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

Redémarrez Active IQ Unified Manager sous Windows

Il se peut que vous deviez redémarrer Unified Manager après avoir effectué des modifications de configuration.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Étapes

1. Connectez-vous à Windows en utilisant le compte administrateur local par défaut.
2. Arrêtez les services Unified Manager :

Depuis…	Arrêtez les services dans l'ordre suivant…
Ligne de commandes	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
Microsoft Service Manager	a. Service d'acquisition NetApp Active IQ (Ocie-au) b. NetApp Service du serveur de gestion Active IQ (Oncommandsvc)

3. Démarrez les services Unified Manager :

Depuis…	Démarrez les services dans l'ordre suivant…
Ligne de commandes	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. NetApp Service du serveur de gestion Active IQ (Oncommandsvc) b. Service d'acquisition NetApp Active IQ (Ocie-au)

Désinstaller Active IQ Unified Manager

Vous pouvez désinstaller Unified Manager en utilisant l'assistant Programmes et fonctionnalités, ou en effectuant une désinstallation sans assistance depuis l'interface de ligne de commandes.

Avant de commencer

- Vous devez disposer des privilèges d'administrateur Windows.

- Tous les clusters (sources de données) doivent être supprimés du serveur Unified Manager avant de désinstaller le logiciel.
- Vous devez supprimer manuellement les règles de pare-feu créées pour autoriser ou bloquer le port 3306 de MySQL. 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 depuis l'assistant **Programmes et fonctionnalités**, procédez comme suit :
     i. Accédez à **Panneau de configuration** > **Programmes et fonctionnalités**.
     ii. Sélectionnez Active IQ Unified Manager, puis cliquez sur **Désinstaller**.
   - Si vous désinstallez Unified Manager depuis la ligne de commandes, procédez comme suit :
     i. Connectez-vous à la ligne de commandes Windows avec 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 en ligne de commande.

   Unified Manager a été désinstallé de votre système.
2. Désinstallez les packages tiers et les données suivants qui ne sont pas supprimés lors de la désinstallation de Unified Manager :
   - Logiciels tiers : JRE, MySQL, Microsoft Visual C++ 2015 Redistributable, Python et 7zip
   - Données d'application MySQL générées par Unified Manager
   - Journaux d'application et contenu du répertoire de données d'application

Effectuer des tâches de configuration et d'administration

Configurer Active IQ Unified Manager

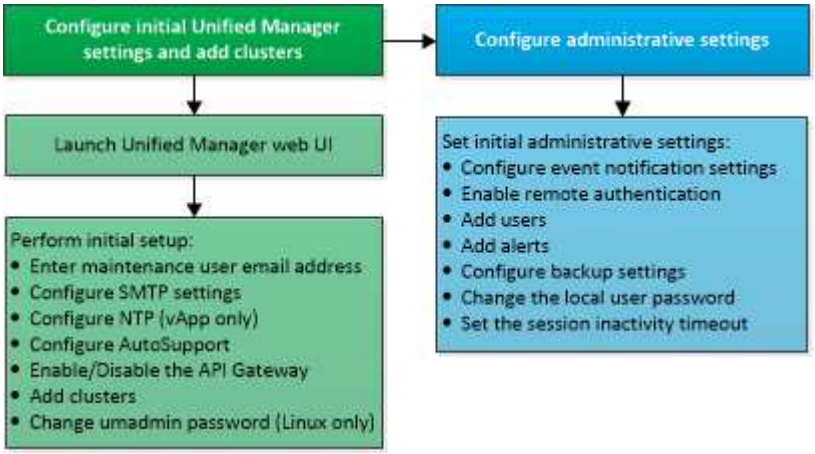
Découvrez comment configurer Active IQ Unified Manager

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

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

Découvrez la séquence de configuration dans Active IQ Unified Manager

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



Accédez à l'interface utilisateur Web dans Active IQ Unified Manager

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

Avant de commencer

- 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 en utilisant le nom court au lieu du domaine complet (FQDN) ou de l'adresse IP, votre configuration réseau doit résoudre ce nom court en un FQDN valide.

- Si le serveur utilise un certificat numérique auto-signé, le navigateur peut afficher un avertissement indiquant que le certificat n'est pas fiable. Vous pouvez soit accepter le risque pour continuer l'accès, soit installer un certificat numérique signé par une autorité de certification (AC) pour l'authentification du serveur.

Étapes

1. Démarrez l'interface utilisateur web de Unified Manager depuis votre navigateur en utilisant l'URL affichée à la fin de l'installation. L'URL correspond à l'adresse IP ou au domaine complet (FQDN) du serveur Unified Manager.

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

2. Connectez-vous à l'interface web de Unified Manager en utilisant vos identifiants d'utilisateur de maintenance.

   Si vous effectuez trois tentatives consécutives infructueuses de connexion à l'interface utilisateur web dans un délai d'une heure, l'accès au système vous sera refusé et vous devrez contacter votre administrateur système. Cela s'applique uniquement aux utilisateurs locaux.

Effectuez la configuration initiale de l'interface utilisateur Web Active IQ Unified Manager

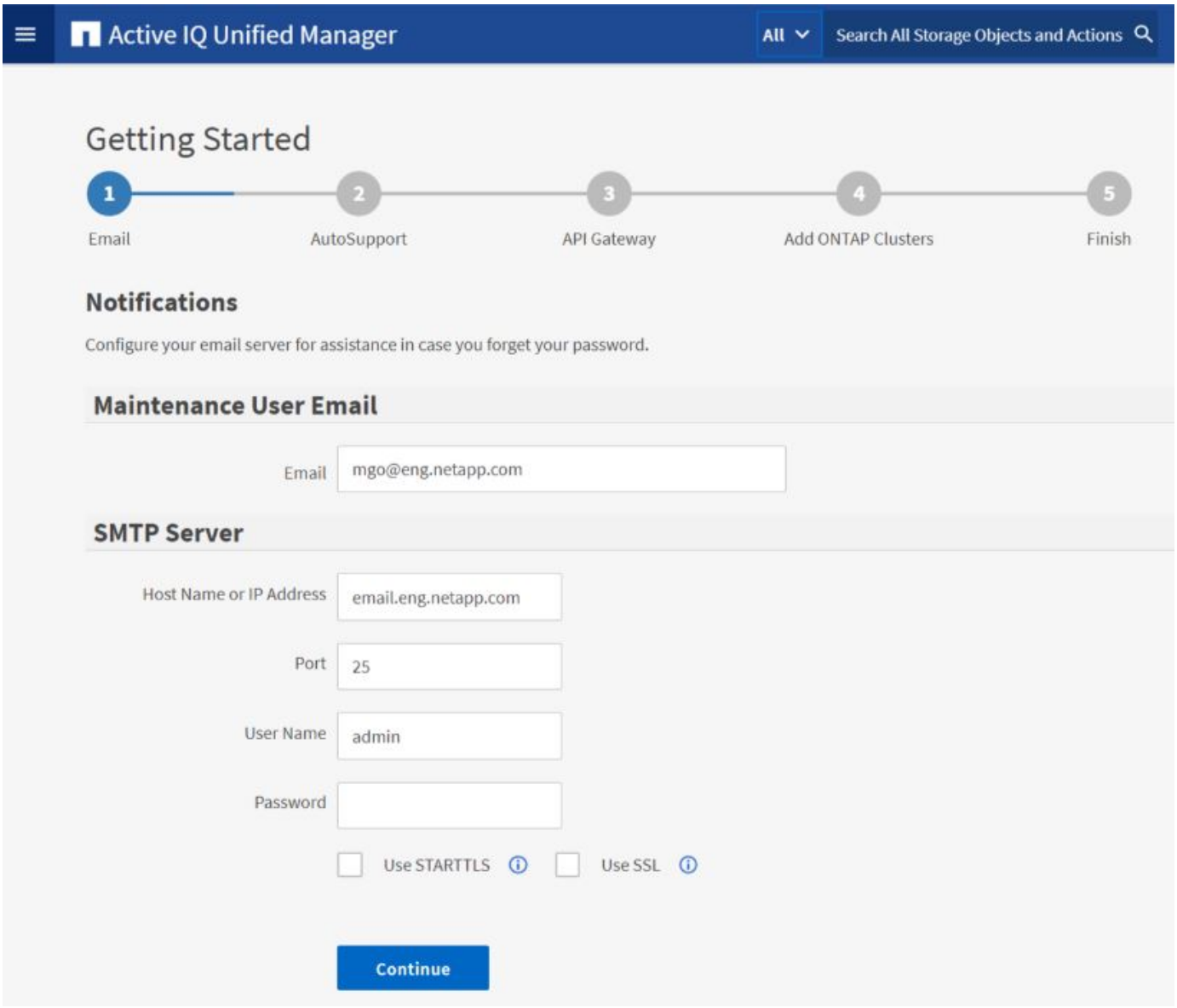
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, l'hôte du serveur SMTP et ajouter des clusters ONTAP.

Avant de commencer

Vous devez avoir effectué les opérations suivantes :

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

La page de démarrage de Active IQ Unified ManagerGetting 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 ultérieurement l'une de ces options, vous pouvez sélectionner votre choix dans les options générales du volet de navigation de gauche d'Unified Manager. Notez que le paramètre NTP concerne uniquement les installations VMware et peut être modifié ultérieurement à l'aide de la console de maintenance d'Unified Manager.

Étapes

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

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

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

   Si vous devez désigner un proxy pour fournir un accès à Internet afin d'envoyer du contenu AutoSupport, ou si vous souhaitez désactiver AutoSupport, utilisez l'option **General** > **AutoSupport** dans l'interface

utilisateur Web.

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

   Vous pouvez activer ou désactiver ce paramètre ultérieurement dans l'interface web sous **Général** > **Paramètres des fonctionnalités** > **Passerelle API**. Pour plus d'informations sur les API, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

5. Ajoutez les clusters que vous souhaitez confier à Unified Manager, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez disposer du nom de l'hôte ou de l'adresse IP de gestion du cluster (IPv4 ou IPv6), ainsi que des identifiants de connexion (nom d'utilisateur et mot de passe) ; l'utilisateur doit avoir le rôle "admin".

   Cette étape est facultative. Vous pouvez ajouter des clusters ultérieurement dans l'interface web, sous **Gestion du stockage** > **Configuration des clusters**.

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

La page « Premiers pas » se ferme et la page du tableau de bord Unified Manager s'affiche.

Ajouter des clusters à Active IQ Unified Manager

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de le surveiller. Vous pourrez ainsi obtenir des informations sur le cluster, telles que son état, sa capacité, ses performances et sa configuration, ce qui vous permettra de détecter et de résoudre tout problème éventuel.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez disposer des informations suivantes :
  - Unified Manager prend en charge les clusters ONTAP sur site, ONTAP Select et Cloud Volumes ONTAP.
  - Nom de l'hôte ou adresse IP de gestion du cluster

    Le nom de l'hôte correspond au nom de domaine complet (FQDN) ou au nom court utilisé par Unified Manager pour se connecter au cluster. Le nom de l'hôte doit se résoudre en l'adresse IP de gestion du cluster.

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

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

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

- Le numéro de port à utiliser pour se connecter au cluster à l'aide du protocole HTTPS (généralement le port 443)
- Vous possédez les certificats requis:

  Certificat SSL (HTTPS) : ce certificat appartient à Unified Manager. Un certificat SSL (HTTPS) auto-signé par défaut est généré lors d'une nouvelle installation d'Unified Manager. NetApp recommande de le remplacer par 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 prennent en compte le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, consultez "Génération d'un certificat de sécurité HTTPS".

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

  Certificats pour la communication TLS mutuelle : utilisés lors de la communication TLS mutuelle entre Unified Manager et ONTAP. L'authentification par certificat est activée pour un cluster, selon la version d'ONTAP. Si le cluster exécute une version d'ONTAP antérieure à 9.5, l'authentification par certificat n'est pas activée.

  L'authentification par certificat n'est pas activée automatiquement pour 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 intégrer le nouveau certificat. Pour plus d'informations sur l'affichage et la régénération du certificat, consultez "Modification des clusters".

  - Vous pouvez ajouter un cluster depuis l'interface web, et l'authentification par certificat est automatiquement activée.
  - Vous pouvez ajouter un cluster via Unified Manager CLI, l'authentification par certificat n'est pas activée par défaut. Si vous ajoutez un cluster via Unified Manager CLI, vous devez le modifier via Unified Manager UI. Vous pouvez consulter "Commandes CLI Unified Manager prises en charge" pour ajouter un cluster via Unified Manager CLI.
  - Si l'authentification par certificat est activée pour un cluster et que vous effectuez la sauvegarde d'Unified Manager depuis un serveur, puis la restaurez sur un autre serveur Unified Manager dont le nom d'hôte ou l'adresse IP a changé, la surveillance du cluster peut échouer. Pour éviter cet échec, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, consultez "Modification des clusters".

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

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

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs requises, telles que le nom de l'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 en la faisant passer d'IPv6 à IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est affichée dans la grille du cluster et sur la page de configuration du cluster une fois le cycle de surveillance suivant terminé.

4. Cliquez sur **Submit**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour consulter les informations du certificat relatives au cluster.
6. Cliquez sur **Oui**.

   Après avoir enregistré les détails du cluster, vous pouvez consulter le certificat pour la communication Mutual TLS d'un cluster.

   Si l'authentification par certificat n'est pas activée, Unified Manager vérifie le certificat uniquement lors de l'ajout initial du cluster. Unified Manager ne vérifie pas le certificat pour chaque appel d'API à ONTAP.

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

Étant donné que la collecte de 15 jours de données de performance est gourmande en ressources CPU, il est recommandé d'échelonner l'ajout de nouveaux clusters afin que les sondages de collecte de continuité des données ne s'exécutent pas sur un trop grand nombre de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte sera interrompue et vous constaterez des lacunes dans les graphiques de performance pour la période manquante.

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

Informations connexes

"Installation d'un certificat HTTPS signé et renvoyé par une autorité de certification"

Configurer les notifications

Configurez Active IQ Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour envoyer des notifications qui vous alertent sur les événements survenant dans votre environnement. Avant que ces notifications puissent être envoyées, vous devez configurer plusieurs autres options d'Unified Manager.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Après avoir déployé Unified Manager et effectué la configuration initiale, vous devriez envisager de configurer votre environnement pour déclencher des alertes et générer des e-mails de notification ou des traps SNMP à la réception d'événements.

Étapes

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

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

2. "Activer l'authentification à distance".

   Si vous souhaitez que les utilisateurs LDAP ou Active Directory distants puissent accéder à l'instance Unified Manager et recevoir 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 différents types d'utilisateurs locaux ou distants et leur attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous désignez un utilisateur pour recevoir les notifications d'alerte.

5. "Ajouter des alertes".

   Une fois que vous avez ajouté l'adresse e-mail pour l'envoi des notifications, ajouté les utilisateurs qui recevront les notifications, configuré vos paramètres réseau et configuré les options SMTP et SNMP nécessaires à votre environnement, vous pouvez alors attribuer des alertes.

Configurez les paramètres de notification d'événements dans Active IQ Unified Manager

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications d'alerte lorsqu'un événement est généré ou attribué à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour l'envoi des alertes et définir différents mécanismes de notification : par exemple, les notifications d'alerte peuvent être envoyées par e-mail ou par traps SNMP.

Avant de commencer

Vous devez disposer des informations suivantes :

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

  L'adresse électronique apparaît dans le champ "From" des notifications d'alerte envoyées. Si l'e-mail ne peut pas être distribué pour une raison quelconque, cette adresse électronique est également utilisée comme destinataire des messages non distribuables.

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

  Pour spécifier plusieurs destinations de trap, séparez chaque hôte par une virgule. Dans ce cas, tous les autres paramètres SNMP, tels que la version et le port de trap sortant, doivent être identiques pour tous les hôtes de la liste.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

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

   Remarques :

   - Si l'adresse d'expéditeur est préremplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la modifier par une adresse électronique valide afin de garantir la bonne réception de toutes les notifications par e-mail.
   - Si le nom de l'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 de l'hôte.
3. Cliquez sur **Enregistrer**.
4. Si vous avez sélectionné l'option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Enregistrer**. Vérifiez les détails du certificat et acceptez-le 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 actuel a expiré, décochez la case **Utiliser STARTTLS** ou **Utiliser SSL**, enregistrez les paramètres de notification, puis cochez à nouveau la case **Utiliser STARTTLS** ou **Utiliser SSL** pour afficher un nouveau certificat.

Activer l'authentification à distance dans Active IQ Unified Manager

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

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

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

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

L'authentification à distance est prise en charge via LDAP et LDAPS (LDAP sécurisé). Unified Manager utilise le port 389 par défaut pour les communications non sécurisées et le port 636 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…	Veuillez saisir les informations suivantes…
Active Directory	• Nom de l'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (en utilisant la notation LDAP appropriée) • Mot de passe administrateur • Nom unique de base (en utilisant la notation LDAP appropriée)
Open LDAP	• Nom unique de liaison (dans la notation LDAP appropriée) • Mot de passe de liaison • nom unique de base

Si l'authentification d'un utilisateur Active Directory prend beaucoup de temps ou expire, il est probable que le serveur d'authentification mette du temps à répondre. La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification.

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

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

Désactivez les groupes imbriqués de l'authentification à distance dans Active IQ Unified Manager

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

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.

- 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 cette prise en charge est désactivée et qu'un groupe distant est ajouté à Unified Manager, chaque utilisateur doit être membre 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 groupes imbriqués**.
3. Cliquez sur **Enregistrer**.

Configurez les services d'authentification dans Active IQ Unified Manager

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

Avant de commencer

- Vous devez avoir activé l'authentification à distance.
- Vous devez posséder le rôle d'administrateur d'application.

Étapes

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

Si vous sélectionnez…	Ensuite, faites ceci…
Active Directory	a. Saisissez le nom d'administrateur et le mot de passe. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Saisissez le nom unique et le mot de passe de liaison. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.

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

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

3. Cliquez sur **Enregistrer**.

Ajouter des serveurs d'authentification à Active IQ Unified Manager

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.

Avant de commencer

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

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

Étapes

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

Si vous voulez…	Ensuite, faites ceci…
Activez-le	a. Sélectionnez l'option **Utiliser une connexion sécurisée**. b. Dans la section 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 du 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 par connexion sécurisée**, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise le port 636 par défaut pour les communications sécurisées et le port 389 pour les communications non sécurisées.
Désactivez-le	a. Décochez l'option **Utiliser une connexion sécurisée**. b. Dans la section Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, spécifiez soit le nom de l'hôte, soit l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les informations sur le port. d. Cliquez sur **Add**.

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 dans le serveur d'authentification que vous avez ajouté.

Testez la configuration des serveurs d'authentification dans Active IQ Unified Manager

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion peut communiquer avec eux. Pour ce faire, recherchez un utilisateur ou un groupe distant sur vos serveurs d'authentification et authentifiez-le à l'aide des paramètres configurés.

Avant de commencer

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

Si le service d'authentification est configuré sur Active Directory et que vous validez l'authentification d'utilisateurs distants appartenant au groupe principal du serveur d'authentification, les informations relatives au groupe principal ne sont pas affichées dans les résultats d'authentification.

Étapes

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

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

Ajouter des alertes dans Active IQ Unified Manager

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

Avant de commencer

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

Vous pouvez créer une alerte directement depuis la page de détails de l'événement après avoir reçu un événement, en plus de la possibilité de créer une alerte depuis la page de configuration des alertes, comme décrit ici.

Étapes

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

   Vous pouvez définir un filtre en saisissant une chaîne de caractères dans le champ « Le nom contient »

afin de sélectionner un groupe de ressources. En fonction de la chaîne de caractères que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtrage. La chaîne de caractères que vous spécifiez est sensible à la casse.

Si une ressource correspond à la fois aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion prévaut sur la règle d'inclusion, et aucune alerte n'est générée pour les événements liés à la ressource exclue.

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



Pour sélectionner plusieurs événements, maintenez la touche Ctrl enfoncée pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions**, puis sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence des notifications, indiquez si un trap SNMP doit être envoyé au récepteur de traps, et attribuez un script à exécuter lorsqu'une alerte est générée.



Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour la modifier, le champ Nom apparaît vide, car l'adresse e-mail modifiée n'est plus associée à l'utilisateur précédemment sélectionné. De même, si vous modifiez l'adresse e-mail de l'utilisateur sélectionné depuis la page Users, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

Vous pouvez également choisir d'informer les utilisateurs via des traps SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

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

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

Dans la boîte de dialogue Ajouter une alerte, procédez comme suit :

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources**, puis dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.
   a. Saisissez **abc** dans le champ **Le nom contient** pour afficher les volumes dont le nom contient « `abc` ».
   b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles et déplacez-le vers la zone Ressources sélectionnées.
   c. Cliquez sur **Exclure**, puis saisissez **xyz** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Événements**, puis sélectionnez **Critique** dans le champ Gravité de l'événement.

4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants, et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions**, puis saisissez **sample@domain.com** dans le champ **Alert these users**.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour notifier l'utilisateur toutes les 15 minutes.

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

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

Modifiez le mot de passe de l'utilisateur local dans Active IQ Unified Manager

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

Avant de commencer

Vous devez être connecté en tant qu'utilisateur local.

Les mots de passe de l'utilisateur de maintenance et des utilisateurs distants ne peuvent pas être modifiés en suivant ces étapes. Pour modifier le mot de passe d'un utilisateur distant, contactez votre administrateur de mots de passe. Pour modifier le mot de passe de l'utilisateur de maintenance, consultez "Utilisation de la console de maintenance".

Étapes

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

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

3. Dans la boîte de dialogue « Changer le mot de passe », saisissez 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 de la configuration. Les deux instances doivent avoir le même mot de passe.

Définissez le délai d'inactivité de la session dans Active IQ Unified Manager

Vous pouvez configurer le délai d'inactivité de Unified Manager pour que la session se termine automatiquement après une certaine période d'inactivité. Par défaut, ce délai est de 4 320 minutes (72 heures).

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Ce paramètre affecte toutes les sessions utilisateur connectées.

Cette option n'est pas disponible si vous avez activé l'authentification Security Assertion Markup

Language (SAML).

Étapes

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

Si vous voulez…	Ensuite, faites ceci…
Ne définissez aucun délai d'expiration afin que la session ne se ferme jamais automatiquement	Dans le panneau **Délai d'inactivité**, déplacez le curseur vers la gauche (désactivé) et cliquez sur **Appliquer**.
Définissez un nombre précis de minutes comme valeur du délai d'expiration	Dans le panneau **Délai d'inactivité**, déplacez le curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes et cliquez sur **Appliquer**.

Définissez le délai d'expiration de la session à l'aide de la CLI dans Active IQ Unified Manager

Vous pouvez définir une durée maximale de session pour Unified Manager via l'interface de ligne de commande (CLI) afin que la session se termine automatiquement après un certain laps de temps. Par défaut, cette durée est fixée à sa valeur maximale, soit 4 320 minutes (72 heures). Cela signifie que votre session se termine automatiquement après 72 heures, même si vous êtes connecté et utilisez activement Unified Manager.

À propos de cette tâche

Vous devez posséder le rôle d'administrateur d'application.

Le paramètre de délai d'expiration de session affecte toutes les sessions utilisateur connectées.

Étapes

1. Connectez-vous à l'interface de ligne de commande Unified Manager en saisissant la `um cli login` commande. Utilisez un nom d'utilisateur et un mot de passe valides pour l'authentification.
2. Saisissez la `um option set max.session.timeout.value=<in mins>` commande permettant de modifier la valeur du délai d'expiration de la session.

Modifier le nom de l'hôte de Unified Manager

Modifier le nom de l'hôte de l'appliance virtuelle Active IQ Unified Manager

L'hôte réseau se voit attribuer un nom lors du premier déploiement de l'appliance virtuelle Unified Manager. Vous pouvez modifier le nom de l'hôte après le déploiement. Si vous modifiez le nom de l'hôte, vous devez également régénérer le certificat HTTPS.

Avant de commencer

Vous devez être connecté à Unified Manager en tant qu'utilisateur de maintenance, ou disposer du rôle Application Administrator pour effectuer ces tâches.

Vous pouvez utiliser le nom de l'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur web de Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors attribué un nom à l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom de l'hôte doit être obtenu à partir du DNS. Si DHCP ou DNS n'est pas correctement configuré, le nom de l'hôte "Unified Manager" est automatiquement attribué et associé au certificat de sécurité.

Quelle que soit la manière dont le nom de l'hôte a été attribué, si vous modifiez le nom de l'hôte et que vous avez l'intention d'utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur Web de Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface web en utilisant l'adresse IP du serveur au lieu du nom de l'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom de l'hôte. Cependant, il est recommandé, conformément aux bonnes pratiques, de mettre à jour le certificat afin que le nom de l'hôte qui y figure corresponde au nom de l'hôte réel.

Si vous modifiez le nom de l'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom de l'hôte dans OnCommand Workflow Automation (WFA). Le nom de l'hôte n'est pas mis à jour automatiquement dans WFA.

Le nouveau certificat ne prendra effet qu'après le redémarrage de la machine virtuelle Unified Manager.

Étapes

1. Générer un certificat de sécurité HTTPS

   Si vous souhaitez utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur web de Unified Manager, vous devez régénérer le certificat HTTPS pour l'associer au nouveau nom de l'hôte.

2. Redémarrez la machine virtuelle Unified Manager

   Après avoir régénéré le certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Générez un certificat de sécurité HTTPS dans Active IQ Unified Manager

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 pour remplacer le certificat existant.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez de meilleures valeurs pour le nom distinctif (DN), une taille de clé plus élevée, une période d'expiration plus longue ou si le certificat actuel a expiré.

Si vous n'avez pas accès à l'interface utilisateur web de Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Lors de la régénération des certificats, vous pouvez définir la taille de la clé et sa durée de validité. Si vous utilisez l' `Reset Server Certificate` option de la console de maintenance, un nouveau certificat HTTPS valable pendant 397 jours est créé. Ce certificat aura une clé RSA de 2048 bits.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Régénérer le certificat HTTPS**.

La boîte de dialogue « Régénérer le certificat HTTPS » s'affiche.

3. Sélectionnez l'une des options suivantes en fonction de la manière dont vous souhaitez générer le certificat :

Si vous voulez…	Faites ceci…
Régénérez le certificat avec les valeurs actuelles	Cliquez sur l'option **Régénérer en utilisant les attributs du certificat actuel**.

Si vous voulez…	Faites ceci…
Générez le certificat en utilisant différentes valeurs	Cliquez sur l'option **Mettre à jour les attributs du certificat actuel**. Les champs Common Name et Alternative Names utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le champ "Common Name" doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez en saisir, par exemple pour EMAIL, COMPANY, DEPARTMENT, City, State et Country si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner parmi les options disponibles de KEY SIZE (l'algorithme de clé est "RSA".) et de VALIDITY PERIOD. • Les valeurs autorisées pour la taille de la clé sont `2048`, `3072` et `4096`. • Les périodes de validité vont de 1 jour minimum à 36500 jours maximum. Bien qu'une période de validité de 36 500 jours soit autorisée, il est recommandé de ne pas utiliser une période de validité supérieure à 397 jours ou 13 mois. En effet, si vous choisissez une période de validité supérieure à 397 jours et prévoyez d'exporter une CSR pour ce certificat et de la faire signer par une CA reconnue, la validité du certificat signé que la CA vous renverra 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, seules les informations que vous saisissez dans le champ sont utilisées dans le champ « Autres noms ». Si ce champ est laissé vide, le certificat obtenu ne comportera aucun champ « Autres noms ».

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

Redémarrez la machine virtuelle Active IQ Unified Manager

Vous pouvez redémarrer la machine virtuelle depuis 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.

Avant de commencer

L'appliance virtuelle est allumée.

Vous êtes connecté à la console de maintenance en tant qu'utilisateur de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere à l'aide de l'option **Restart Guest**. Consultez la documentation VMware pour plus d'informations.

Étapes

1. Accédez à la console de maintenance.
2. Sélectionnez **Configuration système** > **Redémarrer la machine virtuelle**.

Modifier le nom de l'hôte Active IQ Unified Manager sur les systèmes Linux

À un moment donné, vous pourriez souhaiter modifier le nom de l'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous pourriez vouloir renommer cet hôte afin d'identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillés lorsque vous affichez la liste de vos machines Linux.

Avant de commencer

Vous devez disposer d'un accès utilisateur root au système Linux sur lequel Unified Manager est installé.

Vous pouvez utiliser le nom de l'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface web de Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors attribué un nom à l'hôte réseau. Si vous avez configuré le réseau à l'aide du protocole DHCP, le nom de l'hôte doit être récupéré auprès du serveur DNS.

Quelle que soit la manière dont le nom de l'hôte a été attribué, si vous modifiez le nom de l'hôte et avez l'intention d'utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur Web de Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface web en utilisant l'adresse IP du serveur au lieu du nom de l'hôte, vous n'avez pas à générer un nouveau certificat si vous modifiez le nom de l'hôte. Toutefois, il est recommandé, comme bonne pratique, de mettre à jour le certificat afin que le nom de l'hôte qui y figure corresponde au nom de l'hôte réel. Le nouveau certificat ne prend effet qu'après le redémarrage de la machine Linux.

Si vous modifiez le nom de l'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom de l'hôte dans OnCommand Workflow Automation (WFA). Le nom de l'hôte n'est pas mis à jour automatiquement dans WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Unified Manager que vous souhaitez modifier.
2. Arrêtez le logiciel Unified Manager et le logiciel MySQL associé en saisissant la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Régénérez 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 de l'hôte peut se joindre lui-même par ping :

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Cette commande devrait renvoyer la même adresse IP que celle définie précédemment pour le nom de l'hôte d'origine.

7. Après avoir effectué et vérifié la modification du nom de l'hôte, redémarrez Unified Manager en saisissant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

Activer et désactiver la gestion du stockage basée sur des stratégies dans Active IQ Unified Manager

À partir d'Unified Manager 9.7, vous pouvez provisionner des charges de travail de stockage (volumes et LUN) sur vos clusters ONTAP et gérer ces charges de travail en fonction des niveaux de service de performance qui leur sont attribués. Cette fonctionnalité est similaire à la création de charges de travail dans ONTAP System Manager et à l'association de politiques QoS, mais avec Unified Manager, vous pouvez provisionner et gérer des charges de travail sur l'ensemble des clusters surveillés par votre instance d'Unified Manager.

Vous devez posséder le rôle d'administrateur d'application.

Cette option est activée par défaut, mais vous pouvez la désactiver si vous ne souhaitez pas provisionner et gérer les charges de travail à l'aide d'Unified Manager.

Lorsqu'elle est activée, cette option ajoute de nombreux nouveaux éléments à l'interface utilisateur :

Nouveau contenu	Pays
Une page pour provisionner de nouvelles charges de travail	Disponible depuis **Tâches courantes** > **Provisionnement**
Une page pour créer des politiques de niveau de service de performance	Disponible dans **Paramètres** > **Stratégies** > **Niveaux de service de performance**
Une page pour créer des politiques de performances de l'efficacité du stockage	Disponible dans **Paramètres** > **Stratégies** > **Efficacité du stockage**
Panneaux décrivant les performances actuelles de votre charge de travail et les IOPS de la charge de travail	Disponible depuis le Dashboard

Consultez l'aide en ligne du produit pour plus d'informations sur ces pages et sur cette fonctionnalité.

Étapes

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

Si vous voulez…	Ensuite, faites ceci…
Désactiver la gestion du stockage basée sur des stratégies	Dans le panneau **Gestion du stockage basée sur des stratégies**, déplacez le bouton du curseur vers la gauche.
Activer la gestion du stockage basée sur des politiques	Dans le panneau **Gestion du stockage basée sur des stratégies**, déplacez le bouton du curseur vers la droite.

Configurer la sauvegarde Active IQ Unified Manager

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

Pour plus d'informations sur les étapes de configuration, consultez "Gestion des opérations de sauvegarde et de restauration".

Gérer les paramètres des fonctionnalités

Découvrez les paramètres des fonctionnalités dans Active IQ Unified Manager

La page Paramètres des fonctionnalités vous permet d'activer et de désactiver des fonctionnalités spécifiques dans Active IQ Unified Manager. Vous pouvez notamment créer et gérer des objets de stockage en fonction de stratégies, activer la passerelle API et la bannière de connexion, charger des scripts pour gérer les alertes, configurer l'expiration automatique d'une session de l'interface Web en cas d'inactivité et désactiver la réception des événements de la plateforme Active IQ.

La page Feature Settings est uniquement accessible aux utilisateurs ayant le rôle Application Administrator.

Pour plus d'informations sur Scripts Upload, consultez "Activation et désactivation du téléchargement de scripts".

Activez la gestion du stockage basée sur des politiques dans Active IQ Unified Manager

L'option **Gestion du stockage basée sur des politiques** permet de gérer le stockage en fonction des objectifs de niveau de service (SLO). Cette option est activée par défaut.

En activant cette fonctionnalité, vous pouvez provisionner des workloads de stockage sur les clusters ONTAP ajoutés à votre instance Active IQ Unified Manager et gérer ces workloads en fonction des niveaux de service de performance et des politiques d'efficacité du stockage attribués.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité dans **Général** > **Paramètres des fonctionnalités** > **Gestion du stockage basée sur des stratégies**. Une fois cette fonctionnalité activée, les pages suivantes sont disponibles pour l'utilisation et la surveillance :

- Provisionnement (provisionnement du workload de stockage)
- **Politiques** > **Niveaux de service de performance**
- **Politiques** > **Efficacité du stockage**
- workloads gérés par la colonne Niveau de service de performance sur la page Configuration des clusters
- Panneau Performance du workload sur le **Dashboard**

Vous pouvez utiliser ces écrans pour créer des Performance Service Levels et des Storage Efficiency Policies, et provisionner des charges de travail de stockage. Vous pouvez également surveiller les charges de travail de stockage qui sont conformes aux Performance Service Levels attribués, ainsi que celles qui ne le sont pas. Le panneau Workload Performance and Workload IOPS vous permet également d'évaluer la capacité et les performances (IOPS) totales, disponibles et utilisées des clusters dans l'ensemble de votre centre de données, en fonction des charges de travail de stockage qui y sont provisionnées.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST de Unified Manager pour effectuer certaines de ces fonctions à partir de **Menu Bar** > **Help button** > **API Documentation** > catégorie **storage-provider**. Vous pouvez également saisir le nom de l'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, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

Découvrez la fonctionnalité API Gateway dans Active IQ Unified Manager

La fonctionnalité API Gateway permet à Active IQ Unified Manager de constituer un plan de contrôle unique à partir duquel vous pouvez gérer plusieurs clusters ONTAP, sans avoir à vous connecter individuellement à chacun d'eux.

Vous pouvez activer cette fonctionnalité à partir des pages de configuration qui s'affichent lors de votre première connexion à Unified Manager. Vous pouvez également activer ou désactiver cette fonctionnalité à partir de **General** > **Feature Settings** > **API Gateway**.

Les API REST de Unified Manager sont différentes des API REST de ONTAP, et toutes les fonctionnalités des API REST de ONTAP ne sont pas accessibles à l'aide des API REST de Unified Manager. Cependant, si vous avez un besoin métier spécifique d'accéder aux API de ONTAP pour gérer des fonctionnalités particulières qui ne sont pas exposées à Unified Manager, vous pouvez activer la fonctionnalité API Gateway et exécuter les API de ONTAP. La passerelle agit comme un proxy pour acheminer les requêtes API en conservant les en-têtes et le corps des requêtes dans le même format que dans les API de ONTAP. Vous pouvez utiliser vos identifiants Unified Manager et exécuter les API spécifiques pour accéder aux clusters ONTAP et les gérer sans transmettre les identifiants de chaque cluster. Unified Manager agit comme point de gestion unique pour exécuter les API sur les clusters ONTAP gérés par votre instance Unified Manager. La réponse renvoyée par les API est la même que celle renvoyée par les API REST de ONTAP correspondantes exécutées directement depuis ONTAP.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST de Unified Manager depuis **Menu Bar** > **Help button** > **API Documentation** > la catégorie **gateway**. Vous pouvez également saisir le nom de l'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, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

Spécifiez le délai d'inactivité dans Active IQ Unified Manager

Vous pouvez spécifier la valeur du délai d'inactivité pour Active IQ Unified Manager. Après une inactivité de la durée spécifiée, l'application se déconnecte automatiquement. Cette option est activée par défaut.

Vous pouvez désactiver cette fonctionnalité ou modifier la durée dans **Général** > **Paramètres des fonctionnalités** > **Délai d'inactivité**. Une fois que vous activez cette fonctionnalité, vous devez indiquer la limite de temps d'inactivité (en minutes) dans le champ **DÉCONNEXION APRÈS**, après quoi le système vous déconnecte automatiquement. La valeur par défaut est de 4 320 minutes (72 heures).

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

Activer les événements du portail Active IQ dans Active IQ Unified Manager

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

Lorsque cette fonctionnalité est activée, Active IQ Unified Manager affiche les événements détectés par le portail Active IQ. Ces événements sont créés par l'application d'un ensemble de règles aux messages AutoSupport générés à partir de tous les systèmes de stockage surveillés. Ces événements sont différents des autres événements d'Unified Manager, et ils identifient des incidents ou des risques liés à la configuration du système, au câblage, aux bonnes pratiques et aux problèmes de disponibilité.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité depuis **General** > **Feature Settings** > **Active IQ Portal Events**. Sur les sites sans accès au réseau externe, vous devez télécharger les règles manuellement depuis **Storage Management** > **Event Setup** > **Upload Rules**.

Cette fonctionnalité est activée par défaut. La désactivation de cette fonctionnalité empêche la détection ou

l'affichage des événements Active IQ dans Unified Manager. Lorsqu'elle est désactivée, l'activation de cette fonctionnalité permet à Unified Manager de recevoir les événements Active IQ sur un cluster à l'heure prédéfinie de 00:15 pour le fuseau horaire de ce cluster.

Activez et désactivez les paramètres de sécurité pour la conformité dans Active IQ Unified Manager

En utilisant le bouton **Customize** du panneau **Security Dashboard** de la page **Features Settings**, vous pouvez activer ou désactiver les paramètres de sécurité pour la surveillance de la conformité dans Unified Manager.

Les paramètres activés ou désactivés sur cette page déterminent l'état de conformité global des clusters et des machines virtuelles de stockage sur Unified Manager. Selon vos sélections, les colonnes correspondantes s'affichent dans la vue « Sécurité : Tous les clusters » de la page d'inventaire des clusters et dans la vue « Sécurité : Toutes les machines virtuelles de stockage » de la page d'inventaire des machines virtuelles de stockage.

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

Les critères de sécurité de vos clusters ONTAP, machines virtuelles de stockage et volumes sont évalués par rapport aux recommandations définies dans le "Guide de renforcement de la sécurité pour NetApp ONTAP 9". Le panneau Sécurité du tableau de bord et la page Sécurité affichent l'état de conformité de sécurité par défaut de vos clusters, machines virtuelles de stockage et volumes. Des événements de sécurité sont également générés et des actions de gestion sont activées pour les clusters et les machines virtuelles de stockage présentant des violations de sécurité.

Personnaliser les paramètres de sécurité

Pour personnaliser les paramètres de surveillance de la conformité applicables à votre environnement ONTAP, suivez ces étapes :

Étapes

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

   Les paramètres de conformité de sécurité que vous activez ou désactivez peuvent affecter directement les vues de sécurité par défaut, les rapports et les rapports planifiés sur les écrans Clusters et Storage VMs. Si vous avez téléversé un rapport Excel à partir de ces écrans avant de modifier les paramètres de sécurité, les rapports Excel téléchargés risquent d'être défectueux.

2. Pour activer ou désactiver les paramètres personnalisés de vos clusters ONTAP, sélectionnez le paramètre général souhaité sous **Cluster**. Pour plus d'informations sur les options de personnalisation de la conformité du cluster, consultez "Catégories de conformité des clusters".
3. Pour activer ou désactiver les paramètres personnalisés de vos machines virtuelles de stockage, sélectionnez le paramètre général requis sous **Storage VM**. Pour plus d'informations sur les options de personnalisation de la conformité des machines virtuelles de stockage, voir "Catégories de conformité des machines virtuelles de stockage".

Personnaliser les paramètres de AutoSupport et d'authentification

Dans la section **AutoSupport Settings**, vous pouvez spécifier si le transport HTTPS doit être utilisé pour l'envoi des messages AutoSupport depuis ONTAP.

Dans la section **Paramètres d'authentification**, vous pouvez activer l'envoi d'alertes Unified Manager pour l'utilisateur administrateur ONTAP par défaut.

Activer et désactiver le chargement de scripts dans Active IQ Unified Manager

La possibilité de télécharger des scripts sur Unified Manager et de les exécuter est activée par défaut. Si votre organisation souhaite interdire cette activité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Paramètres des fonctionnalités**.
2. Sur la page **Feature Settings**, désactivez ou activez les scripts en choisissant l'une des options suivantes :

Si vous voulez…	Ensuite, faites ceci…
Désactiver les scripts	Dans le panneau **Téléchargement de script**, déplacez le curseur vers la gauche.
Activer les scripts	Dans le panneau **Script Upload**, déplacez le curseur vers la droite.

Ajouter une bannière de connexion dans Active IQ Unified Manager

L'ajout d'une bannière de connexion permet à votre organisation d'afficher des informations telles que les personnes autorisées à accéder au système et les conditions générales d'utilisation lors de la connexion et de la déconnexion.

Tout utilisateur, tel qu'un opérateur de stockage ou un administrateur, peut voir cette fenêtre contextuelle de bannière de connexion lors de la connexion, de la déconnexion et de l'expiration de la session.

Utilisez la console de maintenance

Découvrez la console de maintenance dans Active IQ Unified Manager

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

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

- Résolvez tout problème lié à votre appliance virtuelle, en particulier si l'interface web Unified Manager n'est pas disponible
- Mettez à niveau vers des versions plus récentes d'Unified Manager
- Générer des kits de support à envoyer au support technique
- Configurer les paramètres réseau
- Modifier le mot de passe de l'utilisateur de maintenance
- Se connecter à un fournisseur de données externe pour envoyer des statistiques de performances
- Modifier le paramètre interne de collecte des données de performances
- Restaurez la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

Découvrez l'utilisateur de maintenance dans Active IQ Unified Manager

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

L'utilisateur de maintenance, ou utilisateur umadmin, peut également accéder à la console de maintenance Unified Manager.

Fonctionnalités de diagnostic utilisateur dans Active IQ Unified Manager

L'accès aux diagnostics a pour but de permettre au support technique de vous aider à résoudre les problèmes, et vous ne devez l'utiliser que sur instruction du support technique.

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

Accédez à la console de maintenance dans Active IQ Unified Manager

Si l'interface utilisateur d'Unified Manager n'est pas opérationnelle, ou si vous devez exécuter des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour gérer votre système Unified Manager.

Avant de commencer

Vous devez avoir installé et configuré Unified Manager.

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

> 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. Suivez ces étapes pour accéder à la console de maintenance :

Sur ce système d'exploitation…	Suivez ces étapes…
VMware	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. b. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe de maintenance.
Linux	a. Utilisez Secure Shell pour vous connecter à l'adresse IP ou au nom de domaine complet du système Unified Manager. b. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de l'utilisateur de maintenance (umadmin). c. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
Windows	a. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Saisissez la commande `maintenance_console` et appuyez sur Entrée.

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

Accédez à la console de maintenance via la console VM vSphere dans Active IQ Unified Manager

Si l'interface utilisateur de Unified Manager n'est pas opérationnelle, 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 votre appliance virtuelle.

Avant de commencer

- 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, localisez l'appliance virtuelle Unified Manager.
2. Cliquez sur l'onglet **Console**.
3. Cliquez dans la fenêtre de 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

Découvrez les menus de la console de maintenance dans Active IQ Unified Manager

La console se compose de différents menus qui vous permettent de gérer et de maintenir les fonctionnalités spéciales et les paramètres de configuration du serveur Unified Manager.

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

- Mise à niveau d'Unified Manager (VMware uniquement)
- Configuration réseau (VMware uniquement)
- Configuration système (VMware uniquement)
  a. Assistance/Diagnostics
  b. Réinitialiser le certificat du serveur
  c. Régénérer le certificat client
  d. Restauration de sauvegarde
  e. Fournisseur de données externe
  f. Configuration de l'intervalle d'interrogation des performances
  g. Désactiver l'authentification SAML
  h. Afficher/Modifier les ports de l'application
  i. Configuration du journal de débogage
  j. Contrôler l'accès au port 3306 de MySQL
  k. Sortie

Vous sélectionnez le numéro dans la liste pour accéder à l'option de menu spécifique. Par exemple, pour la sauvegarde et la restauration, vous sélectionnez *4*.

Menu Configuration réseau dans Active IQ Unified Manager

Le menu Configuration réseau vous permet de gérer les paramètres réseau. Utilisez 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 ou sur Microsoft Windows.

Les options de menu suivantes sont disponibles.

- **Afficher les paramètres de l'adresse IP**

  Affiche les paramètres réseau actuels de l'appliance virtuelle, notamment l'adresse IP, le réseau, l'adresse de diffusion, le masque de sous-réseau, la passerelle et les serveurs DNS.

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

  Vous permet de modifier n'importe lequel des paramètres réseau de l'appliance virtuelle, y compris

l’adresse IP, le masque de sous-réseau, la passerelle ou les serveurs DNS. Si vous faites passer vos paramètres réseau de DHCP à une configuration réseau statique à l’aide de la console de maintenance, vous ne pouvez pas modifier le nom de l’hôte. Vous devez sélectionner **Commit Changes** pour que les modifications prennent effet.

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

  Affiche la liste de recherche de noms de domaine utilisée pour la résolution des noms d’hôtes.

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

  Permet de modifier les noms de domaine à rechercher lors de la résolution des noms d’hôte. Vous devez sélectionner **Valider les modifications** pour que celles-ci soient prises en compte.

- **Afficher les itinéraires statiques**

  Affiche les routes réseau statiques actuelles.

- **Modifier les itinéraires statiques**

  Permet d’ajouter ou de supprimer des routes réseau statiques. Vous devez sélectionner **Valider les modifications** pour que les modifications soient prises en compte.

  - **Ajouter une route**

    Permet d’ajouter une route statique.

  - **Supprimer la route**

    Permet de supprimer un itinéraire statique.

  - **Retour**

    Vous ramène au **menu principal**.

  - **Sortie**

    Quitte la console de maintenance.

- **Désactiver l’interface réseau**

  Désactive toutes les interfaces réseau disponibles. Si une seule interface réseau est disponible, vous ne pouvez pas la désactiver. Vous devez sélectionner **Valider les modifications** pour que les modifications prennent effet.

- **Activer l’interface réseau**

  Active les interfaces réseau disponibles. Vous devez sélectionner **Valider les modifications** pour que les modifications soient prises en compte.

- **Valider les modifications**

  Applique toutes les modifications apportées aux paramètres réseau de l’appliance virtuelle. Vous devez sélectionner cette option pour appliquer toutes les modifications apportées, sinon les modifications ne prennent pas effet.

- **Envoyer un ping à l'hôte**

  Envoie une requête ping à un hôte cible pour confirmer les modifications d'adresse IP ou les configurations DNS.

- **Restaurer les paramètres par défaut**

  Réinitialise tous les paramètres aux valeurs d'usine. Vous devez sélectionner **Valider les modifications** pour que les modifications soient prises en compte.

- **Retour**

  Vous ramène au **menu principal**.

- **Sortie**

  Quitte la console de maintenance.

Utilisez le menu Configuration système dans Active IQ Unified Manager

Le menu Configuration système vous permet de gérer votre appliance virtuelle en proposant diverses options, telles que la consultation 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 "Restore from a Unified Manager Backup" est disponible dans ce menu.

Les options de menu suivantes sont disponibles :

- **Afficher l'état du serveur**

  Affiche l'état actuel du serveur. Les options d'état incluent « En cours d'exécution » et « À l'arrêt ».

  Si le serveur ne fonctionne pas, vous devrez peut-être contacter le support technique.

- **Redémarrer la machine virtuelle**

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

- **Arrêter la machine virtuelle**

  Arrête la machine virtuelle et tous les services.

  Vous pouvez sélectionner cette option uniquement depuis la console de la machine virtuelle.

- **Modifier <logged in user> le 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) dans la machine virtuelle.

- **Augmenter la taille du disque swap**

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

- **Changer de fuseau horaire**

  Modifie le fuseau horaire en fonction de votre emplacement.

- **Changer le serveur NTP**

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

- **Modifier le service NTP**

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

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

  Restaure la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

- **Réinitialiser le certificat du serveur**

  Réinitialise le certificat de sécurité du serveur.

- **Changer le nom de l'hôte**

  Modifie le nom de l'hôte sur lequel l'appliance virtuelle est installée.

- **Retour**

  Quitte le menu de configuration système et revient au menu principal.

- **Sortie**

  Quitte le menu de la console de maintenance.

Utilisez le menu Support et Diagnostics dans Active IQ Unified Manager

Le menu Assistance et diagnostics vous permet de générer un pack d'assistance que vous pouvez envoyer au support technique pour obtenir de l'aide au dépannage.

Les options de menu suivantes sont disponibles :

- **Générer le Light Support Bundle**

  Vous permet de produire un ensemble de support léger contenant seulement 30 jours de journaux et d'enregistrements de la base de données de configuration — il exclut les données de performance, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

- **Générer un pack de support**

  Permet de créer un package de support complet (fichier 7-Zip) contenant des informations de diagnostic dans le répertoire local de l'utilisateur de diagnostic. Si votre système est connecté à Internet, vous pouvez également charger ce package de support vers NetApp.

Le fichier comprend des informations générées par un message AutoSupport, le contenu de la base de données de Unified Manager, des données détaillées sur le fonctionnement interne du serveur Unified Manager et des journaux de niveau détaillé qui ne sont normalement pas inclus dans les messages AutoSupport ni dans le module de support léger.

Découvrez les options supplémentaires du menu de la console de maintenance dans Active IQ Unified Manager

Les options de menu suivantes vous permettent d'effectuer diverses tâches d'administration 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 du serveur dans l'interface graphique d'Unified Manager en cliquant sur **Général** > **Certificats HTTPS** > **Régénérer le certificat HTTPS**.

- **Désactiver l'authentification SAML**

  Désactive l'authentification SAML afin que le fournisseur d'identité (IdP) ne fournisse plus l'authentification de connexion aux utilisateurs accédant à l'interface graphique d'Unified Manager. Cette option de console est généralement utilisée lorsqu'un problème avec le serveur IdP ou la configuration SAML empêche les utilisateurs d'accéder à l'interface graphique d'Unified Manager.

- **Fournisseur de données externe**

  Propose des options pour connecter Unified Manager à un fournisseur de données externe. Une fois la connexion établie, les données de performance sont envoyées à un serveur externe afin que les experts en performances du stockage puissent représenter graphiquement les indicateurs de performance à l'aide d'un logiciel tiers. Les options suivantes s'affichent :

  - **Configuration du serveur d'affichage**--Affiche la connexion actuelle et les paramètres de configuration d'un fournisseur de données externe.
  - **Ajouter / modifier la connexion au serveur**--Vous permet de saisir de nouveaux paramètres de connexion pour un fournisseur de données externe ou de modifier les paramètres existants.
  - **Modifier la configuration du serveur**--Permet de saisir de nouveaux paramètres de configuration pour un fournisseur de données externe ou de modifier les paramètres existants.
  - **Supprimer la connexion au serveur**--Supprime la connexion à un fournisseur de données externe.

    Une fois la connexion supprimée, Unified Manager perd sa connexion au serveur externe.

- **Restauration de sauvegarde**

  Pour plus d'informations, consultez les rubriques sous "Gestion des opérations de sauvegarde et de restauration".

- **Configuration de l'intervalle d'interrogation des performances**

  Permet de configurer la fréquence à laquelle Unified Manager collecte les données statistiques de performance des clusters. L'intervalle de collecte par défaut est de 5 minutes.

Vous pouvez régler cet intervalle sur 10 ou 15 minutes si vous constatez que les collectes provenant de grands clusters ne se terminent pas à temps.

- **Afficher/Modifier les ports de l'application**

  Offre la possibilité de modifier les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS, si nécessaire pour des raisons de sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

- **Contrôler l'accès au port 3306 de MySQL**

  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 d'activer ou de désactiver la visibilité de ce port entre localhost et les hôtes distants, c'est-à-dire que, s'il est activé pour localhost uniquement dans votre environnement, vous pouvez également rendre ce port disponible pour les hôtes distants. À l'inverse, lorsqu'il est activé pour tous les hôtes, vous pouvez restreindre 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 modifié la visibilité du port, et désactiver les paramètres du pare-feu s'ils sont configurés pour restreindre l'accès au port MySQL 3306.

- **Sortie**

  Quitte le menu de la console de maintenance.

Modifiez le mot de passe de l'utilisateur de maintenance sous Windows dans Active IQ Unified Manager

Vous pouvez modifier le mot de passe de l'utilisateur de maintenance d'Unified Manager en cas de besoin.

Étapes

1. Depuis la page de connexion de 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. Saisissez le nom d'utilisateur et cliquez sur **Soumettre**.

   Un courriel contenant un lien pour réinitialiser le mot de passe est envoyé à l'adresse électronique définie pour ce nom d'utilisateur.

3. Cliquez sur le lien **de réinitialisation du mot de passe** dans l'e-mail et définissez le nouveau mot de passe.
4. Retournez à l'interface web et connectez-vous à Unified Manager à l'aide du nouveau mot de passe.

Modifiez le mot de passe umadmin d'Active IQ Unified Manager sur les systèmes Linux

Pour des raisons de sécurité, vous devez modifier le mot de passe par défaut de l'utilisateur umadmin de Unified Manager immédiatement après avoir terminé le

processus d'installation. Si nécessaire, vous pourrez modifier à nouveau le mot de passe ultérieurement.

Avant de commencer

- Unified Manager doit être installé sur un système Red Hat Enterprise Linux.
- Vous devez disposer des identifiants de l'utilisateur root pour le système Linux sur lequel Unified Manager est installé.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Linux sur lequel Unified Manager s'exécute.
2. Modifier le mot de passe umadmin:

   ```
   passwd umadmin
   ```

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

Modifier les ports qu'Active IQ Unified Manager utilise pour les protocoles HTTP et HTTPS

Les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS peuvent être modifiés après l'installation si nécessaire pour des raisons de sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

> Certains ports sont considérés comme non sécurisés lors de l'utilisation des navigateurs Mozilla Firefox ou Google Chrome. Consultez votre navigateur avant d'attribuer un nouveau numéro de port pour le trafic HTTP et HTTPS. Le choix d'un port non sécurisé pourrait rendre le système inaccessible, ce qui vous obligerait à contacter le support client pour résoudre le problème.

L'instance d'Unified Manager redémarre automatiquement après la modification du port ; assurez-vous donc que c'est le bon moment pour arrêter brièvement le système.

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

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

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

   Laisser le numéro de port vide attribue le port par défaut pour le protocole.

   Il vous est demandé si vous souhaitez modifier les ports et redémarrer Unified Manager maintenant.

5. Tapez **y** pour modifier les ports et redémarrer Unified Manager.
6. Quittez 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 de Unified Manager, par exemple https://host.company.com:1234, https://12.13.14.15:1122, ou https://[2001:db8:0:1]:2123.

Ajouter des interfaces réseau à Active IQ Unified Manager

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

Avant de commencer

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

L'appliance virtuelle doit être mise sous tension.

> Vous ne pouvez pas effectuer cette opération si Unified Manager est installé sur Red Hat Enterprise Linux ou sur Microsoft Windows.

Étapes

1. Dans le menu principal de la console vSphere, sélectionnez **Configuration système** > **Redémarrer le système d'exploitation**.

   Après le redémarrage, la console de maintenance peut détecter la nouvelle interface réseau ajoutée.

2. Accédez 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. Saisissez les paramètres du réseau.

   Vous serez invité à saisir les paramètres réseau si vous utilisez une interface statique ou si le DHCP n'est pas détecté.

   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.

Régénérez le certificat client dans Active IQ Unified Manager

Vous pouvez utiliser la console de maintenance pour régénérer votre certificat client Unified Manager. Votre certificat bénéficie d'une période de validité étendue à cinq ans.

Étapes

1. Connectez-vous en tant qu'utilisateur de maintenance.
2. Sélectionnez **Régénérer le certificat client** et appuyez sur **Entrée**.
3. Si le système vous demande une authentification, saisissez les informations d'identification requises.

4. Sélectionnez **Confirmer la régénération** et appuyez sur **Entrée**.
5. Une fois le certificat régénéré, redémarrez le service Unified Manager pour appliquer les modifications.
6. Pour vérifier le certificat mis à jour, connectez-vous à ONTAP. Consultez l'état du certificat client et sa validité.

Informations connexes "Gérez les certificats ONTAP avec System Manager"

Ajouter de l'espace disque

Ajoutez de l'espace disque au répertoire de la base de données Active IQ Unified Manager

Le répertoire de la base de données Unified Manager contient toutes les données de santé et de performance collectées à partir des systèmes ONTAP. Dans certains cas, il peut être nécessaire d'augmenter la taille du répertoire de la base de données.

Par exemple, le répertoire de la base de données peut se remplir si Unified Manager collecte des données à partir d'un grand nombre de clusters, chacun comportant de nombreux nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de la base de données sera rempli à 90 % et un événement critique lorsqu'il sera rempli à 95 %.

Aucune donnée supplémentaire n'est collectée à partir des clusters une fois que le répertoire est rempli à 95 %.

Les étapes nécessaires pour ajouter de la capacité au répertoire de données diffèrent selon que Unified Manager est exécuté sur un serveur VMware ESXi, sur un serveur Red Hat ou sur un serveur Microsoft Windows.

Ajouter de l'espace au répertoire de données sur un hôte Linux dans Active IQ Unified Manager

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

Avant de commencer

Vous devez disposer d'un accès utilisateur root à la machine Red Hat Enterprise Linux sur laquelle Unified Manager est installé.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'augmenter la taille du répertoire de données.

Étapes

1. Connectez-vous en tant qu'utilisateur root à la machine Linux sur laquelle vous souhaitez ajouter de l'espace disque.
2. Arrêtez le service Unified Manager et le logiciel MySQL associé dans l'ordre indiqué :

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Créez un dossier de sauvegarde temporaire (par exemple, `/backup-data`) avec suffisamment d'espace

disque pour contenir les données dans le répertoire `/opt/netapp/data` actuel.

4. Copiez le contenu et la configuration des privilèges du répertoire `/opt/netapp/data` existant vers le répertoire de données de sauvegarde :

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Si SE Linux est activé:

   a. Obtenez le type SE Linux pour les dossiers du dossier `/opt/netapp/data` existant :

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

      Le système renvoie une confirmation similaire à la suivante :

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Exécutez la commande chcon pour définir le type SE Linux 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 les 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 le monter `/opt/netapp/data` en tant que partage NFS ou CIFS. En effet, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` pourraient 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 la suivante :

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

9. Si SE Linux est activé, vérifiez que le contexte du répertoire `/opt/netapp/data` est toujours défini sur mysqld_db_t :

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

Le système renvoie une confirmation similaire à la suivante :

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

10. Supprimez le fichier abc afin que ce fichier superflu ne provoque pas d'erreur de base de données à l'avenir.
11. Copiez le contenu de backup-data vers le répertoire étendu `/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, démarrez les services ocie et ocieau dans l'ordre indiqué :

    ```
    systemctl start ocie ocieau
    ```

15. Une fois tous les services démarrés, supprimez le dossier de sauvegarde `/backup-data`:

    ```
    rm -rf /backup-data
    ```

Ajouter de l'espace au disque de données d'une machine virtuelle VMware dans Active IQ Unified Manager

Si vous devez augmenter l'espace disque alloué à la base de données Unified Manager, vous pouvez ajouter de la capacité après l'installation en augmentant l'espace disque à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez avoir accès au vSphere Client.
- La machine virtuelle ne doit comporter aucun instantané stocké localement.
- Vous devez disposer des identifiants 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 augmentez la capacité de disque des données `disk 3`. Consultez la documentation VMware pour plus de détails.

   Dans de rares cas, le déploiement Unified Manager utilise "Hard Disk 2" pour le disque de données au lieu de "Hard Disk 3". Si cela s'est produit dans votre déploiement, augmentez l'espace du disque le plus grand. Le disque de données aura toujours plus d'espace que l'autre disque.

2. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis sélectionnez l'onglet **Console**.
3. Cliquez dans la fenêtre de 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, saisissez le numéro correspondant à l'option **Configuration système**.
5. Dans le menu Configuration système, saisissez le numéro correspondant à l'option **Augmenter la taille du disque de données**.

Ajouter de l'espace au lecteur logique d'un serveur Windows dans Active IQ Unified Manager

Si vous devez augmenter l'espace disque de la base de données Unified Manager, vous pouvez ajouter de la capacité au lecteur logique sur lequel Unified Manager est installé.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'ajouter de l'espace disque.

Étapes

1. Connectez-vous en tant qu'administrateur au serveur Windows sur lequel vous souhaitez ajouter de l'espace disque.
2. Suivez l'étape correspondant à la méthode que vous souhaitez utiliser pour ajouter de l'espace :

Option	Description
Sur un serveur physique, augmentez la capacité du lecteur logique sur lequel le serveur Unified Manager est installé.	Suivez les étapes décrites dans la rubrique Microsoft : "Étendre un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes décrites dans la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes décrites dans la rubrique VMware : "Augmenter la taille d'une partition de disque"

Gérer l'accès des utilisateurs

Ajouter des utilisateurs

Ajouter des utilisateurs dans Active IQ Unified Manager

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 distants ou des groupes appartenant à un serveur d'authentification. Vous pouvez attribuer des rôles à ces utilisateurs et, en fonction des privilèges de ces rôles, les utilisateurs peuvent gérer

les objets de stockage et les données avec Unified Manager, ou consulter les données dans une base de données.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.
- Pour ajouter un utilisateur ou un groupe distant, vous devez avoir activé l'authentification à distance et configuré votre serveur d'authentification.
- Si vous prévoyez de configurer l'authentification SAML afin qu'un fournisseur d'identité (IdP) authentifie les utilisateurs accédant à l'interface graphique, assurez-vous que ces utilisateurs sont définis comme des utilisateurs "remote".

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

Si vous ajoutez un groupe depuis Windows Active Directory, tous ses membres directs et ses sous-groupes imbriqués peuvent s'authentifier auprès d'Unified Manager, sauf si les sous-groupes imbriqués sont désactivés. Si vous ajoutez un groupe depuis OpenLDAP ou un autre service 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 saisissez les informations requises.

   Lors de la saisie des informations utilisateur requises, vous devez indiquer une adresse électronique unique pour cet utilisateur. Vous devez éviter d'indiquer des adresses électroniques partagées par plusieurs utilisateurs.

4. Cliquez sur **Add**.

Créer un utilisateur de base de données dans Active IQ Unified Manager

Pour prendre en charge une connexion entre Workflow Automation et Unified Manager, ou pour accéder aux vues de la base de données, vous devez d'abord créer un utilisateur de la base de données avec le rôle Integration Schema ou Report Schema dans l'interface utilisateur Web de Unified Manager.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Les utilisateurs de la base de données assurent l'intégration avec Workflow Automation et l'accès aux vues de base de données spécifiques aux rapports. Les utilisateurs de la base de données n'ont pas accès à l'interface utilisateur web de Unified Manager ni à la console de maintenance, et ne peuvent pas exécuter d'appels d'API.

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 **Utilisateur de base de données** dans la liste déroulante **Type**.

4. Saisissez un nom et un mot de passe pour l'utilisateur de la base de données.
5. Dans la liste déroulante **Role**, sélectionnez le rôle approprié.

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

6. Cliquez sur **Add**.

Modifier les paramètres utilisateur dans Active IQ Unified Manager

Vous pouvez modifier les paramètres utilisateur, tels que l'adresse e-mail et le rôle, attribués à chaque utilisateur. Par exemple, vous pouvez modifier le rôle d'un utilisateur opérateur de stockage et lui attribuer les privilèges d'administrateur de stockage.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Lorsque vous modifiez le rôle attribué à un utilisateur, les modifications sont appliquées lorsque l'une des actions suivantes se produit :

- L'utilisateur se déconnecte puis se reconnecte à Unified Manager.
- Le délai d'expiration de la session de 24 heures est atteint.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue Modifier l'utilisateur, modifiez les paramètres appropriés définis pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

Afficher les utilisateurs dans Active IQ Unified Manager

La page Utilisateurs vous permet de consulter la liste des utilisateurs qui gèrent les objets de stockage et les données à l'aide d'Unified Manager. Vous pouvez y voir des informations détaillées sur chaque utilisateur, telles que son nom, son type, son adresse e-mail et le rôle qui lui est attribué.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.

Supprimer des utilisateurs ou des groupes dans Active IQ Unified Manager

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

Avant de commencer

- Lorsque vous supprimez des groupes distants, vous devez avoir réattribué les événements qui sont attribués aux utilisateurs de ces groupes.

  Si vous supprimez des utilisateurs locaux ou distants, les événements qui leur sont attribués ne leur sont plus attribués automatiquement.

- Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur 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.

Découvrez le contrôle d'accès basé sur les rôles dans Active IQ Unified Manager

Le RBAC (contrôle d'accès basé sur les rôles) offre la possibilité de contrôler qui a accès aux différentes fonctionnalités et ressources sur le serveur Active IQ Unified Manager. Le RBAC permet aux administrateurs de gérer des groupes d'utilisateurs en définissant des rôles. Si vous devez restreindre l'accès à certaines fonctionnalités à des administrateurs spécifiques, vous devez créer des comptes d'administrateur pour eux. Si vous souhaitez limiter les informations que les administrateurs peuvent consulter et les opérations qu'ils peuvent effectuer, vous devez appliquer des rôles aux comptes d'administrateur que vous créez.

Le serveur d'administration utilise le contrôle d'accès basé sur les rôles (RBAC) pour la connexion des utilisateurs et les autorisations des rôles. Si vous n'avez pas modifié les paramètres par défaut du serveur d'administration relatifs à l'accès des utilisateurs administratifs, vous n'avez pas besoin de vous connecter pour les consulter.

Lorsque vous lancez une opération nécessitant des privilèges spécifiques, le serveur de gestion vous invite à vous connecter. Par exemple, pour créer des comptes d'administrateur, vous devez vous connecter avec un accès au compte Application Administrator.

Découvrez les types d'utilisateurs dans Active IQ Unified Manager

Un type d'utilisateur spécifie le type de compte détenu par l'utilisateur et inclut les utilisateurs distants, les groupes distants, les utilisateurs locaux, les utilisateurs de base de données et les utilisateurs de maintenance. Chacun de ces types possède son propre rôle, qui est attribué par un utilisateur disposant du rôle d'Administrator.

Les types d'utilisateurs de Unified Manager sont les suivants :

- **Utilisateur de maintenance**

  Créé lors de la configuration initiale d'Unified Manager. L'utilisateur de maintenance crée ensuite d'autres utilisateurs et attribue des rôles. L'utilisateur de maintenance est également le seul utilisateur à avoir accès à la console de maintenance. Lorsque Unified Manager est installé sur un système Red Hat Enterprise Linux, le nom d'utilisateur « `umadmin.` » est attribué à l'utilisateur de maintenance.

- **Utilisateur local**

  Accède à l'interface utilisateur de Unified Manager et exécute des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle Application Administrator.

- **Groupe distant**

  Un groupe d'utilisateurs accède à l'interface utilisateur de Unified Manager à l'aide des identifiants stockés sur le serveur d'authentification. Le nom de ce compte doit correspondre au nom d'un groupe stocké sur le serveur d'authentification. Tous les utilisateurs du groupe distant ont accès à l'interface utilisateur de Unified Manager à l'aide de leurs identifiants utilisateur individuels. Les groupes distants peuvent exécuter des fonctions en fonction des rôles qui leur sont attribués.

- **Utilisateur distant**

  Accède à l'interface utilisateur de Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Un utilisateur distant exécute des fonctions en fonction du rôle qui lui est attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle Application Administrator.

- **Utilisateur de la 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 API.

Découvrez les rôles des utilisateurs dans Active IQ Unified Manager

L'utilisateur en charge de la maintenance ou l'Application Administrator attribue un rôle à chaque utilisateur. Chaque rôle confère des privilèges spécifiques. L'étendue des actions que vous pouvez effectuer dans Unified Manager dépend du rôle qui vous est attribué et des privilèges associés.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

  Permet de consulter les informations du système de stockage et les autres données collectées par Unified Manager, notamment les historiques et les tendances de capacité. Ce rôle permet à l'opérateur de stockage de consulter, d'attribuer, d'acquitter, de résoudre et d'ajouter des notes aux événements.

- **Administrateur de stockage**

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

- **Administrateur d'applications**

  Configure les paramètres non liés à la gestion du stockage. Ce rôle permet la gestion des utilisateurs, des certificats de sécurité, de l'accès à la base de données et des options d'administration, notamment l'authentification, SMTP, la mise en réseau et AutoSupport.

  > Lors de l'installation de Unified Manager sur les systèmes Linux, l'utilisateur initial doté du rôle Application Administrator est automatiquement nommé "umadmin".

- **Schéma d'intégration**

  Ce rôle permet un accès en lecture seule aux vues de la base de données Unified Manager pour intégrer Unified Manager à OnCommand Workflow Automation (WFA).

- **Schéma du rapport**

  Ce rôle permet un accès en lecture seule aux rapports et aux autres vues de la base de données directement depuis la base de données Unified Manager. Les bases de données consultables sont les suivantes :

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Découvrez les rôles et les capacités des utilisateurs dans Active IQ Unified Manager

En fonction du rôle utilisateur qui vous a été attribué, vous pouvez déterminer les opérations que vous pouvez effectuer dans Unified Manager.

Le tableau suivant présente les fonctions que chaque rôle utilisateur peut effectuer :

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma du rapport
Afficher les informations du système de stockage	•	•	•	•	•
Consultez d'autres données, telles que les historiques et les tendances de capacité	•	•	•	•	•

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma du rapport
Afficher, attribuer et résoudre les événements	•	•	•		
Afficher les objets du service de stockage, tels que les associations SVM et les pools de ressources	•	•	•		
Consultez les politiques de seuil	•	•	•		
Gérer les objets de service de stockage, tels que les associations SVM et les pools de ressources		•	•		
Définir les alertes		•	•		
Gérer les options de gestion du stockage		•	•		
Gérer les politiques de gestion du stockage		•	•		
Gérer les utilisateurs			•		
Gérer les options d'administration			•		
Définir des politiques de seuil			•		
Gérer l'accès à la base de données			•		
Gérer l'intégration avec WFA et fournir l'accès aux vues de la base de données				•	

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma du rapport
Planifier et enregistrer les rapports		•	•		
Exécutez les opérations "Fix It" depuis Management Actions		•	•		
Fournir un accès en lecture seule aux vues de la base de données					•

Gérer les paramètres d'authentification SAML

Activer l'authentification SAML dans Active IQ Unified Manager

Une fois les paramètres d'authentification à distance configurés, vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d'identité sécurisé (IdP) avant de pouvoir accéder à l'interface utilisateur Web Unified Manager.

Notez que seuls les utilisateurs distants auront accès à l'interface utilisateur graphique de Unified Manager après l'activation de l'authentification SAML. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'affecte pas les utilisateurs qui accèdent à la console de maintenance.

Utilisez un fournisseur d'identité dans Active IQ Unified Manager

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

Vous devez saisir l'URI et les métadonnées d'Unified Manager dans le serveur IdP. Vous pouvez copier ces informations depuis la page Unified ManagerSAML Authentication. Unified Manager est considéré comme le fournisseur de services (SP) dans la norme SAML (Security Assertion Markup Language).

Normes de chiffrement prises en charge

- Norme de chiffrement avancée (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Fournisseurs d'identité validés

- Shibboleth
- Services de fédération Active Directory (ADFS)

Exigences de configuration d'ADFS

- Vous devez définir trois règles de revendication dans l'ordre suivant, nécessaires pour que Unified Manager puisse analyser les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance.

Règle de revendication	Valeur
SAM-account-name	ID de 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 "Forms Authentication", sinon les utilisateurs risquent de recevoir une erreur lors de leur déconnexion de Unified Manager. Procédez comme suit :
  a. Ouvrez la Console de gestion ADFS.
  b. Cliquez sur le dossier « Stratégies d'authentification » dans l'arborescence de gauche.
  c. Dans Actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.
  d. Définissez la méthode d'authentification Intranet sur « `Forms Authentication` » au lieu de la valeur par défaut « `Windows Authentication` ».
- Dans certains cas, la connexion via l'IdP est refusée lorsque le certificat de sécurité d'Unified Manager est signé par une autorité de certification. Deux solutions permettent de résoudre ce problème :
  - Suivez les instructions indiquées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour le certificat d'autorité de certification chaîné associé à la partie de confiance :

    "Désactiver la vérification de révocation par approbation de partie de confiance"

  - Le serveur d'autorité de certification doit résider sur le serveur ADFS pour signer la demande de certificat du serveur Unified Manager.

Autres exigences de configuration

- Le décalage horaire d'Unified Manager est fixé à 5 minutes. La différence de temps entre le serveur IdP et le serveur Unified Manager ne peut donc pas dépasser 5 minutes, sinon l'authentification échouera.

Activer l'authentification SAML dans Active IQ Unified Manager

Vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin qu'un fournisseur d'identité sécurisé (IdP) authentifie les utilisateurs distants avant qu'ils puissent accéder à l'interface utilisateur web de Unified Manager.

Avant de commencer

- Vous devez avoir configuré l'authentification à distance et vérifié son bon fonctionnement.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle Application Administrator.

- Le fournisseur d'identité (IdP) doit être pris en charge par Unified Manager et doit être configuré.
- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès au serveur IdP.

Une fois que vous avez activé l'authentification SAML depuis Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que le fournisseur d'identité (IdP) n'a pas été configuré avec les informations sur l'hôte du serveur Unified Manager. Vous devez donc être prêt à effectuer les deux parties de la connexion avant de commencer le processus de configuration. Le fournisseur d'identité peut être configuré avant ou après la configuration de Unified Manager.

Seuls les utilisateurs distants auront accès à l'interface graphique de Unified Manager après l'activation de l'authentification SAML. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'affecte pas les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPIs.

Unified Manager redémarre automatiquement une fois la configuration SAML terminée sur cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Cochez la case **Activer l'authentification SAML**.

   Les champs nécessaires à la configuration de la connexion IdP sont affichés.

3. Saisissez l'URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager au serveur IdP.

   Si le serveur IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URI IdP pour renseigner automatiquement le champ Métadonnées IdP.

4. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.

   Vous pouvez configurer le serveur IdP avec ces informations dès maintenant.

5. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.

La prochaine fois que des utilisateurs distants autorisés tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion IdP au lieu de la page de connexion de Unified Manager.

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

Lorsque vous utilisez ADFS comme fournisseur d'identité, l'interface graphique de Unified Manager ne tient pas compte du délai d'expiration de 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 **General** > **Feature Settings** > **Inactivity Timeout**.

Modifier le fournisseur d'identité d'authentification SAML dans Active IQ Unified Manager

Vous pouvez modifier le fournisseur d'identité (IdP) utilisé par Unified Manager pour authentifier les utilisateurs distants.

Avant de commencer

- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès à l'IdP.

Le nouvel IdP peut être configuré avant ou après la configuration d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Saisissez le nouvel URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager à l'IdP.

   Si l'IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IdP Metadata** après avoir saisi l'URL de l'IdP pour renseigner automatiquement le champ IdP Metadata.

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

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouvel IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

La prochaine fois que des utilisateurs distants autorisés tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la nouvelle page de connexion IdP au lieu de l'ancienne page de connexion IdP.

Mettez à jour les paramètres d'authentification SAML après une modification du certificat de sécurité d'Active IQ 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, lui attribuez une nouvelle adresse IP ou modifiez manuellement son certificat de sécurité.

Après la modification du certificat de sécurité et le redémarrage du serveur Unified Manager, l'authentification SAML ne fonctionnera plus et les utilisateurs ne pourront pas accéder à l'interface graphique de Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IdP et sur le serveur Unified Manager pour rétablir l'accès à l'interface utilisateur.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Main Menu**, saisissez le numéro correspondant à l'option **Disable SAML authentication**.

   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 identifiants de l'utilisateur de maintenance.
4. Dans la page **Setup/Authentication**, sélectionnez l'onglet **SAML Authentication** et configurez la connexion IdP.
5. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.
6. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

7. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.
8. Accédez à votre serveur IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

fournisseur d'identité	Étapes de configuration
ADFS	a. Supprimez l'entrée d'approbation de partie de confiance existante dans l'interface graphique de gestion ADFS. b. Ajoutez une nouvelle entrée d'approbation de partie de confiance à l'aide de celle du serveur Unified Manager mis à jour `saml_sp_metadata.xml`. c. Définissez les trois règles de revendication requises pour que Unified Manager puisse analyser les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance. d. Redémarrez le service ADFS sous Windows.
Shibboleth	a. Mettez à jour le nouveau nom de domaine complet (FQDN) du serveur Unified Manager dans les fichiers `attribute-filter.xml` et `relying-party.xml`. b. Redémarrez le serveur web Apache Tomcat et attendez que le port 8005 devienne disponible.

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

Désactiver l’authentification SAML dans Active IQ Unified Manager

Vous pouvez désactiver l’authentification SAML lorsque vous souhaitez cesser d’authentifier les utilisateurs distants via un fournisseur d’identité sécurisé (IdP) avant qu’ils puissent se connecter à l’interface utilisateur web de Unified Manager. Lorsque l’authentification SAML est désactivée, les fournisseurs de services d’annuaire configurés, tels qu’Active Directory ou LDAP, assurent l’authentification de connexion.

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 de Unified Manager si vous n’avez pas accès à l’interface utilisateur graphique.

Unified Manager redémarre automatiquement après la désactivation de l’authentification SAML.

Étapes

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**.

   Une boîte de dialogue s’affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

4. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d’accéder à l’interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion de Unified Manager au lieu de la page de connexion IdP.

Accédez à votre IdP et supprimez l’URI et les métadonnées du serveur Unified Manager.

Désactivez l’authentification SAML depuis la console de maintenance Active IQ Unified Manager

Il peut être nécessaire de désactiver l’authentification SAML depuis la console de maintenance lorsqu’il n’est pas possible d’accéder à l’interface graphique de Unified Manager. Cela peut se produire en cas de mauvaise configuration ou si l’IdP n’est pas accessible.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu’utilisateur de maintenance.

Lorsque l’authentification SAML est désactivée, les fournisseurs de services d’annuaire configurés, tels qu’Active Directory ou LDAP, assurent l’authentification de connexion. Les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l’interface utilisateur graphique, en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l’authentification SAML depuis la page Setup/Authentication de l’interface utilisateur.

Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Main Menu**, saisissez le numéro correspondant à l'option **Disable SAML authentication**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Tapez **y**, puis appuyez sur Entrée, et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur 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 et les métadonnées du serveur Unified Manager.

Utilisez la page d'authentification SAML dans Active IQ Unified Manager

Vous pouvez utiliser la page d'authentification SAML pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identité sécurisé (IdP) avant qu'ils puissent se connecter à l'interface utilisateur web d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application pour créer ou modifier la configuration SAML.
- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez cocher la case « Activer l'authentification SAML » pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI du fournisseur d'identité**

  L'URI permettant d'accéder à l'IdP depuis le serveur Unified Manager. Des exemples d'URI sont fournis ci-dessous.

  Exemple d'URI ADFS :

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemple d'URI Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Métadonnées du fournisseur d'identité**

  Les métadonnées du fournisseur d'identité au format XML.

  Si l'URL IdP est accessible depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IdP Metadata** pour renseigner ce champ.

- **Système hôte (FQDN)**

  Le nom de domaine complet (FQDN) du système hôte d'Unified Manager, tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI de l'hôte**

  L'URI permettant d'accéder au système hôte Unified Manager depuis l'IdP.

- **Métadonnées de l'hôte**

  Les métadonnées du système hôte au format XML.

Gérer l'authentification

Modifier les serveurs d'authentification dans Active IQ Unified Manager

Vous pouvez modifier le port utilisé par le serveur Unified Manager pour communiquer avec votre serveur d'authentification.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Cochez la case **Désactiver la recherche de groupes imbriqués**.
3. Dans la section **Serveurs d'authentification**, sélectionnez le serveur d'authentification que vous souhaitez modifier, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Modifier le serveur d'authentification**, modifiez les détails du port.
5. Cliquez sur **Enregistrer**.

Supprimer les serveurs d'authentification dans Active IQ Unified Manager

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 le serveur d'authentification utilisé par le serveur de gestion, vous pouvez supprimer le serveur d'authentification et en ajouter un nouveau.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Lorsque vous supprimez un serveur d'authentification, les utilisateurs ou groupes distants de ce serveur ne pourront plus accéder à Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Sélectionnez un ou plusieurs serveurs d'authentification que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Cliquez sur **Oui** pour confirmer la demande de suppression.

   Si l'option **Utiliser une connexion sécurisée** est activée, les certificats associés au serveur d'authentification sont supprimés en même temps que le serveur d'authentification.

Authentifiez-vous avec Active Directory ou OpenLDAP dans Active IQ Unified Manager

Vous pouvez activer l'authentification à distance sur le serveur de gestion et configurer ce dernier 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 d'administration gère sa propre base de données de noms d'utilisateur et de mots de passe. Le serveur d'administration effectue l'authentification et n'utilise pas Active Directory ni OpenLDAP pour l'authentification.

Journalisation d'audit

Découvrez les journaux d'audit dans Active IQ Unified Manager

Vous pouvez détecter si le journal des audits a été compromis en utilisant Audit Logs. Toutes les activités effectuées par un utilisateur sont surveillées et consignées dans Audit Logs. Les audits sont effectués pour toutes les fonctionnalités de l'interface utilisateur et des API exposées publiquement de Active IQ Unified Manager.

Vous pouvez utiliser la vue **Journal des audits : fichier** pour afficher et consulter tous les fichiers du journal des audits disponibles dans votre Active IQ Unified Manager. Les fichiers de la vue Journal des audits : fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux des audits capturés dans le système depuis l'installation ou la mise à niveau jusqu'à aujourd'hui. 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 "File Integrity Status", qui est surveillé activement pour détecter toute altération ou suppression du fichier journal. Les journaux des audits peuvent avoir l'un des états suivants lorsqu'ils sont disponibles dans le système :

État	Description
ACTIVE	Fichier dans lequel les journaux sont actuellement enregistrés.
NORMAL	Fichier inactif, compressé et stocké dans le système.
ALTÉRÉ	Fichier compromis par un utilisateur qui l'a modifié manuellement.
MANUAL_DELETE	Fichier supprimé par un utilisateur autorisé.
ROLLOVER_DELETE	Fichier supprimé en raison d'une rotation conformément à la stratégie de configuration de rotation.
SUPPRESSION_INATTENDUE	Fichier supprimé pour des raisons inconnues.

La page Journal des audits comprend les boutons de commande suivants :

- Configurer
- Supprimer
- Télécharger

Le bouton **DELETE** vous permet de supprimer n'importe lequel des journaux des audits répertoriés dans la vue Audit Logs. Vous pouvez supprimer un journal des audits et, si vous le souhaitez, indiquer le motif de la suppression du fichier, ce qui aidera ultérieurement à déterminer si la suppression était valide. La colonne REASON répertorie le motif ainsi que le nom de l'utilisateur qui a effectué l'opération de suppression.

La suppression d'un fichier journal supprime le fichier du système, mais pas l'entrée correspondante dans la table de la base de données.

Vous pouvez télécharger les journaux des audits depuis Active IQ Unified Manager à l'aide du bouton **TÉLÉCHARGER** dans la section Journaux des audits et exporter les fichiers de journal des audits. Les fichiers marqués « `NORMAL` » ou « `TAMPERED` » sont téléchargés au format `.gzip` compressé.

Les fichiers du journal des audits sont archivés périodiquement et enregistrés dans la base de données à titre de référence. Avant leur archivage, les journaux des audits sont signés numériquement afin de garantir leur sécurité et leur intégrité.

Lorsqu'un bundle AutoSupport complet est généré, le bundle de support inclut à la fois les fichiers du journal des audits archivés et actifs. Mais lorsqu'un bundle de support allégé est généré, il inclut uniquement les journaux des audits actifs. Les journaux des audits archivés ne sont pas inclus.

Configurer les journaux d'audit d'Active IQ Unified Manager

Vous pouvez utiliser le bouton **Configure** dans la section Journal des audits pour configurer la politique de rotation des fichiers du journal des audits et activer également la journalisation à distance pour le journal des audits.

Vous pouvez définir les valeurs de **MAX FILE SIZE** et de **AUDIT LOG RETENTION DAYS** en fonction de la quantité et de la fréquence des données que vous souhaitez stocker dans le système. La valeur du champ **TOTAL AUDIT LOG SIZE** correspond à la taille totale des données du journal des audits présentes dans le système. La politique de rotation est déterminée par les valeurs des champs **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** et **TOTAL AUDIT LOG SIZE**. Lorsque la taille de la sauvegarde du journal des audits atteint

la valeur configurée dans **TOTAL AUDIT LOG SIZE**, le fichier archivé en premier est supprimé. Cela signifie que le fichier le plus ancien est supprimé. Cependant, l'entrée du fichier reste disponible dans la base de données et est marquée comme "Rollover Delete". La valeur de **AUDIT LOG RETENTION DAYS** correspond au nombre de jours pendant lesquels les fichiers du journal des audits sont conservés. Tout fichier plus ancien que la valeur définie dans ce champ fait l'objet d'une rotation.

Étapes

1. Cliquez sur **Journaux des audits** > > **Configurer**.
2. Saisissez les valeurs dans les champs **TAILLE MAXIMALE DU FICHIER**, **TAILLE TOTALE DU JOURNAL DES AUDITS** et **JOURS DE CONSERVATION DU JOURNAL DES AUDITS**.

   Pour activer la journalisation à distance, sélectionnez **Activer la journalisation à distance**.

Activer la journalisation à distance des journaux d'audit dans Active IQ Unified Manager

Vous pouvez cocher la case **Enable Remote Logging** dans la boîte de dialogue Configure Audit Logs pour activer la journalisation à distance. Vous pouvez utiliser cette fonctionnalité pour transférer les journaux des audits vers un serveur Syslog distant. Cela vous permettra de gérer vos journaux des audits en cas de contraintes d'espace.

La journalisation à distance des journaux des audits fournit une sauvegarde inviolable au cas où les fichiers du journal des audits sur le serveur Active IQ Unified Manager seraient altérés.

Étapes

1. Dans la boîte de dialogue **Configurer les journaux des audits**, cochez la case **Activer la journalisation à distance**.

   Des champs supplémentaires pour configurer la journalisation à distance s'affichent.

2. Saisissez le **nom de l'hôte** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **CERTIFICAT D'AC DU SERVEUR**, cliquez sur **PARCOURIR** pour sélectionner un certificat public du serveur cible.

   Le certificat doit être téléchargé au format `.pem`. Ce certificat doit être obtenu à partir du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le "hostname" sélectionné dans l'attribut `SubjectAltName` (SAN).

4. Saisissez les valeurs pour les champs suivants : **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Les valeurs de ces champs doivent être exprimées en millisecondes.

5. Sélectionnez le format Syslog requis et la version requise du protocole TLS dans les champs **FORMAT** et **PROTOCOL**.
6. Cochez la case **Activer l'authentification de clients** si le serveur Syslog cible requiert une authentification basée sur des certificats.

   Vous devrez télécharger le certificat d'authentification de clients et le charger 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 de clients.

   Exemple : syslog-ng exige qu'un <hash> du certificat soit créé à l'aide de la commande `openssl x509`

`-noout -hash -in cert.pem`, puis vous devez créer un lien symbolique vers le certificat d'authentification de clients dans 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 des journaux d'audit.

   La valeur de **Connection Timeout** peut affecter la configuration. Si la configuration met plus de temps à répondre que la valeur définie, cela peut entraîner un échec de la configuration en raison d'une erreur de connexion. Pour établir une connexion réussie, augmentez la valeur de **Connection Timeout** et réessayez la configuration.

Utilisez la page d'authentification à distance dans Active IQ Unified Manager

Vous pouvez utiliser la page Authentification à distance pour configurer Unified Manager afin qu'il communique avec votre serveur d'authentification pour authentifier les utilisateurs distants qui tentent de se connecter à la web UI de Unified Manager.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Après avoir coché la case « Activer l'authentification à distance », vous pouvez activer l'authentification à distance à l'aide d'un serveur d'authentification.

- **Service d'authentification**

  Permet de configurer le serveur d'administration pour authentifier les utilisateurs via des fournisseurs de services d'annuaire, tels qu'Active Directory ou OpenLDAP, ou de spécifier votre propre mécanisme d'authentification. Vous pouvez spécifier un service d'authentification uniquement si l'authentification à distance est activée.

  - **Active Directory**
    - Nom de l'administrateur

      Spécifie le nom de l'administrateur du serveur d'authentification.

    - Mot de passe

      Spécifie le mot de passe pour accéder au serveur d'authentification.

    - Nom distinctif de base

      Spécifie l'emplacement des utilisateurs distants sur le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.

    - Désactiver la recherche de groupes imbriqués

      Indique si l'option de recherche de groupes imbriqués doit être activée ou désactivée. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

    - Utiliser une connexion sécurisée

Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

- **OpenLDAP**
  - Nom unique de liaison

    Spécifie le nom unique de liaison utilisé avec le nom unique de base pour trouver les utilisateurs distants sur le serveur d'authentification.

  - Mot de passe de liaison

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom distinctif de base

    Spécifie l'emplacement des utilisateurs distants sur le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.

  - Utiliser une connexion sécurisée

    Indique que le protocole LDAP sécurisé est utilisé pour communiquer avec les serveurs d'authentification LDAP.

- **Autres**
  - Nom unique de liaison

    Spécifie le nom unique de liaison utilisé avec le nom unique de base pour trouver les utilisateurs distants sur le serveur d'authentification que vous avez configuré.

  - Mot de passe de liaison

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom distinctif de base

    Spécifie l'emplacement des utilisateurs distants sur le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.

  - Version du protocole

    Spécifie la version du protocole LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez indiquer si la version du protocole doit être détectée automatiquement ou définir la version sur 2 ou 3.

  - Attribut de nom d'utilisateur

    Spécifie le nom de l'attribut du serveur d'authentification contenant les noms de connexion des utilisateurs que le serveur de gestion doit authentifier.

  - Attribut d'appartenance à un groupe

    Spécifie une valeur qui attribue l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut et d'une valeur spécifiés dans le serveur d'authentification de

l'utilisateur.

- UGID

  Si les utilisateurs distants sont inclus en tant que membres d'un objet GroupOfUniqueNames dans le serveur d'authentification, cette option vous permet d'attribuer l'appartenance au groupe du serveur de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet GroupOfUniqueNames.

- Désactiver la recherche de groupes imbriqués

  Indique si l'option de recherche de groupes imbriqués doit être activée ou désactivée. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Membre

  Spécifie le nom de l'attribut que votre serveur d'authentification utilise pour stocker les informations relatives aux membres individuels d'un groupe.

- Classe d'objet utilisateur

  Spécifie la classe d'objet d'un utilisateur sur le serveur d'authentification distant.

- Classe d'objet de groupe

  Spécifie la classe d'objet de tous les groupes sur le serveur d'authentification distant.

  Les valeurs que vous saisissez 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 risque d'échouer.

- Utiliser une connexion sécurisée

  Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

  Si vous souhaitez modifier le service d'authentification, veillez à supprimer tous les serveurs d'authentification existants et à ajouter de nouveaux serveurs d'authentification.

Zone des serveurs d'authentification

La section 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 à haute disponibilité (utilisant la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsqu'un des serveurs d'authentification

est injoignable.

- 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 de l'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 des tests, si vous ne spécifiez que le nom d'utilisateur, le serveur de gestion recherche l'utilisateur distant sur le serveur d'authentification, mais ne l'authentifie pas. Si vous spécifiez à la fois le nom d'utilisateur et le mot de passe, le serveur de gestion recherche et authentifie l'utilisateur distant.

  Vous ne pouvez pas tester l'authentification si l'authentification à distance est désactivée.

Gérer les certificats de sécurité

Consultez le certificat de sécurité HTTPS dans Active IQ Unified Manager

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.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

L'affichage du certificat vous permet de vérifier le contenu d'un certificat régénéré ou d'afficher les noms alternatifs du sujet (SAN) à partir desquels vous pouvez accéder à Unified Manager.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.

   Le certificat HTTPS est affiché en haut de la page

Si vous souhaitez consulter des informations plus détaillées sur le certificat de sécurité que celles affichées sur la page du certificat HTTPS, vous pouvez visualiser le certificat de connexion dans votre navigateur.

Téléchargez une demande de signature de certificat HTTPS dans Active IQ Unified Manager

Vous pouvez télécharger une demande de signature de certificat pour le certificat de sécurité HTTPS actuel afin de fournir le fichier à une autorité de certification pour qu'elle le signe. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l'homme du milieu et offre une meilleure protection de sécurité qu'un certificat autosigné.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Télécharger la demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

Vous pouvez soumettre le fichier à une autorité de certification pour qu'elle le signe, puis installer le certificat signé.

Installez un certificat HTTPS signé par une autorité de certification dans Active IQ Unified Manager

Vous pouvez téléverser et installer un certificat de sécurité après qu'une autorité de certification l'a signé et renvoyé. Le fichier que vous téléversez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification aide à prévenir les attaques de type man-in-the-middle et offre une meilleure protection de sécurité qu'un certificat auto-signé.

*Quoi .Avant de commencer

Vous devez avoir effectué les actions suivantes :

- Téléchargement du fichier de demande de signature de certificat et signature par une autorité de certification
- Chaîne de certificats enregistrée au format PEM
- Inclure tous les certificats de la chaîne, du certificat de serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

Vous devez posséder le rôle d'administrateur d'application.

Si la durée de validité du certificat pour lequel une CSR a été créée est supérieure à 397 jours, elle sera ramenée à 397 jours par la CA avant de signer et de renvoyer le certificat

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Installer le certificat HTTPS**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir un fichier…** pour localiser le fichier à

télécharger.

4. Sélectionnez le fichier, puis cliquez sur **Installer** pour l'installer.

   Pour plus d'informations, consultez "Installation d'un certificat HTTPS généré à l'aide d'outils externes".

Exemple de chaîne de certificats

L'exemple suivant montre à quoi peut ressembler un fichier de chaîne de certificats :

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Découvrez les certificats HTTPS générés à l'aide d'outils externes dans Active IQ Unified Manager Unified Manager

Vous pouvez installer des certificats auto-signés ou signés par une autorité de certification et générés à l'aide d'un outil externe comme OpenSSL, BoringSSL, LetsEncrypt.

Vous devez charger la clé privée avec la chaîne de certificats, car ces certificats sont des paires de clés publique/privée générées en externe. Les algorithmes de paires de clés autorisés sont "RSA" et "EC". L'option **Installer le certificat HTTPS** est disponible sur la page Certificats HTTPS, dans la section Général. Le fichier que vous téléchargez doit respecter 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. Certificats des autorités de certification (AC) en ordre inverse jusqu'à la racine, utilisés pour signer le certificat ci-dessus

Format pour charger un certificat avec une paire de clés EC

Les courbes autorisées sont « `prime256v1` » et « `secp384r1` ». Exemple de certificat avec une paire EC générée en externe :

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
```

```
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Format pour charger 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 soient prises en compte.

Vérifications lors du chargement de certificats générés en externe

Le système effectue des vérifications lors du chargement d'un certificat généré à l'aide d'outils externes. Si l'une de ces vérifications échoue, le certificat est rejeté. Des validations sont également incluses pour les certificats générés à partir de la CSR au sein du produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée fournie en entrée est validée par rapport au certificat de l'hôte fourni en entrée.
- Le nom commun (CN) du certificat de l'hôte est comparé au nom de domaine complet (FQDN) de l'hôte.
- Le nom commun (CN) du certificat de l'hôte ne doit pas être vide ou blanc et ne doit pas être défini sur localhost.
- La date de début de validité ne doit pas être dans le futur et la date d'expiration de validité du certificat ne doit pas être dans le passé.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être dans le futur et la date d'expiration de validité ne doit pas être dans le passé.

La clé privée fournie en entrée ne doit pas être chiffrée. Si des clés privées sont chiffrées, elles sont rejetées par le système.

Exemple 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemple 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemple 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Si l'installation du certificat échoue, consultez l'article de la base de connaissances (KB) : "ActiveIQ Unified Manager ne parvient pas à installer un certificat généré en externe"

Descriptions des pages pour la gestion des certificats

Découvrez la page relative au certificat HTTPS dans Active IQ Unified Manager

La page Certificat HTTPS vous permet de consulter 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 celui qui a été généré lors de l’installation.

Boutons de commande

Les boutons de commande vous permettent d’effectuer les opérations suivantes :

- **Télécharger la demande de signature de certificat HTTPS**

  Télécharge une demande de certification pour le certificat HTTPS actuellement installé. Votre navigateur vous invite à enregistrer le fichier <hostname>.csr afin que vous puissiez fournir le fichier à une autorité de certification pour signature.

- **Installer le certificat HTTPS**

  Permet de télécharger et d’installer un certificat de sécurité après sa signature et son renvoi par une autorité de certification. Le nouveau certificat prend effet après le redémarrage du serveur d’administration.

- **Régénérer le certificat HTTPS**

  Permet de générer un nouveau certificat HTTPS auto-signé, qui remplace le certificat de sécurité actuel. Le nouveau certificat prend effet après le redémarrage d’Unified Manager.

Boîte de dialogue « Régénérer un certificat HTTPS » dans Active IQ Unified Manager

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 relatives au certificat actuel figurent sur cette page.

Les options « `Regenerate Using Current Certificate Attributes` » et « `Update the Current Certificate Attributes` » 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 à haute disponibilité d’Unified Manager, utilisez l’adresse IP virtuelle.

- **E-mail**

  Facultatif. Une adresse électronique pour contacter votre organisation ; généralement l’adresse électronique de l’administrateur du certificat ou du service informatique.

- **Entreprise**

  Facultatif. Généralement, la dénomination sociale de votre entreprise.

- **Département**

  Facultatif. Le nom du département au sein de votre entreprise.

- **Ville**

Facultatif. La ville où se situe votre entreprise.

- **État**

  Facultatif. Indiquez, en toutes lettres, l'État ou la province où se situe votre entreprise.

- **Pays**

  Facultatif. Le pays où est située votre entreprise. Il s'agit généralement du code ISO à deux lettres du pays.

- **Autres noms**

  Obligatoire. Noms de domaine supplémentaires, non principaux, pouvant être utilisés pour accéder à ce serveur en plus de localhost existant ou d'autres adresses réseau. Séparez chaque nom alternatif par une virgule.

  Cochez la case « Exclure les informations d'identification locales (par exemple localhost) » si vous souhaitez supprimer les informations d'identification locales du champ « Autres noms » du certificat. Lorsque cette case est cochée, seules les informations que vous saisissez dans le champ sont utilisées dans le champ « Autres noms ». Si le champ est laissé vide, le certificat obtenu ne comportera aucun champ « Autres noms ».

- **TAILLE DE LA CLÉ (ALGORITHME DE CLÉ: RSA)**

  L'algorithme de clé est défini sur RSA. Vous pouvez sélectionner l'une des tailles de clé suivantes : 2048, 3072 ou 4096 bits. La taille de clé par défaut est définie sur 2048 bits.

- **PÉRIODE DE VALIDITÉ**

  La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau depuis une version précédente, il est possible que la validité du certificat précédent reste inchangée.

Pour plus d'informations, consultez "Génération de certificats HTTPS".

Surveiller et gérer le stockage

Introduction à Active IQ Unified Manager

Découvrez Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) vous permet de surveiller et de gérer l'état et les performances de vos systèmes de stockage ONTAP à partir d'une interface unique.

Unified Manager offre les fonctionnalités suivantes :

- Découverte, surveillance et notifications pour les systèmes équipés du logiciel ONTAP.
- Tableau de bord permettant d'afficher la capacité, la sécurité et l'état des performances de l'environnement.
- Infrastructure améliorée pour les alertes, les événements et les seuils.
- Affiche des graphiques détaillés qui représentent l'activité du workload au fil du temps, notamment les IOPS (opérations), les MBps (débit), la latence (temps de réponse), l'utilisation, la capacité de performance et le taux de cache.
- Identifie les workloads qui utilisent excessivement les composants du cluster et ceux dont les performances sont affectées par l'augmentation de l'activité.
- Il fournit des actions correctives suggérées qui peuvent être effectuées pour remédier à certains incidents et événements, ainsi qu'un bouton « Fix It » pour certains événements afin que vous puissiez résoudre le problème immédiatement.
- S'intègre à OnCommand Workflow Automation pour exécuter des workflows de protection automatisés.
- Possibilité de créer de nouveaux workloads, tels qu'un LUN ou un partage de fichiers, directement depuis Unified Manager et d'attribuer un Performance Service Level pour définir les objectifs de performance et de stockage pour les utilisateurs accédant à l'application à l'aide de ce workload.

Découvrez la surveillance de l'état de santé dans Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous permet de superviser un grand nombre de systèmes exécutant le logiciel ONTAP via une interface utilisateur centralisée. L'infrastructure serveur d'Unified Manager offre une évolutivité, une facilité de maintenance et des fonctionnalités avancées de surveillance et de notification.

Les principales fonctionnalités d'Unified Manager incluent la surveillance, l'émission d'alertes, la gestion de la disponibilité et de la capacité des clusters, la gestion des fonctionnalités de protection, ainsi que le regroupement des données de diagnostic et leur envoi à l'assistance technique.

Vous pouvez utiliser Unified Manager pour surveiller vos clusters. Lorsque des problèmes surviennent dans le cluster, Unified Manager vous informe des détails de ces problèmes par le biais d'événements. Certains événements vous proposent également une action corrective que vous pouvez entreprendre pour résoudre les problèmes. Vous pouvez configurer des alertes pour les événements afin que, lorsque des problèmes surviennent, vous soyez averti par e-mail et par traps SNMP.

Vous pouvez utiliser Unified Manager pour gérer les objets de stockage de votre environnement en les

associant à des annotations. Vous pouvez créer des annotations personnalisées et associer dynamiquement des clusters, des machines virtuelles de stockage (SVM), et des volumes à ces annotations via des règles.

Vous pouvez également planifier les besoins de stockage de vos objets de cluster à l'aide des informations fournies dans les graphiques de capacité et de santé pour l'objet de cluster correspondant.

Capacité physique et logique

Unified Manager utilise les concepts d'espace physique et d'espace logique pour les objets de stockage ONTAP.

- Capacité physique : l'espace physique désigne les blocs de stockage physiques utilisés dans le volume. La « capacité physique utilisée » est généralement inférieure à la capacité logique utilisée en raison de la réduction des données due aux mécanismes d'optimisation du stockage (tels que la déduplication et la compression).
- Capacité logique : l'espace logique désigne l'espace utilisable (les blocs logiques) dans un volume. L'espace logique indique comment l'espace théorique peut être utilisé, sans tenir compte des résultats de la déduplication ou de la compression. « Espace logique utilisé » correspond à l'espace physique utilisé plus les économies réalisées grâce aux fonctionnalités d'efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure apparaît souvent plus élevée que la capacité physique utilisée, car elle ne reflète pas la compression des données ni les autres réductions de l'espace physique. Ainsi, la capacité logique totale peut être supérieure à l'espace provisionné.

Unités de mesure de capacité

Unified Manager calcule la capacité de stockage sur la base d'unités binaires de 1024 (2^{10}) octets. Dans ONTAP 9.10.0 et les versions antérieures, ces unités étaient affichées sous la forme KB, MB, GB, TB et PB. À partir de ONTAP 9.10.1, elles sont affichées dans Unified Manager sous la forme KiB, MiB, GiB, TiB et PiB.

Les unités utilisées pour le débit restent les kilooctets par seconde (Kbps), les mégaoctets par seconde (Mbps), les gigaoctets par seconde (Gbps) ou les téraoctets par seconde (Tbps), etc., pour toutes les versions de 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

Découvrez la surveillance des performances dans Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) offre des fonctionnalités de surveillance des performances et d'analyse des causes profondes des événements pour les systèmes exécutant le logiciel ONTAP de NetApp.

Unified Manager vous aide à identifier les workloads qui sollicitent excessivement les composants du cluster et dégradent les performances des autres workloads sur le cluster. En définissant des politiques de seuil de performance, vous pouvez également spécifier des valeurs maximales pour certains compteurs de performance afin que des événements soient générés lorsque le seuil est dépassé. Unified Manager vous alerte de ces événements de performance afin que vous puissiez prendre des mesures correctives et rétablir les performances à un niveau de fonctionnement normal. Vous pouvez consulter et analyser les événements dans l'interface utilisateur de Unified Manager.

Unified Manager surveille les performances de deux types de workloads :

- Workloads définis par l'utilisateur

  Ces workloads se composent de volumes FlexVol et de volumes FlexGroup que vous avez créés dans votre cluster.

- Charges de travail définies par le système

  Ces charges de travail se composent d'une activité interne au système.

Utilisez les API REST d'Active IQ Unified Manager

Active IQ Unified Manager met à votre disposition des API REST pour consulter les informations relatives à la surveillance et à la gestion de votre environnement de stockage. Ces API permettent également le provisionnement et la gestion des objets de stockage en fonction de stratégies.

Vous pouvez également exécuter les API ONTAP sur tous les clusters gérés par ONTAP à l'aide de la passerelle API prise en charge par Unified Manager.

Pour plus d'informations sur les API REST d'Unified Manager, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

Que fait le serveur Unified Manager

Découvrez le serveur Active IQ Unified Manager

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

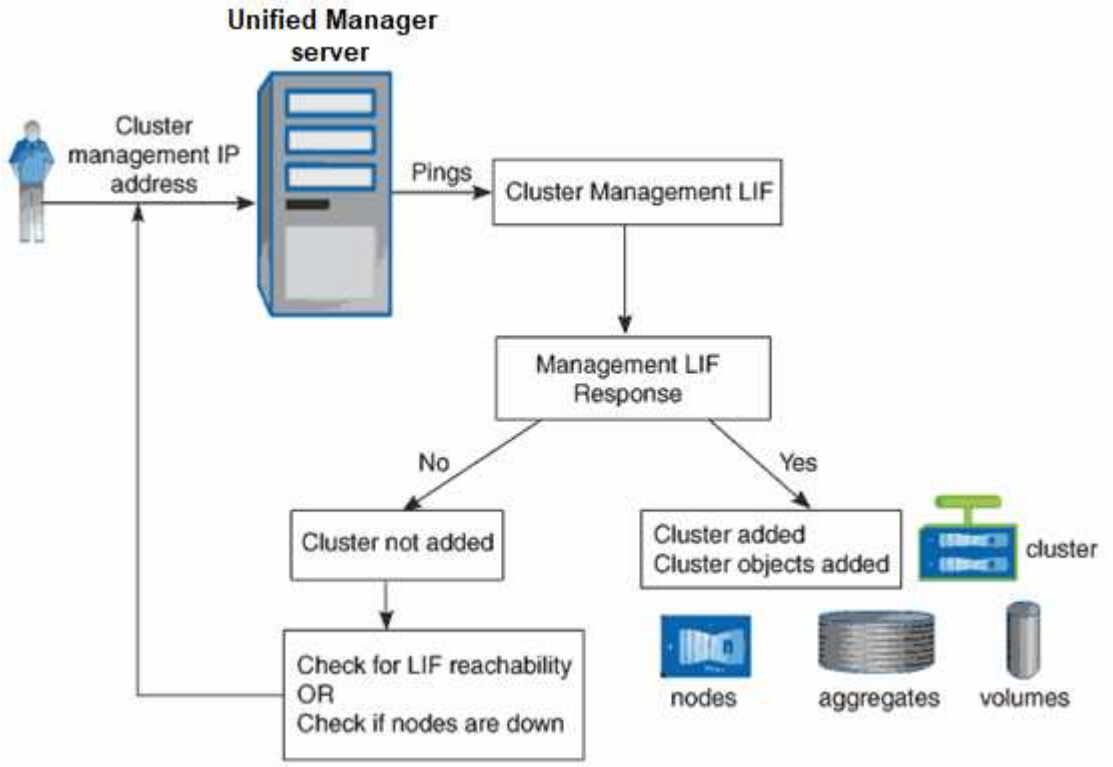
Unified Manager collecte les informations du cluster, stocke les données dans la base de données et les analyse pour détecter d'éventuels problèmes au niveau du cluster.

Découvrez comment fonctionne le processus de découverte de clusters dans Active IQ Unified Manager

Une fois que vous avez ajouté le cluster à Unified Manager, le serveur détecte les objets du cluster et les ajoute à sa base de données. Comprendre le fonctionnement du processus de détection vous aide à gérer les clusters de votre organisation et leurs objets.

L'intervalle de surveillance par défaut est de 15 minutes : si vous avez ajouté un cluster au serveur Unified Manager, l'affichage des détails du cluster dans l'interface utilisateur d'Unified Manager prend 15 minutes.

L'image suivante illustre le processus de découverte dans Active IQ Unified Manager :



Comprendre l'interface utilisateur

Découvrez l'interface utilisateur de Active IQ Unified Manager

L'interface utilisateur d'Unified Manager se compose principalement d'un tableau de bord offrant une vue d'ensemble des objets surveillés. Elle permet également d'accéder à la visualisation de tous les objets du cluster.

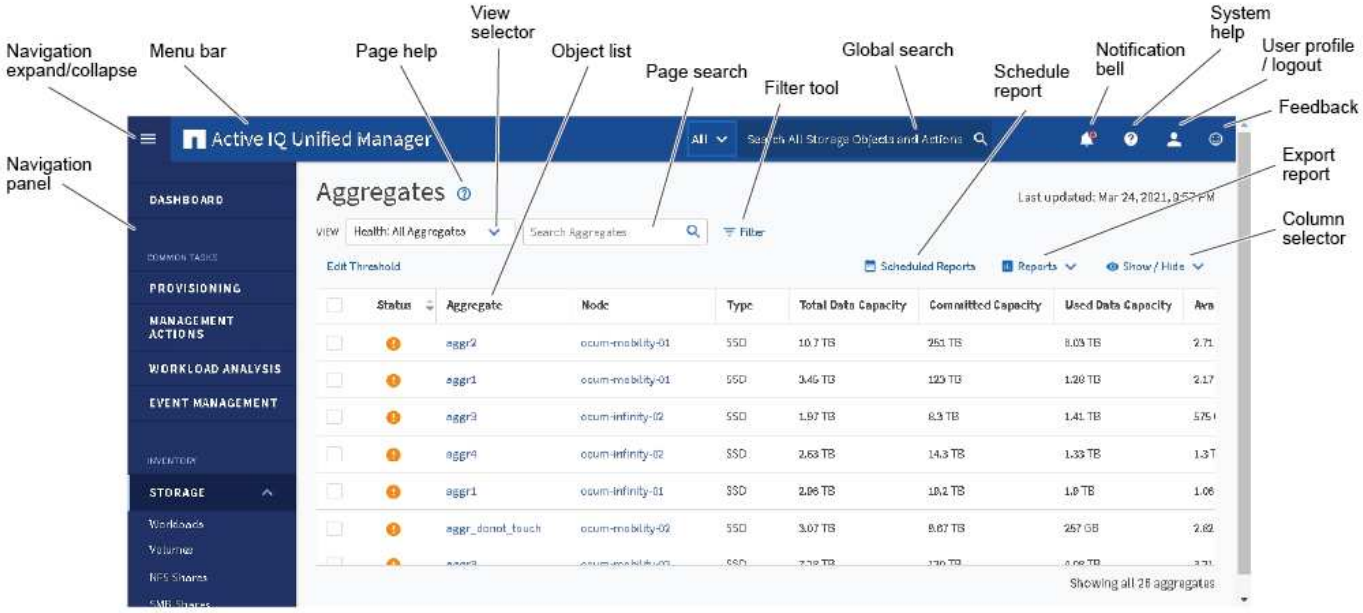
Vous pouvez sélectionner une vue préférée et utiliser les boutons d'action selon vos besoins. Votre configuration d'écran est enregistrée dans un espace de travail afin que toutes les fonctionnalités dont vous avez besoin soient disponibles lorsque vous démarrez Unified Manager. Toutefois, lorsque vous passez d'une vue à une autre, puis revenez à la vue précédente, il est possible que la vue ne soit pas la même.

Agencements de fenêtres typiques dans Active IQ Unified Manager

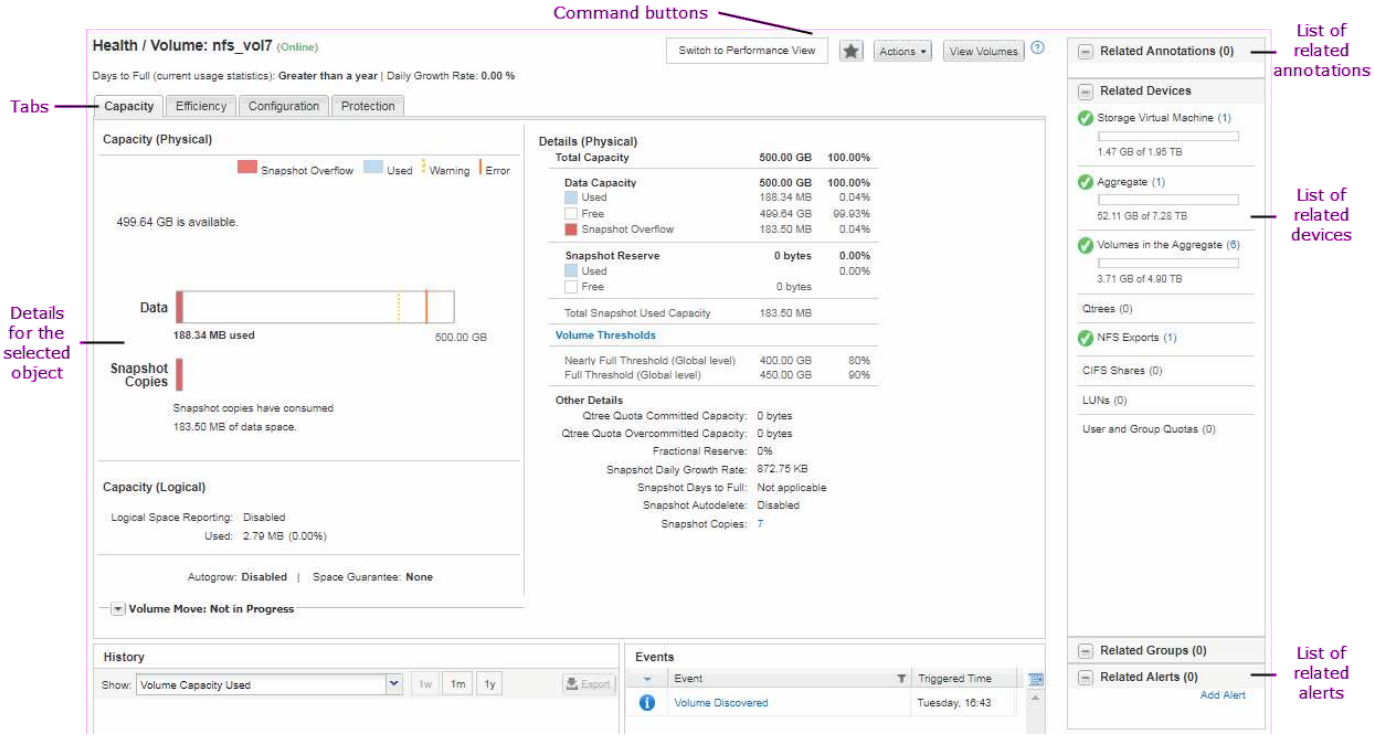
Comprendre la disposition type des fenêtres vous aide à naviguer et à utiliser Active IQ Unified Manager efficacement. La plupart des fenêtres de Unified Manager sont similaires à l'une des deux dispositions générales suivantes : liste d'objets ou détails. Le paramètre d'affichage recommandé est d'au 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 des détails de l'objet



Personnalisation de la disposition des fenêtres dans Active IQ Unified Manager

Active IQ Unified Manager vous permet de personnaliser la mise en page des informations sur les pages des objets de stockage et de réseau. En personnalisant les fenêtres, vous pouvez contrôler les données visibles et leur mode d'affichage.

- **Tri**

Vous pouvez cliquer sur l'en-tête de colonne pour modifier l'ordre de tri des entrées de la 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 et personnaliser l'affichage des informations sur les pages des objets de stockage et de réseau afin que seules les entrées correspondant aux conditions spécifiées soient affichées. Vous appliquez les filtres depuis le volet Filtres.

  Le volet Filtres vous permet de filtrer la plupart des colonnes en fonction des options sélectionnées. Par exemple, dans la vue Health: All Volumes, vous pouvez utiliser le volet Filtres pour afficher tous les volumes hors ligne en sélectionnant l'option de filtre appropriée sous State.

  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 dans la colonne Total Data Capacity de la vue Health: All Aggregates pour filtrer les données supérieures à 20.45 GB, la capacité réelle de 20.454 GB s'affiche comme 20.45 GB. De même, si vous filtrez les données inférieures à 20.45 GB, la capacité réelle de 20.449 GB s'affiche comme 20.45 GB.

  Si vous utilisez le filtre de la colonne « Pourcentage de données disponibles » dans la vue « Santé : Tous les agrégats » pour filtrer les données supérieures à 20,45 %, la capacité réelle de 20,454 % s'affiche comme 20,45 %. De même, si vous filtrez les données inférieures à 20,45 %, la capacité réelle de 20,449 % s'affiche comme 20,45 %.

- **Afficher ou masquer les colonnes**

  Vous pouvez cliquer sur l'icône d'affichage des colonnes (**Afficher/Masquer**) pour sélectionner les colonnes à afficher. Une fois les colonnes sélectionnées, vous pouvez les réorganiser en les faisant glisser avec la souris.

- **Recherche**

  Vous pouvez utiliser le champ de recherche pour rechercher certains attributs d'objet afin d'affiner la liste des éléments dans la page d'inventaire. Par exemple, vous pouvez saisir « cloud » pour affiner la liste des volumes dans la page d'inventaire des volumes et afficher tous les volumes contenant le mot « cloud ».

- **Exportation des données**

  Vous pouvez cliquer sur le bouton **Rapports** (ou sur le bouton **Exporter** pour exporter les données vers un fichier de valeurs séparées par des virgules `(.csv)`, `(.pdf)` un document ou un fichier Microsoft Excel `(.xlsx)` et utiliser les données exportées pour créer des rapports).

Utilisez l'aide d'Active IQ Unified Manager

L'aide contient des informations sur toutes les fonctionnalités incluses dans Active IQ Unified Manager. Vous pouvez utiliser la table des matières, l'index ou l'outil de recherche pour trouver des informations sur les fonctionnalités et leur utilisation.

L'aide est disponible dans chaque onglet et dans la barre de menus de l'interface utilisateur Unified Manager.

L'outil de recherche de l'aide ne fonctionne pas pour les mots partiels.

- Pour en savoir plus sur des champs ou des paramètres spécifiques, cliquez sur .
- Pour afficher tout le contenu de l'Aide, cliquez sur > **Aide/Documentation** dans la barre de menu.

  Vous trouverez des informations plus détaillées en développant n'importe quelle partie de la table des matières dans le volet de navigation.

- Pour rechercher dans le contenu de l'aide, cliquez sur l'onglet **Search** dans le volet de navigation, saisissez le mot ou la série de mots que vous souhaitez trouver, puis cliquez sur **Go!**.
- Pour imprimer les rubriques d'aide, cliquez sur l'icône d'imprimante.

Ajoutez vos rubriques d'aide favorites à vos favoris dans Active IQ Unified Manager

Dans l'onglet Favoris de l'aide, vous pouvez ajouter à vos favoris les rubriques d'aide que vous consultez fréquemment. Les signets d'aide permettent d'accéder rapidement à vos rubriques favorites.

Étapes

1. Accédez à la rubrique d'aide que vous souhaitez ajouter à vos favoris.
2. Cliquez sur **Favoris**, puis sur **Ajouter**.

Rechercher des objets de stockage dans Active IQ Unified Manager

Pour accéder rapidement à un objet spécifique, vous pouvez utiliser le champ **Rechercher dans tous les objets de stockage** en haut de la barre de menu. Cette méthode de recherche globale dans tous les objets vous permet de localiser rapidement des objets spécifiques par type. Les résultats de la recherche sont triés par type d'objet de stockage, et vous pouvez les filtrer davantage par objet à l'aide du menu déroulant.

Avant de commencer

- Vous devez disposer de l'un des rôles suivants pour effectuer cette tâche : Operator, Application Administrator ou Storage Administrator.
- Une recherche valide doit contenir au moins trois caractères.

Lorsque vous sélectionnez « Tous » dans le menu déroulant, la recherche globale affiche le nombre total de résultats trouvés dans toutes les catégories d'objets, avec un maximum de 25 résultats de recherche pour chaque catégorie d'objets. Vous pouvez sélectionner un type d'objet spécifique dans le menu déroulant pour affiner la recherche au sein d'un type d'objet spécifique. Dans ce cas, la liste renvoyée n'est pas limitée aux 25 premiers objets.

Les types d'objets que vous pouvez rechercher incluent :

- Groupes
- Nœuds
- Machines virtuelles de stockage
- Agrégats
- Volumes

- Qtrees
- Partages SMB
- Partages NFS
- Quotas d'utilisateurs ou de groupes
- LUN
- Espaces de noms NVMe
- Groupes d'initiateurs
- Initiateurs
- Groupe de cohérence

La saisie d'un nom de workload renvoie la liste des workloads dans la catégorie Volumes ou LUNs appropriée.

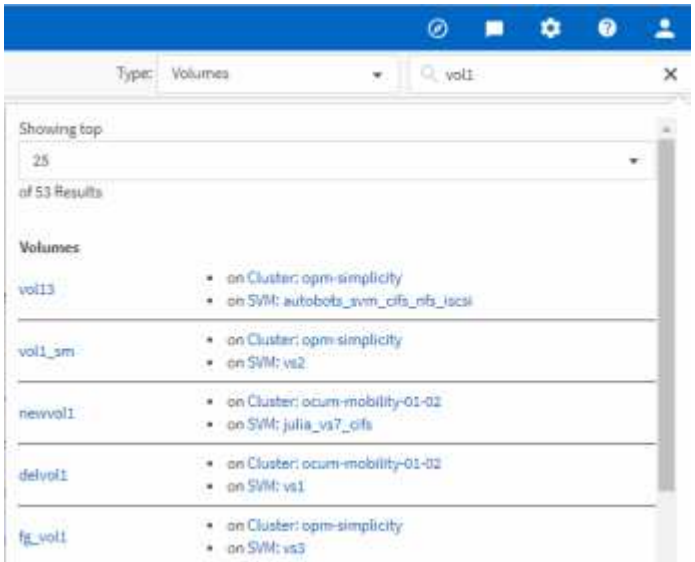
Vous pouvez cliquer sur n'importe quel objet dans les résultats de recherche pour accéder à la page de détails de l'état de cet objet. S'il n'existe pas de page d'état directe pour un objet, la page d'état de l'objet parent s'affiche. Par exemple, lorsque vous recherchez un LUN spécifique, la page de détails du SVM sur lequel réside ce LUN s'affiche.

Les ports et les LIF ne peuvent pas être recherchés dans la barre de recherche globale.

Étapes

1. Sélectionnez un type d'objet dans le menu pour affiner les résultats de la recherche et n'afficher que ce type d'objet.
2. Saisissez au minimum 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 liste déroulante. Lorsque vous saisissez « vol1 » dans le champ **Rechercher tous les objets de stockage**, la liste de tous les volumes dont le nom contient ces caractères s'affiche.



Exportez les données de stockage sous forme de rapports dans Active IQ Unified Manager

Vous pouvez exporter les données de stockage dans différents 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 de la gestion des événements afin de créer un rapport, puis l'envoyer aux administrateurs qui pourront résoudre les problèmes.

Vous pouvez exporter des données vers un fichier `.csv`, un fichier `.xlsx` ou un document `.pdf` depuis les pages d'inventaire **Storage** et **Network**, puis utiliser les données exportées pour créer des rapports. Il existe d'autres emplacements dans le produit où seuls des fichiers `.csv` ou `.pdf` peuvent être générés.

Étapes

1. Effectuez l'une des actions suivantes :

Si vous souhaitez exporter…	Faites ceci…
Détails de l'inventaire des objets de stockage	Dans le menu de navigation de gauche, cliquez sur **Stockage** ou **Réseau**, puis sélectionnez un objet de stockage. Choisissez l'une des vues fournies par le système, ou toute vue personnalisée que vous avez créée.
Détails du groupe de stratégie QoS	Cliquez sur **Stockage** > **QoS Policy Groups** dans le menu de navigation de gauche.
Détails sur la capacité de stockage et l'historique de protection	Cliquez sur **Storage** > **Aggregates** ou **Storage** > **Volumes**, puis sélectionnez un seul agrégat ou volume.
Détails de l'événement	Cliquez sur **Gestion des événements** dans le menu de navigation de gauche.
Détails des 10 principales performances de l'objet de stockage	Cliquez sur **Storage** > **Clusters** > **Performance:All Clusters**, puis sélectionnez un cluster et choisissez l'onglet **Top Performers**. Sélectionnez ensuite un objet de stockage et un compteur de performances.

2. Cliquez sur le bouton **Reports** (ou sur le bouton **Export** sur certaines pages UI).
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 unique que vous consultez ou pour tous les clusters du centre de données.

   Le fichier a été téléchargé.

4. Ouvrez le fichier dans l'application appropriée.

Informations connexes

"page d'inventaire Santé/Clusters"

"Planifier un rapport"

Filtrer le contenu de la page d'inventaire dans Active IQ Unified Manager

Dans Unified Manager, vous pouvez filtrer les données des pages d'inventaire pour localiser rapidement les données selon des critères spécifiques. Le filtrage vous permet d'affiner le contenu des pages d'Unified Manager et de n'afficher que les résultats qui vous intéressent. C'est une méthode très efficace pour afficher uniquement les données qui vous intéressent.

Utilisez **Filtering** pour personnaliser la vue de la grille selon vos préférences. Les options de filtre disponibles dépendent du type d'objet affiché dans la grille. Si des filtres sont actuellement appliqués, le nombre de filtres appliqués s'affiche à droite du bouton Filter.

Trois types de paramètres de filtrage sont pris en charge.

Paramètre	Validation
Chaîne (texte)	Les opérateurs sont **contient**, **commence par**, **se termine par** et **ne contient pas**.
Nombre maximum	Les opérateurs sont **supérieur à**, **inférieur à**, **au cours des derniers** et **entre**.
Énumération (texte)	Les opérateurs sont **is** et **is not**.

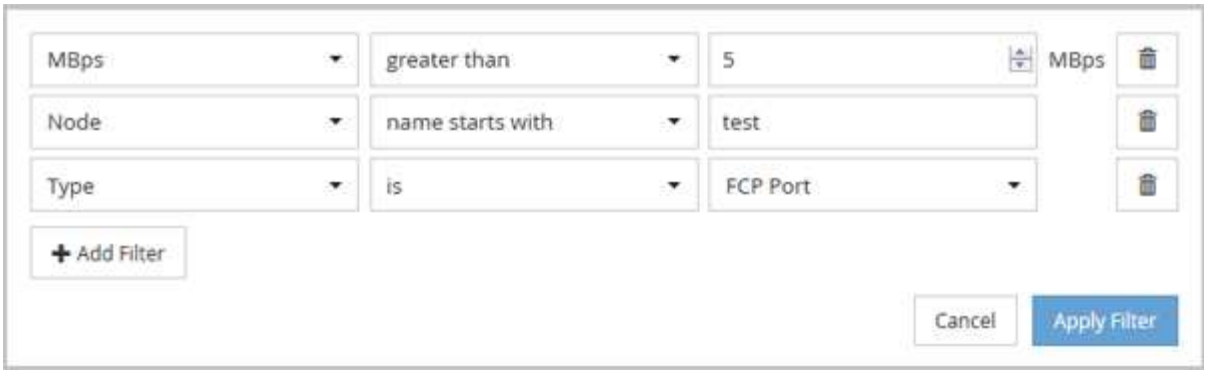
Les champs Colonne, Opérateur et Valeur sont obligatoires pour chaque filtre ; les filtres disponibles correspondent aux colonnes filtrables de la page actuelle. Vous pouvez appliquer jusqu'à quatre filtres. Les résultats filtrés sont basés sur la combinaison des paramètres de filtrage. Les résultats filtrés s'appliquent à toutes les pages de votre recherche filtrée, et pas seulement à la page actuellement affichée.

Vous pouvez ajouter des filtres à l'aide du panneau de filtrage.

1. En haut de la page, cliquez sur le bouton **Filtrer**. Le panneau de filtrage s'affiche.
2. Cliquez sur la liste déroulante de gauche et sélectionnez un objet; par exemple, *Cluster*, ou un compteur de performances.
3. Cliquez sur la liste déroulante centrale et sélectionnez l'opérateur que vous souhaitez utiliser.
4. Dans la dernière liste, sélectionnez ou saisissez une valeur pour compléter le filtre pour cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Add Filter**. Un champ de filtre supplémentaire s'affiche. Complétez ce filtre en suivant la procédure décrite dans les étapes précédentes. Notez qu'après l'ajout de votre quatrième filtre, le bouton **+Add Filter** 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 de filtrage pour supprimer des filtres individuels en cliquant sur l'icône de la 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 de filtrage avec trois filtres. Le bouton **+Ajouter un filtre** s'affiche lorsque vous avez moins du maximum de quatre filtres.



Après avoir cliqué sur **Appliquer le filtre**, le panneau de filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Consultez les événements actifs à partir de la cloche de notification dans Active IQ Unified Manager

La cloche de notification ( ) dans la barre de menu offre un moyen rapide de visualiser 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'erreurs, d'avertissements et de mises à niveau sur tous les clusters. Cette liste inclut les événements des 7 derniers jours, à l'exclusion des 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 cette information sur cette page. Vous pouvez consulter 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 liés à l'évolutivité, tels qu'un espace disque ou une mémoire vive insuffisants sur le poste de gestion, sont également affichés sur cette page.

Étapes

1. Dans la barre de menu, cliquez sur .
2. Pour afficher les détails de l'un des événements actifs, cliquez sur le lien de texte de l'événement, tel que « 2 Capacité » ou « 4 Performance ».

Surveillez et gérez les clusters depuis le tableau de bord

Surveillez et gérez les clusters depuis le tableau de bord dans Active IQ Unified Manager

Le tableau de bord fournit des informations cumulatives en un coup d'œil sur l'état de santé actuel de vos systèmes ONTAP surveillés. Le tableau de bord fournit des "panels" qui vous permettent d'évaluer l'état global de la capacité, des performances et de la sécurité des clusters que vous surveillez.

De plus, certains problèmes ONTAP peuvent être résolus directement depuis l'interface utilisateur de Unified Manager au lieu d'utiliser ONTAP System Manager ou l'interface de ligne de commande ONTAP.

En haut du tableau de bord, vous pouvez choisir d'afficher les informations pour tous les clusters surveillés ou

pour un cluster en particulier. Vous pouvez commencer par consulter l'état de tous les clusters, puis passer à des clusters individuels lorsque vous souhaitez afficher des informations détaillées.

Certains des panneaux répertoriés ci-dessous peuvent ne pas apparaître sur la page en fonction de votre configuration.

Panneaux	Description
Actions de gestion	Lorsque Unified Manager peut diagnostiquer un problème et déterminer une solution unique, cette solution est affichée dans ce panneau avec un bouton **Corriger**.
Capacité	Affiche la capacité totale et utilisée pour le niveau local et le niveau cloud, ainsi que le nombre de jours avant que la capacité locale n'atteigne la limite supérieure.
Capacité de performance	Affiche la valeur de capacité de performance pour chaque cluster et le nombre de jours restants avant que cette capacité n'atteigne la limite supérieure.
IOPS du workload	Affiche le nombre total de workloads actuellement exécutés dans une certaine plage d'IOPS.
Performances du workload	Affiche le nombre total de workloads conformes et non conformes affectés à chaque niveau de service de performance défini.
Sécurité	Affiche le nombre de clusters conformes ou non conformes, le nombre de SVM conformes ou non conformes et le nombre de volumes chiffrés ou non chiffrés.
Protection	Affiche le nombre de machines virtuelles de stockage protégées par une relation SVM-DR, de volumes protégés par une relation SnapMirror, de volumes protégés par Snapshot et de clusters protégés par MetroCluster.
Aperçu de l'utilisation	Affiche les clusters triés par nombre d'IOPS le plus élevé, débit le plus élevé (MBps) ou capacité physique utilisée la plus élevée.

Découvrez la page du tableau de bord Active IQ Unified Manager

La page Tableau de bord comporte des « panneaux » qui affichent un aperçu général de la capacité, des performances et de l'état 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, ainsi que le nombre de nouveaux événements ajoutés au cours des 24 dernières heures. Ces informations vous aident à déterminer quels clusters vous devrez peut-être analyser plus en détail pour résoudre les événements. En cliquant sur les événements, vous affichez les principaux événements et obtenez un lien vers la page d'inventaire Event Management filtrée pour afficher les événements actifs de cette catégorie.

En haut du tableau de bord, vous pouvez choisir d'afficher les informations pour tous les clusters surveillés (« Tous les clusters ») ou pour un cluster spécifique. Vous pouvez commencer par consulter l'état de tous les clusters, puis approfondir jusqu'aux clusters individuels lorsque vous souhaitez afficher des informations détaillées.

Certains des panneaux répertoriés ci-dessous apparaissent sur le tableau de bord en fonction de votre configuration.

panneau Actions de gestion

Unified Manager peut diagnostiquer certains problèmes en détail et proposer une solution unique. Le cas échéant, ces solutions s'affichent dans ce panneau avec un bouton **Corriger** ou **Tout corriger**. Vous pouvez résoudre ces problèmes immédiatement depuis Unified Manager, sans avoir à utiliser ONTAP System Manager ni l'ONTAP CLI. Pour afficher tous les problèmes, cliquez sur Voir "Résolvez directement les problèmes ONTAP depuis Unified Manager" pour plus d'informations.

Panneau de capacité

Lors de la consultation de tous les clusters, ce panneau affiche la capacité physique utilisée (après application des gains d'efficacité du stockage) et la capacité physique disponible (sans inclure les gains potentiels d'efficacité du stockage) pour chaque cluster, le nombre de jours avant que les disques ne soient supposés être pleins, ainsi que le taux de réduction des données (sans les copies Snapshot) basé sur les paramètres d'efficacité du stockage ONTAP configurés. Il indique également la capacité utilisée pour tous les niveaux cloud configurés. Cliquer sur l'histogramme vous amène à la page d'inventaire des agrégats de ce cluster. Cliquer sur le texte "Days To Full" affiche un message qui identifie l'agrégat avec le plus petit nombre de jours de capacité restants ; cliquez sur le nom de l'agrégat pour voir plus de détails.

Lorsque vous consultez un seul cluster, ce panneau affiche la capacité physique utilisée et la capacité physique disponible pour les agrégats de données triés par chaque type de disque individuel sur le niveau local, ainsi que pour le niveau cloud. Le fait de cliquer sur l'histogramme d'un type de disque vous amène à la page d'inventaire des volumes pour les volumes qui utilisent ce type de disque.

Panneau de capacité de performance

Lorsque vous consultez tous les clusters, ce panneau affiche la valeur de capacité de performance de chaque cluster (moyenne sur l'heure précédente) et le nombre de jours jusqu'à ce que la capacité de performance atteigne la limite supérieure (en fonction du taux de croissance quotidien). Cliquer sur le graphique à barres vous redirige vers 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. Cliquer sur le texte « Days To Full » affiche un message qui identifie le nœud avec le moins de jours de capacité de performance restants ; cliquez sur le nom du nœud pour voir plus de détails.

Lors de l'affichage d'un seul cluster, ce panneau indique le pourcentage de capacité de performance du cluster utilisé, le total des IOPS et le débit total (Mo/s), ainsi que le nombre de jours avant que chacune de ces trois métriques n'atteigne sa limite supérieure.

Panneau des IOPS du workload

Lorsque vous consultez un seul cluster, ce panneau affiche le nombre total de workloads actuellement exécutés dans une certaine plage d'IOPS et indique le nombre pour chaque type de disque lorsque vous survolez le graphique avec votre curseur.

Panneau des performances du workload

Ce panneau affiche le nombre total de workloads conformes et non conformes attribués à chaque stratégie de niveau de service de performance (PSL). Il affiche également le nombre de workloads qui ne sont attribués à aucun PSL. Cliquer sur un graphique à barres vous amène aux workloads conformes attribués à cette stratégie dans la page Workloads. Cliquer sur le nombre qui suit le graphique à barres vous amène aux workloads conformes et non conformes attribués à cette stratégie.

Panneau de sécurité

Le panneau Sécurité présente l'état de sécurité global de tous les clusters ou d'un seul cluster, selon votre vue actuelle. Ce panneau affiche :

- une liste des événements de sécurité reçus au cours des dernières 24 heures. Cliquez sur un événement pour afficher les détails dans la page Event details
- l'état de sécurité du cluster (nombre de clusters conformes et non conformes)
- état de sécurité des VM de stockage (nombre de VM de stockage conformes et non conformes)
- l'état de chiffrement des volumes (nombre de volumes chiffrés ou non chiffrés)
- État de la protection anti-ransomware des volumes (nombre de volumes dont la protection anti-ransomware est activée ou désactivée)

Vous pouvez cliquer sur les graphiques à barres des clusters conformes et non conformes, des machines virtuelles de stockage, des volumes chiffrés et non chiffrés, et de l'état anti-ransomware des volumes pour accéder aux pages respectives et consulter les détails de sécurité des clusters, des machines virtuelles de stockage et des volumes filtrés.

La conformité est basée sur les règles de sécurité "NetApp Guide de renforcement de la sécurité pour ONTAP 9". Cliquez sur la flèche vers la droite en haut du panneau pour afficher les détails de sécurité de tous les clusters sur la page Sécurité. Pour plus d'informations, consultez "Affichage de l'état de sécurité détaillé des clusters et des machines virtuelles de stockage".

Panneau de protection des données

Ce panneau affiche le résumé de la protection des données pour un seul cluster ou tous les clusters d'un centre de données. Il affiche le nombre total d'événements de protection des données, les événements MetroCluster et le nombre d'événements actifs générés au cours des dernières 24 heures dans ONTAP. Cliquer sur le lien de chacun de ces événements vous amène à la page de détails de l'événement. Vous pouvez cliquer sur le lien **View All** pour afficher tous les événements de protection actifs dans la page d'inventaire de la gestion des événements. Le panneau affiche :

- Le nombre de volumes dans un cluster ou dans l'ensemble des clusters d'un centre de données protégés par des copies Snapshot.
- Le nombre de volumes dans un cluster ou dans l'ensemble des clusters d'un centre de données protégés par des relations SnapMirror. Pour les relations SnapMirror, le nombre de volumes du cluster source est pris en compte.
- Le nombre de clusters ou l'ensemble des clusters d'un centre de données protégés par une configuration MetroCluster sur IP ou FC.
- Le nombre de relations de volume avec retard de l'objectif de point de récupération (RPO) SnapMirror en fonction de l'état du retard.

Vous pouvez survoler avec votre souris pour afficher les décomptes et les légendes correspondants. Vous pouvez cliquer sur la flèche droite en haut du panneau pour afficher les détails d'un seul cluster ou de tous les

clusters sur la page Protection des données. Vous pouvez également cliquer sur :

- Les histogrammes des volumes non protégés et des volumes protégés par des copies Snapshot permettent d'accéder à la page Volumes et d'afficher les détails.
- Les graphiques à barres des clusters protégés ou non protégés par la configuration MetroCluster permettent d'accéder à la page Clusters et d'afficher les détails.
- Les graphiques à barres de toutes les relations mènent à la page Relations, où les détails sont filtrés en fonction du cluster source.

Pour plus d'informations, consultez "Affichage de l'état de protection du volume".

Panneau Vue d'ensemble de l'utilisation

Lors de la consultation de tous les clusters, vous pouvez choisir de les afficher triés par nombre d'IOPS le plus élevé, débit le plus élevé (MB/s) ou capacité physique utilisée la plus élevée.

Lorsque vous affichez un seul cluster, vous pouvez choisir d'afficher les workloads triés par IOPS les plus élevés, débit le plus élevé (Mo/s) ou capacité logique utilisée la plus élevée.

Informations connexes

"Résolution des problèmes à l'aide des corrections automatiques d'Unified Manager"

"Affichage d'informations sur les événements de performance"

"Gestion des performances à l'aide des informations sur la capacité de performance et les IOPS disponibles"

"Page de détails sur le volume et la santé"

"Analyse et notification des événements de performance"

"Description des types de gravité des événements"

"Sources d'événements de performance"

"Gérer les objectifs de sécurité du cluster"

"Surveillez les performances du cluster depuis la page de destination du cluster de performances"

"Surveillez les performances à l'aide des pages d'inventaire des performances"

Résolvez ou gérez directement les problèmes ONTAP depuis Unified Manager

Gérez les problèmes ou les fonctionnalités ONTAP directement depuis Active IQ Unified Manager

Vous pouvez résoudre certains problèmes ONTAP ou gérer certaines fonctionnalités ONTAP directement depuis l'interface utilisateur d'Unified Manager, sans avoir à utiliser ONTAP System Manager ou l'ONTAP CLI. L'option « Management Actions » permet de corriger un certain nombre de problèmes ONTAP qui ont déclenché des événements Unified Manager.

Vous pouvez résoudre les problèmes directement depuis la page Management Actions en sélectionnant l'option **Management Actions** dans le volet de navigation de gauche. Management Actions est également

disponible depuis le panneau Management Actions du Dashboard, la page Event details, et la sélection Workload Analysis dans le menu de navigation de gauche.

Unified Manager peut diagnostiquer en détail certains problèmes et proposer une solution unique. Pour certaines fonctionnalités ONTAP, comme la surveillance anti-ransomware, Unified Manager effectue des vérifications internes et recommande des actions spécifiques. Le cas échéant, ces solutions s'affichent dans Management Actions avec un bouton **Fix It**. Cliquez sur le bouton **Fix It** pour corriger le problème. Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Unified Manager envoie des commandes ONTAP au cluster pour effectuer la correction demandée. Une fois la correction terminée, l'événement est marqué comme obsolète.

Certaines actions de gestion vous permettent de corriger le même problème sur plusieurs objets de stockage à l'aide du bouton **Tout corriger**. Par exemple, il peut y avoir 5 volumes qui présentent l'événement « Espace du volume saturé », ce problème pouvant être résolu en cliquant sur l'action de gestion **Tout corriger** pour « Activer l'augmentation automatique du volume ». Un seul clic vous permet de corriger ce problème sur 5 volumes.

Pour plus d'informations sur les problèmes et les fonctionnalités d'ONTAP que vous pouvez gérer à l'aide de la correction automatique, consultez "Quels problèmes Unified Manager peut-il résoudre".

Découvrez les options des boutons « Corriger » et « Tout corriger » dans Active IQ Unified Manager

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, le cas échéant. Toutefois, si vous n'êtes pas certain de vouloir résoudre le problème comme recommandé par Unified Manager, vous pouvez effectuer les actions suivantes :

Qu'est-ce que vous voulez faire?	Action
Demandez à Unified Manager de corriger le problème sur tous les objets identifiés.	Cliquez sur le bouton **Tout corriger**.
Pour le moment, ne corrigez le problème sur aucun des objets identifiés et masquez cette action de gestion jusqu'à ce que l'événement soit de nouveau signalé.	Cliquez sur la flèche vers le bas et cliquez sur **Tout ignorer**.
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 **Fix It** individuelles. Suivez ensuite les étapes pour corriger ou ignorer les actions de gestion individuelles.

Qu'est-ce que vous voulez faire?	Action
Demandez à Unified Manager de résoudre le problème.	Cliquez sur le bouton **Fix It**.
Ne corrigez pas le problème pour le moment et masquez cette action de gestion jusqu'à ce que l'événement se reproduise.	Cliquez sur la flèche vers le bas, puis sur **Ignorer**.

Qu'est-ce que vous voulez faire?	Action
Affichez les détails de cet événement afin de mieux comprendre le problème.	• Cliquez sur le bouton **Fix It** et examinez la correction qui sera appliquée dans la boîte de dialogue qui s'affiche. • Cliquez sur la flèche vers le bas et cliquez sur **View Event Detail** pour afficher la page de détails de l'événement. Cliquez ensuite sur **Fix It** sur l'une ou l'autre de ces pages qui s'affichent si vous souhaitez résoudre le problème.
Affichez les détails de cet objet de stockage afin de mieux comprendre le problème.	Cliquez sur le nom de l'objet de stockage pour afficher les détails dans Performance Explorer ou sur la page Health Details.

Dans certains cas, la correction est prise en compte lors de la prochaine interrogation de configuration de 15 minutes. Dans d'autres cas, la vérification de la modification de configuration et l'obsolescence de l'événement peuvent prendre jusqu'à plusieurs heures.

Pour afficher la liste des actions de gestion terminées ou en cours, cliquez sur l'icône de filtre et sélectionnez **Terminées** ou **En cours**.

Les opérations Fix All s'exécutent en série, donc lorsque vous consultez le panneau **In Progress** certains objets auront le statut **In Progress** tandis que d'autres auront le statut **Scheduled**; cela signifie qu'ils sont toujours en attente d'être implémentés.

Consultez l'état des actions de gestion à corriger dans Active IQ Unified Manager

Vous pouvez consulter l'état de toutes les actions de gestion que vous avez choisi de corriger sur la page Actions de gestion. La plupart des actions s'affichent comme **Terminées** assez rapidement après que Unified Manager a envoyé la commande ONTAP au cluster. Cependant, certaines actions, comme le déplacement d'un volume, peuvent prendre plus de temps.

Trois filtres sont disponibles sur la page Actions de gestion :

- La section « Terminé » affiche à la fois les actions de gestion qui se sont terminées avec succès et celles qui ont échoué. Les actions « Échec » indiquent la raison de l'échec afin que vous puissiez résoudre le problème manuellement.
- La section **En cours** affiche à la fois les actions de gestion en cours de mise en œuvre et celles dont la mise en œuvre est prévue.
- **Recommandé** affiche toutes les actions de gestion actuellement actives pour tous les clusters surveillés.

Étapes

1. Cliquez sur **Actions de gestion** dans le volet de navigation de gauche. Vous pouvez également cliquer sur
   ⋮ en haut du panneau **Actions de gestion** dans le **Tableau de bord** et sélectionner la vue souhaitée.

   La page Actions de gestion s'affiche.

2. Vous pouvez cliquer sur l'icône d'accent circonflexe située à côté de l'action de gestion dans le champ

Description pour afficher des détails sur le problème et la commande utilisée pour le corriger.

3. Pour afficher les actions qui ont **échoué**, triez selon la colonne **Statut** dans la vue **Terminé**. Vous pouvez utiliser l'outil **Filtrer** dans le même but.
4. Si vous souhaitez afficher plus d'informations sur une action de gestion ayant échoué, ou si vous décidez de corriger une action de gestion recommandée, vous pouvez cliquer sur **View Event Detail** dans la zone développée après avoir cliqué sur l'icône d'accent circonflexe à côté de l'action de gestion. Un bouton **Fix It** est disponible sur cette page.

Découvrez les problèmes ONTAP que Active IQ Unified Manager peut résoudre

En utilisant la fonction de correction automatique d'Active IQ Unified Manager, vous pouvez choisir de résoudre efficacement certains problèmes ONTAP ou de gérer certaines fonctionnalités ONTAP, telles que la surveillance anti-ransomware, via Unified Manager.

Ce tableau décrit les problèmes ou fonctionnalités ONTAP que vous pouvez gérer directement à l'aide du bouton **Corriger** ou **Tout corriger** dans l'interface utilisateur Web de Unified Manager.

Nom et description de l'événement	Action de gestion	Opération « Réparer »
Espace du volume plein Le volume est presque à court d'espace et a dépassé le seuil de capacité pleine. Ce seuil est fixé par défaut à 90 % de la taille du volume.	Activer l'augmentation automatique du volume	Unified Manager détermine que la croissance automatique n'est pas configurée pour ce volume ; il active donc cette fonctionnalité afin que le volume augmente en capacité en cas de besoin.
Inodes pleins Ce volume n'a plus d'inodes et ne peut plus accepter de nouveaux fichiers.	Augmenter le nombre d'inodes sur le volume	Augmente le nombre d'inodes sur le volume de 2 %.
Incompatibilité de stratégie de niveau de stockage détectée Le volume contient beaucoup de données inactives et la politique de hiérarchisation actuelle est définie sur « snapshot-only » ou « none ».	Activer la hiérarchisation automatique du cloud	Étant donné que le volume réside déjà sur un FabricPool, il modifie la politique de hiérarchisation en « auto » afin de déplacer les données inactives vers le niveau cloud le moins coûteux.
Incompatibilité de niveau de stockage détectée Le volume contient beaucoup de données inactives, mais il n'est pas situé sur un niveau de stockage compatible avec le cloud (FabricPool).	Modifier le niveau de stockage des volumes	Déplace le volume vers un niveau de stockage compatible avec le cloud et définit la politique de hiérarchisation sur "auto" pour déplacer les données inactives vers le niveau cloud.

Nom et description de l'événement	Action de gestion	Opération « Réparer »
Journal d'audit désactivé Le journal des audits n'est pas activé pour la machine virtuelle de stockage	Activez la journalisation d'audit pour la VM de stockage	Active la journalisation des audits sur la machine virtuelle de stockage. Notez que la machine virtuelle de stockage doit déjà avoir configuré un emplacement de journal des audits, local ou distant.
Bannière de connexion désactivée La bannière de connexion au cluster doit être activée afin d'améliorer la sécurité en rendant les restrictions d'accès explicites.	Définir la bannière de connexion pour le cluster	Définit la bannière de connexion au cluster sur "Accès restreint aux utilisateurs autorisés".
Bannière de connexion désactivée La bannière de connexion de la machine virtuelle de stockage doit être activée afin d'améliorer la sécurité en précisant clairement les restrictions d'accès.	Configurer la bannière de connexion pour la machine virtuelle de stockage	Définit la bannière de connexion de la VM de stockage sur « Accès restreint aux utilisateurs autorisés ».
SSH utilise des algorithmes de chiffrement non sécurisés Les algorithmes de chiffrement comportant le suffixe « -cbc » sont considérés comme non sécurisés.	Supprimez les algorithmes de chiffrement non sécurisés du cluster	Supprime du cluster les algorithmes de chiffrement non sécurisés, tels que aes192-cbc et aes128-cbc.
SSH utilise des algorithmes de chiffrement non sécurisés Les algorithmes de chiffrement comportant le suffixe « -cbc » sont considérés comme non sécurisés.	Supprimez les algorithmes de chiffrement non sécurisés de la machine virtuelle de stockage	Supprime les algorithmes de chiffrement non sécurisés — tels que aes192-cbc et aes128-cbc — de la VM de stockage.
AutoSupport transport HTTPS désactivé Le protocole de transport utilisé pour envoyer des messages AutoSupport au support technique doit être chiffré.	Définissez HTTPS comme protocole de transport pour les messages AutoSupport	Définit HTTPS comme protocole de transport pour les messages AutoSupport sur le cluster.
Seuil de déséquilibre de charge du cluster dépassé Indique un déséquilibre de charge entre les nœuds du cluster. Cet événement est généré lorsque l'écart de capacité de performance utilisée entre les nœuds dépasse 30 %.	Équilibrer les charges de travail du cluster	Unified Manager identifie le volume optimal à déplacer d'un nœud à l'autre pour réduire le déséquilibre, puis déplace ce volume.

Nom et description de l'événement	Action de gestion	Opération « Réparer »
Seuil de déséquilibre de capacité du cluster dépassé Indique un déséquilibre de capacité entre les agrégats du cluster. Cet événement se produit lorsque l'écart de capacité utilisée entre les agrégats dépasse 70 %.	Équilibrer la capacité du cluster	Unified Manager identifie le meilleur volume à déplacer d'un agrégat à un autre pour réduire le déséquilibre, puis déplace ce volume.
Dépassement du seuil de capacité de performance utilisée Indique que la charge du nœud pourrait devenir surutilisée si vous ne réduisez pas l'utilisation d'une ou plusieurs charges de travail très actives. Cet événement est généré lorsque la valeur de capacité de performance du nœud utilisée dépasse 100 % pendant plus de 12 heures.	Limiter la charge élevée sur le nœud	Unified Manager identifie le volume présentant le nombre d'IOPS le plus élevé et applique une politique QoS en utilisant les niveaux d'IOPS historiques attendus et de pointe afin de réduire la charge sur le nœud.
Seuil d'avertissement d'événement dynamique dépassé Indique que le nœud fonctionne déjà dans un état de surcharge en raison de la charge anormalement élevée de certaines charges de travail.	Réduire la surcharge du nœud	Unified Manager identifie le volume présentant le nombre d'IOPS le plus élevé et applique une politique QoS en utilisant les niveaux d'IOPS historiques attendus et de pointe afin de réduire la charge sur le nœud.
Le basculement n'est pas possible Le basculement est actuellement désactivé, de sorte que l'accès aux ressources du nœud serait perdu pendant une panne ou un redémarrage jusqu'à ce que le nœud soit de nouveau disponible.	Activer le basculement des nœuds	Unified Manager envoie la commande appropriée pour activer le basculement sur tous les nœuds du cluster.
L'option Cf.takeover.on_panic est configurée sur OFF L'option nodeshell « cf.takeover.on_panic » est définie sur **off**, ce qui pourrait entraîner un problème sur les systèmes configurés en haute disponibilité.	Activer la prise de contrôle en cas de panique	Unified Manager envoie la commande appropriée au cluster pour définir ce paramètre sur **on**.

Nom et description de l'événement	Action de gestion	Opération « Réparer »
Désactiver l'option nodeshell snapmirror.enable L'ancienne option nodeshell « snapmirror.enable » est définie sur **on**, ce qui pourrait entraîner un problème lors du démarrage après la mise à niveau vers ONTAP 9.3 ou une version ultérieure.	Définissez l'option snapmirror.enable sur off	Unified Manager envoie la commande appropriée au cluster pour définir ce paramètre sur **off**.
Telnet activé Indique un problème de sécurité potentiel, car Telnet n'est pas sécurisé et transmet les données sans chiffrement.	Désactiver Telnet	Unified Manager envoie la commande appropriée au cluster pour désactiver Telnet.
Configurer l'apprentissage anti-ransomware de la VM de stockage Effectue des vérifications périodiques pour les clusters disposant de licences de surveillance anti-ransomware. Vérifie si une machine virtuelle de stockage prend uniquement en charge les volumes NFS ou SMB dans un tel cluster.	Mettez les machines virtuelles de stockage en `learning`mode de surveillance anti-ransomware	Unified Manager définit la surveillance anti-ransomware à l'état `learning` pour les machines virtuelles de stockage via la gestion des clusters. La surveillance anti-ransomware de tous les nouveaux volumes créés sur la machine virtuelle de stockage passe automatiquement en mode d'apprentissage. Grâce à cette activation, ONTAP peut analyser l'activité sur les volumes et détecter les anomalies dues à d'éventuelles attaques malveillantes.
Configurer l'apprentissage anti-ransomware du volume Effectue des vérifications périodiques pour les clusters disposant de licences de surveillance anti-ransomware. Vérifie si un volume prend uniquement en charge les services NFS ou SMB dans un tel cluster.	Mettez les volumes en `learning` mode de surveillance anti-ransomware	Unified Manager définit l'état `learning` de la surveillance anti-ransomware pour les volumes via la gestion des clusters. Grâce à cette activation, ONTAP peut analyser l'activité sur les volumes et détecter les anomalies dues à d'éventuelles attaques malveillantes.

Nom et description de l'événement	Action de gestion	Opération « Réparer »
Activer la protection anti-ransomware sur un volume Effectue des vérifications périodiques des clusters disposant de licences de surveillance anti-ransomware. Détecte si les volumes sont dans le mode `learning` de surveillance anti-ransomware depuis plus de 45 jours et détermine la possibilité de les mettre en mode actif.	Mettez les volumes en `active` mode de surveillance anti-ransomware	Unified Manager active la surveillance anti-ransomware `active` sur les volumes via la gestion des clusters. Grâce à cette activation, ONTAP peut apprendre le schéma d'activité sur les volumes, détecter les anomalies dues à d'éventuelles attaques malveillantes et créer des alertes pour les actions de protection des données.
Désactiver la protection anti-ransomware du volume Effectue régulièrement des vérifications des clusters disposant de licences pour la surveillance anti-ransomware. Détecte les notifications répétitives lors de la surveillance anti-ransomware active sur les volumes (par exemple, plusieurs avertissements d'attaques de ransomware potentielles sont renvoyés sur 30 jours).	Désactiver la surveillance anti-ransomware sur les volumes	Unified Manager désactive la surveillance anti-ransomware sur les volumes via la gestion des clusters.

Remplacez les actions de gestion par des scripts dans Active IQ Unified Manager

Vous pouvez créer des scripts personnalisés et les associer à des alertes afin d'effectuer des actions spécifiques pour des événements spécifiques, au lieu d'opter pour les actions de gestion par défaut disponibles sur la page Management Actions ou le tableau de bord Unified Manager.

Si vous souhaitez entreprendre des actions spécifiques pour un type d'événement et choisissez de ne pas les corriger dans le cadre de la fonctionnalité d'action de gestion fournie par Unified Manager, vous pouvez configurer un script personnalisé pour l'action spécifique. Vous pouvez ensuite associer le script à une alerte pour ce type d'événement et traiter ces événements individuellement. Dans ce cas, aucune action de gestion n'est générée pour ce type d'événement sur la page Actions de gestion ou sur le tableau de bord Unified Manager.

Gérer les clusters

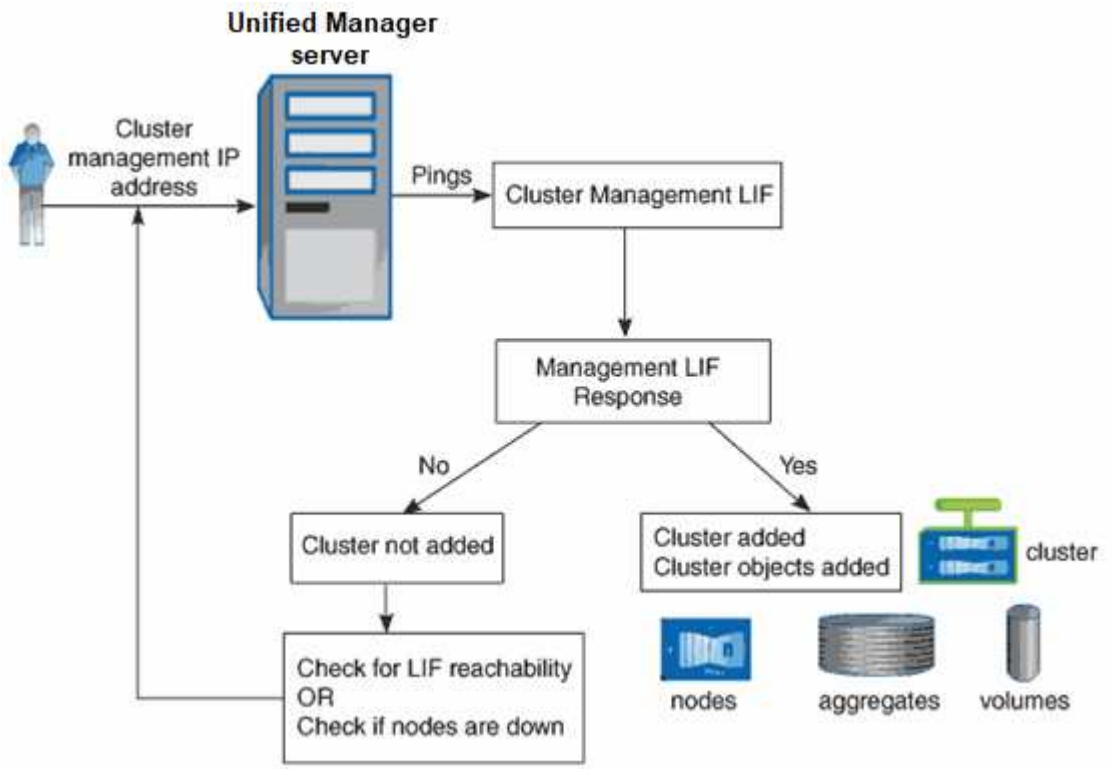
Découvrez comment fonctionne le processus de découverte de clusters dans Active IQ Unified Manager

Une fois un cluster ajouté à Unified Manager, le serveur détecte les objets du cluster et les ajoute à sa base de données. Comprendre ce processus de détection vous permettra

de mieux gérer les clusters de votre organisation et leurs objets.

L'intervalle de surveillance pour la collecte des informations de configuration du cluster est de 15 minutes. Par exemple, après avoir ajouté un cluster, il faut 15 minutes pour afficher les objets du cluster dans l'interface utilisateur de Unified Manager. Ce délai s'applique également lorsque vous apportez des modifications à un cluster. Par exemple, si vous ajoutez deux nouveaux volumes à une SVM dans un cluster, vous voyez ces nouveaux objets dans l'interface utilisateur après le prochain intervalle d'interrogation, qui peut atteindre 15 minutes.

L'image suivante illustre le processus de découverte :



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

Étant donné que la collecte de 15 jours de données de performance sollicite fortement le processeur, il est conseillé d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur un trop grand nombre de clusters en même temps.

Consultez la liste des clusters surveillés par Active IQ Unified Manager

Vous pouvez utiliser la page Cluster Setup pour consulter votre inventaire de clusters. Vous pouvez consulter des détails sur les clusters, tels que leur nom, leur adresse IP et leur état de communication.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.

   Tous les clusters de votre environnement de stockage gérés par Unified Manager sont affichés. La liste des clusters est triée selon la colonne du niveau de gravité de l'état de collecte. Vous pouvez cliquer sur l'en-tête d'une colonne pour trier les clusters selon différentes colonnes.

Ajouter des clusters à Active IQ Unified Manager

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de le surveiller. Vous pourrez ainsi obtenir des informations sur le cluster, telles que son état, sa capacité, ses performances et sa configuration, ce qui vous permettra de détecter et de résoudre tout problème éventuel.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'applications ou le rôle d'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.
  - Vous devez disposer du nom de l'hôte ou de l'adresse IP de gestion (IPv4 ou IPv6) du cluster.

    Lorsque vous utilisez le nom de l'hôte, celui-ci doit se résoudre en l'adresse IP de gestion du cluster pour la LIF de gestion du cluster. Si vous utilisez une LIF de gestion de nœud, l'opération échoue.
  - Vous devez disposer du nom d'utilisateur et du mot de passe pour accéder au cluster.

    Ce compte doit avoir le rôle *admin* avec un accès à l'application défini sur *ontapi*, *amqp*, *console* et *http*.
  - Vous devez connaître le numéro de port pour vous connecter au cluster à l'aide du protocole HTTPS (généralement le port 443).
  - Le cluster doit exécuter le logiciel ONTAP version 9.9 ou ultérieure.
  - Vous devez disposer d'un espace suffisant sur le serveur Unified Manager. L'ajout d'un cluster au serveur est impossible si plus de 90 % de l'espace est déjà utilisé.
  - Vous possédez les certificats requis:

    Certificat SSL (HTTPS) : ce certificat appartient à Unified Manager. Un certificat SSL (HTTPS) auto-signé par défaut est généré lors d'une nouvelle installation d'Unified Manager. NetApp recommande de le remplacer par 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 prennent en compte le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, consultez "Génération d'un certificat de sécurité HTTPS".

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

    Certificats pour la communication TLS mutuelle : utilisés lors de la communication TLS mutuelle

entre Unified Manager et ONTAP. L'authentification par certificat est activée pour un cluster, selon la version d'ONTAP. Si le cluster exécute une version d'ONTAP antérieure à 9.5, l'authentification par certificat n'est pas activée.

L'authentification par certificat n'est pas activée automatiquement pour 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 intégrer le nouveau certificat. Pour plus d'informations sur l'affichage et la régénération du certificat, consultez "Modification des clusters".

- Vous pouvez ajouter un cluster depuis l'interface web, et l'authentification par certificat est automatiquement activée.
- Vous pouvez ajouter un cluster via Unified Manager CLI, l'authentification par certificat n'est pas activée par défaut. Si vous ajoutez un cluster via Unified Manager CLI, vous devez le modifier via Unified Manager UI. Vous pouvez consulter "Commandes CLI Unified Manager prises en charge" pour ajouter un cluster via Unified Manager CLI.
- Si l'authentification par certificat est activée pour un cluster et que vous effectuez la sauvegarde d'Unified Manager depuis un serveur, puis la restaurez sur un autre serveur Unified Manager dont le nom d'hôte ou l'adresse IP a changé, la surveillance du cluster peut échouer. Pour éviter cet échec, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, consultez "Modification des clusters".
- Au niveau du cluster, l'interface Active IQ ajoute deux nouvelles entrées de groupe d'utilisateurs pour la méthode d'authentification "cert".

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

- Une seule instance d'Unified Manager peut prendre en charge un nombre spécifique de nœuds. Si vous devez surveiller un environnement dont le nombre de nœuds dépasse le nombre pris en charge, vous devez installer une instance supplémentaire d'Unified Manager pour surveiller certains clusters. Pour consulter la liste du nombre de nœuds pris en charge, reportez-vous à "guide des bonnes pratiques Unified Manager".

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs requises, puis cliquez sur **Submit**.
4. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour consulter les informations du certificat relatives au cluster.
5. Cliquez sur **Oui**.

   Après avoir enregistré les détails du cluster, vous pouvez consulter le certificat pour la communication Mutual TLS d'un cluster.

   Si l'authentification par certificat n'est pas activée, Unified Manager vérifie le certificat uniquement lors de l'ajout initial du cluster. Unified Manager ne vérifie pas le certificat pour chaque appel d'API à ONTAP.

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

- La collecte de 15 jours de données de performance sollicite fortement le processeur. NetApp recommande d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur un trop grand nombre de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte s'interrompt et vous constaterez des lacunes dans les graphiques de performance pour la période manquante.
- Lorsque vous ajoutez un cluster ONTAP version 9.14.1 ou ultérieure, la communication s'effectue via la fonctionnalité d'agent cloud. ONTAP crée automatiquement un compte utilisateur de service interne avec des privilèges en lecture seule (par exemple, clus-agent-xxxx). Unified Manager cesse de collecter les données de ces clusters si l' `clus-agent`utilisateur est supprimé.

Si vous recevez un message d'erreur indiquant que vous ne pouvez pas ajouter le cluster, vérifiez si les problèmes suivants existent :

- Si les horloges des deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS de Unified Manager est postérieure à la date du cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide de NTP ou d'un service similaire.
- Si le cluster a atteint le nombre maximal de destinations de notification EMS, l'adresse Unified Manager ne peut pas être ajoutée. Par défaut, seules 20 destinations de notification EMS peuvent être définies sur le cluster.

Informations connexes

"Ajout d'utilisateurs"

"Affichage de la liste et des détails des clusters"

"Installation d'un certificat HTTPS signé et renvoyé par une autorité de certification"

Modifier les paramètres du cluster dans Active IQ Unified Manager

Vous pouvez modifier les paramètres d'un cluster existant, tels que le nom de l'hôte ou l'adresse IP, le nom d'utilisateur, le mot de passe et le port, à l'aide de la boîte de dialogue Edit Cluster.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'applications ou le rôle d'administrateur de stockage.

À partir de Unified Manager 9.7, vous pouvez ajouter des clusters uniquement à l'aide de HTTPS.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.

2. Sur la page **Configuration du cluster**, sélectionnez le cluster que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le cluster**, modifiez les valeurs selon vos besoins. + Si vous avez modifié les détails d'un cluster ajouté à Unified Manager, vous pouvez consulter les détails du certificat pour la communication TLS mutuelle, en fonction de la version d'ONTAP. Pour plus d'informations sur la version d'ONTAP, consultez "Certificats pour la communication TLS mutuelle". + Vous pouvez afficher les détails du certificat en cliquant sur **Détails du certificat**. Si le certificat a expiré, cliquez sur le bouton **Régénérer** pour intégrer le nouveau certificat.
4. Cliquez sur **Submit**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour consulter les informations du certificat relatives au cluster.
6. Cliquez sur **Oui**.

Informations connexes

"Ajout d'utilisateurs"

"Affichage de la liste et des détails des clusters"

Supprimez les clusters d'Active IQ Unified Manager

Vous pouvez supprimer un cluster de Unified Manager à l'aide de la page Configuration du cluster. Par exemple, vous pouvez supprimer un cluster si la découverte du cluster échoue, ou lorsque vous souhaitez mettre hors service un système de stockage.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'applications ou le rôle d'administrateur de stockage.

Cette tâche supprime le cluster sélectionné de Unified Manager. Une fois supprimé, le cluster n'est plus surveillé. L'instance de Unified Manager enregistrée auprès du cluster supprimé est également désenregistrée du cluster.

La suppression d'un cluster entraîne également la suppression de tous ses objets de stockage, de ses données historiques, de ses services de stockage et de tous les événements associés dans Unified Manager. Ces modifications sont visibles sur les pages d'inventaire et les pages de détails après le prochain cycle de collecte de données.

> Vous devez supprimer un cluster de Unified Manager avant de le mettre hors service. Si le cluster est déjà hors ligne ou inaccessible lorsque vous tentez de le supprimer, Unified Manager ne peut pas communiquer avec le cluster pour supprimer l'enregistrement de l'application et les abonnements Event Management System (EMS) configurés. Cela entraînera l'échec du processus de suppression ou le rendra non réactif avant son achèvement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.
2. Sur la page Configuration du cluster, sélectionnez le cluster que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Supprimer la source de données**, cliquez sur **Supprimer** pour confirmer la demande de suppression.

Informations connexes

"Ajout d'utilisateurs"

"Affichage de la liste et des détails des clusters"

Redécouvrez les clusters dans Active IQ Unified Manager

Vous pouvez relancer manuellement la découverte d'un cluster depuis la page Configuration du cluster afin d'obtenir les informations les plus récentes sur l'état, le statut de surveillance et les performances du cluster.

Vous pouvez redécouvrir manuellement un cluster lorsque vous souhaitez le mettre à jour — par exemple, en augmentant la taille d'un agrégat lorsque l'espace est insuffisant — et que vous souhaitez qu'Unified Manager détecte les modifications que vous apportez.

Lorsque Unified Manager est associé à OnCommand Workflow Automation (WFA), l'association déclenche la réacquisition des données mises en cache par WFA.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.
2. Sur la page **Configuration du cluster**, cliquez sur **Redécouvrir**.

   Unified Manager redécouvre le cluster sélectionné et affiche les derniers états de santé et de performances.

Informations connexes

"Affichage de la liste et des détails des clusters"

Surveiller l'infrastructure virtuelle VMware

Comprenez comment Active IQ Unified Manager surveille l'infrastructure virtuelle VMware

Active IQ Unified Manager offre une visibilité sur les machines virtuelles (VMs) de votre infrastructure virtuelle et vous permet de surveiller et de résoudre les problèmes de stockage et de performance dans votre environnement virtuel. Vous pouvez utiliser cette fonctionnalité pour déterminer tout problème de latence dans votre environnement de stockage ou lorsqu'un événement de performance est signalé sur votre vCenter Server.

Un déploiement d'infrastructure virtuelle typique sur ONTAP comporte divers composants répartis entre les couches de calcul, de réseau et de stockage. Tout ralentissement des performances d'une application de VM peut être dû à une combinaison de latences subies par les différents composants dans leurs couches respectives. Cette fonctionnalité est utile aux administrateurs du stockage et de vCenter Server, ainsi qu'aux généralistes de l'informatique qui doivent analyser un problème de performances dans un environnement virtuel et comprendre dans quel composant le problème s'est produit.

Vous pouvez désormais accéder au serveur vCenter depuis le menu vCenter de la section VMware. L'aperçu de chaque machine virtuelle répertoriée comporte le lien **VCENTER SERVER** dans la TOPOLOGY VIEW, qui ouvre le serveur vCenter dans un nouveau navigateur. Vous pouvez également utiliser le bouton **Expand**

Topology pour lancer le serveur vCenter et cliquer sur le bouton **View in vCenter** pour afficher les datastores dans le serveur vCenter.

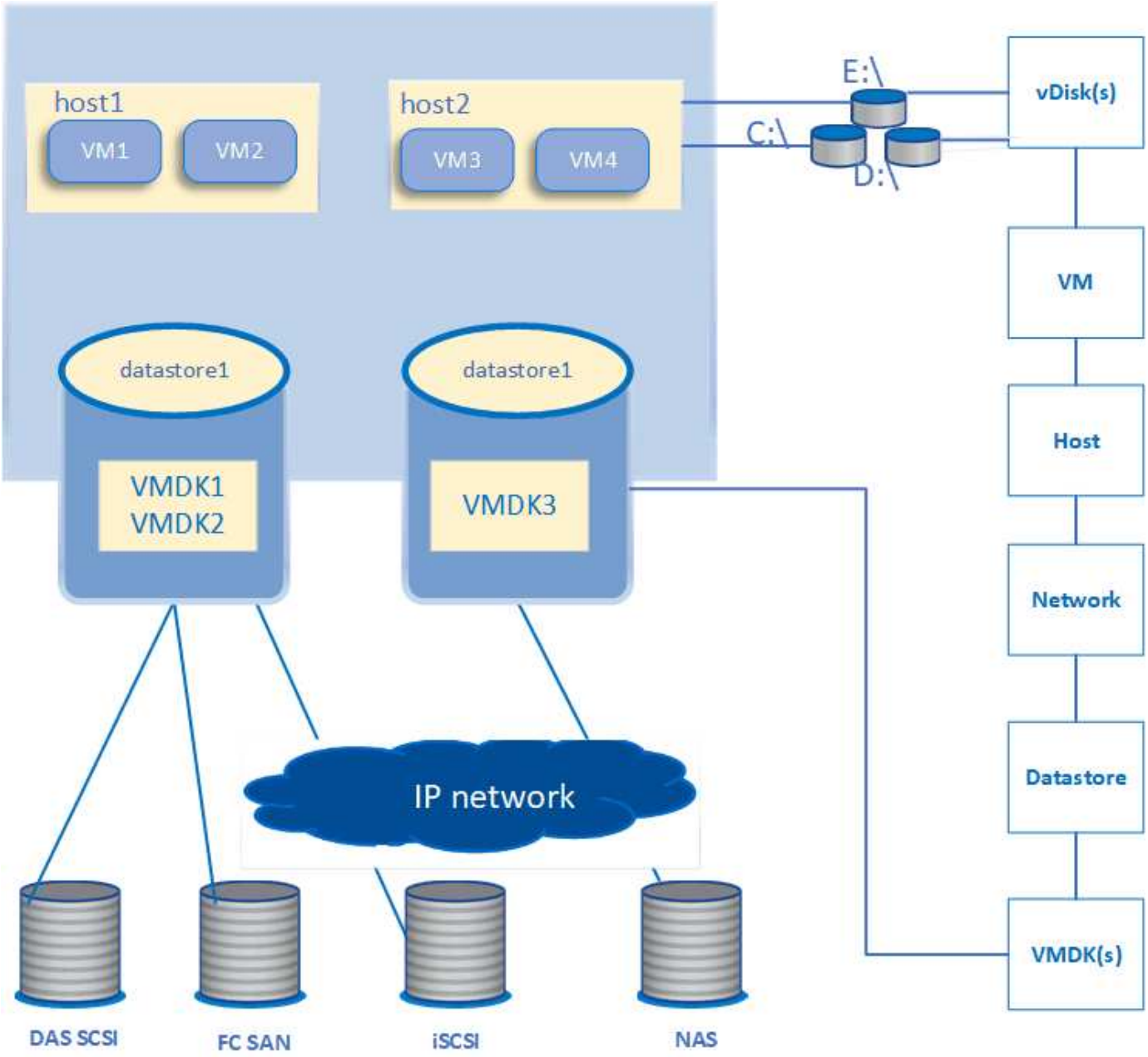
Unified Manager présente le sous-système sous-jacent d'un environnement virtuel dans une vue topologique, afin de déterminer si un problème de latence s'est produit au niveau du nœud de calcul, du réseau ou du stockage. La vue met également en évidence l'objet spécifique à l'origine du ralentissement des performances afin de prendre des mesures correctives et de résoudre le problème sous-jacent.

Une infrastructure virtuelle déployée sur le stockage ONTAP comprend les objets suivants :

- vCenter Server : un plan de contrôle centralisé pour gérer les machines virtuelles VMware, les hôtes ESXi et tous les composants associés dans un environnement virtuel. Pour plus d'informations sur vCenter Server, consultez la documentation VMware.
- Hôte : Système physique ou virtuel exécutant ESXi, le logiciel de virtualisation de VMware, et hébergeant la machine virtuelle.
- Banque de données : Les banques de données sont des objets de stockage virtuels connectés aux hôtes ESXi. Les banques de données sont des entités de stockage ONTAP gérables, telles que des LUN ou des volumes, utilisées comme référentiel pour les fichiers de VM, tels que les fichiers journaux, les scripts, les fichiers de configuration et les disques virtuels. Elles sont connectées aux hôtes de l'environnement via une connexion réseau SAN ou IP. Les banques de données en dehors d'ONTAP qui sont mappées à vCenter Server ne sont pas prises en charge et ne sont pas affichées dans Unified Manager.
- VM : une machine virtuelle VMware.
- Disques virtuels : les disques virtuels sur les datastores appartenant aux machines virtuelles qui ont une extension VMDK. Les données d'un disque virtuel sont stockées sur le VMDK correspondant.
- VMDK : disque de machine virtuelle sur le datastore qui fournit de l'espace de stockage pour les disques virtuels. À chaque disque virtuel correspond un VMDK.

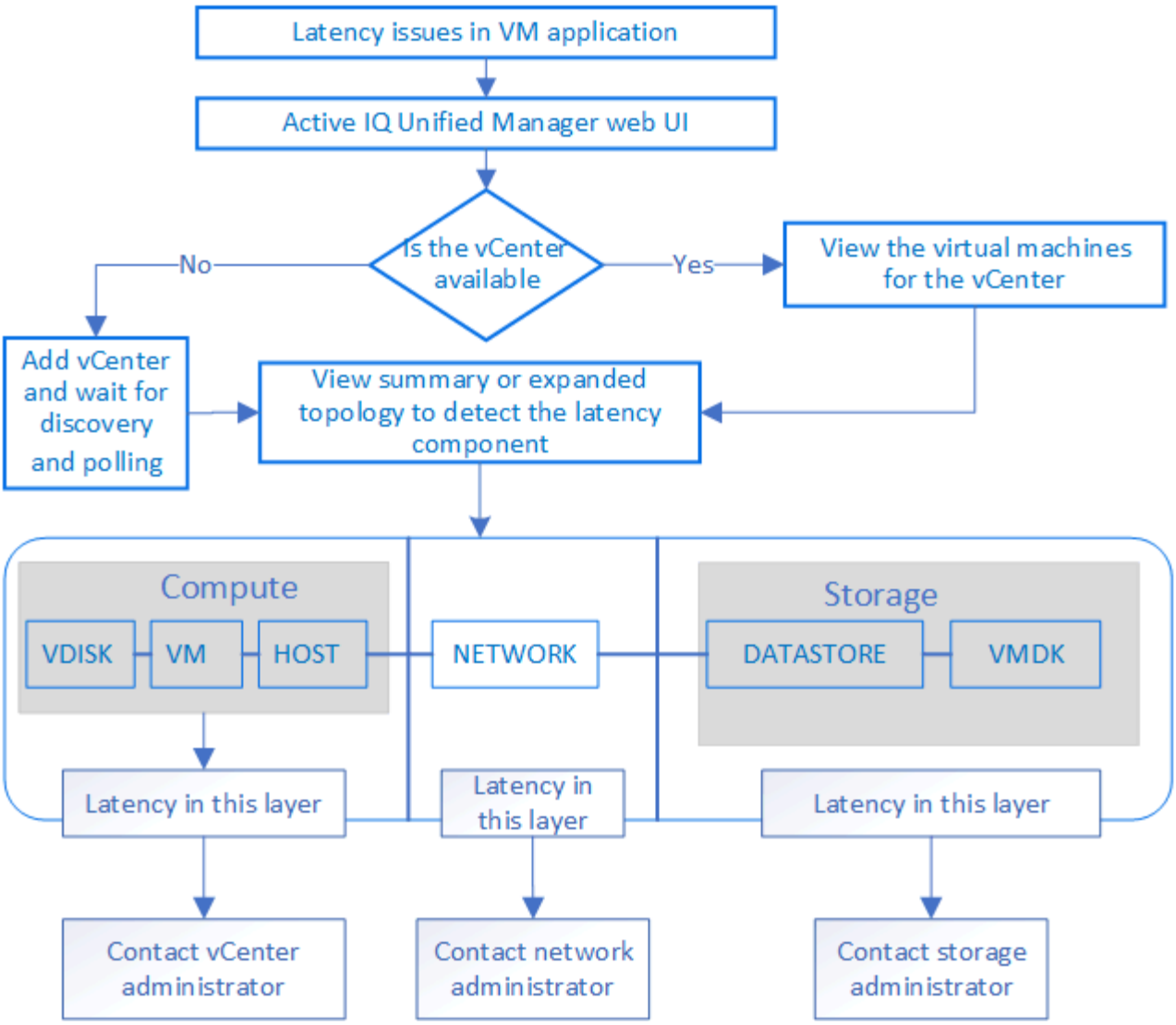
Ces objets sont représentés dans une vue de topologie de machine virtuelle.

Virtualisation VMware sur ONTAP



Flux de travail de l'utilisateur

Le diagramme suivant illustre une utilisation typique de la vue de topologie de la machine virtuelle :



Ce qui n'est pas pris en charge

- Les datastores situés en dehors de ONTAP et mappés aux instances de serveur vCenter ne sont pas pris en charge dans Unified Manager. Les VM avec des disques virtuels sur ces datastores ne sont pas non plus prises en charge.
- Une banque de données répartie sur plusieurs LUN n'est pas prise en charge.
- Les datastores utilisant la traduction d'adresses 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 à plusieurs LIF n'est pas prise en charge, car Unified Manager est incapable d'identifier quel datastore appartient à quel cluster.

  Exemple : supposons que le cluster A possède le datastore A. Le datastore A est exporté via une LIF de données avec la même adresse IP x.x.x.x et que la VM A est créée sur ce datastore. De même, le cluster B possède le datastore B. Le datastore B est exporté via une LIF de données avec la même adresse IP x.x.x.x et la VM B est créée sur le datastore B. UM ne pourra ni associer le datastore A pour la topologie de la VM A au volume/LUN ONTAP correspondant, ni associer la VM B.

- Seuls les volumes NAS et SAN (iSCSI et FCP pour VMFS) sont pris en charge en tant que banques de données, les volumes virtuels (vVols) ne sont pas pris en charge.

- Seuls les disques virtuels iSCSI sont pris en charge. Les disques virtuels de type NVMe et SATA ne sont pas pris en charge.
- Ces vues ne permettent pas de générer des rapports pour analyser les performances des différents composants.
- Pour la configuration de reprise après sinistre (DR) de la machine virtuelle de stockage (storage VM), prise en charge uniquement pour l'infrastructure virtuelle sur Unified Manager, la configuration doit être modifiée manuellement dans vCenter Server afin de pointer vers les LUN actifs dans les scénarios de basculement et de rétablissement. Sans intervention manuelle, leurs datastores deviennent inaccessibles.

Afficher et ajouter des serveurs vCenter dans Active IQ Unified Manager

Pour visualiser et dépanner les performances des machines virtuelles (VM), les serveurs vCenter associés doivent être ajoutés à votre instance Active IQ Unified Manager.

Avant de commencer

Avant d'ajouter ou de consulter des serveurs vCenter, veuillez vérifier les points suivants :

- Vous connaissez les noms des serveurs vCenter.
- Vous connaissez l'adresse IP du serveur vCenter et disposez des identifiants requis. Les identifiants doivent être ceux d'un administrateur du serveur vCenter ou d'un utilisateur root disposant d'un accès en lecture seule au serveur vCenter.
- Le serveur vCenter que vous souhaitez ajouter exécute vSphere 6.5 ou une version ultérieure.

  Le support d'Unified Manager pour VMware ESXi et vCenter Server est disponible en anglais et en japonais.

- Le paramètre de collecte de données dans le serveur vCenter est défini sur le niveau de statistiques de `Level 3`, garantissant ainsi le niveau requis de collecte de métriques pour tous les objets surveillés. La durée de l'intervalle doit être de `5 minutes`, et la période d'enregistrement doit être de `1 day`.

  Pour plus d'informations, consultez la section "Data Collection Levels" du *vSphere Monitoring and Performance Guide* dans la documentation VMware.

- Les valeurs de latence dans vCenter Server sont configurées en millisecondes, et non en microsecondes, pour que les calculs des valeurs de latence soient corrects.
- Lors de l'ajout du datastore à vCenter Server, vous pouvez utiliser à la fois l'adresse IP de l'hôte ou le domaine complet (FQDN). Si vous ajoutez le 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 fichier `/etc/resolv.conf`.
- L'heure actuelle du serveur vCenter est synchronisée avec le fuseau horaire du serveur vCenter.
- vCenter Server est joignable pour une découverte réussie.
- Vous disposez d'un accès en lecture au kit de développement logiciel VMware (SDK) lorsque vous ajoutez le vCenter Server à Unified Manager. Cet accès est nécessaire pour l'interrogation de la configuration.

Pour chaque serveur vCenter ajouté et détecté, Unified Manager collecte les données de configuration, telles que les détails du serveur vCenter et du serveur ESXi, le mappage ONTAP, les détails du datastore et le nombre de VM hébergées. Il collecte également les indicateurs de performance des composants.

Étapes

1. Accédez à **VMWARE** > **vCenter**, et vérifiez si votre serveur vCenter est disponible dans la liste.

   Si votre vCenter Server n'est pas disponible, vous devez ajouter vCenter Server.

   a. Cliquez sur **Add**.
   b. Ajoutez l'adresse IP correcte du serveur vCenter 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 disposant d'un accès en lecture seule au serveur vCenter.
   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 vous est présenté pour acceptation.

   Lorsque vous acceptez le certificat, vCenter Server est ajouté à la liste des vCenter Servers disponibles. L'ajout du périphérique n'entraîne pas de collecte de données pour les VM associées, et la collecte a lieu aux intervalles planifiés.

2. Si votre serveur vCenter est disponible sur la page **vCenters**, vérifiez son état en plaçant le pointeur de la souris sur le champ **Status** pour voir si votre serveur vCenter fonctionne comme prévu ou s'il existe un avertissement ou une erreur.

   L'ajout de vCenter Server vous permet de consulter les statuts suivants. Cependant, les données de performance et de latence des VM correspondantes peuvent prendre jusqu'à une heure après l'ajout de vCenter Server pour être correctement reflétées.

   - Vert : « Normal », indiquant que vCenter Server a été découvert et que les indicateurs de performance ont été collectés avec succès
   - Jaune : « Avertissement » (par exemple, lorsque le niveau de statistiques pour vCenter Server n'a pas été défini sur 3 ou plus afin d'obtenir des statistiques pour chaque objet)
   - Orange : « Erreur » (indique toute erreur interne, telle qu'une exception, un échec de la collecte des données de configuration, ou un serveur vCenter inaccessible) Vous pouvez cliquer sur l'icône d'affichage de la colonne (**Afficher/Masquer**) pour afficher le message d'état d'un serveur vCenter et résoudre le problème.

3. Si le serveur vCenter est inaccessible ou si les informations d'identification ont changé, modifiez les détails du serveur vCenter en sélectionnant **vCenter** > **Modifier**.
4. Apportez les modifications nécessaires sur la page **Modifier le serveur VMware vCenter**.
5. Cliquez sur **Enregistrer**.

vCenter Server commence la collecte de données

vCenter Server collecte des échantillons de données de performances en temps réel toutes les 20 secondes et les regroupe en échantillons de 5 minutes. Le calendrier de collecte des données de performances de Unified Manager est basé sur les paramètres par défaut de vCenter Server. Unified Manager traite les échantillons de 5 minutes obtenus à partir de vCenter Server et calcule une moyenne horaire des IOPS et de la latence pour les disques virtuels, les VM et les hôtes. Pour les datastores, Unified Manager calcule une moyenne horaire des IOPS et de la latence à partir d'échantillons obtenus depuis ONTAP. Ces valeurs sont disponibles au début de l'heure. Les mesures de performances ne sont pas disponibles immédiatement après l'ajout de vCenter Server et ne le deviennent qu'au début de l'heure suivante. L'interrogation des données de performances commence une fois un cycle de collecte des données de configuration terminé.

Pour interroger les données de configuration du serveur vCenter, 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 configuration et de performances du serveur vCenter, consultez « Activité de collecte des données de configuration et de performances du cluster ».

Informations connexes

"Activité de collecte des données de configuration et de performances du cluster"

Supprimer un serveur vCenter d'Active IQ Unified Manager

Vous pouvez supprimer des serveurs vCenter de votre instance Active IQ Unified Manager. Par exemple, vous pouvez supprimer un serveur vCenter si la découverte du serveur vCenter échoue ou s'il n'est plus nécessaire.

La suppression d'un vCenter Server entraîne également la suppression de toutes les machines virtuelles (VM) hébergées sur ce vCenter ainsi que de ses données de configuration. Une fois le vCenter Server supprimé, il ne sera plus surveillé, de même que ses objets associés et ses données historiques. Ces modifications seront répercutées sur les pages d'inventaire de vCenter et des machines virtuelles.

Avant de commencer

Avant de supprimer les serveurs vCenter, assurez-vous des points suivants :

- Vous avez le rôle d'administrateur d'applications ou le rôle d'administrateur de stockage.
- Vous devez connaître les noms des serveurs vCenter et les adresses IP respectives qui leur sont associées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **VMWARE>vCenter**.
2. Sur la page vCenters, sélectionnez le serveur vCenter que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue de message **Supprimer vCenter**, cliquez sur **OK** pour confirmer la demande de suppression.

Comprendre comment Active IQ Unified Manager surveille les machines virtuelles

En cas de problème de latence sur les applications de machines virtuelles (VM), il peut être nécessaire de surveiller les VM afin d'analyser la cause et de la résoudre. Les VM sont disponibles lorsque leur vCenter Server et les clusters ONTAP hébergeant le stockage des VM sont ajoutés à Unified Manager.

Vous voyez les détails des VM sur la page **VMWARE** > > **Virtual Machines**. 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 VM, du datastore et de l'hôte s'affichent. Pour une VM prenant en charge plusieurs datastores, la grille affiche les métriques du datastore présentant la pire latence, une icône en forme d'astérisque (*) indiquant des datastores supplémentaires. Si vous cliquez sur l'icône, les métriques du datastore supplémentaire s'affichent. Certaines de ces colonnes ne sont pas disponibles pour le tri et le filtrage.

Pour consulter une machine virtuelle et ses détails, la découverte (interrogation ou collecte de métriques) du cluster ONTAP doit être terminée. Si le cluster est supprimé d'Unified Manager, la

machine virtuelle n'est plus disponible après le prochain cycle de découverte.

Cette page permet également de visualiser la topologie détaillée d'une machine virtuelle, en affichant les composants auxquels elle est associée, par exemple l'hôte, le disque virtuel et la banque de données qui y sont connectés. La vue topologique présente les composants sous-jacents dans leurs couches respectives, dans l'ordre suivant : **Disque virtuel** > **VM** > **Hôte** > **Réseau** > **Banque de données** > **VMDK**.

Vous pouvez déterminer le chemin d'E/S et les latences au niveau des composants d'un point de vue topologique et identifier si le stockage est à l'origine du problème de performance. La vue récapitulative de la topologie affiche le chemin d'E/S et met en évidence le composant présentant des problèmes d'IOPS et de latence, vous permettant ainsi de définir les étapes de dépannage. Vous pouvez également afficher une vue détaillée de la topologie, représentant chaque composant individuellement ainsi que sa latence. Vous pouvez sélectionner un composant pour visualiser le chemin d'E/S mis en évidence à travers les différentes couches.

Afficher la topologie récapitulative

Pour identifier les problèmes de performance en visualisant les machines virtuelles dans une topologie récapitulative:

1. Accédez à **VMWARE** > **Machines virtuelles**.
2. Recherchez votre machine virtuelle en saisissant son nom dans le champ de recherche. Vous pouvez également filtrer vos résultats de recherche selon des critères spécifiques en cliquant sur le bouton **Filtrer**. Cependant, si vous ne trouvez pas votre machine virtuelle, vérifiez que le serveur vCenter correspondant a bien été ajouté et détecté.

   Les serveurs vCenter autorisent les caractères spéciaux (tels que %, &, *, $, #, @, !, \, /, :, *, ?, "`, <, >, |, ;, ') dans les noms des entités vSphere, telles que les VM, les clusters, les datastores, les dossiers ou les fichiers. Le serveur VMware vCenter et le serveur ESX/ESXi n'échappent pas les caractères spéciaux utilisés dans les noms d'affichage. Cependant, lorsque le nom est traité dans Unified Manager, il s'affiche différemment. Par exemple, une VM nommée `%$VC_AIQUM_clone_191124%` dans le serveur vCenter s'affiche comme `%25$VC_AIQUM_clone_191124%25` dans Unified Manager. Vous devez tenir compte de ce problème lorsque vous interrogez une VM dont le nom contient des caractères spéciaux.

3. Vérifiez l'état de la VM. Les états de la VM sont récupérés depuis vCenter Server. Les états suivants sont disponibles. Pour plus d'informations sur ces états, consultez la documentation VMware.
   - Normal
   - Avertissement
   - Alerte
   - Non surveillé
   - Inconnu
4. Cliquez sur la flèche vers le bas à côté de la machine virtuelle pour afficher la vue récapitulative de la topologie des composants dans les couches de calcul, de réseau et de stockage. Le nœud présentant des problèmes de latence est mis en évidence. La vue récapitulative affiche la latence la plus élevée des composants. Par exemple, si une machine virtuelle possède plusieurs disques virtuels, cette vue affiche le disque virtuel qui présente la latence la plus élevée 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 au-dessus de l'icône de l'objet datastore. Vous accédez à la page Workload Analysis, où vous pouvez sélectionner une plage horaire et afficher les graphiques de performances du datastore. Pour plus d'informations sur Workload Analyzer, consultez la section *Dépannage des workloads à l'aide de*

Workload Analyzer.

Afficher la topologie étendue

Vous pouvez examiner chaque composant séparément en affichant la topologie développée de la VM.

Étapes

1. Dans la vue topologique récapitulative, cliquez sur **Développer la topologie**. Vous pouvez voir la topologie détaillée de chaque composant séparément avec les valeurs de latence pour chaque objet. S'il y a plusieurs nœuds dans une catégorie, par exemple plusieurs nœuds dans le datastore ou le VMDK, le nœud présentant la latence la plus élevée est mis en évidence en rouge.
2. Pour vérifier le chemin d'E/S d'un objet spécifique, cliquez dessus afin d'afficher ce chemin et le mappage correspondant. Par exemple, pour afficher le mappage d'un disque virtuel, cliquez dessus pour voir son mappage mis en évidence vers le VMDK correspondant. En cas de ralentissement de ces composants, vous pouvez collecter davantage de données depuis ONTAP et dépanner le problème.

> Les métriques ne sont pas rapportées pour les VMDKs. Dans la topologie, seuls les noms des VMDKs sont affichés, et non les métriques.

Informations connexes

"Dépannage des workloads à l'aide du workload Analyzer"

Affichez la visibilité de l'infrastructure virtuelle dans un environnement de reprise après sinistre avec Active IQ Unified Manager

Vous pouvez consulter les indicateurs de configuration et de performance des banques de données hébergées dans une configuration MetroCluster ou une configuration de reprise après sinistre de machine virtuelle de stockage (storage VM) (SVM DR).

Dans Unified Manager, vous pouvez afficher les volumes NAS ou les LUN dans une configuration MetroCluster qui sont rattachés en tant que datastores dans vCenter Server. Les datastores hébergés dans une 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 d'une configuration de reprise après sinistre de machine virtuelle de stockage qui sont mappés aux banques de données dans vCenter Server.

Afficher les banques de données dans la configuration MetroCluster

Notez les prérequis suivants avant d'afficher les datastores dans une configuration MetroCluster :

- En cas de basculement et de rétablissement, la découverte des clusters principal et secondaire de la paire haute disponibilité et des serveurs vCenter doit être terminée.
- Les clusters principal et secondaire de la paire haute disponibilité, ainsi que les serveurs vCenter, doivent être gérés par Unified Manager.
- La configuration requise doit être effectuée sur ONTAP et le serveur vCenter. Pour plus d'informations, consultez la documentation ONTAP et vCenter.

  "Centre de documentation ONTAP 9"

Suivez ces étapes pour afficher les datastores :

1. Sur la page **VMWARE** > **Machines virtuelles**, cliquez sur la machine virtuelle qui héberge le datastore. Cliquez sur **Workload Analyzer** ou sur le lien de l'objet datastore. Dans le scénario standard où le site principal hébergeant le volume ou la LUN fonctionne comme prévu, vous pouvez voir les détails du cluster vServer du site principal.
2. En cas de sinistre et de basculement consécutif vers le site secondaire, le lien vers la banque de données pointe vers les indicateurs de performance du volume ou du LUN dans le cluster secondaire. Cela est pris en compte une fois le prochain cycle de découverte des clusters et des vServer (acquisition) terminé.
3. Après un switchback réussi, le lien du datastore reflète à nouveau les indicateurs de performance du volume ou du LUN dans le cluster principal. Cela se reflète une fois le cycle suivant de découverte des clusters et de vServer terminé.

Afficher les datastores dans la configuration de reprise après sinistre de la VM de stockage

Notez les prérequis suivants avant d'afficher les datastores dans une configuration de reprise après sinistre d'une machine virtuelle de stockage :

- En cas de basculement et de rétablissement, la découverte des clusters principal et secondaire de la paire haute disponibilité et des serveurs vCenter doit être terminée.
- Les clusters source et de destination ainsi que les pairs de VM de stockage doivent être gérés par Unified Manager.
- La configuration requise doit être effectuée sur ONTAP et vCenter Server.
    - Pour les banques de données NAS (NFS et VMFS), en cas de sinistre, les étapes comprennent la mise en service de la VM de stockage secondaire, la vérification des LIF de données et des routes, le rétablissement des connexions perdues sur vCenter Server et le démarrage des VM.

      Pour un retour au site principal, les données entre les volumes doivent être synchronisées avant que le site principal ne commence à servir les données.
    - Pour les datastores SAN (iSCSI et FC pour VMFS), vCenter Server formate la LUN montée au format VMFS. En cas de sinistre, les étapes consistent à démarrer la VM de stockage secondaire et à vérifier les LIF de données et les routes. 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. Ensuite, de nouveaux datastores VMFS avec les nouvelles LUN doivent être créés et les anciennes VM enregistrées avec de nouveaux noms. Les VM doivent être démarrées et opérationnelles.

      En cas de récupération, les données entre les volumes doivent être synchronisées. De nouveaux datastores VMFS doivent être recréés à partir des LUN et les anciennes machines virtuelles doivent être enregistrées sous de nouveaux noms.

      Pour plus d'informations sur la configuration, consultez la documentation de ONTAP et de vCenter Server.

  "Centre de documentation ONTAP 9"

Suivez ces étapes pour afficher les datastores :

1. Sur la page **VMWARE** > **Virtual Machines**, cliquez sur l'inventaire de la VM qui héberge le datastore. Cliquez sur le lien de l'objet datastore. Dans le scénario standard, vous pouvez voir les données de performance des volumes et des LUN dans la VM de stockage principale.
2. En cas de sinistre et de basculement consécutif vers la machine virtuelle de stockage secondaire, le lien de la banque de données pointe vers les indicateurs de performance du volume ou du LUN dans la machine virtuelle de stockage secondaire. Cela est pris en compte une fois le prochain cycle de

découverte (acquisition) des clusters et des vServer terminé.

3. Après un switchback réussi, le lien de la banque de données reflète à nouveau les mesures de performances du volume ou du LUN dans la VM de stockage principale. Cela se reflète une fois le cycle suivant de découverte des clusters et de vServer terminé.

Scénarios non pris en charge

- Pour une configuration MetroCluster, notez les limitations suivantes :
  - Seuls les clusters dans les états `NORMAL` et `SWITCHOVER` sont pris en charge. Les autres états, tels que `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK` et `NOT_REACHABLE`, ne sont pas pris en charge.
  - Sauf si Automatic Switch Over (ASO) est activé, si le cluster principal tombe en panne, le cluster secondaire ne peut pas être découvert, et la topologie continue de pointer vers le volume ou le LUN du cluster principal.
- Pour une configuration de reprise après sinistre d'une machine virtuelle de stockage, notez la limitation suivante :
  - Une configuration dans laquelle Site Recovery Manager (SRM) ou Storage Replication Adapter (SRA) est activé pour un environnement de stockage SAN n'est pas prise en charge.

Provisionner et gérer les charges de travail

Provisionnez et gérez les charges de travail dans Active IQ Unified Manager

La fonctionnalité de gestion active d'Active IQ Unified Manager fournit des niveaux de service de performances, des politiques d'efficacité du stockage et des API de fournisseur de stockage pour le provisionnement, la surveillance et la gestion des workloads de stockage dans un centre de données.

Unified Manager fournit cette fonctionnalité par défaut. Vous pouvez la désactiver dans **Gestion du stockage** > **Paramètres des fonctionnalités** si vous ne prévoyez pas d'utiliser cette fonctionnalité.

Lorsqu'elle est activée, cette fonctionnalité vous permet de provisionner des workloads sur les clusters ONTAP gérés par votre instance de Unified Manager. Vous pouvez également attribuer aux workloads des stratégies, telles que des niveaux de service de performances et des stratégies d'efficacité du stockage, et gérer votre environnement de stockage en fonction de ces stratégies.

Cette fonctionnalité permet les fonctions suivantes :

- Découverte automatique des workloads de stockage sur les clusters ajoutés, permettant une évaluation et un déploiement faciles des workloads de stockage
- Provisionnement des workloads NAS prenant en charge les protocoles NFS et CIFS
- Provisionnement des workloads SAN prenant en charge les protocoles iSCSI et FCP
- Prise en charge des protocoles NFS et CIFS sur le même partage de fichiers
- Gestion des niveaux de service de performances et des politiques d'efficacité du stockage
- Attribution de niveaux de service de performance et de politiques d'efficacité du stockage aux workloads de stockage

Les options **Provisionnement**, **Stockage** > **workloads** et **Stratégies** du volet gauche de l'interface utilisateur vous permettent de modifier différentes configurations.

Vous pouvez effectuer les opérations suivantes à l'aide de ces options :

- Consultez les workloads de stockage sur la page **Storage** > **Workloads**
- Créez des workloads de stockage à partir de la page Provision Workload
- Créer et gérer les niveaux de service de performance à partir des politiques
- Créer et gérer des stratégies d'efficacité du stockage à partir de Policies
- Attribuez des stratégies aux workloads de stockage à partir de la page Workloads

Informations connexes

"Gestion du stockage basée sur des politiques"

Aperçu des workloads

Découvrez le tableau de bord des charges de travail dans Active IQ Unified Manager

Un workload représente les opérations d'entrée/sortie (E/S) d'un objet de stockage, tel qu'un volume ou un LUN. La manière dont le stockage est provisionné repose sur les exigences prévues du workload. Les statistiques du workload sont suivies par Active IQ Unified Manager uniquement après qu'il y a du trafic vers et depuis l'objet de stockage. Par exemple, les valeurs d'IOPS et de latence du workload sont disponibles une fois que les utilisateurs commencent à utiliser une base de données ou une application de messagerie.

La page Charges de travail présente un résumé des charges de travail de stockage des clusters ONTAP gérés par Unified Manager. Elle fournit des informations synthétiques sur les charges de travail de stockage conformes au niveau de service de performance, ainsi que sur celles qui ne le sont pas. Elle permet également d'évaluer la capacité totale, disponible et utilisée, ainsi que les performances (IOPS) des clusters de votre centre de données.

Il est recommandé d'évaluer le nombre de workloads de stockage non conformes, indisponibles ou non gérés par un Performance Service Level, et de prendre les mesures nécessaires pour garantir leur conformité, leur utilisation de la capacité et leurs IOPS.

La page Workloads comporte les deux sections suivantes :

- Aperçu des workloads : fournit un aperçu du nombre de workloads de stockage sur les clusters ONTAP gérés par Unified Manager.
- Vue d'ensemble du centre de données : Fournit une vue d'ensemble de la capacité et des IOPS des charges de travail de stockage dans le centre de données. Les données pertinentes sont affichées au niveau du centre de données et pour chaque élément.

Section Vue d'ensemble des workloads

La section « Aperçu des charges de travail » fournit des informations synthétiques sur les charges de travail de stockage. L'état des charges de travail de stockage est affiché en fonction des niveaux de service de performance attribués et non attribués.

- **Attribué** : Les statuts suivants sont signalés pour les charges de travail de stockage auxquelles des niveaux de service de performance ont été attribués :
  - **Conforme** : les performances des workloads de stockage sont basées sur les niveaux de service de performances qui leur sont attribués. Si les workloads de stockage respectent le seuil de latence défini dans les niveaux de service de performances associés, ils sont marqués comme « `conforme` ». Les workloads conformes sont affichés en bleu.
  - **Non conforme** : Lors de la surveillance des performances, les workloads de stockage sont marqués comme « `non-conforming` » si la latence des workloads de stockage dépasse le seuil de latence défini dans le niveau de service de performances associé. Les workloads non conformes sont marqués en orange.
  - **Indisponible** : Les charges de travail de stockage sont marquées comme « `unavailable` » si elles sont hors ligne ou si le cluster correspondant est inaccessible. Les charges de travail indisponibles sont signalées en rouge.
- **Non attribué** : les workloads de stockage auxquels aucun niveau de service de performances n'est attribué sont signalés comme « `unassigned` ». Le nombre est indiqué par l'icône d'information.

Le nombre total de workloads correspond à la somme des workloads attribués et non attribués.

Vous pouvez cliquer sur le nombre total de workloads affichés dans cette section et les consulter sur la page Workloads.

La sous-section Conformité par niveaux de service de performance affiche le nombre total de workloads de stockage disponibles :

- Conforme à chaque type de niveau de service de performances
- Pour lequel il existe un décalage entre les niveaux de service de performance attribués et les niveaux de service recommandés

Section Vue d'ensemble du centre de données

La section « Vue d'ensemble du centre de données » représente graphiquement la capacité disponible et utilisée, ainsi que les IOPS, pour tous les clusters du centre de données. En utilisant ces données, vous devez gérer la capacité et les IOPS des workloads de stockage. Cette section affiche également les informations suivantes pour les workloads de stockage de l'ensemble des clusters :

- La capacité totale, disponible et utilisée pour tous les clusters de votre centre de données
- Les IOPS totales, disponibles et utilisées pour tous les clusters de votre centre de données
- La capacité disponible et utilisée en fonction de chaque niveau de service de performance
- Les IOPS disponibles et utilisées en fonction de chaque niveau de service de performance
- L'espace total et les IOPS utilisés par les charges de travail auxquelles aucun niveau de service de performance n'est attribué

Comment la capacité et les performances du centre de données sont calculées en fonction des niveaux de service de performance

La capacité utilisée et les IOPS sont récupérés en fonction de la capacité totale utilisée et des performances de tous les workloads de stockage dans les clusters.

Les IOPS disponibles sont calculées en fonction de la latence attendue et des niveaux de service de performance recommandés sur les nœuds. Elles incluent les IOPS disponibles pour tous les niveaux de service de performance dont la latence attendue est inférieure ou égale à leur propre latence attendue.

La capacité disponible est calculée en fonction de la latence attendue et des niveaux de service de performance recommandés pour les agrégats. Elle inclut la capacité disponible pour tous les niveaux de service de performance dont la latence attendue est inférieure ou égale à leur propre latence attendue.

Afficher les charges de travail dans Active IQ Unified Manager

Lorsque vous ajoutez des clusters à Unified Manager, les workloads de stockage de chaque cluster sont automatiquement détectés et affichés sur la page Workloads.

Unified Manager ne commence à analyser les workloads afin de formuler des recommandations (PSL recommandés) qu'après le démarrage des opérations d'E/S sur les workloads de stockage.

FlexGroup volumes et leurs constituants sont exclus.

Aperçu des workloads

La page Workloads Overview affiche la vue d'ensemble des workloads du data center ainsi que la vue d'ensemble de l'espace et des performances du data center.

- Panneau **Workloads Overview** : affiche le nombre total de workloads et le nombre de workloads avec ou sans PSL qui leur sont attribués. La répartition du nombre de workloads pour chaque PSL est également affichée. En cliquant sur les nombres, vous accédez à la vue **All Workloads** avec les workloads filtrés. Vous pouvez également consulter le nombre de workloads non conformes à la recommandation du système et leur attribuer les PSL recommandés par le système en cliquant sur le bouton **Assign System-Recommended PSLs**.
- Panneau **Vue d'ensemble du centre de données** : affiche l'espace disponible et utilisé (Tio) ainsi que les performances (IOPS) du centre de données. La répartition de l'espace disponible et utilisé (Tio) ainsi que des performances (IOPS) de tous les workloads sous chaque PSL est également affichée.

Vue de tous les workloads

La page **Stockage > Workloads > All Workloads** répertorie les workloads de stockage associés aux clusters ONTAP gérés par Unified Manager.

Pour les workloads de stockage nouvellement découverts sur lesquels aucune opération d'E/S n'a eu lieu, le statut est « `Waiting for I/O` ». Après le début des opérations d'E/S sur les workloads de stockage, Unified Manager commence l'analyse et le statut du workload devient « `Learning…` ». Une fois l'analyse terminée (dans les 24 heures suivant le début des opérations d'E/S), les PSL recommandés s'affichent pour les workloads de stockage.

Cette page vous permet également d'attribuer des politiques d'efficacité du stockage (SEP) et des niveaux de service de performance (PSL) aux workloads de stockage. Vous pouvez effectuer plusieurs tâches :

- Ajouter ou provisionner des workloads de stockage
- Afficher et filtrer la liste des workloads
- Attribuer des PSL aux workloads de stockage
- Évaluer les PSL recommandés par le système et les affecter aux workloads
- Attribuer des SEP aux workloads de stockage

Ajout ou provisionnement de workloads de stockage

Vous pouvez ajouter ou provisionner des workloads de stockage sur les LUN prises en charge (prenant en

charge les protocoles iSCSI et FCP), les partages de fichiers NFS et les partages SMB.

Étapes

1. Cliquez sur **Stockage > Workloads > Tous les workloads > Créer**.
2. Créez des workloads. Pour plus d'informations, consultez "Provisionnement et gestion des workloads".

Affichage et filtrage des workloads

Sur l'écran « Toutes les charges de travail », vous pouvez afficher toutes les charges de travail de votre centre de données ou rechercher des charges de travail de stockage spécifiques en fonction de leurs PSL ou de leur nom. Vous pouvez utiliser l'icône de filtre pour saisir des conditions spécifiques pour votre recherche. Vous pouvez effectuer une recherche selon différents critères de filtre, tels que le cluster hôte ou la machine virtuelle de stockage. L'option « Capacité totale » permet de filtrer selon la capacité totale des charges de travail (en MB). Toutefois, dans ce cas, le nombre de charges de travail renvoyées peut varier, car la capacité totale est comparée au niveau de l'octet.

Pour chaque workload, des informations telles que le cluster hôte et la VM de stockage sont affichées, ainsi que le PSL et le SEP attribués.

Cette page vous permet également de consulter les détails de performance d'un workload. Vous pouvez afficher des informations détaillées sur les IOPS, la capacité et la latence du workload en cliquant sur le bouton **Choisir / Ordonner les colonnes** et en sélectionnant les colonnes spécifiques à afficher. La colonne « Vue des performances » affiche les IOPS moyennes et de pointe d'un workload, et vous pouvez cliquer sur l'icône de l'analyseur de workload pour afficher l'analyse détaillée des IOPS.

Analyse des critères de performance et de capacité d'un workload

Le bouton **Analyze Workload** de la fenêtre contextuelle **IOPS Analysis** vous redirige vers la page Workload Analysis, où vous pouvez sélectionner une plage horaire et afficher les tendances de latence, de débit et de capacité pour le workload sélectionné. Pour plus d'informations sur l'analyseur de workload, consultez "Dépannage des workloads à l'aide de l'analyseur de workload".

Pour faciliter le dépannage, vous pouvez consulter les informations de performance d'un workload en cliquant sur l'icône de graphique à barres dans la colonne **Performance View**. Pour afficher les graphiques de performance et de capacité sur la page **Workload Analysis** afin d'analyser l'objet, cliquez sur le bouton **Analyze Workload**.

Pour plus d'informations, consultez "Quelles données l'analyseur de workload affiche-t-il ?".

Attribuez des stratégies aux charges de travail dans Active IQ Unified Manager

Vous pouvez attribuer des politiques d'efficacité du stockage (SEP) et des niveaux de service de performance (PSL) aux workloads de stockage à partir de la page Toutes les charges de travail, à l'aide des différentes options de navigation.

Attribuer des politiques à un seul workload

Vous pouvez affecter un PSL, un SEP ou les deux à un même workload. Procédez comme suit :

1. Sélectionnez le workload.
2. Cliquez sur l'icône de modification à côté de la ligne, puis cliquez sur **Modifier**.

   Les champs **Niveau de service de performance attribué** et **Politique d'efficacité du stockage** sont

activés.

3. Sélectionnez le PSL ou le SEP requis, ou les deux.
4. Cliquez sur l'icône de validation pour appliquer les modifications.

Vous pouvez également sélectionner un workload et cliquer sur **Plus d'actions** pour attribuer les stratégies.

Attribuer des politiques à plusieurs workloads de stockage

Vous pouvez affecter un PSL ou un SEP à plusieurs workloads de stockage simultanément. Procédez comme suit :

1. Cochez les cases correspondant aux workloads auxquels vous souhaitez attribuer la stratégie, ou sélectionnez tous les workloads de votre data center.
2. Cliquez sur **More Actions**.
3. Pour attribuer un PSL, sélectionnez **Assign Performance Service Level**. Pour attribuer un SEP, sélectionnez **Assign Storage Efficiency Policy**. Une fenêtre contextuelle s'affiche pour vous permettre de sélectionner la stratégie.
4. Sélectionnez la stratégie appropriée et cliquez sur **Appliquer**. Le nombre de workloads auxquels les stratégies sont attribuées s'affiche. Les workloads auxquels les stratégies ne sont pas attribuées sont également répertoriés, avec la raison.

L'application de stratégies à des charges de travail en masse peut prendre un certain temps selon le nombre de charges de travail sélectionnées. Vous pouvez cliquer sur le bouton **Exécuter en arrière-plan** et poursuivre vos autres tâches pendant l'exécution de l'opération en arrière-plan. Une fois l'attribution en masse terminée, vous pouvez consulter l'état d'achèvement. Si vous appliquez une PSL à plusieurs charges de travail, vous ne pouvez pas déclencher une autre requête pendant l'exécution de la tâche précédente d'attribution en masse.

Attribuer les PSL recommandés par le système aux workloads

Vous pouvez attribuer des PSLs recommandées par le système aux workloads de stockage d'un centre de données qui n'ont aucune PSL attribuée, ou dont les PSLs attribuées ne correspondent pas à la recommandation du système. Pour utiliser cette fonctionnalité, cliquez sur le bouton **Attribuer les PSLs recommandées 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 workloads dont les IOPS et les autres paramètres ne correspondent à aucune définition de PSL disponible. Les workloads de stockage avec les statuts `Waiting for I/O` et « Apprentissage » sont également exclus.

Unified Manager recherche des mots-clés spécifiques dans le nom du workload afin de remplacer l'analyse du système et de recommander un autre PSL pour le workload. Lorsque le nom du workload contient les lettres "ora", le PSL **Extreme Performance** est recommandé. Et lorsque le nom du workload contient les lettres "vm", le PSL **Performance** est recommandé.

Voir également l'article de la base de connaissances (KB) "La fonctionnalité « Attribuer au système le niveau de service de performance recommandé » d'ActiveIQ Unified Manager ne s'adapte pas à un workload très variable"

Provisionnez des volumes de partage de fichiers dans Active IQ Unified Manager

Vous pouvez créer des volumes de partage de fichiers qui prennent en charge les protocoles CIFS/SMB et NFS sur un cluster existant et une Storage Virtual Machine (storage VM) existante à partir de la page Provision Workload.

Avant de commencer

- La machine virtuelle de stockage doit disposer d'espace pour le provisionnement du volume de partage de fichiers.
- L'un des services SMB ou NFS, ou les deux, doit être activé sur votre machine virtuelle de stockage.
- Pour sélectionner et attribuer le niveau de service de performance (PSL) et la politique d'efficacité du stockage (SEP) au workload, vous devez avoir créé les politiques avant de commencer à créer le workload.

Étapes

1. Sur la page **Provisionner le workload**, ajoutez le nom du workload que vous souhaitez créer, puis sélectionnez le cluster dans la liste disponible.
2. En fonction du cluster sélectionné, le champ **VM de stockage** filtre les VM de stockage disponibles pour ce cluster. Sélectionnez la VM de stockage souhaitée dans la liste.

   En fonction des services SMB et NFS pris en charge par la machine virtuelle de stockage, l'option NAS est activée dans la section Informations sur l'hôte.

3. Dans la section Stockage et optimisation, attribuez la capacité de stockage et le PSL, et éventuellement un SEP pour la workload.

   Les spécifications du SEP sont attribuées au LUN et les définitions du PSL sont appliquées au workload lors de sa création.

4. Cochez la case à cocher **Enforce performance limits** si vous souhaitez appliquer le PSL que vous avez attribué au workload.

   L'attribution d'un PSL à un workload garantit que l'agrégat sur lequel le workload est créé peut prendre en charge les objectifs de performance et de capacité définis dans la politique correspondante. Par exemple, si un workload se voit attribuer le PSL « Extreme Performance », l'agrégat sur lequel le workload doit être provisionné doit être capable de prendre en charge les objectifs de performance et de capacité de la politique « Extreme Performance », comme le stockage SSD.

   Si vous ne cochez pas cette case à cocher, le PSL n'est pas appliqué au workload et l'état du workload sur le tableau de bord apparaît comme non attribué.

5. Sélectionnez l'option **NAS**.

   Si vous ne voyez pas l'option **NAS** activée, vérifiez si la machine virtuelle de stockage que vous avez sélectionnée prend en charge SMB ou NFS, ou les deux.

   Si votre machine virtuelle de stockage est activée pour les services SMB et NFS, vous pouvez cocher les cases à cocher **Partager par NFS** et **Partager par SMB** et créer un partage de fichiers prenant en charge les protocoles NFS et SMB. Si vous souhaitez créer un partage SMB ou un partage CIFS, cochez uniquement la case à cocher correspondante.

6. Pour les volumes de partage de fichiers NFS, spécifiez l'adresse IP de l'hôte ou du réseau permettant d'accéder au volume de partage de fichiers. Vous pouvez saisir des valeurs séparées par des virgules pour plusieurs hôtes.

   Lors de l'ajout de l'adresse IP de l'hôte, une vérification interne est effectuée pour faire correspondre les détails de l'hôte avec la machine virtuelle de stockage, et les règles d'export pour cet hôte sont créées ou, si une règle existe déjà, elles sont réutilisées. Si plusieurs partages NFS sont créés pour le même hôte, des règles d'export disponibles pour le même hôte avec des règles correspondantes sont réutilisées pour tous les partages de fichiers. La fonction permettant de spécifier les règles de stratégies individuelles ou de réutiliser des stratégies en fournissant des clés de stratégie spécifiques est disponible lorsque vous provisionnez le partage NFS à l'aide des 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**.

   Le workload est ajouté à la liste des workloads de stockage.

Provisionnez des LUN dans Active IQ Unified Manager

Vous pouvez créer des LUN qui prennent en charge les protocoles CIFS/SMB et NFS sur un cluster existant et une Storage Virtual Machine (storage VM) existante à partir de la page Provision Workload.

Avant de commencer

- La machine virtuelle de stockage doit disposer d'espace pour provisionner le LUN.
- Les protocoles 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 performance (PSL) et la politique d'efficacité du stockage (SEP) au workload, vous devez avoir créé les politiques avant de commencer à créer le workload.

Étapes

1. Sur la page **Provisionner le workload**, ajoutez le nom du workload que vous souhaitez créer, puis sélectionnez le cluster dans la liste disponible.

   En fonction du cluster que vous avez sélectionné, le champ **STORAGE VM** filtre les machines virtuelles de stockage disponibles pour ce cluster.

2. Sélectionnez dans la liste la machine virtuelle de stockage qui prend en charge les services iSCSI et FCP.

   En fonction de votre sélection, l'option SAN est activée dans la section Informations sur l'hôte.

3. Dans la section **Stockage et optimisation**, attribuez la capacité de stockage et le PSL, et éventuellement le SEP pour le workload.

   Les spécifications du SEP sont attribuées au LUN et les définitions du PSL sont appliquées au workload lors de sa création.

4. Cochez la case à cocher **Enforce performance limits** si vous souhaitez appliquer le PSL attribué au workload.

   L'attribution d'un PSL à un workload garantit que l'agrégat sur lequel le workload est créé peut prendre en

charge les objectifs de performance et de capacité définis dans la politique correspondante. Par exemple, si un workload se voit attribuer le PSL « Performances extrêmes », l'agrégat sur lequel le workload doit être provisionné doit être capable de prendre en charge les objectifs de performance et de capacité de la politique « Performances extrêmes », comme le stockage SSD.

> À moins que vous ne cochiez cette case à cocher, le PSL n'est pas appliqué au workload, et l'état du workload sur le tableau de bord apparaît comme `unassigned`.

5. Sélectionnez l'option **SAN**. Si vous ne voyez pas l'option **SAN** activée, vérifiez si la machine virtuelle de stockage que vous avez sélectionnée prend en charge iSCSI et FCP.
6. Sélectionnez le système d'exploitation hôte.
7. Spécifiez le mappage de l'hôte pour contrôler l'accès des initiateurs au LUN. Vous pouvez affecter des groupes d'initiateurs existants (igroups) ou définir et mapper de nouveaux igroups.

   > Si vous créez un nouvel igroup lors du provisionnement du LUN, vous devrez attendre le prochain cycle de découverte (jusqu'à 15 minutes) avant de pouvoir l'utiliser. Il est donc recommandé d'utiliser un igroup existant dans la liste des igroups disponibles.

   Si vous souhaitez créer un nouvel igroup, sélectionnez le bouton **Créer un nouveau groupe d'initiateurs** et saisissez les informations pour l'igroup.

8. Cliquez sur **Enregistrer**.

   Le LUN est ajouté à la liste des workloads de stockage.

Gérer les niveaux de service de performance

Gérer les niveaux de service de performance dans Active IQ Unified Manager

Un niveau de service de performance (PSL) vous permet de définir les objectifs de performance et de stockage d'un workload. Vous pouvez attribuer un PSL à un workload lors de sa création initiale, ou ultérieurement en le modifiant.

La gestion et la surveillance des ressources de stockage reposent sur les objectifs de niveau de service (SLO). Les SLO sont définis par des accords de niveau de service basés sur les performances et la capacité requises. Dans Unified Manager, les SLO font référence aux définitions PSL des applications exécutées sur le stockage NetApp. Les services de stockage se différencient selon les performances et l'utilisation des ressources sous-jacentes. Un PSL est une description des objectifs du service de stockage. Un PSL permet au fournisseur de stockage de spécifier les objectifs de performance et de capacité pour le workload. Lorsque vous attribuez un PSL à un workload, le workload correspondant sur ONTAP est géré en fonction de ses objectifs de performance et de capacité. Chaque PSL est régi par des IOPS de pointe, attendues et minimales absolues, ainsi que par la latence attendue.

Unified Manager comprend les types de PSL suivants :

- **Définies par le système** : Unified Manager fournit quelques stratégies prédéfinies qui ne peuvent pas être modifiées. Ces PSL prédéfinies sont :
  - Performances extrêmes
  - Performances
  - Valeur

Les PSL Extreme Performance, Performance et Value s'appliquent à la plupart des workloads de stockage courants dans un centre de données.

Unified Manager propose également trois niveaux de service de performance pour les applications de base de données. Il s'agit de PSL à très hautes performances qui prennent en charge des pics d'IOPS et conviennent aux applications de base de données exigeant le débit le plus élevé.

  - Extrême pour les journaux de bases de données
  - Extrême pour les données partagées de bases de données
  - Extrême pour les données de base de données

- **Personnalisé par l'utilisateur** : Si les niveaux de service de performance prédéfinis ne répondent pas à vos exigences, vous pouvez créer de nouveaux niveaux de service de performance (PSL) adaptés à vos besoins. Pour plus d'informations, consultez "Créer et modifier les niveaux de service de performances".
- **Beyond Extreme** : les PSL Beyond Extreme sont les PSL recommandés par le système pour les workloads qui exigent des IOPS supérieures à celles d'**Extreme**. Les workloads sont analysés en interne en fonction de leurs IOPS, de leur capacité et de leur latence, et un PSL Beyond Extreme est recommandé pour chacun de ces workloads sur l'écran **Storage > Workloads > All Workloads**. Vous pouvez appliquer les PSL aux workloads pour garantir des performances optimales.

  Les paramètres IOPs des charges de travail sont générés dynamiquement en fonction du comportement de la charge de travail et ajoutés au nom du PSL Beyond Extreme au format `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Par exemple, si le système détermine qu'une charge de travail a des IOPs de pointe et attendues de `106345` et `37929` respectivement, le PSL Beyond Extreme généré pour la charge de travail est nommé `Beyond Extreme 106345 37929`. Bien que ces PSL soient recommandés par le système, lorsque vous les affectez à des charges de travail, leur type est indiqué comme `User-defined`.

Gérez les workloads en attribuant des PSL

Vous pouvez accéder aux PSLs depuis la page **Stratégies** > **Niveaux de service de performance** et à l'aide des API du fournisseur de stockage. La gestion des workloads de stockage par l'attribution de PSLs est pratique, car vous n'avez pas à gérer individuellement les workloads de stockage. Toute modification peut également être gérée en réattribuant un autre PSL plutôt qu'en les gérant individuellement. Unified Manager vous aide à attribuer des PSLs à vos workloads en fonction d'évaluations et de recommandations internes.

Pour plus d'informations sur l'attribution des PSL recommandés par le système aux workloads, consultez "Attribuer les PSL recommandés par le système aux workloads"

La page « Niveaux de service de performance » répertorie les politiques PSL disponibles et vous permet de les ajouter, de les modifier et de les supprimer.

> Vous ne pouvez pas modifier une PSL définie par le système ou actuellement assignée à une workload. Vous ne pouvez pas supprimer une PSL assignée à une workload, ou s'il s'agit de la seule PSL disponible.

Cette page affiche les informations suivantes :

Champ	Description
Nom	Nom du PSL.
Type	Si la stratégie est définie par le système ou par l'utilisateur.

Champ	Description
IOPS/TB attendus	Nombre minimal d'IOPS qu'une application est censée effectuer sur un LUN ou un partage de fichiers. Les IOPS attendues spécifient le nombre minimal d'IOPS allouées, en fonction de la taille allouée à l'objet de stockage.
Pic d'IOPS/TB	Nombre maximal d'IOPS qu'une application peut effectuer sur un LUN ou un partage de fichiers. Les IOPS maximales indiquent le nombre maximal d'IOPS pouvant être allouées, en fonction de la taille allouée ou de la taille utilisée de l'objet de stockage. Les IOPS maximales sont basées sur une politique d'allocation. La politique d'allocation est soit allocated-space, soit used-space. Lorsque la politique d'allocation est définie sur allocated-space, les IOPS maximales sont calculées en fonction de la taille de l'objet de stockage. Lorsque la politique d'allocation est définie sur used-space, les IOPS maximales sont calculées en fonction de la quantité de données stockées dans l'objet de stockage, en tenant compte des efficacités de stockage. Par défaut, la politique d'allocation est définie sur used-space.

Champ	Description
IOPS minimales absolues	La valeur minimale absolue d'IOPS est utilisée en priorité lorsque les IOPS attendues sont inférieures à cette valeur. Les valeurs par défaut des PSL définies par le système sont les suivantes : • Performances extrêmes : si les IOPS attendues sont supérieures ou égales à 6144/To, alors le minimum absolu d'IOPS est de 1000 • Performances : si le nombre d'IOPS attendu est supérieur ou égal à 2048/To et inférieur à 6144/To, alors le nombre minimal absolu d'IOPS est de 500 • Valeur : Si le nombre d'IOPS attendu est >= 128/To et < 2048/To, alors le nombre minimal absolu d'IOPS = 75 Les valeurs par défaut des PSL de base de données définies par le système sont les suivantes : • Extrême pour les journaux de base de données : si le nombre d'IOPS attendu est supérieur ou égal à 22 528, alors le nombre minimal absolu d'IOPS est de 4 000 • Extrême pour les données partagées de base de données : si le nombre d'IOPS attendu est supérieur ou égal à 16 384, alors le nombre minimal absolu d'IOPS est de 2 000 • Extrême pour les données de base de données : si le nombre d'IOPS attendu est supérieur ou égal à 12288, alors le nombre minimal absolu d'IOPS est de 2000 La valeur supérieure de l'IOPS minimale absolue pour les PSL personnalisés peut être de 75000 au maximum. La valeur inférieure est calculée comme suit : 1000/latence attendue
Latence attendue	Latence attendue pour les IOPS de stockage en millisecondes par opération (ms/op).
Capacité	Capacité totale disponible et utilisée dans les clusters.
Charges de travail	Nombre de charges de travail de stockage auxquelles le PSL a été attribué.

Pour plus d'informations sur la manière dont les IOPS de pointe et les IOPS attendues contribuent à l'obtention de performances différenciées et cohérentes sur les clusters ONTAP, consultez l'article de la base de connaissances suivant : "Qu'est-ce que la budgétisation axée sur les résultats ?"

Événements générés pour les workloads dépassant le seuil défini par les PSL

Notez que si les charges de travail dépassent la valeur de latence attendue pendant 30 % du temps au cours de l'heure précédente, Unified Manager génère l'un des événements suivants pour vous avertir d'un problème de performance potentiel :

- Le seuil de latence du volume de workload a été dépassé, comme défini par la stratégie de niveau de service de performances.
- La latence de la LUN du workload a dépassé le seuil défini par la politique de niveau de service de performance.

Vous souhaiterez peut-être analyser le workload pour déterminer 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'un seuil de performance est dépassé"
- "Comment Unified Manager utilise la latence du workload pour identifier les problèmes de performance"
- "Que sont les événements de performance"

PSL définis par le système

Le tableau suivant fournit des informations sur les PSL définis par le système :

Niveau de service de performances	Description et utilisation	Latence attendue (ms/op)	IOPS de pointe	IOPS attendus	IOPS minimales absolues
Performances extrêmes	Offre un débit extrêmement élevé avec une latence très faible Idéal pour les applications sensibles à la latence	1	12288	6144	1000
Performances	Offre un débit élevé avec une faible latence Idéal pour les bases de données et les applications virtualisées	2	4096	2048	500

Niveau de service de performances	Description et utilisation	Latence attendue (ms/op)	IOPS de pointe	IOPS attendus	IOPS minimales absolues
Valeur	Offre une capacité de stockage élevée et une latence modérée Idéal pour les applications à haute capacité telles que la messagerie électronique, le contenu web, le partage de fichiers et les cibles de sauvegarde	17	512	128	75
Extrême pour les journaux de bases de données	Offre un débit maximal avec une latence minimale. Idéal pour les applications de base de données prenant en charge les journaux de base de données. Ce PSL offre le débit le plus élevé, car les journaux de base de données présentent des pics d'activité très importants et la journalisation est constamment sollicitée.	1	45056	22528	4000

Niveau de service de performances	Description et utilisation	Latence attendue (ms/op)	IOPS de pointe	IOPS attendus	IOPS minimales absolues
Extrême pour les données partagées de bases de données	Offre un débit très élevé à la latence la plus faible. Idéal pour les applications de base de données dont les données sont stockées dans un espace de stockage commun, mais partagées entre plusieurs bases de données.	1	32768	16384	2000
Extrême pour les données de base de données	Offre un débit élevé avec la latence la plus faible. Idéal pour les données d'applications de base de données, telles que les informations de table de base de données et les métadonnées.	1	24576	12288	2000

Créer et modifier les niveaux de service de performance dans Active IQ Unified Manager

Lorsque les niveaux de service de performance définis par le système ne correspondent pas aux exigences de votre workload, vous pouvez créer vos propres niveaux de service de performance optimisés pour vos workloads.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.
- Le nom du niveau de service de performance doit être unique, et vous ne pouvez pas utiliser les mots-clés réservés suivants :

  `Prime`, `Extreme`, `Performance`, `Value`, `Unassigned`, `Learning`, `Idle`, `Default`, et `None`.

Vous créez et modifiez des Performance Service Levels personnalisés à partir de la page Performance Service Levels en définissant les objectifs de niveau de service requis pour les applications qui accéderont au stockage.

Vous ne pouvez pas modifier un niveau de service de performance s'il est actuellement attribué à un workload.

Étapes

1. Dans le volet de navigation de gauche sous **Paramètres**, sélectionnez **Stratégies** > **Niveaux de service de performance**.
2. Sur la page **Niveaux de service de performance**, cliquez sur le bouton approprié selon que vous souhaitez créer un nouveau niveau de service de performance ou modifier un niveau de service de performance existant.

À…	Suivez ces étapes…
Créer un nouveau niveau de service de performance	Cliquez sur **Add**.
Modifier un niveau de service de performance 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 Performance Service Level en spécifiant les objectifs de performance, puis cliquez sur **Submit** pour enregistrer le Performance Service Level.

Vous pouvez appliquer le niveau de service de performance nouveau ou modifié aux workloads (LUN, partages de fichiers NFS, partages CIFS) à partir de la page Charges de travail ou lors du provisionnement d'un nouveau workload.

Gérer les stratégies d'efficacité du stockage

Gérer les politiques d'efficacité du stockage dans Active IQ Unified Manager

Une stratégie d'efficacité du stockage (SEP) vous permet de définir les caractéristiques d'efficacité du stockage d'un workload. Vous pouvez attribuer une SEP à un workload lors de la création initiale du workload, ou ultérieurement en modifiant le workload.

L'efficacité du stockage comprend l'utilisation de technologies telles que le thin provisioning, la déduplication et la compression des données, qui augmentent l'utilisation du stockage et réduisent les coûts de stockage. Lors de la création de SEP, vous pouvez utiliser ces technologies d'économie d'espace individuellement ou conjointement pour obtenir une efficacité maximale du stockage. Lorsque vous associez les stratégies à vos workloads de stockage, les paramètres de stratégie spécifiés leur sont attribués. Unified Manager vous permet d'attribuer des SEP définies par le système et par l'utilisateur afin d'optimiser les ressources de stockage de votre centre de données.

Unified Manager fournit deux SEP définies par le système : High et Low. Ces SEP s'appliquent à la plupart des workloads de stockage dans un centre de données, toutefois, vous pouvez créer vos propres politiques si les SEP définies par le système ne répondent pas à vos exigences.

Vous ne pouvez pas modifier une SEP définie par le système ou actuellement affectée à un workload. Vous ne pouvez pas supprimer une SEP affectée à un workload, ou s'il s'agit de la seule SEP disponible.

La page « Politiques d'efficacité du stockage » répertorie les SEP disponibles et vous permet d'ajouter, de modifier et de supprimer des SEP personnalisées. Cette page affiche les informations suivantes :

Champ	Description
Nom	Nom du SEP.
Type	Si la stratégie est définie par le système ou par l'utilisateur.
Réserve d'espace	Si le volume est à provisionnement fin ou à provisionnement épais.
Déduplication	Si la déduplication est activée sur la workload: • En ligne : la déduplication s'effectue pendant l'écriture sur le workload • Contexte : La déduplication se produit dans le workload • Désactivée : la déduplication est désactivée sur le workload
Compression	Indique si la compression des données est activée sur le workload : • En ligne : la compression des données s'effectue lors de leur écriture sur le workload • Contexte : la compression des données se produit dans le workload • Désactivation : la compression des données est désactivée sur le workload
Charges de travail	Nombre de workloads de stockage auxquels le SEP a été attribué

Lignes directrices pour la création d'une politique d'efficacité du stockage personnalisée

Si les SEP existants ne répondent pas aux exigences de stratégie pour vos workloads de stockage, vous pouvez créer un SEP personnalisé. Toutefois, il est recommandé d'utiliser les SEP définis par le système pour vos workloads de stockage et de ne créer des SEP personnalisés qu'en cas de nécessité.

Vous pouvez consulter le SEP attribué aux workloads sur la page « Tous les workloads » et sur la page des détails du volume / de l'état de santé. Vous pouvez consulter le taux de réduction des données au niveau du cluster (sans les copies Snapshot) en fonction de ces gains d'efficacité du stockage dans le panneau « Capacité » du tableau de bord et dans la vue « Capacité : Tous les clusters ».

Créez et modifiez des stratégies d'efficacité du stockage dans Active IQ Unified Manager

Lorsque les politiques d'efficacité du stockage définies par le système ne correspondent pas aux exigences de votre workload, vous pouvez créer vos propres politiques d'efficacité du stockage optimisées pour vos workloads.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.
- 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 Storage Efficiency Policies personnalisées depuis la page Storage Efficiency Policies en définissant les caractéristiques d'efficacité du stockage requises pour les applications qui accéderont au stockage.

> Vous ne pouvez pas modifier une stratégie d'efficacité du stockage si elle est actuellement attribuée à un workload.

Étapes

1. Dans le volet de navigation de gauche, sous **Paramètres**, sélectionnez **Stratégies** > **Efficacité du stockage**.
2. Dans la page **Storage Efficiency Policies**, cliquez sur le bouton approprié selon que vous souhaitez créer une nouvelle Storage Efficiency Policy ou modifier une Storage Efficiency Policy existante.

À…	Suivez ces étapes…
Créer une nouvelle politique d'efficacité du stockage	Cliquez sur **Ajouter**
Modifier une politique d'efficacité du stockage existante	Sélectionnez une politique d'efficacité du stockage existante et cliquez sur **Modifier**

   La page permettant d'ajouter ou de modifier une politique d'efficacité du stockage s'affiche.

3. Personnalisez la politique d'efficacité du stockage en spécifiant les caractéristiques d'efficacité du stockage, puis cliquez sur **Submit** pour enregistrer la politique d'efficacité du stockage.

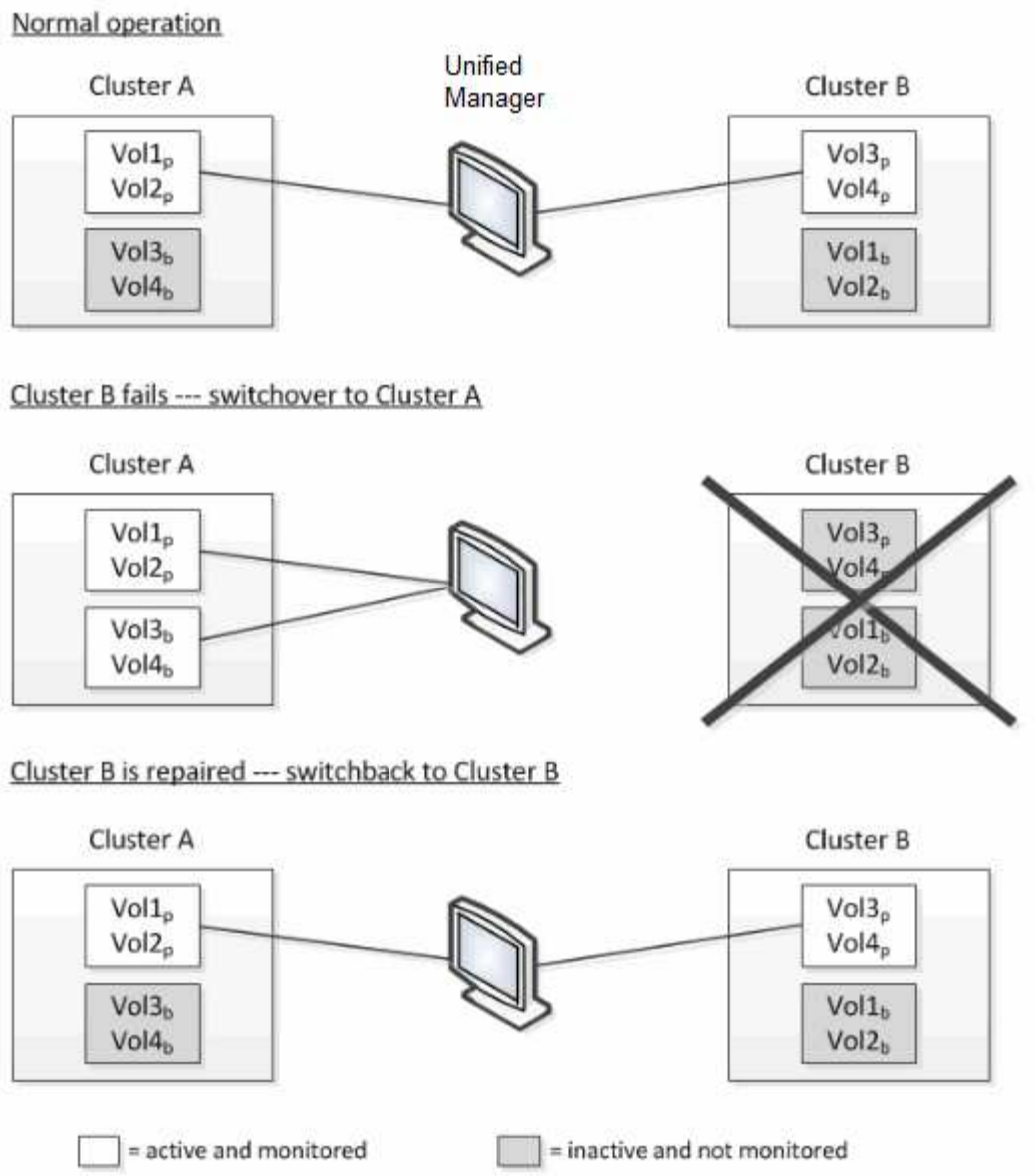
Vous pouvez appliquer la nouvelle stratégie d'efficacité du stockage ou la stratégie modifiée aux workloads (LUN, partages de fichiers NFS, partages CIFS) à partir de la page Workloads ou lors du provisionnement d'un nouveau workload.

Gérer et surveiller les configurations MetroCluster

Découvrez le comportement du volume lors des basculements et des retours en arrière dans Active IQ Unified Manager

Les événements qui déclenchent un switchover ou un switchback entraînent le déplacement des volumes actifs d'un cluster à l'autre dans le groupe de reprise après sinistre. Les volumes du cluster qui étaient actifs et fournissaient des données aux clients sont arrêtés, tandis que les volumes de l'autre cluster sont activés et commencent à fournir des données. Unified Manager surveille uniquement les volumes qui sont actifs et en service.

Étant donné que des volumes sont déplacés d'un cluster à l'autre, il est recommandé de surveiller les deux clusters. Une seule instance de Unified Manager peut surveiller les deux clusters dans une configuration MetroCluster, mais la distance entre les deux emplacements nécessite parfois l'utilisation de deux instances de Unified Manager pour surveiller les deux clusters. La figure suivante montre une seule instance de Unified Manager :



Les volumes dont le nom contient un p indiquent les volumes principaux, et les volumes dont le nom contient un b sont des volumes de sauvegarde en miroir créés par SnapMirror.

En fonctionnement normal:

- Le cluster A comporte deux volumes actifs : Vol1p et Vol2p.
- Le cluster B comporte deux volumes actifs : Vol3p et Vol4p.
- Le cluster A comporte deux volumes inactifs : Vol3b et Vol4b.
- Le cluster B comporte deux volumes inactifs : Vol1b et Vol2b.

Unified Manager collecte les informations relatives à chaque volume actif (statistiques, événements, etc.). Les statistiques des volumes Vol1p et Vol2p sont collectées par Cluster A, et celles des volumes Vol3p et Vol4p par Cluster B.

Suite à une panne catastrophique entraînant un basculement des volumes actifs du Cluster B vers le Cluster A :

- Le cluster A comporte quatre volumes actifs : Vol1p, Vol2p, Vol3b et Vol4b.

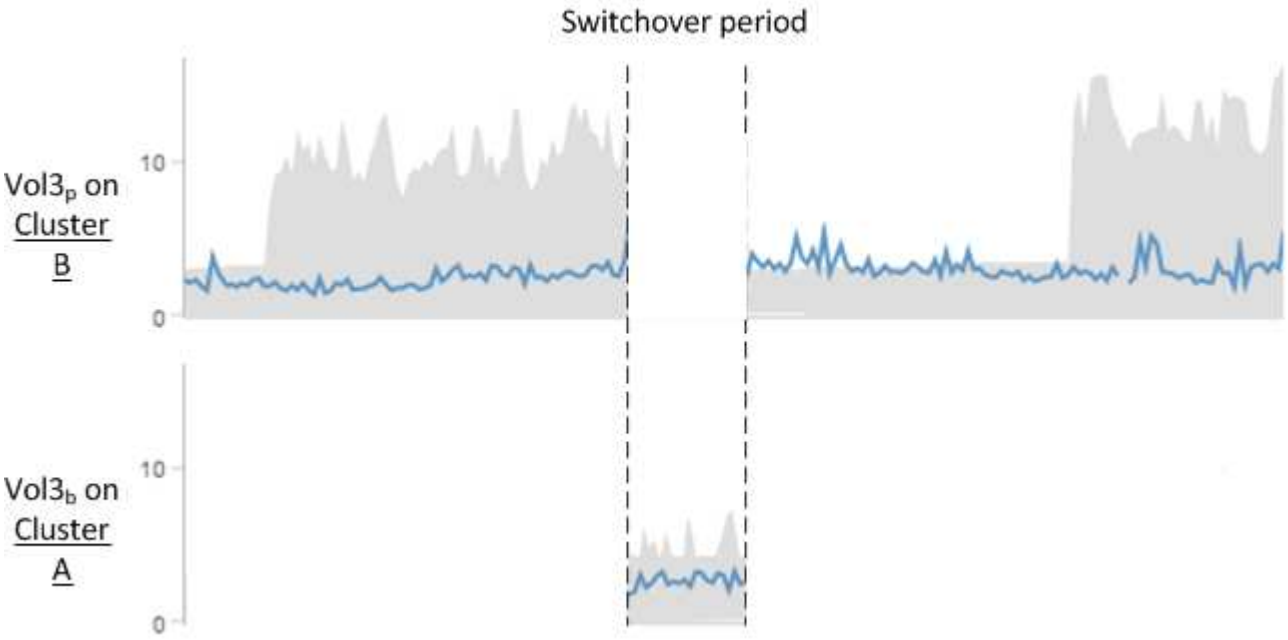
- Le cluster B comporte quatre volumes inactifs : Vol3p, Vol4p, Vol1b et Vol2b.

Comme pendant le fonctionnement normal, Unified Manager collecte les informations relatives à chacun des volumes actifs. Mais dans ce cas, les statistiques de Vol1p et Vol2p sont collectées par Cluster A, et les statistiques de Vol3b et Vol4b sont également collectées par Cluster A.

Notez que Vol3p et Vol3b ne sont pas les mêmes volumes, car ils se trouvent sur des clusters différents. Les informations affichées dans Unified Manager pour Vol3p diffèrent de celles de Vol3b.

- Lors du basculement vers Cluster A, les statistiques et les événements Vol3p ne sont pas visibles.
- Dès le premier basculement, Vol3b apparaît comme un nouveau volume sans aucune information historique.

Une fois le Cluster B réparé et le basculement rétabli effectué, Vol3p est de nouveau actif sur le Cluster B, avec l'historique des statistiques et une absence de statistiques pour la période du basculement. Vol3b n'est pas visible depuis le Cluster A tant qu'un autre basculement ne se produit pas :



- Les volumes MetroCluster inactifs, par exemple Vol3b sur le cluster A après switchback, sont identifiés par le message « `This volume was deleted` ». Le volume n'est pas réellement supprimé, mais il n'est pas actuellement surveillé par Unified Manager, car il ne s'agit pas du volume actif.
- Si un seul Unified Manager surveille les deux clusters dans une configuration MetroCluster, la recherche de volume renvoie les informations du volume actif à ce moment-là. Par exemple, une recherche sur « Vol3 » renverra les statistiques et les événements de Vol3b sur Cluster A si un basculement a eu lieu et que Vol3 est devenu actif sur Cluster A.

Comprendre la connectivité des clusters dans une configuration MetroCluster sur FC dans Active IQ Unified Manager

La connectivité entre les clusters dans une configuration MetroCluster over FC peut présenter l'un des états suivants : Optimal, Impacted ou Down. La compréhension des états de connectivité vous permet de gérer efficacement vos configurations MetroCluster.

État de la connectivité	Description	Icône affichée
Optimal	La connectivité entre les clusters dans la configuration MetroCluster est normale.	
Impacté	Une ou plusieurs erreurs compromettent l'état de disponibilité du basculement ; toutefois, les deux clusters de la configuration MetroCluster restent opérationnels. Par exemple, en cas de panne de la liaison ISL, de panne de la liaison IP intercluster ou d'inaccessibilité du cluster partenaire.	
En panne	La connectivité entre les clusters dans la configuration MetroCluster est interrompue, car l'un des clusters ou les deux sont hors service ou que les clusters sont en mode de basculement. Par exemple, lorsque le cluster partenaire est hors service à la suite d'un sinistre ou lors d'un basculement planifié à des fins de test.	Basculement avec erreurs:  Basculement réussi: 

Découvrez la mise en miroir des données MetroCluster sur FC dans Active IQ Unified Manager

Les configurations MetroCluster over FC offrent la mise en miroir des données ainsi que la possibilité supplémentaire de lancer un basculement si un site entier devient indisponible. L'état de la mise en miroir des données entre les clusters dans une configuration MetroCluster over FC peut être normal ou mise en miroir indisponible. La compréhension de cet état vous permet de gérer efficacement vos configurations MetroCluster.

État de la mise en miroir des données	Description	Icône affichée
Normal	La réplication des données entre les clusters de la configuration MetroCluster est normale.	

État de la mise en miroir des données	Description	Icône affichée
Mise en miroir indisponible	La réplication des données entre les clusters de la configuration MetroCluster est indisponible en raison d'un basculement. Par exemple, lorsque le cluster partenaire est hors service à la suite d'un sinistre ou lors d'un basculement planifié à des fins de test.	Basculement avec erreurs:  Basculement réussi: 

Surveillez les configurations MetroCluster dans Active IQ Unified Manager

Vous pouvez surveiller les problèmes de connectivité dans votre configuration MetroCluster. Les détails incluent l'état des composants et la connectivité au sein d'un cluster, ainsi que l'état de la connectivité entre les clusters dans la configuration MetroCluster. Vous découvrirez ici comment surveiller les problèmes de connectivité dans les clusters protégés par les configurations MetroCluster over FC et MetroCluster over IP.

Vous pouvez surveiller les configurations MetroCluster à partir des vues suivantes dans le volet de navigation gauche de Active IQ Unified Manager :

- **Stockage** > **Clusters** > **Protection : MetroCluster** vue
- **Protection** > **Relations** > **Relation : MetroCluster** vue

Unified Manager utilise des alertes d'état du système pour indiquer l'état des composants et de la connectivité dans la configuration MetroCluster.

Avant de commencer

- Les clusters locaux et distants d'une configuration MetroCluster doivent tous deux être ajoutés à Active IQ Unified Manager.
- Dans une configuration MetroCluster sur IP, si un Mediator doit être pris en charge, il doit être configuré et ajouté au cluster via l'API correspondante.
- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Surveiller les problèmes de connectivité dans la configuration MetroCluster over FC

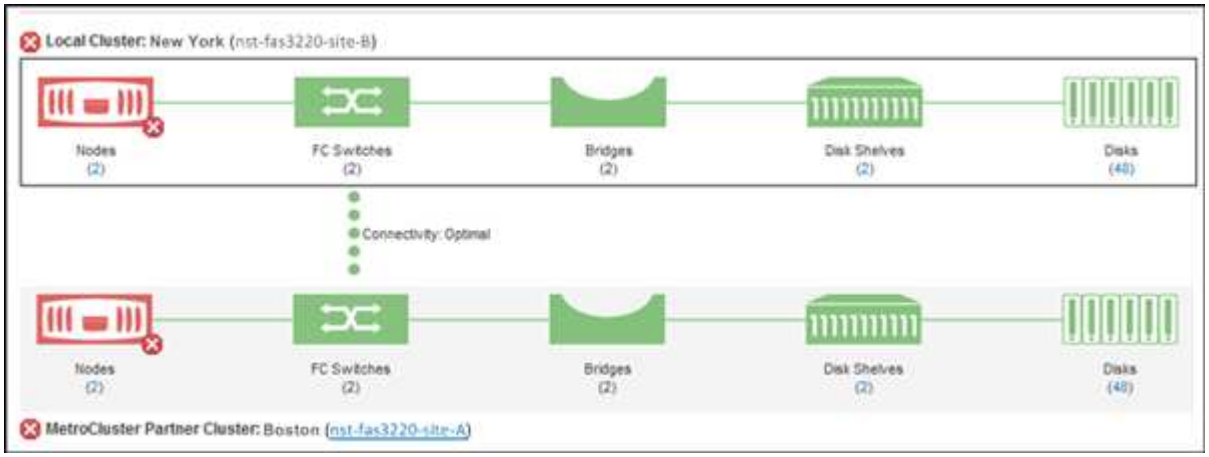
Pour les clusters dans une configuration MetroCluster sur FC, les graphiques de connectivité s'affichent sur la page de détails **Cluster / Health**. Suivez ces étapes.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.

   La liste de tous les clusters surveillés s'affiche.

2. Dans la vue **Protection : MetroCluster**, cliquez sur le nom du cluster dont vous souhaitez afficher les détails de configuration MetroCluster over FC. Vous pouvez également filtrer par clusters dans une configuration MetroCluster.
3. Sur la page de détails **Cluster / Santé**, cliquez sur l'onglet **MetroCluster Connectivity**. L'onglet **MetroCluster Connectivity** est disponible uniquement pour les configurations MetroCluster over FC.



La topologie de la configuration MetroCluster est affichée dans la zone de l'objet cluster correspondant. Vous pouvez utiliser les informations affichées sur la page Détails du cluster / état pour résoudre les problèmes de connectivité. Par exemple, si la connectivité entre le nœud et le commutateur d'un cluster est interrompue, l'icône suivante s'affiche :



Si vous déplacez le pointeur sur l'icône, vous pouvez consulter des informations détaillées sur l'événement généré.

Si vous découvrez des problèmes de connectivité dans votre configuration MetroCluster, vous devez vous connecter à System Manager ou accéder à l'ONTAP CLI pour résoudre ces problèmes.

Pour plus d'informations sur la détermination de l'état de santé du cluster, voir "Déterminer l'état du cluster dans une configuration MetroCluster sur FC".

Surveiller les problèmes de connectivité dans la configuration MetroCluster sur IP

Pour les clusters dans une configuration MetroCluster sur IP, les schémas de connectivité sont affichés sur la page **Clusters**. Suivez ces étapes.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.

   La liste de tous les clusters surveillés s'affiche.

2. Dans la vue **Protection : MetroClusters**, cliquez sur le nom du cluster dont vous souhaitez afficher les détails de configuration de MetroCluster over IP. Vous pouvez également filtrer par clusters dans une configuration MetroCluster.
3. Développez la ligne en cliquant sur l'icône ⌄ en forme de flèche. L'icône en forme de flèche n'apparaît que pour un cluster protégé par la configuration MetroCluster over IP.

   Vous pouvez consulter la topologie des sites source et miroir, ainsi que le Mediator utilisé pour la

connexion, le cas échéant. Vous pouvez consulter les informations suivantes :

- Connectivité entre les sites
- Problèmes d'état et de disponibilité, le cas échéant, sur les deux sites
- Problèmes liés au médiateur
- Problèmes liés à la réplication.

> Les statuts suivants sont signalés : Critique (), Erreur () ou Normal (). Vous pouvez également consulter l'état global de la réplication des données primaires et miroir dans la même topologie.

Dans le diagramme suivant, vous pouvez constater que la connectivité intersite entre les clusters source et de destination est indisponible et que le Mediator 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 déclenché pour ce problème dans votre configuration MetroCluster over IP, vous pouvez cliquer sur le bouton **Afficher l'événement** du message pour consulter les détails de l'événement. Une fois le problème et l'événement résolus, l'icône d'état de cette topologie retrouve son état normal ().
5. Vous pouvez afficher des détails de configuration supplémentaires dans les sections **MetroCluster Overview** et **Protection** de l'onglet **Configuration** de la page de détails **Cluster / Health**.

> Uniquement pour une configuration MetroCluster sur IP, vous pouvez afficher la topologie du cluster sur la page **Clusters**. Pour les clusters dans une configuration MetroCluster sur FC, la topologie s'affiche dans l'onglet **MetroCluster Connectivity** de la page de détails **Cluster / Health**.

Informations connexes

- "Page de détails Cluster / Santé"
- Pour plus d'informations sur la vue **Relation :MetroCluster**, voir "Surveiller les configurations MetroCluster".
- Pour plus d'informations sur la vue **Relation : État des transferts du dernier mois**, voir "Relation : affichage du statut des transferts 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 **Relations : Toutes les relations**, voir "Relation : vue Toutes les relations".

Surveillez la réplication MetroCluster dans Active IQ Unified Manager

Vous pouvez surveiller et diagnostiquer l'état de santé global des connexions logiques pendant la mise en miroir des données. Vous pouvez identifier les problèmes ou les risques susceptibles d'interrompre la mise en miroir des composants du cluster, tels que les agrégats, les nœuds et les machines virtuelles de stockage.

Unified Manager utilise les alertes d'état du système pour surveiller l'état des composants et la connectivité dans la configuration MetroCluster.

Avant de commencer

Les clusters local et distant de la configuration MetroCluster doivent tous deux être ajoutés à Unified Manager

Afficher la réplication pour les configurations MetroCluster sur IP

Pour les configurations MetroCluster over IP, l'état de la réplication des données s'affiche dans la vue d'aperçu de la topologie d'un cluster protégé par MetroCluster over IP à partir des vues suivantes du volet de navigation gauche de Unified Manager :

- **Stockage** > **Clusters** > **Protection : MetroCluster** vue
- **Protection** > **Relations** > **Relation : MetroCluster** vue

Pour plus d'informations, consultez "Surveiller les problèmes de connectivité dans MetroCluster over IP".

Afficher la réplication pour les configurations MetroCluster sur FC

Suivez ces étapes pour identifier tout problème de réplication des données pour la configuration MetroCluster over FC.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.

   La liste des clusters surveillés s'affiche.

2. Dans la vue **État : Tous les clusters**, cliquez sur le nom du cluster pour lequel vous souhaitez afficher les détails de réplication MetroCluster. Sur la page **Détails du cluster / État**, cliquez sur l'onglet **MetroCluster Replication**.

   La topologie de la configuration MetroCluster à répliquer s'affiche sur le site local dans la zone de l'objet de cluster correspondant, 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 des détails Cluster / Health pour résoudre tout problème de réplication. Si vous constatez des problèmes de mise en miroir dans votre configuration MetroCluster, vous devez vous connecter à System Manager ou accéder à la CLI ONTAP pour les résoudre.

Informations connexes

"Page de détails Cluster / Santé"

Gérer les quotas

Découvrez les limites de quota dans Active IQ Unified Manager

Les limites de quota utilisateur sont des valeurs que le serveur Unified Manager utilise pour évaluer si la consommation d'espace par un utilisateur approche de la limite ou a atteint la limite définie par le quota de l'utilisateur. Si la limite souple est franchie ou si la limitation stricte est atteinte, le serveur Unified Manager génère des événements de quota utilisateur.

Par défaut, le serveur Unified Manager envoie un e-mail de notification aux utilisateurs qui ont dépassé la limite de quota souple ou atteint la limitation stricte du quota et pour lesquels des événements de quota utilisateur sont configurés. Les utilisateurs disposant du rôle d'Application Administrator peuvent configurer des alertes qui informent les destinataires spécifiés des événements de quota utilisateur ou de quota au groupe.

Vous pouvez spécifier les limites de quota en utilisant soit ONTAP System Manager, soit l'ONTAP CLI.

Consultez les quotas des utilisateurs et des groupes d'utilisateurs dans Active IQ Unified Manager

La page de détails Storage VM / Health affiche des informations sur les quotas des utilisateurs et des groupes d'utilisateurs configurés sur la SVM. Vous pouvez consulter le nom de l'utilisateur ou du groupe d'utilisateurs, les limites définies sur les disques et les fichiers, l'espace disque et l'espace fichier utilisés, ainsi que l'adresse e-mail de notification.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Machines virtuelles de stockage**.
2. Dans la vue **Santé : Toutes les machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, puis cliquez sur l'onglet **Quotas utilisateur et groupe**.

Informations connexes

"Ajout d'utilisateurs"

Créez des règles pour générer des adresses e-mail dans Active IQ Unified Manager

Vous pouvez créer des règles pour spécifier l'adresse e-mail en fonction du quota utilisateur associé aux clusters, aux machines virtuelles de stockage (SVM), aux volumes, aux qtrees, aux utilisateurs ou aux groupes d'utilisateurs. Une notification est envoyée à l'adresse e-mail spécifiée en cas de dépassement de quota.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir consulté les directives sur la page « Règles de génération de l'adresse e-mail de quota utilisateur et de quota au groupe ».

Vous devez définir les règles relatives aux adresses e-mail de quota et les saisir dans l'ordre dans lequel vous souhaitez les exécuter. Par exemple, si vous souhaitez utiliser l'adresse e-mail abc@xyz.com pour recevoir des notifications sur les dépassements de quota pour abc et l'adresse e-mail dl-$GROUP@$DOMAIN pour tous les autres groupes, les règles doivent être répertoriées dans l'ordre suivant :

- si ($USER == 'abc') alors abc@xyz.com
- si ($GROUP == *) alors dl-$GROUP@$DOMAIN

Si aucun des critères des règles que vous avez spécifiées n'est rempli, la règle par défaut est utilisée:

si ($USER_OR_GROUP == *) alors $USER_OR_GROUP@$DOMAIN

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Règles d'e-mails de quota**.
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 **Valider**.

4. Cliquez sur **Enregistrer**.
5. Vérifiez que l'adresse e-mail que vous avez créée s'affiche dans l'onglet **User and Group Quotas** de la page de détails **Storage VM / Health**.

Créez un format de notification par e-mail pour les quotas d'utilisateurs et de groupes d'utilisateurs dans Active IQ Unified Manager

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 aux quotas (limite souple dépassée ou limitation stricte atteinte).

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Format de l'e-mail de quota**.
2. Saisissez ou modifiez les informations dans les champs **De**, **Sujet** et **Détails de l'e-mail**.
3. Cliquez sur **Aperçu** pour prévisualiser la notification par e-mail.
4. Cliquez sur **Fermer** pour fermer la fenêtre d'aperçu.
5. Modifiez le contenu de la notification par courriel, si nécessaire.
6. Cliquez sur **Enregistrer**.

Modifier les adresses e-mail des quotas d'utilisateurs et de groupes dans Active IQ Unified Manager

Vous pouvez modifier les adresses e-mail en fonction du quota utilisateur associé aux clusters, aux machines virtuelles de stockage (SVM), aux volumes, aux qtrees, aux utilisateurs ou aux groupes d'utilisateurs. Vous pouvez modifier l'adresse e-mail lorsque vous souhaitez remplacer celle générée par les règles définies dans la boîte de dialogue « Règles de génération des adresses e-mail de quota utilisateur et groupe ».

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous devez avoir examiné le "lignes directrices pour la création de règles".

Si vous modifiez une adresse e-mail, les règles de génération des adresses e-mail de quota utilisateur et de quota au groupe ne s'appliquent plus au quota. Pour que les notifications soient envoyées à l'adresse e-mail générée par les règles spécifiées, vous devez supprimer l'adresse e-mail et enregistrer la modification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **SVMs**.
2. Dans la vue **Santé : Toutes les machines virtuelles de stockage**, sélectionnez une SVM, puis cliquez sur l'onglet **Quotas utilisateur et groupe**.
3. Cliquez sur **Modifier l'adresse e-mail** sous la rangée d'onglets.
4. Dans la boîte de dialogue **Modifier l'adresse e-mail**, effectuez l'action appropriée :

Si…	Ensuite…
Vous souhaitez que les notifications soient envoyées à l'adresse e-mail générée par les règles spécifiées	a. Supprimez l'adresse e-mail du champ **Adresse e-mail**. b. Cliquez sur **Enregistrer**. c. Actualisez le navigateur en appuyant sur F5 pour recharger la boîte de dialogue Modifier l'adresse e-mail. L'adresse e-mail générée par la règle spécifiée s'affiche dans le champ **Adresse e-mail**.
Vous souhaitez que les notifications soient envoyées à une adresse e-mail spécifique	a. Modifiez l'adresse e-mail dans le champ **Adresse e-mail**. b. Cliquez sur **Enregistrer**. Les règles de génération des adresses e-mail de quota utilisateur et de quota au groupe ne s'appliquent plus au quota.

En savoir plus sur les quotas

Découvrez le processus de quota dans Active IQ Unified Manager

Les quotas peuvent être souples ou stricts. Les quotas souples amènent ONTAP à envoyer une notification lorsque les limites spécifiées sont dépassées, tandis que les quotas stricts empêchent une opération d'écriture de réussir lorsque les limites spécifiées

sont dépassées.

Lorsque ONTAP reçoit une requête d'un utilisateur ou d'un groupe d'utilisateurs pour écrire sur un volume FlexVol, il vérifie si des quotas sont activés sur ce volume pour l'utilisateur ou le groupe d'utilisateurs et détermine les éléments suivants :

- La limitation stricte sera-t-elle atteinte ?

  Si oui, l'opération d'écriture échoue lorsque la limitation stricte est atteinte et la notification de quota strict est envoyée.

- Si la limite souple sera dépassée

  Si oui, l'opération d'écriture réussit lorsque la limite souple est dépassée et que la notification de quota souple est envoyée.

- Si une opération d'écriture ne dépassera pas la limite souple

  Si oui, l'opération d'écriture réussit et aucune notification n'est envoyée.

Découvrez les quotas dans Active IQ Unified Manager

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 les quotas à l'aide du fichier `/etc/quotas`. Les quotas s'appliquent à un volume ou à un qtree spécifique.

Découvrez les quotas dans Active IQ Unified Manager

Vous pouvez utiliser des quotas pour limiter l'utilisation des ressources dans des volumes FlexVol, pour fournir une notification lorsque l'utilisation des ressources atteint des niveaux spécifiques, ou pour suivre l'utilisation des ressources.

Vous spécifiez un quota pour les raisons suivantes :

- Pour limiter l'espace disque ou le nombre de fichiers pouvant être utilisés par un utilisateur ou un groupe, ou pouvant être contenus dans un qtree
- Pour suivre la quantité d'espace disque ou le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree, sans imposer de limite
- Pour avertir les utilisateurs lorsque leur utilisation de l'espace disque ou des fichiers est élevée

Description des boîtes de dialogue de quotas

Utilisez la boîte de dialogue Quotas dans Active IQ Unified Manager

Vous pouvez utiliser l'option appropriée dans l'onglet User and Group Quotas de la vue Health: All Storage VMs pour configurer le format de la notification par e-mail envoyée lorsqu'un problème lié aux quotas survient et pour configurer des règles afin de spécifier les adresses e-mail en fonction du quota utilisateur.

Découvrez la page Format des notifications par e-mail dans Active IQ Unified Manager

La page Format de notification par e-mail affiche les règles de l'e-mail envoyé à un utilisateur ou à un groupe d'utilisateurs en cas de problème lié au quota (limite logicielle dépassée ou limitation stricte atteinte).

La notification par e-mail est envoyée uniquement lorsque les événements de quota utilisateur ou de quota au groupe suivants sont générés : dépassement de la limite souple d'espace disque du quota utilisateur ou du quota au groupe, dépassement de la limite souple du nombre de fichiers du quota utilisateur ou du quota au groupe, atteinte de la limitation stricte d'espace disque du quota utilisateur ou du quota au groupe, ou atteinte de la limitation stricte du nombre de fichiers du quota utilisateur ou du quota au groupe.

- **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 e-mail indiquée sur la page Notifications.

- **Objet**

  Affiche l'objet de l'e-mail de notification.

- **Détails de l'adresse e-mail**

  Affiche le texte de l'e-mail de notification. Vous pouvez le modifier selon vos besoins. Par exemple, vous pouvez ajouter des informations relatives aux attributs du quota et réduire le nombre de mots-clés. Toutefois, vous ne devez pas modifier les mots-clés.

  Les mots-clés valides sont les suivants :

  - $EVENT_NAME

    Indique le nom de l'événement qui a déclenché la notification par e-mail.

  - $QUOTA_TARGET

    Spécifie le qtree ou le volume auquel le quota s'applique.

  - $QUOTA_USED_PERCENT

    Spécifie le pourcentage de limitation stricte du disque, de limitation souple du disque, de limitation stricte des fichiers ou de limitation souple des fichiers utilisé par l'utilisateur ou le groupe d'utilisateurs.

  - $QUOTA_LIMIT

    Spécifie la limitation stricte de disque ou la limitation stricte de fichier atteinte par l'utilisateur ou le groupe d'utilisateurs et pour laquelle l'un des événements suivants est généré :

    - Limitation stricte de l'espace disque du quota utilisateur ou du quota au groupe atteinte
    - Limite logicielle d'espace disque du quota utilisateur ou du quota au groupe atteinte
    - Limitation stricte du nombre de fichiers du quota au groupe ou à l'utilisateur atteinte
    - Limitation souple du nombre de fichiers du quota utilisateur ou du quota au groupe atteinte

  - $QUOTA_USED

Spécifie l'espace disque utilisé ou le nombre de fichiers créés par l'utilisateur ou le groupe d'utilisateurs.

- $QUOTA_USER

  Spécifie le nom de l'utilisateur ou du groupe d'utilisateurs.

Boutons de commande

Les boutons de commande vous permettent 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.

- **Restaurer les paramètres d'usine**

  Permet de rétablir les valeurs par défaut d'usine du format de notification.

- **Sauvegarder**

  Enregistre les modifications apportées au format de notification.

Découvrez les règles relatives aux adresses e-mail de quota dans Active IQ Unified Manager

La page « Règles de génération des adresses e-mail de quota utilisateur et de groupe » vous permet de créer des règles pour spécifier des adresses e-mail en fonction du quota utilisateur associé aux clusters, SVMs, volumes, qtrees, utilisateurs ou groupes d'utilisateurs. Une notification est envoyée à l'adresse e-mail spécifiée lorsqu'un quota est dépassé.

Zone des règles

Vous devez définir les règles pour une adresse e-mail de quota. Vous pouvez également ajouter des commentaires pour expliquer les règles.

Comment définir les règles

Vous devez saisir les règles dans l'ordre dans lequel vous souhaitez les exécuter. Si le critère de la première règle est rempli, l'adresse e-mail est alors générée en fonction de cette règle. Si le critère n'est pas rempli, le critère de la règle suivante est alors pris en compte, et ainsi de suite. Chaque ligne répertorie une règle distincte. La règle par défaut est la dernière règle de la liste. Vous pouvez modifier l'ordre de priorité des règles. Cependant, vous ne pouvez pas modifier l'ordre de la règle par défaut.

Par exemple, si vous souhaitez utiliser l'adresse e-mail qtree1@xyz.com pour recevoir des notifications concernant les dépassements de quota pour qtree1 et l'adresse e-mail admin@xyz.com pour tous les autres qtrees, vous devez répertorier les règles dans l'ordre suivant :

- si ($QTREE == 'qtree1') alors qtree1@xyz.com
- si ($QTREE == *) alors admin@xyz.com

Si aucun des critères des règles que vous avez spécifiées n'est rempli, la règle par défaut est utilisée:

si ($USER_OR_GROUP == *) alors $USER_OR_GROUP@$DOMAIN

Si plusieurs utilisateurs ont le même quota, leurs noms sont affichés sous forme de valeurs séparées par des virgules et les règles ne s'appliquent pas à ce quota.

Comment ajouter des commentaires

Vous pouvez ajouter des commentaires pour expliquer les règles. Vous devez utiliser # au début de chaque commentaire et chaque ligne répertorie un commentaire distinct.

Syntaxe des règles

La syntaxe de la règle doit être l'une des suivantes :

- si (`valid variableoperator *`) alors `email ID@domain name`

  if est un mot-clé et s'écrit en minuscules. L'opérateur est ==. L'identifiant e-mail peut contenir n'importe quel caractère, les variables valides $USER_OR_GROUP, $USER, ou $GROUP, ou une combinaison de n'importe quel caractère et des variables valides $USER_OR_GROUP, $USER, ou $GROUP. Le nom de domaine peut contenir n'importe quel caractère, la variable valide $DOMAIN, ou une combinaison de n'importe quel caractère et de la variable valide $DOMAIN. Les variables valides peuvent être en majuscules ou en minuscules, mais ne doivent pas être une combinaison des deux. Par exemple, $domain et $DOMAIN sont valides, mais $Domain n'est pas une variable valide.

- si (`valid variableoperator `string``) alors `email ID@domain name`

  if est un mot-clé et s'écrit en minuscules. L'opérateur peut être contains ou ==. L'identifiant e-mail peut contenir n'importe quel caractère, les variables valides $USER_OR_GROUP, $USER ou $GROUP, ou une combinaison de n'importe quel caractère et des variables valides $USER_OR_GROUP, $USER ou $GROUP. Le nom de domaine peut contenir n'importe quel caractère, la variable valide $DOMAIN, ou une combinaison de n'importe quel caractère et de la variable valide $DOMAIN. Les variables valides peuvent être en majuscules ou en minuscules, mais ne doivent pas être une combinaison des deux. Par exemple, $domain et $DOMAIN sont valides, mais $Domain n'est pas une variable valide.

Boutons de commande

Les boutons de commande vous permettent d'enregistrer, de valider ou d'annuler les règles créées:

- **Valider**

  Valide la syntaxe de la règle créée. En cas d'erreur lors de la validation, la règle concernée est affichée accompagnée d'un message d'erreur.

- **Restaurer les paramètres d'usine**

  Permet de rétablir les règles d'adresse à leurs valeurs par défaut d'usine.

- **Sauvegarder**

  Valide la syntaxe de la règle et l'enregistre en l'absence d'erreurs. En cas d'erreurs lors de la validation, la règle concernée est affichée accompagnée d'un message d'erreur.

Dépannage

Ajouter de l’espace disque au répertoire de la base de données Unified Manager

Ajoutez de l’espace disque au répertoire de la base de données dans Active IQ Unified Manager

Le répertoire de la base de données Unified Manager contient toutes les données de santé et de performance collectées à partir des systèmes ONTAP. Dans certains cas, il peut être nécessaire d’augmenter la taille du répertoire de la base de données.

Par exemple, le répertoire de la base de données peut se remplir si Unified Manager collecte des données à partir d’un grand nombre de clusters, chacun comportant de nombreux nœuds. Vous recevrez un événement d’avertissement lorsque le répertoire de la base de données sera rempli à 90 % et un événement critique lorsqu’il sera rempli à 95 %.

Aucune donnée supplémentaire n’est collectée à partir des clusters une fois que le répertoire est rempli à 95 %.

Les étapes nécessaires pour ajouter de la capacité au répertoire de données diffèrent selon que Unified Manager est exécuté sur un serveur VMware ESXi, sur un serveur Red Hat Linux ou sur un serveur Microsoft Windows.

Ajoutez de l’espace au disque de données de la machine virtuelle VMware dans Active IQ Unified Manager

Si vous devez augmenter l’espace disque alloué à la base de données Unified Manager, vous pouvez ajouter de la capacité après l’installation en augmentant l’espace disque à l’aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez avoir accès au vSphere Client.
- La machine virtuelle ne doit comporter aucun instantané stocké localement.
- Vous devez disposer des identifiants 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 augmentez la capacité de disque des données `disk 3`. Consultez la documentation VMware pour plus de détails.

   Dans de rares cas, le déploiement de Unified Manager utilise « Hard Disk 2 » pour le disque de données au lieu de « Hard Disk 3 ». Si cela s’est produit dans votre déploiement, augmentez l’espace du disque le plus grand. Le disque de données aura toujours plus d’espace que l’autre disque.

2. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis sélectionnez l’onglet **Console**.
3. Cliquez dans la fenêtre de 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**, saisissez le numéro correspondant à l'option **configuration système**.
5. Dans le **menu Configuration système**, saisissez le numéro correspondant à l'option **Augmenter la taille du disque de données**.

Ajoutez de l'espace au répertoire de données de l'hôte Linux dans Active IQ Unified Manager

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

Avant de commencer

Vous devez disposer d'un accès utilisateur root à la machine Red Hat Enterprise Linux sur laquelle Unified Manager est installé.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'augmenter la taille du répertoire de données.

Étapes

1. Connectez-vous en tant qu'utilisateur root à la machine Linux sur laquelle vous souhaitez ajouter de l'espace disque.
2. Arrêtez le service Unified Manager et le logiciel MySQL associé dans l'ordre indiqué : `systemctl stop ocieau ocie mysqld`
3. Créez un dossier de sauvegarde temporaire (par exemple, `/backup-data`) avec suffisamment d'espace disque pour contenir les données dans le répertoire `/opt/netapp/data` actuel.
4. Copiez le contenu et la configuration des privilèges du répertoire `/opt/netapp/data` existant vers le répertoire de données de sauvegarde :

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Si SE Linux est activé:

   a. Obtenez le type SE Linux pour les dossiers du dossier `/opt/netapp/data` existant :

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

      Le système renvoie une confirmation similaire à la suivante :

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Exécutez la `chcon` 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 les 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 le monter `/opt/netapp/data` en tant que partage NFS ou CIFS. En effet, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` pourraient 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 la suivante :

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

9. Si SE Linux est activé, vérifiez que le contexte du répertoire `/opt/netapp/data` est toujours défini sur mysqld_db_t :

a. `touch /opt/netapp/data/abc`

b. `ls -Z /opt/netapp/data/abc`

Le système renvoie une confirmation similaire à la suivante :

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

10. Supprimez le fichier `abc` afin que ce fichier superflu ne provoque pas d'erreur de base de données à l'avenir.

11. Copiez le contenu depuis `backup-data` vers le répertoire décompressé `/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, démarrez les services ocie et ocieau dans l'ordre indiqué :

```
systemctl start ocie ocieau
```

15. Une fois tous les services démarrés, supprimez le dossier de sauvegarde `/backup-data`:

```
rm -rf /backup-data
```

Ajoutez de l'espace au lecteur logique du serveur Microsoft Windows dans Active IQ Unified Manager

Si vous devez augmenter l'espace disque de la base de données Unified Manager, vous pouvez ajouter de la capacité au lecteur logique sur lequel Unified Manager est installé.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'ajouter de l'espace disque.

Étapes

1. Connectez-vous en tant qu'administrateur au serveur Windows sur lequel vous souhaitez ajouter de l'espace disque.
2. Suivez l'étape correspondant à la méthode que vous souhaitez utiliser pour ajouter de l'espace :

Option	Description
Sur un serveur physique, augmentez la capacité du lecteur logique sur lequel le serveur Unified Manager est installé.	Suivez les étapes décrites dans la rubrique Microsoft : "Étendre un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes décrites dans la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes décrites dans la rubrique VMware : "Augmenter la taille d'une partition de disque"

Modifiez l'intervalle de collecte des statistiques de performance dans Active IQ Unified Manager

L'intervalle de collecte par défaut des statistiques de performance est de 5 minutes. Vous pouvez le modifier à 10 ou 15 minutes si la collecte des données provenant de grands clusters ne se termine pas dans le délai par défaut. Ce paramètre affecte la collecte des statistiques de tous les clusters surveillés par cette instance d'Unified Manager.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

Les messages d'avertissement indiquent que la collecte des statistiques de performance ne s'est pas terminée à temps `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

Vous ne devez modifier l'intervalle de collecte que si cela s'avère nécessaire en raison d'un problème lié à la collecte de statistiques. Ne modifiez pas ce paramètre pour toute autre raison.

> Modifier cette valeur par rapport au paramètre par défaut de 5 minutes peut affecter le nombre et la fréquence des événements de performance signalés par Unified Manager. Par exemple, les seuils de performance définis par le système déclenchent des événements lorsque la règle est dépassée pendant 30 minutes. Avec des collectes toutes les 5 minutes, la règle doit être dépassée pendant six collectes consécutives. Avec des collectes toutes les 15 minutes, la règle doit être dépassée pendant seulement deux périodes de collecte.

Un message en bas de la page de configuration du cluster indique l'intervalle actuel de collecte des données statistiques.

Étapes

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

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

2. Saisissez le numéro de l'option de menu intitulée **Configuration de l'intervalle d'interrogation des performances**, puis appuyez sur Entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe de l'utilisateur de maintenance.
4. Saisissez le numéro du nouvel intervalle d'interrogation que vous souhaitez définir, puis appuyez sur Entrée.

Si vous avez modifié l'intervalle de collecte d'Unified Manager à 10 ou 15 minutes et que vous disposez d'une connexion actuelle à un fournisseur de données externe (tel que Graphite), vous devez modifier l'intervalle de transmission du fournisseur de données afin qu'il soit égal ou supérieur à l'intervalle de collecte d'Unified Manager.

Modifiez la durée pendant laquelle Active IQ Unified Manager conserve les données d'événements et de performances

Par défaut, Unified Manager conserve les données d'événement et de performances pendant 6 mois pour tous les clusters surveillés. Passé ce délai, les données les plus anciennes sont automatiquement supprimées pour libérer de l'espace pour les nouvelles. Cette durée par défaut convient à la plupart des configurations, mais les très grandes configurations comportant de nombreux clusters et nœuds peuvent nécessiter de réduire cette période de conservation afin qu'Unified Manager fonctionne de manière optimale.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Vous pouvez modifier les durées de conservation de ces deux types de données sur la page Conservation des données. Ces paramètres affectent la conservation des données de tous les clusters surveillés par cette instance de Unified Manager.

> Unified Manager collecte des statistiques de performance toutes les 5 minutes. Chaque jour, les statistiques de 5 minutes sont résumées en statistiques de performance horaires. Il conserve 30 jours de données historiques de performance à intervalles de 5 minutes et 6 mois de données de performance horaires résumées (par défaut).

Vous ne devriez réduire la période de conservation que si vous manquez d'espace ou si les sauvegardes et autres opérations prennent très longtemps à se terminer. La réduction de la période de conservation a les effets suivants :

- Les anciennes données de performance 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 visibles dans l'interface utilisateur.
- Les emplacements de l'interface utilisateur affichant les statistiques de performance horaires seront vides avant la période de conservation.
- Si la période de conservation des événements dépasse la période de conservation des données de performance, un message s'affichera sous le curseur de performance pour avertir que les événements de performance plus anciens peuvent ne pas disposer de données de prise en charge dans les graphiques associés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Politiques** > **Conservation des données**.
2. Sur la page **Conservation des données**, sélectionnez le curseur dans la zone Conservation des événements ou Conservation des données de performance, déplacez-le sur le nombre de mois pendant lesquels les données doivent être conservées, puis cliquez sur **Enregistrer**.

Résoudre une erreur d'authentification inconnue dans Active IQ Unified Manager

Lors de l'exécution d'une opération liée à l'authentification, telle que l'ajout, la modification, la suppression ou le test d'utilisateurs ou de groupes distants, le message d'erreur suivant peut s'afficher : `Unknown authentication error.`

Cause

Ce problème peut survenir si vous avez défini une valeur incorrecte pour les options suivantes :

- Nom de l'administrateur du service d'authentification Active Directory
- Nom unique de liaison du service d'authentification OpenLDAP

Mesure corrective

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. En fonction du service d'authentification que vous avez sélectionné, saisissez les informations appropriées pour le nom de l'administrateur ou le nom unique de liaison.
3. Cliquez sur **Tester l'authentification** pour tester l'authentification avec les informations que vous avez spécifiées.
4. Cliquez sur **Enregistrer**.

Résoudre l'erreur « Utilisateur introuvable » dans Active IQ Unified Manager

Lorsque vous effectuez une opération liée à l'authentification, telle que l'ajout, la modification, la suppression ou le test d'utilisateurs ou de groupes distants, le message

d’erreur suivant s’affiche : `User not found.`

Cause

Ce problème peut survenir si l’utilisateur existe sur le serveur AD ou le serveur LDAP, et si vous avez défini le nom unique de base sur une valeur incorrecte.

Mesure corrective

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Saisissez les informations appropriées pour le nom unique de base.
3. Cliquez sur **Enregistrer**.

Résolvez le problème causé par l’ajout de LDAP à l’aide d’Other authentication service dans Active IQ Unified Manager

Lorsque vous sélectionnez « Autres » comme service d’authentification, les classes d’objets utilisateur et 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.

Mesure corrective

Vous pouvez résoudre ce problème manuellement en utilisant l’une des solutions de contournement suivantes.

Si vos classes d’objets utilisateur et groupe LDAP sont respectivement « user » et « group », procédez comme suit :

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Dans le menu déroulant **Service d’authentification**, sélectionnez **Active Directory**, puis **Autres**.
3. Remplissez les champs de texte.

Si votre classe d’objet utilisateur LDAP et votre classe d’objet groupe sont respectivement posixAccount et posixGroup, procédez comme suit :

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Dans le menu déroulant **Service d’authentification**, sélectionnez **OpenLDAP**, puis **Autres**.
3. Remplissez les champs de texte.

Si les deux premières solutions de contournement ne s’appliquent pas, appelez l' `option-set`API, et définissez les `auth.ldap.userObjectClass` et `auth.ldap.groupObjectClass` options sur les valeurs correctes.

Résolvez un problème de rotation des journaux du SDK de gestion NetApp dans Active IQ Unified Manager

Après avoir ajouté un cluster basé sur l'API ONTAPI à Unified Manager sur un système d'exploitation Windows, la `nmsdk.log`taille du fichier augmente et dépasse la limite de 10 Mo.

Cause

Ce problème peut survenir si la rotation des journaux n'a pas lieu.

Mesure corrective

1. Arrêtez Unified Manager.
2. Lors de l'installation d'Unified Manager sous Windows, installez Logrotate version 0.0.0.18. Pour plus d'informations, consultez le "Guide de renforcement de la sécurité pour le rapport technique du SDK Manageability de NetApp".
3. Démarrez Unified Manager.

Gérer les événements et les alertes

Gérer les événements

Découvrez les événements de la plateforme Active IQ dans Active IQ Unified Manager

Unified Manager peut afficher les événements détectés par la plateforme Active IQ. Ces événements sont créés en appliquant un ensemble de règles aux messages AutoSupport générés à partir de tous les systèmes de stockage surveillés par Unified Manager.

Pour plus d'informations, consultez "Comment les événements de la plateforme Active IQ sont générés".

Unified Manager vérifie automatiquement la présence d'un nouveau fichier de règles et ne le télécharge que lorsque des règles plus récentes sont disponibles. Sur les sites sans accès au réseau externe, vous devez importer les règles manuellement via **Gestion du stockage** > **Configuration des événements** > **Importer les règles**.

Ces événements Active IQ ne chevauchent pas les événements Unified Manager existants et identifient des incidents ou des risques liés à la configuration du système, au câblage, aux bonnes pratiques et aux problèmes de disponibilité.

Pour plus d'informations sur l'activation des événements de plateforme, consultez "Activation des événements du portail Active IQ". Pour plus d'informations sur le chargement du fichier de règles, consultez "Téléchargement d'un nouveau fichier de règles Active IQ".

NetApp Active IQ est un service cloud qui fournit des analyses prédictives et une assistance proactive pour optimiser le fonctionnement des systèmes de stockage dans le NetApp cloud hybride. Voir "NetApp Active IQ" pour plus d'informations.

Que sont les événements de l'Event Management System

Découvrez les événements du système de gestion d'événements dans Active IQ Unified Manager

Le système de gestion des événements (EMS) collecte les données d'événements provenant de différentes parties du noyau ONTAP et fournit des mécanismes de transmission des événements. Ces événements ONTAP peuvent être signalés comme des événements EMS dans Unified Manager. La surveillance et la gestion centralisées simplifient la configuration des événements EMS critiques 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 qu'il se produit dans le cluster.

Il existe deux méthodes pour recevoir les événements EMS dans Unified Manager :

- Un certain nombre d'événements EMS importants sont signalés automatiquement.
- Vous pouvez vous abonner pour recevoir des événements EMS individuels.

Les événements EMS générés par Unified Manager sont signalés différemment selon la méthode de

génération de l'événement :

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 lors du déclenchement	Nom de l'événement Unified Manager (converti à partir du nom de l'événement EMS)	Message non spécifique au format « Erreur EMS reçue ». Le message détaillé fournit le format en notation par points de l'événement EMS réel.
Messages reçus	Dès que le cluster a été découvert	Après avoir ajouté chaque événement EMS requis à Unified Manager, et après le cycle d'interrogation de 15 minutes suivant
Cycle de vie d'un événement	Identique aux autres événements Unified Manager : états Nouveau, Accusé de réception, Résolu et Obsolète	L'événement EMS devient obsolète après l'actualisation du cluster, soit 15 minutes après sa création
Capture les événements pendant l'interruption de Unified Manager	Oui, au démarrage, le système communique avec chaque cluster pour récupérer les événements manquants	Non
Détails de l'événement	Les actions correctives suggérées sont importées directement depuis ONTAP afin de fournir des solutions cohérentes	Les mesures correctives ne sont pas disponibles sur la page Détails de l'événement

Certains des nouveaux événements EMS automatiques sont des événements d'information qui indiquent qu'un événement précédent a été résolu. Par exemple, l'événement d'information "FlexGroup Constituents Space Status All OK" indique que l'événement d'erreur "FlexGroup Constituents Have Space Issues" a été résolu. Les événements d'information ne peuvent pas être gérés en utilisant le même cycle de vie des événements que les autres types de gravité des événements. Cependant, l'événement devient automatiquement obsolète si le même volume reçoit un autre événement d'erreur “Space Issues”.

Événements EMS ajoutés automatiquement à Active IQ Unified Manager

Les événements ONTAP EMS suivants sont automatiquement ajoutés à Unified Manager. Ces événements sont générés lorsqu'ils sont déclenchés sur un cluster surveillé par Unified Manager.

Les événements EMS suivants sont disponibles lors de la surveillance des clusters exécutant le logiciel ONTAP 9.5 ou une version ultérieure :

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité d'Unified Manager
Accès au niveau cloud refusé pour la relocalisation d'agrégat	arl.netra.ca.check.failed	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation de l'agrégat lors d'un basculement du stockage	gb.netra.ca.check.failed	Agrégat	Erreur
FabricPool Resynchronisation de la réplication miroir terminée	wafl.ca.resync.complete	Cluster	Erreur
FabricPool Espace presque plein	fabricpool.nearly.full	Cluster	Erreur
Début de la période de grâce NVMe-oF	nvmf.graceperiod.start	Cluster	Avertissement
Période de grâce NVMe-oF active	nvmf.graceperiod.active	Cluster	Avertissement
Délai de grâce NVMe-oF expiré	nvmf.graceperiod.expired	Cluster	Avertissement
LUN détruite	lun.destroy	LUN	Informations
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Nœud	Erreur
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	Nœud	Erreur
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Nœud	Erreur
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Nœud	Erreur
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Nœud	Informations
Rôle IAM invalide dans le cloud AWS	cloud.aws.iamRoleInvalid	Nœud	Erreur
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Nœud	Erreur
Hôte du niveau cloud non résolvable	objstore.host.unresolvable	Nœud	Erreur
Interface réseau intercluster du niveau cloud indisponible	objstore.interclusterlifDown	Nœud	Erreur
Signature de niveau cloud de requête non concordante	osc.signatureMismatch	Nœud	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité d'Unified Manager
L'un des pools NFSv4 est épuisé	Nblade.nfsV4PoolExhaust	Nœud	Primordial
Mémoire du moniteur QoS saturée	qos.monitor.memory.maxed	Nœud	Erreur
Mémoire de QoS Monitor réduite	qos.monitor.memory.abated	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 manque d'espace	NVMeNS.out.of.space	Espace de noms	Avertissement
Réplication synchrone désynchronisée	sms.status.out.of.sync	SnapMirror relation	Avertissement
Réplication synchrone rétablie	sms.status.in.sync	SnapMirror relation	Informations
Échec de la resynchronisation automatique de la réplication synchrone	sms.resync.attempt.failed	SnapMirror relation	Erreur
Nombreuses connexions CIFS	Nblade.cifsManyAuths	SVM	Erreur
Nombre maximal de connexions CIFS dépassé	Nblade.cifsMaxOpenSameFile	SVM	Erreur
Nombre maximal de connexions CIFS par utilisateur dépassé	Nblade.cifsMaxSessPerUsrConn	SVM	Erreur
Conflit de noms CIFS NetBIOS	Nblade.cifsNbNameConflict	SVM	Erreur
Tentatives de connexion à un partage CIFS inexistant	Nblade.cifsNoPrivShare	SVM	Primordial
L'opération de copie instantanée CIFS a échoué	cifs.shadowcopy.failure	SVM	Erreur
Virus détecté par le serveur antivirus	Nblade.vscanVirusDetected	SVM	Erreur
Aucune connexion au serveur AV pour l'analyse antivirus	Nblade.vscanNoScannerConn	SVM	Primordial
Aucun serveur antivirus enregistré	Nblade.vscanNoRegdScanner	SVM	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité d'Unified Manager
Aucune connexion à un serveur AV répondant.	Nblade.vscanConnInactive	SVM	Informations
Le serveur antivirus est trop occupé pour accepter une nouvelle demande d'analyse	Nblade.vscanConnBackPressure	SVM	Erreur
Tentative d'accès d'un utilisateur non autorisé à AV Server	Nblade.vscanBadUserPrivAccess	SVM	Erreur
FlexGroup Constituants présentent des problèmes d'espace	flexgroup.constituents.have.space.issues	Volume	Erreur
FlexGroup État de l'espace des constituants : tous OK	flexgroup.constituents.space.status.all.ok	Volume	Informations
FlexGroup Les composants ont des problèmes d'inodes	flexgroup.constituents.have.inodes.issues	Volume	Erreur
FlexGroup Statut de tous les inodes constitutifs : OK	flexgroup.constituents.inodes.status.all.ok	Volume	Informations
Espace logique du volume presque plein	monitor.vol.nearFull.inc.sav	Volume	Avertissement
Espace logique du volume plein	monitor.vol.full.inc.sav	Volume	Erreur
Espace logique du volume normal	monitor.vol.one.ok.inc.sav	Volume	Informations
Volume WAFL AutoSize en échec	wafl.vol.autoSize.fail	Volume	Erreur
Volume WAFL AutoSize terminé	wafl.vol.autoSize.done	Volume	Informations
Expiration du délai de l'opération de fichier WAFL READDIR	wafl.readdir.expired	Volume	Erreur

Abonnez-vous aux événements ONTAP EMS dans Active IQ Unified Manager

Vous pouvez vous abonner pour recevoir les événements Event Management System (EMS) générés par les systèmes sur lesquels le logiciel ONTAP est installé. Un sous-ensemble des événements EMS est automatiquement signalé à Unified Manager, mais d'autres événements EMS ne sont signalés que si vous vous êtes abonné à ces événements.

Avant de commencer

Ne vous abonnez pas aux événements EMS déjà ajoutés automatiquement à Unified Manager, car cela peut engendrer de la confusion si vous recevez deux événements concernant le même problème.

Vous pouvez vous abonner à n'importe quel nombre d'événements EMS. Tous les événements auxquels vous vous abonnez sont validés, et seuls les événements validés sont appliqués aux clusters que vous surveillez dans Unified Manager. Le *ONTAP 9 EMS Event Catalog* fournit des informations détaillées sur tous les messages EMS pour la version spécifiée du logiciel ONTAP 9. Repérez la version appropriée de *EMS Event Catalog* sur la page ONTAP 9 Product Documentation pour obtenir la liste des événements applicables.

"Bibliothèque de produits ONTAP 9"

Vous pouvez configurer des alertes pour les 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 se peut qu'un problème de configuration DNS du cluster 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 permettra de transmettre les événements EMS en attente au serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration de l'événement**.
2. Sur la page de configuration de l'événement, cliquez sur le bouton **S'abonner aux événements EMS**.
3. Dans la boîte de dialogue S'abonner aux événements EMS, saisissez le nom de l'événement EMS ONTAP auquel vous souhaitez vous abonner.

   Pour afficher les noms des événements EMS auxquels vous pouvez vous abonner, depuis le shell du cluster ONTAP, vous pouvez utiliser la commande `event route show` (avant ONTAP 9) ou la commande `event catalog show` (ONTAP 9 ou version ultérieure).

   "Comment configurer et recevoir des alertes de ONTAP EMS Event Subscription dans Active IQ Unified Manager"

4. Cliquez sur **Add**.

   L'événement EMS est ajouté à la liste Subscribed EMS events, mais la colonne Applicable to Cluster affiche l'état « `Unknown` » pour l'événement EMS que vous avez ajouté.

5. Cliquez sur **Enregistrer et fermer** pour enregistrer l'abonnement à l'événement EMS dans le cluster.
6. Cliquez à nouveau sur **S'abonner aux événements EMS**.

   Le statut "Yes" apparaît dans la colonne Applicable to Cluster pour l'événement EMS que vous avez ajouté.

   Si le statut n'est pas « `Yes` », vérifiez l'orthographe du nom de l'événement EMS ONTAP. Si le nom est saisi incorrectement, vous devez supprimer l'événement incorrect, puis ajouter à nouveau l'événement.

Lorsqu'un événement ONTAP EMS se produit, l'événement s'affiche sur la page Événements. Vous pouvez sélectionner l'événement pour afficher les détails de l'événement EMS dans la page Détails de l'événement. Vous pouvez également gérer le traitement de l'événement ou créer des alertes pour l'événement.

Comprendre comment Active IQ Unified Manager gère un événement reçu

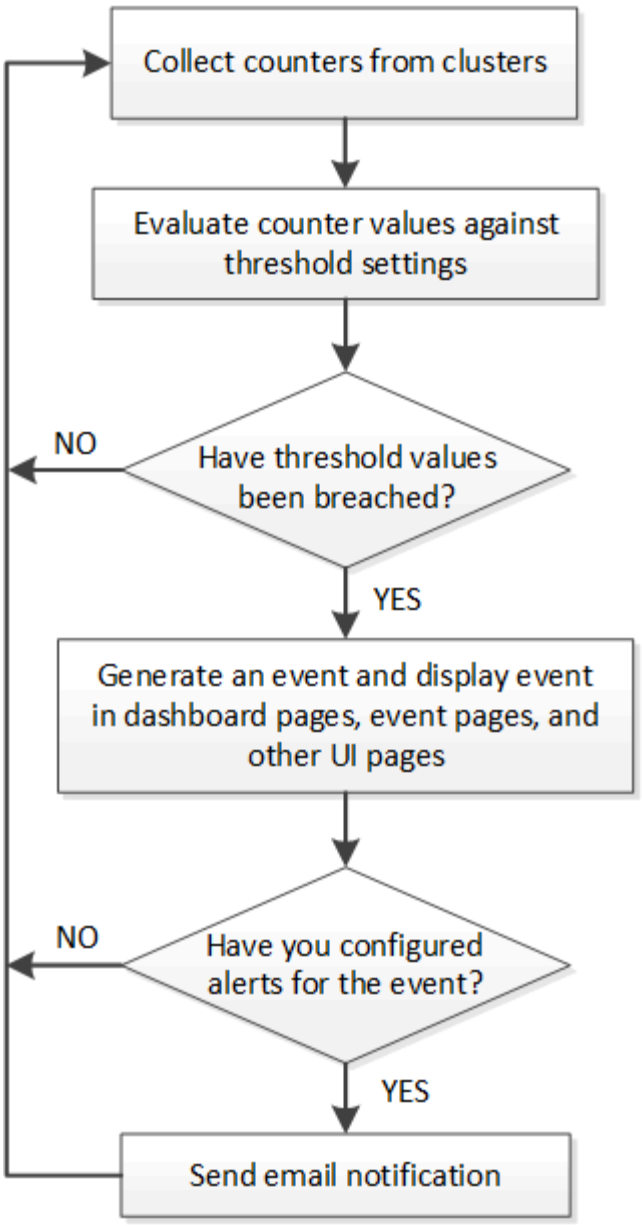
Lorsque Unified Manager reçoit un événement, celui-ci s'affiche sur la page Dashboard, sur la page d'inventaire Event Management, dans les onglets Summary et Explorer de la page Cluster/Performance, et sur la page d'inventaire spécifique à l'objet (par exemple, la page d'inventaire Volumes/Health).

Lorsque Unified Manager détecte plusieurs occurrences consécutives d'une même condition d'événement pour un même composant de cluster, il les considère comme un seul événement, et non comme des événements distincts. La durée de l'événement est incrémentée pour indiquer qu'il est toujours actif.

Selon la configuration choisie dans la page « Configuration des alertes », vous pouvez informer d'autres utilisateurs de ces événements. L'alerte déclenche les actions suivantes :

- Un courriel concernant l'événement peut être envoyé à tous les utilisateurs administrateurs de Unified Manager.
- L'événement peut être envoyé à d'autres destinataires par courriel.
- Un trap SNMP peut être envoyé au récepteur de traps.
- Vous pouvez exécuter un script personnalisé pour effectuer une action.

Ce flux de travail est illustré dans le diagramme suivant.



Consultez les détails de l'événement dans Active IQ Unified Manager

Vous pouvez consulter les détails d'un événement déclenché par Unified Manager afin de prendre des mesures correctives. Par exemple, en cas d'événement d'intégrité « Volume Offline », vous pouvez cliquer dessus pour afficher les détails et effectuer les actions correctives nécessaires.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Les détails de l'événement comprennent des informations telles que la source de l'événement, sa cause et toute note s'y rapportant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

Par défaut, la vue Tous les événements actifs affiche les événements Nouveaux et Acquittés (actifs) qui ont été générés au cours des 7 derniers jours et qui ont un niveau d'impact Incident ou Risque.

2. Si vous souhaitez consulter une catégorie particulière d'événements, par exemple les événements de capacité ou les événements de performance, cliquez sur **Afficher** et sélectionnez-la dans le menu des types d'événements.
3. Cliquez sur le nom de l'événement dont vous souhaitez consulter les détails.

   Les détails de l'événement sont affichés sur la page Détails de l'événement.

Consultez les événements non attribués dans Active IQ Unified Manager

Vous pouvez consulter les événements non attribués, puis les attribuer un par un à un utilisateur capable de les résoudre.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

   Par défaut, les événements New et Acknowledged sont affichés sur la page d'inventaire Event Management.

2. Dans le volet **Filtres**, sélectionnez l'option de filtre **Non attribué** dans la zone **Attribué à**.

Accuser réception et résoudre les événements dans Active IQ Unified Manager

Vous devez accuser réception d'un événement avant de commencer à travailler sur le problème qui l'a généré afin de ne pas recevoir de notifications d'alerte répétées. Après avoir pris des mesures correctives pour un événement particulier, vous devez marquer l'événement comme résolu.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez acquitter et résoudre plusieurs événements simultanément.

Vous ne pouvez pas acquitter les événements d'information.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. À partir de la liste des événements, effectuez les actions suivantes pour accuser réception des événements :

Si vous voulez…	Faites ceci…
Accuser réception et marquer un événement comme résolu	a. Cliquez sur le nom de l'événement. b. Sur la page des détails de l'événement, déterminez la cause de celui-ci. c. Cliquez sur **Acknowledge**. d. Prenez 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 de détails de l'événement correspondante. b. Sélectionnez les événements. c. Cliquez sur **Acknowledge**. d. Prenez les mesures correctives appropriées. e. Cliquez sur **Marquer comme résolu**.

Une fois l'événement marqué comme résolu, il est déplacé vers la liste des événements résolus.

3. **Facultatif**: Dans la zone **Notes and Updates**, ajoutez une note sur la façon dont vous avez traité l'événement, puis cliquez sur **Post**.

Attribuer des événements à des utilisateurs spécifiques dans Active IQ Unified Manager

Vous pouvez vous attribuer des événements non attribués ou les attribuer à d'autres utilisateurs, y compris des utilisateurs distants. Vous pouvez réattribuer des événements attribués à un autre utilisateur, si nécessaire. Par exemple, en cas de problèmes fréquents sur un objet de stockage, vous pouvez attribuer les événements correspondants à l'utilisateur qui gère cet objet.

Avant de commencer

- Le nom d'utilisateur et l'adresse électronique doivent être correctement configurés.
- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Sur la page d'inventaire **Event Management**, sélectionnez un ou plusieurs événements que vous souhaitez attribuer.
3. Attribuez l'événement en choisissant l'une des options suivantes :

Si vous souhaitez attribuer l'événement à…	Ensuite, faites ceci…
Vous-même	Cliquez sur **Attribuer à** > **Moi**.

Si vous souhaitez attribuer l'événement à…	Ensuite, faites ceci…
Un autre utilisateur	a. Cliquez sur **Attribuer à** > **Un autre utilisateur**. b. Dans la boîte de dialogue « Attribuer un propriétaire », saisissez le nom d'utilisateur ou sélectionnez un utilisateur dans la liste déroulante. c. Cliquez sur **Attribuer**. Une notification par courriel est envoyée à l'utilisateur. Si vous ne saisissez pas de nom d'utilisateur ou ne sélectionnez pas d'utilisateur dans la liste déroulante et cliquez sur **Assign**, l'événement reste non attribué.

Désactivez les événements indésirables dans Active IQ Unified Manager

Tous les événements sont activés par défaut. Vous pouvez désactiver les événements globalement afin d'éviter la génération de notifications pour les événements non pertinents dans votre environnement. Vous pouvez réactiver les événements désactivés lorsque vous souhaitez à nouveau recevoir des notifications les concernant.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous désactivez des événements, ceux précédemment générés dans le système sont marqués comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications pour ces événements sont générées à partir du prochain cycle de surveillance.

Lorsque vous désactivez un événement pour un objet (par exemple, l' `vol offline` événement), puis que vous le réactivez ultérieurement, Unified Manager ne génère pas de nouveaux événements pour les objets qui étaient hors ligne lorsque l'événement était désactivé. Unified Manager génère un nouvel événement uniquement lorsqu'un changement d'état survient pour l'objet après la réactivation de l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration de l'événement**.
2. Sur la page **Configuration des événements**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Si vous voulez…	Ensuite, faites ceci…
Désactiver les événements	a. Cliquez sur **Disable**. b. Dans la boîte de dialogue Désactiver les événements, sélectionnez le niveau de gravité de l'événement. c. Dans la colonne Événements correspondants, sélectionnez les événements que vous souhaitez désactiver en fonction de leur gravité, puis cliquez sur la flèche vers la droite pour déplacer ces événements vers la colonne Événements désactivés. d. Cliquez sur **Enregistrer et fermer**. e. Vérifiez que les événements que vous avez désactivés apparaissent dans la vue de liste de la page Configuration des événements.
Activer les événements	a. Cochez la case à cocher de l'événement ou des événements que vous souhaitez activer. b. Cliquez sur **Enable**.

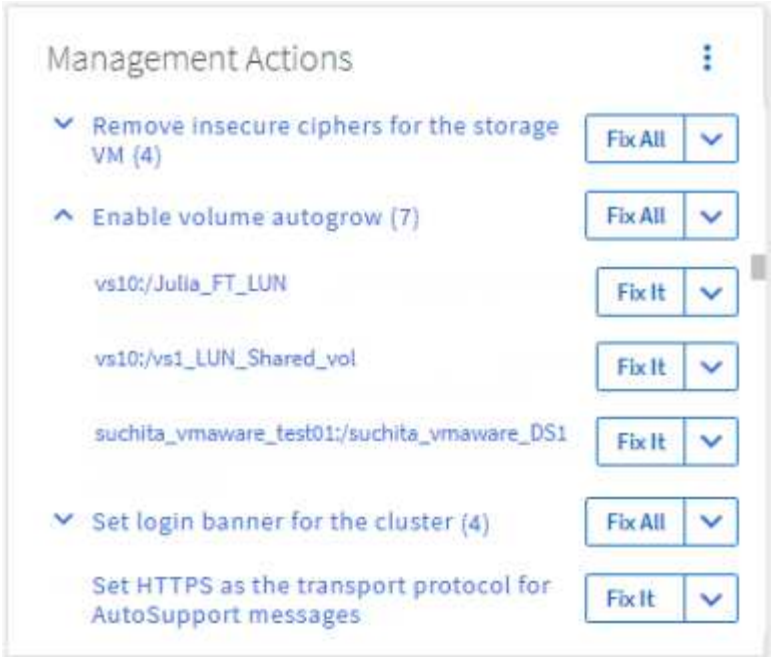
Résolvez les problèmes à l'aide de la correction automatique dans Active IQ Unified Manager

Unified Manager peut diagnostiquer certains événements en détail et proposer une solution unique grâce au bouton **Fix It**. Le cas échéant, ces solutions s'affichent dans le tableau de bord, sur la page de détails de l'événement et dans l'option « Analyse de la charge de travail » du menu de navigation de gauche.

La plupart des événements ont plusieurs résolutions possibles, affichées sur la page de détails de l'événement, afin que vous puissiez mettre en œuvre la meilleure solution à l'aide de ONTAP System Manager ou de l'interface de ligne de commande ONTAP. Une action **Fix It** est disponible lorsque Unified Manager a déterminé qu'il existe une seule résolution pour corriger le problème et qu'elle peut être mise en œuvre à l'aide d'une commande de l'interface de ligne de commande ONTAP.

Étapes

1. Pour afficher les événements qui peuvent être corrigés depuis **Dashboard**, cliquez sur **Dashboard**.



2. Pour résoudre l'un des problèmes que Unified Manager peut corriger, cliquez sur le bouton **Fix It**. Pour corriger un problème qui existe sur plusieurs objets, cliquez sur le bouton **Fix All**.

Pour plus d'informations sur les problèmes pouvant être résolus par une correction automatique, consultez "Quels problèmes Unified Manager peut-il résoudre".

Activer et désactiver la génération de rapports d'événements Active IQ dans Active IQ Unified Manager

Les événements de la plateforme Active IQ sont générés et affichés par défaut dans l'interface utilisateur d'Unified Manager. Si vous jugez ces événements trop fréquents ou si vous ne souhaitez pas les consulter dans Unified Manager, vous pouvez désactiver leur génération. Vous pourrez les réactiver ultérieurement si vous souhaitez à nouveau recevoir ces notifications.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Lorsque vous désactivez cette fonctionnalité, Unified Manager cesse immédiatement de recevoir les événements de la plateforme Active IQ.

Lorsque vous activez cette fonctionnalité, Unified Manager commence à recevoir les événements de plateforme Active IQ peu après minuit, en fonction du fuseau horaire du cluster. L'heure de début dépend du moment où Unified Manager reçoit les messages AutoSupport de chaque cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Paramètres des fonctionnalités**.
2. Sur la page **Paramètres des fonctionnalités**, désactivez ou activez les événements de la plateforme Active IQ en choisissant l'une des options suivantes :

Si vous voulez…	Ensuite, faites ceci…
Désactiver les événements de la plateforme Active IQ	Dans le panneau **Active IQ Portal Events**, déplacez le bouton du curseur vers la gauche.
Activer les événements de plateforme Active IQ	Dans le volet **Active IQ Portal Events**, déplacez le curseur vers la droite.

Téléversez un nouveau fichier de règles Active IQ dans Active IQ Unified Manager

Unified Manager vérifie automatiquement la présence d'un nouveau fichier d'événements (règles) Active IQ et télécharge un nouveau fichier lorsque des règles plus récentes sont disponibles. Toutefois, sur les sites sans accès au réseau externe, vous devez télécharger manuellement le fichier de règles.

Les règles Active IQ sont également appelées règles de sécurité Config Advisor (CA).

Lorsque vous installez ou mettez à niveau Unified Manager vers une version spécifique sur un site sans connectivité réseau, les règles Active IQ intégrées sont automatiquement disponibles pour le téléversement. Cependant, il est recommandé de télécharger un nouveau fichier de règles environ une fois par mois depuis le site de support de NetApp afin de garantir que des événements mis à jour sont générés et que vos systèmes de stockage continuent de fonctionner de manière optimale.

Avant de commencer

- La génération de rapports d'événements du portail Active IQ doit être activée. Cette fonctionnalité est activée par défaut. Pour plus d'informations, consultez "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'emplacement suivant : 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 `.zip` actuel.

   Le package de règles intégré comprend le référentiel de règles, les sources de données et un article de la base de connaissances NetApp.

   Sur les systèmes Windows, sur un site sans connectivité réseau, l'article de la base de connaissances NetApp n'est pas inclus par défaut dans le programme d'installation. Vous pouvez télécharger le fichier *secure_rules.zip* depuis le site de support et l'importer pour consulter l'article de la base de connaissances pour toutes les règles.

2. Transférez le fichier de règles sur un support que vous pourrez emporter dans la zone sécurisée, puis copiez-le sur un système situé dans cette zone.
3. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration de l'événement**.
4. Sur la page **Configuration de l'événement**, cliquez sur le bouton **Téléverser les règles**.
5. Dans la boîte de dialogue **Téléverser les règles**, accédez au fichier de règles `.zip` que vous avez téléchargé, sélectionnez-le et cliquez sur **Téléverser**.

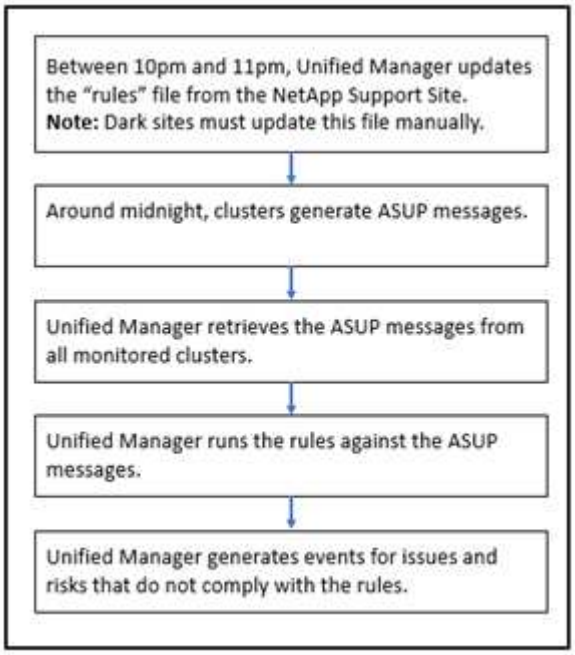
Ce processus peut prendre quelques minutes.

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 événements de risque et d'incident selon les besoins.

Pour plus d'informations, consultez cet article de la base de connaissances (KB) : "Comment mettre à jour manuellement les règles AIQCASecure dans Active IQ Unified Manager".

Comment Active IQ Unified Manager génère des événements de la plateforme Active IQ

Les incidents et les risques de la plateforme Active IQ sont convertis en événements Unified Manager, comme illustré dans le diagramme suivant.

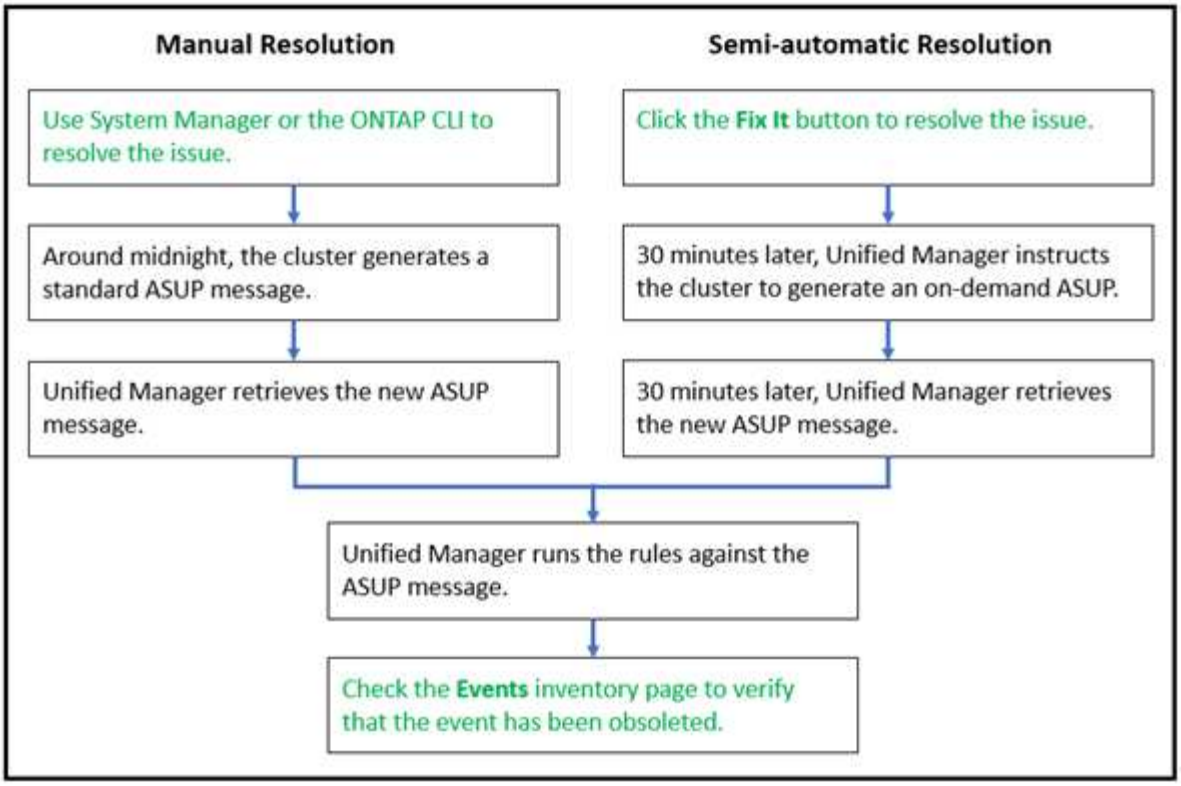


Comme vous pouvez le constater, le fichier de règles compilé sur la plateforme Active IQ est maintenu à jour, les messages AutoSupport du cluster sont générés quotidiennement, et Unified Manager met à jour la liste des événements chaque jour.

Résoudre les événements de la plateforme Active IQ dans Active IQ Unified Manager

Les incidents et les risques de la plateforme Active IQ sont similaires aux autres événements d'Unified Manager, car ils peuvent être attribués à d'autres utilisateurs pour être résolus et présentent les mêmes états possibles. Cependant, 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 illustre les actions que vous devez entreprendre (en vert) et l'action que Unified Manager entreprend (en noir) lors de la résolution des événements générés par la plateforme Active IQ.



Pour résoudre le problème manuellement, vous devez vous connecter à System Manager ou à l'interface de ligne de commande ONTAP pour corriger le problème. Vous ne pourrez vérifier le problème qu'après que le cluster aura généré un nouveau message AutoSupport à minuit.

Lors d'une résolution semi-automatique à l'aide du bouton **Fix It**, vous pouvez vérifier que la réparation a réussi en quelques heures.

Configurez les paramètres de conservation des événements dans Active IQ Unified Manager

Vous pouvez spécifier le nombre de mois pendant lesquels un événement est conservé sur le serveur Unified Manager avant d'être automatiquement supprimé.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

La conservation des événements pendant plus de 6 mois peut affecter les performances du serveur et n'est pas recommandée.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Conservation des données**.
2. Sur la page **Conservation des données**, sélectionnez le curseur dans la zone **Conservation des événements** et déplacez-le jusqu'au nombre de mois pendant lesquels les événements doivent être conservés, puis cliquez sur **Enregistrer**.

Qu'est-ce qu'une fenêtre de maintenance Unified Manager

Découvrez les fenêtres de maintenance d'Active IQ Unified Manager

Vous définissez une fenêtre de maintenance Unified Manager pour supprimer temporairement les événements et les alertes pendant une période spécifique lorsque vous avez planifié la maintenance du cluster et que vous ne souhaitez pas recevoir un flot de notifications indésirables.

Lorsque la fenêtre de maintenance commence, un événement « Démarrage de la fenêtre de maintenance de l'objet » est publié sur la page d'inventaire de la gestion des événements. Cet événement devient automatiquement obsolète à la fin de la fenêtre de maintenance.

Pendant une fenêtre de maintenance, les événements relatifs à tous les objets de ce cluster sont toujours générés, mais ils n'apparaissent sur aucune des pages de l'interface utilisateur, et aucune alerte ni aucun autre type de notification n'est envoyé pour ces événements. Vous pouvez toutefois afficher les événements générés pour tous les objets de stockage pendant une fenêtre de maintenance en sélectionnant l'une des options View sur la page d'inventaire Event Management.

Vous pouvez programmer une fenêtre de maintenance à une date ultérieure, modifier les heures de début et de fin d'une fenêtre de maintenance programmée et annuler une fenêtre de maintenance programmée.

Planifiez une fenêtre de maintenance pour désactiver les notifications d'événements de cluster dans Active IQ Unified Manager

Si vous avez prévu une interruption pour un cluster, par exemple pour mettre à niveau le cluster ou déplacer l'un des nœuds, vous pouvez supprimer les événements et les alertes qui seraient normalement générés pendant cette période en planifiant une fenêtre de maintenance de Unified Manager.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Pendant une fenêtre de maintenance, les événements liés à tous les objets de ce cluster sont toujours générés, mais ils n'apparaissent pas sur la page des événements, et aucune alerte ni autre type de notification n'est envoyée pour ces événements.

L'heure que vous saisissez pour la fenêtre de maintenance correspond à l'heure du serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.
2. Dans la colonne **Mode de maintenance** du cluster, sélectionnez le bouton curseur et déplacez-le vers la droite.

   La fenêtre du calendrier s'affiche.

3. Sélectionnez la date et l'heure de début et de fin de la période de maintenance, puis cliquez sur **Appliquer**.

   Le message « Planifié » apparaît à côté du curseur.

Lorsque l'heure de début est atteinte le cluster passe en mode de maintenance et un événement « Fenêtre de maintenance d'objet démarrée » est généré.

Modifier ou annuler une fenêtre de maintenance planifiée dans Active IQ Unified Manager

Si vous avez configuré une fenêtre de maintenance Unified Manager pour une date ultérieure, vous pouvez modifier les heures de début et de fin ou empêcher la fenêtre de maintenance d'avoir lieu.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

L'annulation d'une fenêtre de maintenance en cours est utile si vous avez terminé la maintenance du cluster avant l'heure de fin prévue de la fenêtre de maintenance et que vous souhaitez recommencer à recevoir des événements et des alertes du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration du cluster**.
2. Dans la colonne **Mode de maintenance** du cluster :

Si vous voulez…	Effectuez cette étape…
Modifier la plage horaire d'une fenêtre de maintenance planifiée	a. Cliquez sur le texte « Planifié » à côté du curseur. b. Modifiez la date et l'heure de début et/ou de fin, puis cliquez sur **Appliquer**.
Prolonger la durée d'une fenêtre de maintenance active	a. Cliquez sur le texte « Actif » à côté du bouton coulissant. b. Modifiez la date et l'heure de fin, puis cliquez sur **Apply**.
Annuler une fenêtre de maintenance programmée	Sélectionnez le bouton coulissant et déplacez-le vers la gauche.
Annuler une fenêtre de maintenance active	Sélectionnez le bouton coulissant et déplacez-le vers la gauche.

Consultez les événements générés pendant une fenêtre de maintenance dans Active IQ Unified Manager

Au besoin, vous pouvez consulter les événements générés pour tous les objets de stockage pendant une fenêtre de maintenance d'Unified Manager. La plupart des événements apparaîtront à l'état Obsolète une fois la fenêtre de maintenance terminée et toutes les ressources système de nouveau opérationnelles.

Avant de commencer

Au moins une période de maintenance doit être terminée avant que des événements ne soient disponibles.

Les événements survenus pendant une période de maintenance n'apparaissent pas par défaut sur la page d'inventaire Event Management.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Événements**.

   Par défaut, tous les événements actifs (nouveaux et reconnus) sont affichés sur la page d'inventaire de

gestion des événements.

2. Dans le volet Affichage, sélectionnez l'option **Tous les événements générés pendant la maintenance**.

   La liste des événements déclenchés au cours des 7 derniers jours, provenant de toutes les sessions de maintenance et de tous les clusters, est affichée.

3. S'il y a eu plusieurs fenêtres de maintenance pour un seul cluster, vous pouvez cliquer sur l'icône de calendrier **Heure de déclenchement** et sélectionner la période pour les événements de fenêtre de maintenance que vous souhaitez consulter.

Gérer les événements liés aux ressources du système hôte dans Active IQ Unified Manager

Unified Manager inclut un service qui surveille les problèmes de ressources sur le système hôte sur lequel Unified Manager est installé. Des problèmes tels qu'un manque d'espace disque disponible ou un manque de mémoire sur le système hôte peuvent déclencher des événements de la station de gestion, qui s'affichent sous forme de bannières en haut de l'interface utilisateur.

Les événements de la station de gestion indiquent un problème avec le système hôte sur lequel Unified Manager est installé. Parmi les problèmes de station de gestion, on peut citer un espace disque insuffisant sur le système hôte, l'absence d'un cycle régulier de collecte de données par Unified Manager, ainsi que la non-exécution ou l'exécution tardive de l'analyse statistique parce que l'interrogation de collecte suivante a été lancée.

Contrairement à tous les autres messages d'événement Unified Manager, ces avertissements et événements critiques particuliers de la station de gestion sont affichés dans des bannières.

Étape

1. Pour consulter les informations relatives aux événements de la station de gestion, procédez comme suit :

Si vous voulez…	Faites ceci…
Voir les détails de l'événement	Cliquez sur la bannière de l'événement pour afficher la page des détails de l'événement, qui comprend des solutions suggérées pour le problème.
Voir tous les événements de la station de gestion	a. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**. b. Dans le volet Filtres de la page d'inventaire de gestion des événements, cliquez sur la case correspondant à Station de gestion dans la liste Type de source.

Apprenez-en davantage sur les événements

États des événements dans Active IQ Unified Manager

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 Nouveau et Accusé de réception sont tous deux considérés

comme des événements actifs.

Les états de l'événement sont les suivants :

- **Nouveau**

  L'état d'un nouvel événement.

- **Reconnu**

  L'état d'un événement lorsque vous en avez pris connaissance.

- **Résolu**

  L'état d'un événement lorsqu'il est marqué comme résolu.

- **Obsolète**

  L'état d'un événement lorsqu'il est automatiquement corrigé ou lorsque la cause de l'événement n'est plus valable.

  Vous ne pouvez ni acquitter ni résoudre un événement obsolète.

Exemple de différents états d'un événement

Les exemples suivants illustrent les changements d'état manuels et automatiques des événements.

Lorsque l'événement « Cluster Not Reachable » est déclenché, son état est « New ». Lorsque vous accusez réception de l'événement, son état passe à « Acknowledged ». Lorsque vous avez pris la mesure corrective appropriée, vous devez marquer l'événement comme résolu. Son état passe alors à « Resolved ».

Si l'événement « Cluster Not Reachable » est généré à la suite d'une coupure de courant, le cluster recommence à fonctionner une fois le courant rétabli, sans aucune intervention de l'administrateur. Par conséquent, l'événement « Cluster Not Reachable » n'est plus valide, et son état passe à « Obsolete » lors du prochain cycle de surveillance.

Unified Manager envoie une alerte lorsqu'un événement est à l'état Obsolète ou Résolu. L'objet et le contenu de l'e-mail d'alerte fournissent des informations sur l'état de l'événement. Un trap SNMP contient également des informations sur l'état de l'événement.

Découvrez les différents types de gravité des événements dans Active IQ Unified Manager

Chaque événement est associé à un niveau de gravité afin de vous aider à prioriser les événements qui nécessitent une action corrective immédiate.

- **Critique**

  Un problème est survenu et pourrait entraîner une interruption de service si vous ne prenez pas immédiatement les mesures correctives nécessaires.

  Les événements critiques pour les performances ne sont envoyés qu'à partir des seuils définis par l'utilisateur.

- **Erreur**

La source d'événement continue de fonctionner; toutefois, des mesures correctives sont nécessaires pour éviter toute interruption de service.

- **Avertissement**

  La source de l'événement a connu un incident dont vous devriez être informé, ou un compteur de performance d'un objet du cluster présente une valeur anormale et doit être surveillé afin d'éviter qu'il n'atteigne le seuil critique. Les événements de cette gravité n'entraînent pas d'interruption de service et ne nécessitent généralement pas d'intervention immédiate.

  Les alertes d'avertissement de performance sont envoyées à partir de seuils définis par l'utilisateur, par le système ou de seuils dynamiques.

- **Informations**

  Cet événement se produit lorsqu'un nouvel objet est découvert ou lorsqu'une action utilisateur est effectuée. Par exemple, lorsqu'un objet de stockage est supprimé ou que des modifications de configuration sont apportées, un événement de type de gravité Information est généré.

  Les événements d'information sont envoyés directement par ONTAP lorsqu'il détecte une modification de configuration.

Découvrez les niveaux d'impact des événements dans Active IQ Unified Manager

Chaque événement est associé à un niveau d'impact (Incident, Risque, Événement ou Mise à niveau) afin de vous aider à prioriser les événements qui nécessitent une action corrective immédiate.

- **Incident**

  Un incident est un ensemble d'événements qui peut amener un cluster à ne plus servir de données au client et à manquer d'espace pour le stockage des données. Les événements ayant un niveau d'impact Incident sont les plus graves. Vous devez prendre immédiatement des mesures correctives pour éviter toute interruption de service.

- **Risque**

  Un risque est un ensemble d'événements susceptibles d'empêcher un cluster de fournir des données au client et de provoquer une saturation de l'espace de stockage. Les événements de niveau de risque peuvent entraîner une interruption de service. Des mesures correctives peuvent s'avérer nécessaires.

- **Événement**

  Un événement correspond à une modification d'état ou de statut des objets de stockage et de leurs attributs. Les événements de niveau « Événement » sont informatifs et ne nécessitent aucune action corrective.

- **Mise à niveau**

  Les événements de mise à niveau sont un type spécifique d'événement signalé par la plateforme Active IQ. Ils identifient les problèmes dont la résolution nécessite la mise à niveau du logiciel ONTAP, du firmware des nœuds ou du logiciel du système d'exploitation (pour les avis de sécurité). Vous pouvez souhaiter prendre immédiatement des mesures correctives pour certains de ces problèmes, tandis que d'autres peuvent attendre votre prochaine maintenance planifiée.

Découvrez les zones d'impact des événements dans Active IQ Unified Manager

Les événements sont classés en six domaines d'impact (disponibilité, capacité, configuration, performance, protection et sécurité) afin de vous permettre de vous concentrer sur les types d'événements dont vous êtes responsable.

- **Disponibilité**

  Les événements de disponibilité vous avertissent si un objet de stockage se met hors ligne, si un service de protocole tombe en panne, si un problème de basculement du stockage survient ou si un problème matériel survient.

- **Capacité**

  Les événements de capacité vous avertissent si vos agrégats, volumes, LUNs ou espaces de noms approchent ou ont atteint un seuil de taille, ou si le taux de croissance est inhabituel pour votre environnement.

- **Configuration**

  Les événements de configuration vous informent de la découverte, de la suppression, de l'ajout, du retrait ou du renommage de vos objets de stockage. Ces événements ont un niveau d'impact « Événement » et un type de gravité « Information ».

- **Performances**

  Les événements de performance vous informent des conditions de ressources, de configuration ou d'activité sur votre cluster qui pourraient affecter négativement la vitesse d'entrée ou de récupération du stockage des données sur vos objets de stockage surveillés.

- **Protection**

  Les événements de protection vous informent des incidents ou des risques impliquant des relations SnapMirror, des problèmes de capacité de destination, des problèmes avec les relations SnapVault ou des problèmes liés aux tâches de protection. Tout objet ONTAP (en particulier les agrégats, les volumes et les SVM) qui héberge des volumes secondaires et des relations de protection est classé dans la zone d'impact de la protection.

- **Sécurité**

  Les événements de sécurité vous informent du niveau de sécurité de vos clusters ONTAP, de vos machines virtuelles de stockage (SVM) et de vos volumes en fonction des paramètres définis dans le "NetApp Guide de renforcement de la sécurité pour ONTAP 9".

  De plus, cette zone inclut les événements de mise à niveau signalés par la plateforme Active IQ.

Comment Active IQ Unified Manager calcule l'état des objets

L'état d'un objet est déterminé par l'événement le plus grave dont l'état actuel est « Nouveau » ou « Accusé de réception ». Par exemple, si l'état d'un objet est « Erreur », cela signifie que l'un des événements de cet objet est de type « Erreur ». Une fois la correction effectuée, l'état de l'événement passe à « Résolu ».

Découvrez les événements de performance dynamiques dans Active IQ Unified Manager

Pour les événements de performance dynamiques, la section Diagnostic système de la page Détails de l'événement répertorie les principaux workloads présentant la latence ou l'utilisation la plus élevée du composant du cluster en contention.

Les statistiques de performance sont basées sur la période comprise entre le moment où l'événement de performance a été détecté et le dernier moment où l'événement a été analysé. Les graphiques affichent également les statistiques de performance historiques du composant du cluster qui est en contention.

Par exemple, vous pouvez identifier les workloads qui utilisent fortement un composant afin de déterminer quel workload déplacer vers un composant moins utilisé. Le déplacement du workload réduirait la quantité de travail sur le composant actuel, ce qui pourrait faire sortir le composant de la contention. En haut de cette section figurent l'heure et la plage de dates auxquelles un événement a été détecté et analysé pour la dernière fois. Pour les événements actifs (nouveaux ou confirmés), l'heure de la dernière analyse est mise à jour.

Les graphiques de latence et d'activité affichent le nom des principales charges de travail lorsque vous survolez le graphique avec votre curseur. 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 », « harceleurs » ou « victimes », et afficher des détails sur leur latence et leur utilisation sur le composant du cluster en contention. Vous pouvez comparer la valeur réelle à la valeur attendue pour voir quand le workload se situait en dehors de sa plage attendue de latence ou d'utilisation. Pour plus d'informations, consultez "Types de workloads surveillés par Unified Manager".

> Lorsque vous triez par écart maximal de latence, les charges de travail définies par le système ne sont pas affichées dans le tableau, car la latence ne s'applique qu'aux charges de travail définies par l'utilisateur. Les charges de travail présentant des valeurs de latence très faibles ne sont pas affichées dans le tableau.

Pour plus d'informations sur les seuils de performance dynamiques, consultez "Analyse des événements à partir de seuils de performance dynamiques".

Pour plus d'informations sur la façon dont Unified Manager classe les workloads et détermine l'ordre de tri, consultez "Comment Unified Manager détermine l'impact d'un événement sur les performances".

Les données des graphiques présentent les statistiques de performance des 24 heures précédant la dernière analyse de l'événement. Les valeurs réelles et attendues pour chaque workload sont basées sur le moment où le workload a été impliqué dans l'événement. Par exemple, un workload peut être impliqué dans un événement après la détection de l'événement, de sorte que ses statistiques de performance peuvent ne pas correspondre aux valeurs au moment de la détection de l'événement. Par défaut, les workloads sont triés par écart maximal de latence.

> Étant donné que Unified Manager ne conserve qu'un maximum de 30 jours de données historiques de performances et d'événements par tranches de 5 minutes, si l'événement date de plus de 30 jours, aucune donnée de performance n'est affichée.

- **Colonne de tri du workload**
  - **Graphique de latence**

    Affiche l'impact de l'événement sur la latence du workload lors de la dernière analyse.
  - **Colonne d'utilisation des composants**

Affiche des détails sur l'utilisation du workload du composant de cluster en conflit. Dans les graphiques, l'utilisation réelle est représentée par 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, consultez "Valeurs de mesure des performances du workload".

> Pour le composant réseau, étant donné que les statistiques de performance du réseau proviennent d'une activité en dehors du cluster, cette colonne n'est pas affichée.

- **Utilisation des composants**

  Affiche l'historique d'utilisation, en pourcentage, des composants de traitement réseau, de traitement des données et d'agrégat, ou l'historique d'activité, en pourcentage, du composant de groupe de règles QoS. Le graphique n'est pas affiché pour les composants réseau ou d'interconnexion. Vous pouvez pointer sur les statistiques pour afficher les statistiques d'utilisation à un moment précis.

- **Historique du total des écritures en MB/s**

  Pour le composant Ressources de MetroCluster uniquement, affiche le débit d'écriture total, en mégaoctets par seconde (Mo/s), pour toutes les charges de travail de volume mises en miroir vers le cluster partenaire dans une configuration MetroCluster.

- **Historique des événements**

  Affiche des lignes rouges pour indiquer les événements historiques du composant en contention. 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 Active IQ Unified Manager

Unified Manager surveille vos clusters pour détecter les modifications de configuration afin de vous aider à déterminer si une modification a pu provoquer ou contribuer à un événement de performances. Les pages de l'Explorateur de performances affichent une icône d'événement de modification (●) pour indiquer la date et l'heure à laquelle la modification a été détectée.

Vous pouvez consulter les graphiques de performance dans les pages de l'Explorateur de performances et dans la page Analyse de la charge de travail pour déterminer si l'événement de modification a eu un impact sur les performances de l'objet de cluster sélectionné. Si la modification a été détectée simultanément ou presque à un événement de performance, elle a pu contribuer au problème et déclencher l'alerte d'événement.

Unified Manager peut détecter les événements de changement suivants, qui sont catégorisés comme événements d'information :

- Un volume se déplace entre les agrégats.

  Unified Manager peut détecter l'état d'avancement, la fin ou l'échec d'un déplacement de volume. En cas d'indisponibilité d'Unified Manager pendant un déplacement de volume, une fois remis en service, il détecte le déplacement et affiche un événement de modification.

- La limite de débit (Mo/s ou IOPS) d'un groupe de stratégies QoS contenant une ou plusieurs charges de travail surveillées change.

  La modification d'une limite de groupe de règles peut entraîner des pics intermittents de latence (temps de réponse), susceptibles de déclencher des événements pour ce groupe. La latence revient progressivement

à la normale et les événements provoqués par ces pics deviennent caducs.

- Un nœud d'une paire haute disponibilité prend le relais du stockage de son nœud partenaire ou le lui restitue.

  Unified Manager peut détecter la fin d'une prise de contrôle, d'une prise de contrôle partielle ou d'une restitution. En revanche, si la prise de contrôle est due à un nœud défaillant, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de rétablissement d'ONTAP s'est terminée avec succès.

  La version précédente et la nouvelle version sont affichées.

Liste des événements et des types de gravité

Découvrez les événements d'agrégat dans Active IQ Unified Manager

Les événements d'agrégat vous fournissent des informations sur l'état des agrégats afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et comprennent 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 trap)	Niveau d'impact	Type de source	Gravité
Agrégat hors ligne(ocumEvtAggregateStateOffline)	Incident	Agrégat	Primordial
Échec de l'agrégat(ocumEvtAggregateStateFailed)	Incident	Agrégat	Primordial
Agrégat restreint(ocumEvtAggregateStateRestricted)	Risque	Agrégat	Avertissement
Reconstruction de l'agrégat(ocumEvtAggregateRaidStateReconstructing)	Risque	Agrégat	Avertissement
Agrégat dégradé(ocumEvtAggregateRaidStateDegraded)	Risque	Agrégat	Avertissement
Niveau cloud partiellement accessible(ocumEventCloudTierPartiallyReachable)	Risque	Agrégat	Avertissement

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Niveau cloud inaccessible(ocumEventCloudTierUnreachable)	Risque	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation de l'agrégat *(arlNetraCaCheckFailed)	Risque	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation d'agrégat lors du basculement de stockage *(gbNetraCaCheckFailed)	Risque	Agrégat	Erreur
MetroCluster Agrégat laissé derrière(ocumEvtMetroClusterAggregateLeftBehind)	Risque	Agrégat	Erreur
MetroCluster Mise en miroir de l'agrégat dégradée(ocumEvtMetroClusterAggregateMirrorDegraded)	Risque	Agrégat	Erreur

Domaine d'impact : capacité

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Espace d'agrégat presque plein(ocumEvtAggregateNearlyFull)	Risque	Agrégat	Avertissement
Espace d'agrégat complet(ocumEvtAggregateFull)	Risque	Agrégat	Erreur
Jours de l'agrégat avant remplissage complet(ocumEvtAggregateDaysUntilFullSoon)	Risque	Agrégat	Erreur
Agrégat suralloué(ocumEvtAggregateOvercommitted)	Risque	Agrégat	Erreur
Agrégat presque surengagé(ocumEvtAggregateAlmostOvercommitted)	Risque	Agrégat	Avertissement

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Réserve Snapshot de l'agrégat pleine(ocumEvtAggregateSnapReserveFull)	Risque	Agrégat	Avertissement
Taux de croissance agrégé anormal(ocumEvtAggregateGrowthRateAbnormal)	Risque	Agrégat	Avertissement

Domaine d'impact : configuration

Nom de l'événement(Nom du trap)	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

Domaine d'impact : performance

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Dépassement du seuil critique d'IOPS de l'agrégat(ocumAggregateIopsIncident)	Incident	Agrégat	Primordial
Seuil d'avertissement des IOPS agrégées dépassé(ocumAggregateIopsWarning)	Risque	Agrégat	Avertissement
Seuil critique du débit agrégé en MB/s dépassé(ocumAggregateMbpsIncident)	Incident	Agrégat	Primordial
Dépassement du seuil d'alerte global en MB/s(ocumAggregateMbpsWarning)	Risque	Agrégat	Avertissement

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique de latence agrégée dépassé(ocumAggregateLatencyIncident)	Incident	Agrégat	Primordial
Seuil d'alerte de latence de l'agrégat dépassé(ocumAggregateLatencyWarning)	Risque	Agrégat	Avertissement
Capacité de performance d'agrégat utilisée seuil critique dépassé(ocumAggregatePerfCapacityUsedIncident)	Incident	Agrégat	Primordial
Seuil d'avertissement de capacité de performance de l'agrégat utilisée dépassé(ocumAggregatePerfCapacityUsedWarning)	Risque	Agrégat	Avertissement
Seuil critique d'utilisation de l'agrégat dépassé (ocumAggregateUtilizationIncident)	Incident	Agrégat	Primordial
Seuil d'alerte d'utilisation de l'agrégat dépassé (ocumAggregateUtilizationWarning)	Risque	Agrégat	Avertissement
Seuil de surutilisation des disques agrégés dépassé (ocumAggregateDisksOverUtilizedWarning)	Risque	Agrégat	Avertissement
Seuil dynamique de l'agrégat dépassé (ocumAggregateDynamicEventWarning)	Risque	Agrégat	Avertissement

Découvrez les événements de cluster dans Active IQ Unified Manager

Les événements de cluster fournissent des informations sur l'état des clusters, ce qui vous permet de les surveiller et de détecter d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement, le nom du trap, 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 trap)	Niveau d'impact	Type de source	Gravité
Le cluster manque de disques de rechange(ocumEvtDisksNoSpares)	Risque	Cluster	Avertissement
Cluster non accessible(ocumEvtClusterUnreachable)	Risque	Cluster	Erreur
La surveillance du cluster a échoué(ocumEvtClusterMonitoringFailed)	Risque	Cluster	Avertissement
Dépassement des limites de capacité de licence de cluster FabricPool (ocumEvtExternalCapacityTierSpaceFull)	Risque	Cluster	Avertissement
Début de la période de grâce NVMe-oF *(nvmfGracePeriodStart)	Risque	Cluster	Avertissement
Période de grâce NVMe-oF active *(nvmfGracePeriodActive)	Risque	Cluster	Avertissement
Délai de grâce NVMe-oF expiré *(nvmfGracePeriodExpired)	Risque	Cluster	Avertissement
Début de la fenêtre de maintenance de l'objet(objectMaintenanceWindowStarted)	Événement	Cluster	Primordial
Fin de la fenêtre de maintenance des objets(objectMaintenanceWindowEnded)	Événement	Cluster	Informations
MetroCluster Disques de rechange laissés sur place(ocumEvtSpareDiskLeftBehind)	Risque	Cluster	Erreur

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
MetroCluster Basculement automatique non planifié désactivé(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risque	Cluster	Avertissement
Mot de passe de l'utilisateur du cluster modifié *(cluster.passwd.changed)	Événement	Cluster	Informations

Domaine d'impact : capacité

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil de déséquilibre de capacité du cluster dépassé(ocumConformanceNodeImbalanceWarning)	Risque	Cluster	Avertissement
Planification des niveaux de cloud en cluster (clusterCloudTierPlanningWarning)	Risque	Cluster	Avertissement
FabricPool Resynchronisation de la réplication miroir terminée *(waflCaResyncComplete)	Événement	Cluster	Avertissement
FabricPool Espace presque plein *(fabricpoolNearlyFull)	Risque	Cluster	Erreur

Domaine d'impact : configuration

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Nœud ajouté(Non applicable)	Événement	Cluster	Informations
Nœud supprimé(Non applicable)	Événement	Cluster	Informations
Cluster supprimé(non applicable)	Événement	Cluster	Informations

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
L'ajout du cluster a échoué(Non applicable)	Événement	Cluster	Erreur
Nom du cluster modifié(Non applicable)	Événement	Cluster	Informations
EMS d'urgence reçu (Sans objet)	Événement	Cluster	Primordial
EMS critique reçu (Non applicable)	Événement	Cluster	Primordial
Alerte EMS reçue (Non applicable)	Événement	Cluster	Erreur
Erreur EMS reçue (Non applicable)	Événement	Cluster	Avertissement
Avertissement EMS reçu (Non applicable)	Événement	Cluster	Avertissement
EMS de débogage reçu (Non applicable)	Événement	Cluster	Avertissement
Avis EMS reçu (Non applicable)	Événement	Cluster	Avertissement
Message d'information EMS reçu (Non applicable)	Événement	Cluster	Avertissement

Les événements EMS ONTAP sont classés en trois niveaux de gravité des événements Unified Manager.

Niveau de gravité de l'événement Unified Manager	Niveau de gravité des événements EMS de ONTAP
Primordial	Urgence Primordial
Erreur	Alerte
Avertissement	Erreur Avertissement Déboguer Avis Information

Domaine d'impact : performance

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil de déséquilibre de charge du cluster dépassé()	Risque	Cluster	Avertissement
Seuil critique d'IOPS du cluster dépassé(ocumClusterIopsIncident)	Incident	Cluster	Primordial
Seuil d'alerte IOPS du cluster dépassé(ocumClusterIopsWarning)	Risque	Cluster	Avertissement
Seuil critique du cluster MB/s dépassé(ocumClusterMbpsIncident)	Incident	Cluster	Primordial
Seuil d'alerte du cluster MB/s dépassé(ocumClusterMbpsWarning)	Risque	Cluster	Avertissement
Seuil dynamique du cluster dépassé(ocumClusterDynamicEventWarning)	Risque	Cluster	Avertissement

Domaine d'impact : sécurité

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
AutoSupport Transport HTTPS désactivé(ocumClusterASUPHttpsConfiguredDisabled)	Risque	Cluster	Avertissement
Transfert de journal non chiffré(ocumClusterAuditLogUnencrypted)	Risque	Cluster	Avertissement
Utilisateur administrateur local par défaut activé(ocumClusterDefaultAdminEnabled)	Risque	Cluster	Avertissement
Mode FIPS désactivé(ocumClusterFipsDisabled)	Risque	Cluster	Avertissement

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Bannière de connexion désactivée(ocumClusterLoginBannerDisabled)	Risque	Cluster	Avertissement
Bannière de connexion modifiée(ocumClusterLoginBannerChanged)	Risque	Cluster	Avertissement
Destinations de transfert des journaux modifiées(ocumLogForwardDestinationsChanged)	Risque	Cluster	Avertissement
Noms des serveurs NTP modifiés(ocumNtpServerNamesChanged)	Risque	Cluster	Avertissement
Le nombre de serveurs NTP est faible(securityConfigNTPServerCountLowRisk)	Risque	Cluster	Avertissement
Communication entre pairs du cluster non chiffrée(ocumClusterPeerEncryptionDisabled)	Risque	Cluster	Avertissement
SSH utilise des algorithmes de chiffrement non sécurisés(ocumClusterSSHInsecure)	Risque	Cluster	Avertissement
Protocole Telnet activé(ocumClusterTelnetEnabled)	Risque	Cluster	Avertissement
Les mots de passe de certains comptes utilisateur ONTAP utilisent la fonction de hachage MD5, moins sécurisée (ocumClusterMD5PasswordHashUsed)	Risque	Cluster	Avertissement
Le cluster utilise un certificat auto-signé(ocumClusterSelfSignedCertificate)	Risque	Cluster	Avertissement
L'interface de ligne de commande distante du cluster est activée(ocumClusterRshDisabled)	Risque	Cluster	Avertissement

Nom de l'événement(Nom du trap)	Niveau d'impact	Type de source	Gravité
Certificat de cluster sur le point d'expirer(ocumEvtClusterCertificateAboutToExpire)	Risque	Cluster	Avertissement
Certificat de cluster expiré(ocumEvtClusterCertificateExpired)	Risque	Cluster	Erreur

Découvrez les événements de disque dans Active IQ Unified Manager

Les événements liés aux disques vous fournissent des informations sur leur état afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Disques Flash - Blocs de rechange presque épuisés(ocumEvtClusterFlashDiskFewerSpareBlockError)	Risque	Cluster	Erreur
Disques Flash - Pas de blocs de rechange(ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incident	Cluster	Primordial
Certains disques non attribués(ocumEvtClusterUnassignedDisksSome)	Risque	Cluster	Avertissement
Certains disques défectueux(ocumEvtDisksSomeFailed)	Incident	Cluster	Primordial

Découvrez les événements liés aux enclosures dans Active IQ Unified Manager

Les événements relatifs aux boîtiers de tiroir disque vous fournissent des informations sur l'état des boîtiers de tiroir disque dans votre centre de données afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Ventilateurs du tiroir disque en panne(ocumEvtShelfFanFailed)	Incident	Tiroir de stockage	Primordial
Les alimentations du tiroir disque ont échoué(ocumEvtShelfPowerSupplyFailed)	Incident	Tiroir de stockage	Primordial
Multipath du tiroir disque non configuré(ocumDiskShelfConnectivityNotInMultiPath) Cet événement ne s'applique pas à : • Les clusters qui sont dans une configuration MetroCluster • Les plateformes suivantes: FAS2554, FAS2552, FAS2520 et FAS2240	Risque	Nœud	Avertissement
Échec du chemin d'accès du tiroir disque(ocumDiskShelfConnectivityPathFailure)	Risque	Tiroir de stockage	Avertissement

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Tiroir disque détecté(Non applicable)	Événement	Nœud	Informations
Tiroirs disques retirés(Non applicable)	Événement	Nœud	Informations

Découvrez les événements des ventilateurs dans Active IQ Unified Manager

Les événements relatifs aux ventilateurs vous fournissent des informations sur l'état des ventilateurs sur les nœuds de votre centre de données afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la

gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Un ou plusieurs ventilateurs défaillants(ocumEvtFansOneOrMoreFailed)	Incident	Nœud	Primordial

Découvrez les événements liés aux cartes mémoire dans Active IQ Unified Manager

Les événements liés aux cartes flash vous informent de l'état des cartes flash installées sur les nœuds de votre centre de données, vous permettant ainsi de détecter d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Cartes mémoire hors ligne(ocumEvtFlashCardOffline)	Incident	Nœud	Primordial

Découvrez les événements liés aux inodes dans Active IQ Unified Manager

Les événements d'inode fournissent des informations lorsque l'inode est plein ou presque plein, afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Inodes presque pleins(ocumEvtInodesAlmostFull)	Risque	Volume	Avertissement
Inodes complets(ocumEvtInodesFull)	Risque	Volume	Erreur

Événements d'interface réseau dans Active IQ Unified Manager

Les événements d'interface réseau fournissent des informations sur l'état de vos interfaces réseau (LIF), vous permettant ainsi de surveiller d'éventuels problèmes. Les

événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
État de l'interface réseau hors service(ocumEvtLifStatusDown)	Risque	Interface	Erreur
État de l'interface réseau FC/FCoE en panne (ocumEvtFCLifStatusDown)	Risque	Interface	Erreur
Basculement de l'interface réseau impossible(ocumEvtLifFailoverNotPossible)	Risque	Interface	Avertissement
Interface réseau non sur le port de rattachement(ocumEvtLifNotAtHomePort)	Risque	Interface	Avertissement

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Route d'interface réseau non configurée(non applicable)	Événement	Interface	Informations

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique de l'interface réseau en MB/s dépassé(ocumNetworkLifMbpsIncident)	Incident	Interface	Primordial
Seuil d'avertissement MB/s de l'interface réseau dépassé(ocumNetworkLifMbpsWarning)	Risque	Interface	Avertissement
Seuil critique de débit de l'interface réseau FC (MB/s) dépassé(ocumFcpLifMbpsIncident)	Incident	Interface	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil d'alerte MB/s de l'interface réseau FC dépassé(ocumFcpLifMbpsWarning)	Risque	Interface	Avertissement
Seuil critique de débit MB/s de l'interface réseau FC NVMf dépassé(ocumNvmfFcLifMbpsIncident)	Incident	Interface	Primordial
Seuil d'alerte MB/s de l'interface réseau FC NVMf dépassé(ocumNvmfFcLifMbpsWarning)	Risque	Interface	Avertissement

Découvrez les événements LUN dans Active IQ Unified Manager

Les événements LUN vous fournissent des informations sur l'état de vos LUN, afin que vous puissiez surveiller d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du piège, 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 trap)	Niveau d'impact	Type de source	Gravité
LUN hors ligne(ocumEvtLunOffline)	Incident	LUN	Primordial
LUN détruit *(lunDestroy)	Événement	LUN	Informations
LUN mappé avec un système d'exploitation non pris en charge dans igroup(igroupUnsupportedOsType)	Incident	LUN	Avertissement
Chemin actif unique pour accéder au LUN(ocumEvtLunSingleActivePath)	Risque	LUN	Avertissement
Aucun chemin d'accès actif pour accéder au LUN(ocumEvtLunNotReachable)	Incident	LUN	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Aucun chemin optimisé pour accéder à la LUN(ocumEvtLunOptimizedPathInactive)	Risque	LUN	Avertissement
Aucun chemin d'accès au LUN depuis le partenaire HA(ocumEvtLunHaPathInactive)	Risque	LUN	Avertissement
Aucun chemin d'accès au LUN depuis un nœud de la paire HA(ocumEvtLunNodePathStatusDown)	Risque	LUN	Erreur

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Espace insuffisant pour la copie de l'instantané LUN(ocumEvtLunSnapshotNotPossible)	Risque	Volume	Avertissement

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
LUN mappé avec un système d'exploitation non pris en charge dans igroup(igroupUnsupportedOsType)	Risque	LUN	Avertissement

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS LUN dépassé(ocumLunIopsIncident)	Incident	LUN	Primordial
Seuil d'alerte IOPS LUN dépassé(ocumLunIopsWarning)	Risque	LUN	Avertissement
Dépassement du seuil critique en MB/s du LUN(ocumLunMbpsIncident)	Incident	LUN	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil d'alerte LUN MB/s dépassé(ocumLunMbpsWarning)	Risque	LUN	Avertissement
Latence LUN ms/op Seuil critique dépassé(ocumLunLatencyIncident)	Incident	LUN	Primordial
Seuil d'alerte de latence LUN ms/op dépassé(ocumLunLatencyWarning)	Risque	LUN	Avertissement
Dépassement du seuil critique de latence et d'IOPS des LUN(ocumLunLatencyIopsIncident)	Incident	LUN	Primordial
Seuil d'alerte de latence LUN et d'IOPS dépassé(ocumLunLatencyIopsWarning)	Risque	LUN	Avertissement
Latence LUN et seuil critique de MB/s dépassés(ocumLunLatencyMbpsIncident)	Incident	LUN	Primordial
Dépassement du seuil d'avertissement de latence LUN et de MB/s(ocumLunLatencyMbpsWarning)	Risque	LUN	Avertissement
Latence du LUN et capacité de performances agrégées utilisée : seuil critique dépassé(ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incident	LUN	Primordial
Latence du LUN et capacité de performance utilisée de l'agrégat : seuil d'avertissement dépassé(ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risque	LUN	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique de latence des LUN et d'utilisation de l'agrégat dépassé(ocumLunLatencyAggregateUtilizationIncident)	Incident	LUN	Primordial
Seuil d'alerte de latence LUN et d'utilisation de l'agrégat dépassé(ocumLunLatencyAggregateUtilizationWarning)	Risque	LUN	Avertissement
Latence LUN et capacité de performance du nœud : seuil critique dépassé(ocumLunLatencyNodePerfCapacityUsedIncident)	Incident	LUN	Primordial
Seuil d'alerte dépassé pour la latence des LUN et la capacité de performance du nœud utilisée (ocumLunLatencyNodePerfCapacityUsedWarning)	Risque	LUN	Avertissement
Latence LUN et capacité de performance du nœud utilisée - Seuil critique de prise de contrôle dépassé(ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	LUN	Primordial
Latence LUN et capacité de performance du nœud utilisée - Seuil d'avertissement de basculement dépassé(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risque	LUN	Avertissement
Le seuil critique de latence LUN et d'utilisation des nœuds a été dépassé(ocumLunLatencyNodeUtilizationIncident)	Incident	LUN	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil d'alerte de latence de la LUN et d'utilisation du nœud dépassé(ocumLunLatencyNodeUtilizationWarning)	Risque	LUN	Avertissement
Seuil d'alerte QoS LUN Max IOPS dépassé(ocumQosLunMaxIopsWarning)	Risque	LUN	Avertissement
Seuil d'avertissement QoS LUN Max MB/s dépassé(ocumQosLunMaxMbpsWarning)	Risque	LUN	Avertissement
Seuil de latence de la LUN de la charge de travail dépassé tel que défini par la stratégie de niveau de service des performances(ocumConformanceLatencyWarning)	Risque	LUN	Avertissement

Découvrez les événements de la station de gestion dans Active IQ Unified Manager

Les événements de la station de gestion vous fournissent des informations sur l'état du serveur sur lequel Unified Manager est installé, ce qui vous permet de surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Espace disque du serveur de gestion presque plein(ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risque	Station de gestion	Avertissement
Espace disque du serveur de gestion saturé(ocumEvtUnifiedManagerDiskSpaceFull)	Incident	Station de gestion	Primordial
Serveur de gestion avec peu de mémoire(ocumEvtUnifiedManagerMemoryLow)	Risque	Station de gestion	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Le serveur de gestion est presque à court de mémoire(ocumEvtUnifiedManagerMemoryAlmostOut)	Incident	Station de gestion	Primordial
La taille du fichier journal MySQL a augmenté ; un redémarrage est nécessaire(ocumEvtMysqlLogFileSizeWarning)	Incident	Station de gestion	Avertissement
L'espace alloué à la taille totale du journal d'audit est sur le point d'être saturé	Risque	Station de gestion	Avertissement
Certificat du serveur Syslog sur le point d'expirer	Risque	Station de gestion	Avertissement
Certificat du serveur Syslog expiré	Risque	Station de gestion	Erreur
Fichier journal d'audit falsifié	Risque	Station de gestion	Avertissement
Fichier journal d'audit supprimé	Risque	Station de gestion	Avertissement
Erreur de connexion au serveur Syslog	Risque	Station de gestion	Erreur
Configuration du serveur Syslog modifiée	Événement	Station de gestion	Avertissement

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
L'analyse des données de performance est affectée(ocumEvtUnifiedManagerDataMissingAnalyze)	Risque	Station de gestion	Avertissement
La collecte des données de performance est affectée(ocumEvtUnifiedManagerDataMissingCollection)	Incident	Station de gestion	Primordial

Ces deux derniers événements de performances étaient disponibles uniquement pour Unified Manager 7.2. Si l'un de ces événements existe à l'état « Nouveau » et que vous effectuez ensuite une mise à niveau vers une version plus récente du logiciel Unified Manager, les

événements ne seront pas supprimés automatiquement. Vous devrez déplacer manuellement les événements vers l'état « Résolu ».

Découvrez les événements Bridge MetroCluster dans Active IQ Unified Manager

Les événements de pont MetroCluster vous fournissent des informations sur l'état des ponts afin que vous puissiez surveiller d'éventuels problèmes dans une configuration MetroCluster over FC. Les événements sont regroupés par zone d'impact et comprennent 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 du trap)	Niveau d'impact	Type de source	Gravité
Pont inaccessible(ocumEvtBridgeUnreachable)	Incident	Pont MetroCluster	Primordial
Température anormale du pont(ocumEvtBridgeTemperatureAbnormal)	Incident	Pont MetroCluster	Primordial

Découvrez les événements de connectivité MetroCluster dans Active IQ Unified Manager

Les événements de connectivité vous fournissent des informations sur la connectivité entre les composants d'un cluster et entre les clusters dans les configurations MetroCluster over FC et MetroCluster over IP, afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Événements communs aux deux configurations

Ces événements de connectivité sont courants aussi bien pour les configurations MetroCluster over FC que pour les configurations MetroCluster over IP.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Tous les liens entre les partenaires MetroCluster sont hors service (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incident	MetroCluster relation	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
MetroCluster Partenaires non joignables via le réseau de peering (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incident	MetroCluster relation	Primordial
MetroCluster Capacité de reprise après sinistre impactée(ocumEvtMetroClusterDRStatusImpacted)	Risque	MetroCluster relation	Primordial
MetroCluster Configuration basculée (ocumEvtMetroClusterDRStatusImpacted)	Risque	MetroCluster relation	Avertissement

Configuration MetroCluster over FC

Ces événements concernent les configurations MetroCluster sur FC.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Toutes les liaisons inter-commutateurs sont hors service(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Incident	MetroCluster connexion intercommutateurs	Primordial
Liaison FC-SAS Bridge vers la pile de stockage en panne(ocumEvtBridgeSasPortDown)	Incident	MetroCluster connexion de la pile de ponts	Primordial
MetroCluster Configuration partiellement basculée(ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risque	MetroCluster relation	Erreur
Commutateur de nœud vers FC Switch : toutes les liaisons d'interconnexion FC-VI sont hors service(ocumEvtMccNodeSwitchFcviLinksDown)	Incident	MetroCluster connexion du commutateur de nœud	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Nœud vers commutateur FC : une ou plusieurs liaisons d'initiateur FC sont hors service(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risque	MetroCluster connexion du commutateur de nœud	Avertissement
Passage du nœud au commutateur FC : toutes les liaisons d'initiateur FC sont hors service (ocumEvtMccNodeSwitchFcLinksDown)	Incident	MetroCluster connexion du commutateur de nœud	Primordial
Liaison FC du commutateur vers le pont FC-SAS inactive (ocumEvtMccSwitchBridgeFcLinksDown)	Incident	MetroCluster connexion du pont de commutateur	Primordial
Toutes les liaisons FC VI InterConnect inter-nœuds sont hors service (ocumEvtMccInterNodeLinksDown)	Incident	Connexion inter-nœuds	Primordial
Un ou plusieurs liens FC VI InterConnect inter-nœuds sont en panne (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risque	Connexion inter-nœuds	Avertissement
Liaison nœud-pont en panne (ocumEvtMccNodeBridgeLinksDown)	Incident	Connexion au bridge du nœud	Primordial
Tous les liens SAS du nœud vers la pile de stockage sont hors service (ocumEvtMccNodeStackLinksDown)	Incident	Connexion de la pile de nœuds	Primordial
Nœud vers pile de stockage : une ou plusieurs liaisons SAS sont hors service (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risque	Connexion de la pile de nœuds	Avertissement

Configuration MetroCluster sur IP

Ces événements concernent les configurations MetroCluster over IP.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
MetroCluster l'état de la connectivité intersite IP est indisponible (mccIntersiteconnectivityStatusDown)	Risque	MetroCluster Relation	Primordial
MetroCluster-IP Connexion du nœud au commutateur hors ligne (mccIpPortStatusOffline)	Risque	Nœud	Erreur

Découvrez les événements de commutation MetroCluster dans Active IQ Unified Manager

Les événements de commutateur MetroCluster pour les configurations MetroCluster over FC vous fournissent des informations sur l'état des commutateurs MetroCluster afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Température du commutateur anormale(ocumEvtSwitchTemperatureAbnormal)	Incident	Commutateur MetroCluster	Primordial
Commutateur inaccessible(ocumEvtSwitchUnreachable)	Incident	Commutateur MetroCluster	Primordial
Les ventilateurs du commutateur sont tombés en panne(ocumEvtSwitchFansOneOrMoreFailed)	Incident	Commutateur MetroCluster	Primordial
Les alimentations du commutateur sont défaillantes(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incident	Commutateur MetroCluster	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Échec des capteurs de température du commutateur(ocumEvtSwitchTemperatureSensorFailed) Cet événement concerne uniquement les commutateurs Cisco.	Incident	Commutateur MetroCluster	Primordial

Découvrez les événements d'espace de noms NVMe dans Active IQ Unified Manager

Les événements d'espace de noms NVMe vous fournissent des informations sur l'état de vos espaces de noms, vous permettant ainsi de détecter d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, 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 du trap)	Niveau d'impact	Type de source	Gravité
NVMeNS Hors ligne *(nvmeNamespaceStatusOffline)	Événement	Espace de noms	Informations
NVMeNS en ligne *(nvmeNamespaceStatusOnline)	Événement	Espace de noms	Informations
NVMeNS manque d'espace *(nvmeNamespaceSpaceOutOfSpace)	Risque	Espace de noms	Avertissement
NVMeNS Détruire *(nvmeNamespaceDestroy)	Événement	Espace de noms	Informations

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS de l'espace de noms NVMe dépassé(ocumNvmeNamespaceIopsIncident)	Incident	Espace de noms	Primordial
Seuil d'alerte IOPS de l'espace de noms NVMe dépassé(ocumNvmeNamespaceIopsWarning)	Risque	Espace de noms	Avertissement
Seuil critique de MB/s de l'espace de noms NVMe dépassé(ocumNvmeNamespaceMbpsIncident)	Incident	Espace de noms	Primordial
Seuil d'avertissement MB/s de l'espace de noms NVMe dépassé(ocumNvmeNamespaceMbpsWarning)	Risque	Espace de noms	Avertissement
Latence de l'espace de noms NVMe ms/op : seuil critique dépassé(ocumNvmeNamespaceLatencyIncident)	Incident	Espace de noms	Primordial
Seuil d'avertissement dépassé pour la latence de l'espace de noms NVMe en ms/op(ocumNvmeNamespaceLatencyWarning)	Risque	Espace de noms	Avertissement
Seuil critique de latence et d'IOPS de l'espace de noms NVMe dépassé(ocumNvmeNamespaceLatencyIopsIncident)	Incident	Espace de noms	Primordial
Le seuil d'avertissement de latence et d'IOPS de l'espace de noms NVMe est dépassé (ocumNvmeNamespaceLatencyIopsWarning)	Risque	Espace de noms	Avertissement
Latence de l'espace de noms NVMe et seuil critique de Mo/s dépassé(ocumNvmeNamespaceLatencyMbpsIncident)	Incident	Espace de noms	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Latence de l'espace de noms NVMe et seuil d'avertissement MB/s dépassés(ocumNvmeNamespaceLatencyMbpsWarning)	Risque	Espace de noms	Avertissement

Découvrez les événements de nœud dans Active IQ Unified Manager

Les événements de nœud vous fournissent des informations sur l'état des nœuds afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, 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 du trap)	Niveau d'impact	Type de source	Gravité
Espace du volume racine du nœud presque plein(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risque	Nœud	Avertissement
Échec de la connexion aux métadonnées Cloud AWS *(ocumCloudAwsMetadataConnFail)	Risque	Nœud	Erreur
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Risque	Nœud	Erreur
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risque	Nœud	Erreur
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risque	Nœud	Erreur
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Événement	Nœud	Informations

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Rôle IAM invalide dans le cloud AWS *(ocumCloudAwsIamRoleInvalid)	Risque	Nœud	Erreur
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risque	Nœud	Erreur
Hôte de niveau cloud non résolvable *(ocumObjstoreHostUnresolvable)	Risque	Nœud	Erreur
Interface réseau inter-cluster du niveau Cloud hors service *(ocumObjstoreInterClusterLifDown)	Risque	Nœud	Erreur
L'un des pools NFSv4 est épuisé *(nbladeNfsv4PoolEXhaust)	Incident	Nœud	Primordial
Signature de niveau cloud non concordante *(oscSignatureMismatch)	Risque	Nœud	Erreur

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Mémoire du moniteur QoS saturée *(ocumQosMonitorMemoryMaxed)	Risque	Nœud	Erreur
Mémoire du moniteur QoS réduite *(ocumQosMonitorMemoryAbated)	Événement	Nœud	Informations

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Nœud renommé(Non applicable)	Événement	Nœud	Informations

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS du nœud dépassé(ocumNodeIopsIncident)	Incident	Nœud	Primordial
Seuil d'alerte IOPS du nœud dépassé(ocumNodeIopsWarning)	Risque	Nœud	Avertissement
Seuil critique de MB/s du nœud dépassé(ocumNodeMbpsIncident)	Incident	Nœud	Primordial
Seuil d'alerte MB/s du nœud dépassé(ocumNodeMbpsWarning)	Risque	Nœud	Avertissement
Latence du nœud ms/op seuil critique dépassé(ocumNodeLatencyIncident)	Incident	Nœud	Primordial
Latence du nœud ms/op : seuil d'avertissement dépassé(ocumNodeLatencyWarning)	Risque	Nœud	Avertissement
Capacité de performance du nœud utilisée : seuil critique dépassé(ocumNodePerfCapacityUsedIncident)	Incident	Nœud	Primordial
Capacité de performance du nœud utilisée : seuil d'alerte dépassé(ocumNodePerfCapacityUsedWarning)	Risque	Nœud	Avertissement
Capacité de performance du nœud utilisée - Seuil critique de prise de contrôle dépassé(ocumNodePerfCapacityUsedTakeoverIncident)	Incident	Nœud	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Capacité de performance du nœud utilisée - Seuil d'alerte de prise de contrôle dépassé(ocumNodePerfCapacityUsedTakeoverWarning)	Risque	Nœud	Avertissement
Seuil critique d'utilisation du nœud dépassé (ocumNodeUtilizationIncident)	Incident	Nœud	Primordial
Seuil d'alerte d'utilisation du nœud dépassé (ocumNodeUtilizationWarning)	Risque	Nœud	Avertissement
Seuil de surutilisation de la paire HA de nœuds dépassé (ocumNodeHaPairOverUtilizedInformation)	Événement	Nœud	Informations
Seuil de fragmentation du disque du nœud dépassé (ocumNodeDiskFragmentationWarning)	Risque	Nœud	Avertissement
Seuil de capacité de performance utilisée dépassé (ocumNodeOverUtilizedWarning)	Risque	Nœud	Avertissement
Seuil dynamique du nœud dépassé (ocumNodeDynamicEventWarning)	Risque	Nœud	Avertissement

Domaine d'impact : sécurité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Identifiant de l'avis : NTAP-<*advisory ID*>(ocumx)	Risque	Nœud	Primordial

Découvrez les événements liés à la batterie NVRAM dans Active IQ Unified Manager

Les événements de batterie NVRAM vous fournissent des informations sur l'état de vos batteries afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau

d’impact, le type de source et la gravité.

Domaine d’impact : disponibilité

Nom de l’événement (nom du trap)	Niveau d’impact	Type de source	Gravité
Batterie NVRAM faible(ocumEvtNvramBatteryLow)	Risque	Nœud	Avertissement
Batterie NVRAM déchargée(ocumEvtNvramBatteryDischarged)	Risque	Nœud	Erreur
Batterie NVRAM excessivement chargée(ocumEvtNvramBatteryOverCharged)	Incident	Nœud	Primordial

Découvrez les événements de port dans Active IQ Unified Manager

Les événements de ports vous fournissent des informations sur l’état des ports du cluster, ce qui vous permet de surveiller les changements ou les problèmes sur le port, par exemple si le port est hors service.

Domaine d’impact : disponibilité

Nom de l’événement (nom du trap)	Niveau d’impact	Type de source	Gravité
État du port hors service (ocumEvtPortStatusDown)	Incident	Nœud	Primordial

Domaine d’impact : performance

Nom de l’événement (nom du trap)	Niveau d’impact	Type de source	Gravité
Dépassement du seuil critique du débit du port réseau (MB/s)(ocumNetworkPortMbpsIncident)	Incident	Port	Primordial
Seuil d’avertissement MB/s du port réseau dépassé(ocumNetworkPortMbpsWarning)	Risque	Port	Avertissement
Dépassement du seuil critique en MB/s du port FCP(ocumFcpPortMbpsIncident)	Incident	Port	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil d'alerte du port FCP en MB/s dépassé(ocumFcpPortMbpsWarning)	Risque	Port	Avertissement
Seuil critique d'utilisation des ports réseau dépassé(ocumNetworkPortUtilizationIncident)	Incident	Port	Primordial
Seuil d'alerte d'utilisation du port réseau dépassé(ocumNetworkPortUtilizationWarning)	Risque	Port	Avertissement
Seuil critique d'utilisation du port FCP dépassé(ocumFcpPortUtilizationIncident)	Incident	Port	Primordial
Seuil d'alerte d'utilisation du port FCP dépassé(ocumFcpPortUtilizationWarning)	Risque	Port	Avertissement

Découvrez les événements liés à l'alimentation électrique dans Active IQ Unified Manager

Les événements liés aux blocs d'alimentation vous fournissent des informations sur l'état de votre matériel afin de vous permettre de détecter d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Une ou plusieurs alimentations défectueuses(ocumEvtPowerSupplyOneOrMoreFailed)	Incident	Nœud	Primordial

Découvrez les événements de protection dans Active IQ Unified Manager

Les événements de protection vous indiquent si une tâche a échoué ou a été interrompue afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
La tâche de protection a échoué(ocumEvtProtectionJobTaskFailed)	Incident	Volume ou service de stockage	Primordial
Tâche de protection abandonnée(ocumEvtProtectionJobAborted)	Risque	Volume ou service de stockage	Avertissement

Découvrez les événements Qtree dans Active IQ Unified Manager

Les événements qtree vous fournissent des informations sur la capacité du qtree ainsi que sur les limites des fichiers et des disques, ce qui vous permet de surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Espace Qtree presque plein(ocumEvtQtreeSpaceNearlyFull)	Risque	Qtree	Avertissement
Espace Qtree plein(ocumEvtQtreeSpaceFull)	Risque	Qtree	Erreur
Espace Qtree normal(ocumEvtQtreeSpaceThresholdOk)	Événement	Qtree	Informations
Limite stricte de fichiers du Qtree atteinte(ocumEvtQtreeFilesHardLimitReached)	Incident	Qtree	Primordial
Limite logicielle des fichiers Qtree dépassée(ocumEvtQtreeFilesSoftLimitBreached)	Risque	Qtree	Avertissement
Limite stricte d'espace Qtree atteinte(ocumEvtQtreeSpaceHardLimitReached)	Incident	Qtree	Primordial
Limite souple d'espace du Qtree dépassée(ocumEvtQtreeSpaceSoftLimitBreached)	Risque	Qtree	Avertissement

Découvrez les événements du Service Processor dans Active IQ Unified Manager

Les événements du processeur de service vous fournissent des informations sur son état, vous permettant ainsi de détecter d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Processeur de service non configuré(ocumEvtServiceProcessorNotConfigured)	Risque	Nœud	Avertissement
Processeur de service hors ligne(ocumEvtServiceProcessorOffline)	Risque	Nœud	Erreur

Découvrez les événements de relation SnapMirror dans Active IQ Unified Manager

Les événements de relation SnapMirror vous fournissent des informations sur l'état de vos relations SnapMirror asynchrones et synchrones afin que vous puissiez surveiller les problèmes potentiels. Les événements de relation SnapMirror asynchrones sont générés pour les Storage VMs et les volumes, mais les événements de relation SnapMirror synchrones sont générés uniquement pour les relations de volumes. Aucun événement n'est généré pour les volumes constitutifs qui font partie des relations de reprise après sinistre de Storage VM. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, 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 relation SnapMirror sont générés pour les VM de stockage protégées par la reprise après sinistre des VM de stockage, mais pas pour les relations d'objets constitutifs.

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Réplication miroir non saine(ocumEvtSnapmirrorRelationshipUnhealthy)	Risque	SnapMirror relation	Avertissement
Réplication miroir interrompue(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risque	SnapMirror relation	Erreur

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Échec de l'initialisation de la réplication miroir(ocumEvtSnapmirrorRelationshipInitializeFailed)	Risque	SnapMirror relation	Erreur
Échec de la mise à jour de la réplication miroir(ocumEvtSnapmirrorRelationshipUpdateFailed)	Risque	SnapMirror relation	Erreur
Erreur de décalage de réplication miroir(ocumEvtSnapMirrorRelationshipLagError)	Risque	SnapMirror relation	Erreur
Avertissement de retard de réplication miroir(ocumEvtSnapMirrorRelationshipLagWarning)	Risque	SnapMirror relation	Avertissement
Échec de la resynchronisation de la réplication miroir(ocumEvtSnapmirrorRelationshipResyncFailed)	Risque	SnapMirror relation	Erreur
Réplication synchrone désynchronisée *(syncSnapmirrorRelationshipOutofsync)	Risque	SnapMirror relation	Avertissement
Réplication synchrone rétablie *(syncSnapmirrorRelationshipInSync)	Événement	SnapMirror relation	Informations
Échec de la resynchronisation automatique de la réplication synchrone *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risque	SnapMirror relation	Erreur
Ontap Mediator est ajouté au Cluster (snapmirrorMediatorAdded)	Événement	Cluster	Informations
Ontap Mediator a été supprimé du cluster (snapmirrorMediatorRemoved)	Événement	Cluster	Informations

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Ontap Mediator est inaccessible depuis le cluster (snapmirrorMediatorUnreachable)	Risque	Médiateur	Avertissement
Ontap Mediator n'est pas accessible depuis le cluster (snapmirrorMediatorMisconfigured)	Risque	Médiateur	Erreur
La connectivité avec Ontap Mediator a été rétablie, la resynchronisation est effectuée et le système est prêt pour la synchronisation active SnapMirror (snapmirrorMediatorInQuorum)	Événement	Médiateur	Informations

Découvrez les événements liés à la relation Asynchronous Mirror and Vault dans Active IQ Unified Manager

Les événements liés aux relations Asynchronous Mirror et Vault vous fournissent des informations sur l'état de vos relations Asynchronous SnapMirror et Vault afin que vous puissiez surveiller d'éventuels problèmes. Les événements liés aux relations Asynchronous Mirror et Vault sont pris en charge pour les relations de protection des volumes et des Storage VM. Mais seules les relations Vault ne sont pas prises en charge pour la reprise après sinistre des Storage VM. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, 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 sinistre des machines virtuelles de stockage, mais pas pour les relations entre les objets constitutifs.

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Mirror et Vault asynchrones non sains(ocumEvtMirrorVaultRelationshipUnhealthy)	Risque	SnapMirror relation	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Mise en miroir asynchrone et copie de sauvegarde interrompues(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risque	SnapMirror relation	Erreur
Échec de l'initialisation asynchrone de la mise en miroir et de l'archivage (ocumEvtMirrorVaultRelationshipInitializeFailed)	Risque	SnapMirror relation	Erreur
Échec de la mise à jour asynchrone du miroir et du coffre-fort (ocumEvtMirrorVaultRelationshipUpdateFailed)	Risque	SnapMirror relation	Erreur
Erreur de décalage du miroir asynchrone et du vault (ocumEvtMirrorVaultRelationshipLagError)	Risque	SnapMirror relation	Erreur
Avertissement de décalage de Asynchronous Mirror and Vault (ocumEvtMirrorVaultRelationshipLagWarning)	Risque	SnapMirror relation	Avertissement
Échec de la resynchronisation asynchrone de Mirror et Vault(ocumEvtMirrorVaultRelationshipResyncFailed)	Risque	SnapMirror relation	Erreur

L'événement « SnapMirror update failure » est déclenché par le portail Active IQ (Config Advisor).

Découvrez les événements Snapshot dans Active IQ Unified Manager

Les événements Snapshot fournissent des informations sur l'état des snapshots, ce qui vous permet de les surveiller afin de détecter d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement, le nom du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Suppression automatique des instantanés désactivée(Non applicable)	Événement	Volume	Informations
Suppression automatique des instantanés activée(Non applicable)	Événement	Volume	Informations
Configuration de suppression automatique de Snapshot modifiée(Non applicable)	Événement	Volume	Informations

Découvrez les événements de relation SnapVault dans Active IQ Unified Manager

Les événements de relation SnapVault vous fournissent des informations sur l'état de vos relations SnapVault afin que vous puissiez surveiller les problèmes potentiels. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Zone d'impact : protection

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Vault asynchrone en mauvais état(ocumEvtSnapVaultRelationshipUnhealthy)	Risque	SnapMirror relation	Avertissement
Vault asynchrone interrompu (ocumEvtSnapVaultRelationshipStateBrokenoff)	Risque	SnapMirror relation	Erreur
Échec de l'initialisation asynchrone du Vault(ocumEvtSnapVaultRelationshipInitializeFailed)	Risque	SnapMirror relation	Erreur
Échec de la mise à jour asynchrone du coffre-fort(ocumEvtSnapVaultRelationshipUpdateFailed)	Risque	SnapMirror relation	Erreur
Erreur de retard Vault asynchrone(ocumEvtSnapVaultRelationshipLagError)	Risque	SnapMirror relation	Erreur

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Avertissement de décalage asynchrone du coffre-fort(ocumEvtSnapVaultRelationshipLagWarning)	Risque	SnapMirror relation	Avertissement
Échec de la resynchronisation asynchrone de Vault(ocumEvtSnapvaultRelationshipResyncFailed)	Risque	SnapMirror relation	Erreur

Découvrez les événements liés aux paramètres de basculement du stockage dans Active IQ Unified Manager

Les événements liés aux paramètres de basculement du stockage (SFO) vous informent de l'état de votre basculement (désactivé ou non configuré) afin de vous permettre de détecter d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Interconnexion de basculement du stockage : une ou plusieurs liaisons hors service(ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risque	Nœud	Avertissement
Basculement du stockage désactivé(ocumEvtSfoSettingsDisabled)	Risque	Nœud	Erreur
Basculement du stockage non configuré(ocumEvtSfoSettingsNotConfigured)	Risque	Nœud	Erreur
État du basculement du stockage - Prise de contrôle(ocumEvtSfoStateTakeover)	Risque	Nœud	Avertissement
État de basculement du stockage - Remise partielle(ocumEvtSfoStatePartialGiveback)	Risque	Nœud	Erreur

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
État du nœud de basculement du stockage hors service(ocumEvtSfoNodeStatusDown)	Risque	Nœud	Erreur
Basculement du stockage impossible(ocumEvtSfoTakeoverNotPossible)	Risque	Nœud	Erreur

Découvrez les événements liés aux services de stockage dans Active IQ Unified Manager

Les événements liés aux services de stockage vous fournissent des informations sur la création et l'abonnement à ces services, vous permettant ainsi de détecter d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Service de stockage créé(Non applicable)	Événement	Service de stockage	Informations
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 du trap)	Niveau d'impact	Type de source	Gravité
Suppression inattendue de la relation gérée SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Risque	Service de stockage	Avertissement
Suppression inattendue du volume membre du service de stockage(ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incident	Service de stockage	Primordial

Découvrez les événements liés aux étagères de stockage dans Active IQ Unified Manager

Les événements du tiroir de stockage vous indiquent si votre tiroir de stockage présente des anomalies afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du trap, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Plage de tension anormale(ocumEvtShelfVoltageAbnormal)	Risque	Tiroir de stockage	Avertissement
Plage de courant anormale(ocumEvtShelfCurrentAbnormal)	Risque	Tiroir de stockage	Avertissement
Température anormale(ocumEvtShelfTemperatureAbnormal)	Risque	Tiroir de stockage	Avertissement

Découvrez les événements liés aux machines virtuelles de stockage dans Active IQ Unified Manager

Les événements de Storage VM (storage virtual machine, également appelée SVM) vous fournissent des informations sur l'état de vos Storage VM (SVM) afin que vous puissiez surveiller d'éventuels problèmes. Les événements sont regroupés par zone d'impact et incluent le nom de l'événement et du trap, 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 du trap)	Niveau d'impact	Type de source	Gravité
Service CIFS de la machine virtuelle de stockage indisponible (ocumEvtVserverCifsServiceStatusDown)	Incident	SVM	Primordial
Service CIFS SVM non configuré(non applicable)	Événement	SVM	Informations
Tentatives de connexion à un partage CIFS inexistant *(nbladeCifsNoPrivShare)	Incident	SVM	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Conflit de noms CIFS NetBIOS *(nbladeCifsNbNameConflict)	Risque	SVM	Erreur
L'opération de copie instantanée CIFS a échoué *(cifsShadowCopyFailure)	Risque	SVM	Erreur
Nombreuses connexions CIFS *(nbladeCifsManyAuths)	Risque	SVM	Erreur
Nombre maximal de connexions CIFS dépassé *(nbladeCifsMaxOpenSameFile)	Risque	SVM	Erreur
Nombre maximal de connexions CIFS par utilisateur dépassé *(nbladeCifsMaxSessPerUsrConn)	Risque	SVM	Erreur
Service FC/FCoE de SVM indisponible(ocumEvtVserverFcServiceStatusDown)	Incident	SVM	Primordial
Service iSCSI SVM indisponible(ocumEvtVserverIscsiServiceStatusDown)	Incident	SVM	Primordial
Service NFS de la machine virtuelle de stockage indisponible(ocumEvtVserverNfsServiceStatusDown)	Incident	SVM	Primordial
service FC/FCoE SVM non configuré (non applicable)	Événement	SVM	Informations
Service iSCSI SVM non configuré(non applicable)	Événement	SVM	Informations
Service NFS SVM non configuré(non applicable)	Événement	SVM	Informations
Machine virtuelle de stockage arrêtée(ocumEvtVserverDown)	Risque	SVM	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Le serveur antivirus est trop occupé pour accepter une nouvelle demande d'analyse *(nbladeVscanConnBackPressure)	Risque	SVM	Erreur
Aucune connexion au serveur AV pour l'analyse antivirus *(nbladeVscanNoScannerConn)	Incident	SVM	Primordial
Aucun serveur antivirus enregistré *(nbladeVscanNoRegdScanner)	Risque	SVM	Erreur
Aucune connexion à un serveur AV réactif *(nbladeVscanConnInactive)	Événement	SVM	Informations
Tentative d'accès non autorisée au serveur AV *(nbladeVscanBadUserPrivAccess)	Risque	SVM	Erreur
Virus détecté par le serveur antivirus *(nbladeVscanVirusDetected)	Risque	SVM	Erreur

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
SVM détecté(Non applicable)	Événement	SVM	Informations
SVM supprimé(Non applicable)	Événement	Cluster	Informations
SVM renommée(Non applicable)	Événement	SVM	Informations

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique d'IOPS SVM dépassé(ocumSvmIopsIncident)	Incident	SVM	Primordial

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil d'alerte IOPS SVM dépassé(ocumSvmIopsWarning)	Risque	SVM	Avertissement
Seuil critique de débit SVM MB/s dépassé(ocumSvmMbpsIncident)	Incident	SVM	Primordial
Seuil d'alerte MB/s de la SVM dépassé(ocumSvmMbpsWarning)	Risque	SVM	Avertissement
Seuil critique de latence SVM dépassé(ocumSvmLatencyIncident)	Incident	SVM	Primordial
Seuil d'alerte de latence SVM dépassé(ocumSvmLatencyWarning)	Risque	SVM	Avertissement

Domaine d'impact : sécurité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Journal d'audit désactivé(ocumVserverAuditLogDisabled)	Risque	SVM	Avertissement
Bannière de connexion désactivée(ocumVserverLoginBannerDisabled)	Risque	SVM	Avertissement
SSH utilise des chiffrements non sécurisés(ocumVserverSSHInsecure)	Risque	SVM	Avertissement
Bannière de connexion modifiée(ocumVserverLoginBannerChanged)	Risque	SVM	Avertissement
La surveillance anti-ransomware de la Storage VM est désactivée (antiRansomwareSvmStateDisabled)	Risque	SVM	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
La surveillance anti-ransomware des VM de stockage est activée (mode d'apprentissage) (antiRansomwareSvmStateDryrun)	Événement	SVM	Informations
Machine virtuelle de stockage adaptée à la surveillance anti-ransomware (mode d'apprentissage) (ocumEvtSvmArwCandidate)	Événement	SVM	Informations

Découvrez les événements liés aux quotas d'utilisateurs et de quota au groupe dans Active IQ Unified Manager

Les événements de quota utilisateur et de quota au groupe vous fournissent des informations sur la capacité du quota utilisateur et du quota au groupe, ainsi que sur les limites de fichiers et de disques, afin de vous permettre de détecter d'éventuels problèmes. Les événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Limite logicielle d'espace disque du quota utilisateur ou de groupe dépassée(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risque	Quota utilisateur ou quota au groupe	Avertissement
Limite stricte d'espace disque de quota pour l'utilisateur ou le groupe atteinte(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incident	Quota utilisateur ou quota au groupe	Primordial
Limite logicielle du nombre de fichiers du quota utilisateur ou de groupe dépassée(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risque	Quota utilisateur ou quota au groupe	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Limite stricte du nombre de fichiers du quota utilisateur ou groupe atteinte(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incident	Quota utilisateur ou quota au groupe	Primordial

Découvrez les événements de volume dans Active IQ Unified Manager

Les événements de volume fournissent des informations sur l'état des volumes, ce qui vous permet de surveiller d'éventuels problèmes. Ces événements sont regroupés par zone d'impact et comprennent le nom de l'événement, le nom du piège, le niveau d'impact, le type de source et la gravité.

Un astérisque (*) identifie les événements EMS qui ont été convertis en événements Unified Manager.

Domaine d'impact : disponibilité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Volume restreint(ocumEvtVolumeRestricted)	Risque	Volume	Avertissement
Volume hors ligne(ocumEvtVolumeOffline)	Incident	Volume	Primordial
Volume partiellement disponible(ocumEvtVolumePartiallyAvailable)	Risque	Volume	Erreur
Volume non monté(non applicable)	Événement	Volume	Informations
Volume monté(non applicable)	Événement	Volume	Informations
Volume remonté(Non applicable)	Événement	Volume	Informations
Chemin de jonction du volume inactif(ocumEvtVolumeJunctionPathInactive)	Risque	Volume	Avertissement
Ajustement automatique du volume activé(Non applicable)	Événement	Volume	Informations
Ajustement automatique du volume désactivé(non applicable)	Événement	Volume	Informations

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Capacité maximale de dimensionnement automatique du volume modifiée (Non applicable)	Événement	Volume	Informations
Taille d'incrément du redimensionnement automatique du volume modifiée (Non applicable)	Événement	Volume	Informations

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Espace du volume à provisionnement fin à risque(ocumThinProvisionVolumeSpaceAtRisk)	Risque	Volume	Avertissement
Erreur d'opération d'efficacité du volume(ocumEvtVolumeEfficiencyOperationError)	Risque	Volume	Erreur
Espace du volume saturé(ocumEvtVolumeFull)	Risque	Volume	Erreur
Espace du volume presque plein (ocumEvtVolumeNearlyFull)	Risque	Volume	Avertissement
Espace logique du volume plein *(volumeLogicalSpaceFull)	Risque	Volume	Erreur
Espace logique du volume presque plein *(volumeLogicalSpaceNearlyFull)	Risque	Volume	Avertissement
Espace logique du volume normal *(volumeLogicalSpaceAllOK)	Événement	Volume	Informations
Espace de réserve Snapshot du volume plein(ocumEvtSnapshotFull)	Risque	Volume	Avertissement

Nom de l’événement (nom du trap)	Niveau d’impact	Type de source	Gravité
Trop de copies Snapshot(ocumEvtSnapshotTooMany)	Risque	Volume	Erreur
Quota qtree de volume suralloué(ocumEvtVolumeQtreeQuotaOvercommitted)	Risque	Volume	Erreur
Quota qtree de volume presque suralloué(ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risque	Volume	Avertissement
Taux de croissance du volume anormal(ocumEvtVolumeGrowthRateAbnormal)	Risque	Volume	Avertissement
Jours avant saturation du volume(ocumEvtVolumeDaysUntilFullSoon)	Risque	Volume	Erreur
Garantie d’espace du volume désactivée(non applicable)	Événement	Volume	Informations
Garantie d’espace du volume activée(non applicable)	Événement	Volume	Informations
Garantie d’espace du volume modifiée (non applicable)	Événement	Volume	Informations
Réserve de snapshots du volume : jours avant saturation (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risque	Volume	Erreur
FlexGroup Les constituants ont des problèmes d’espace *(flexGroupConstituentsHaveSpaceIssues)	Risque	Volume	Erreur
FlexGroup État de l’espace des constituants Tous OK *(flexGroupConstituentsSpaceStatusAllOK)	Événement	Volume	Informations

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
FlexGroup Les constituants présentent des problèmes d'inodes *(flexGroupConstituentsHaveInodesIssues)	Risque	Volume	Erreur
FlexGroup Statut de tous les inodes des constituants : OK *(flexGroupConstituentsInodesStatusAllOK)	Événement	Volume	Informations
Échec de l'AutoSize du volume WAFL *(waflVolAutoSizeFail)	Risque	Volume	Erreur
Volume WAFL AutoSize terminé *(waflVolAutoSizeDone)	Événement	Volume	Informations
FlexGroup Le volume est utilisé à plus de 80 %*	Incident	Volume	Erreur
FlexGroup Le volume est utilisé à plus de 90 %*	Incident	Volume	Primordial
Anomalie d'efficacité du stockage du volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risque	Volume	Avertissement
Réserve Snapshot de volume sous-utilisée (volumeSnaphotReserveUnderutilizedWarning)	Événement	Volume	Avertissement
Réserve Snapshot de volume sous-utilisée (volumeSnaphotReserveUnderutilizedCleared)	Événement	Volume	Avertissement

Domaine d'impact : configuration

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Volume renommé(Non applicable)	Événement	Volume	Informations
Volume découvert(Non applicable)	Événement	Volume	Informations
Volume supprimé(non applicable)	Événement	Volume	Informations

Domaine d'impact : performance

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil d'alerte QoS Volume Max IOPS dépassé(ocumQosVolumeMaxIopsWarning)	Risque	Volume	Avertissement
Seuil d'alerte QoS Volume Max MB/s dépassé(ocumQosVolumeMaxMbpsWarning)	Risque	Volume	Avertissement
Seuil d'alerte QoS Volume Max IOPS/TB dépassé(ocumQosVolumeMaxIopsPerTbWarning)	Risque	Volume	Avertissement
Le seuil de latence du volume de charge de travail a été dépassé tel que défini par la politique de niveau de service de performance(ocumConformanceLatencyWarning)	Risque	Volume	Avertissement
Seuil critique d'IOPS du volume dépassé(ocumVolumeIopsIncident)	Incident	Volume	Primordial
Seuil d'alerte IOPS du volume dépassé (ocumVolumeIopsWarning)	Risque	Volume	Avertissement
Débit MB/s seuil critique dépassé(ocumVolumeMbpsIncident)	Incident	Volume	Primordial
Seuil d'alerte du débit en MB/s dépassé(ocumVolumeMbpsWarning)	Risque	Volume	Avertissement
Seuil critique de latence du volume dépassé(ocumVolumeLatencyIncident)	Incident	Volume	Primordial
Seuil d'alerte de latence du volume dépassé(ocumVolumeLatencyWarning)	Risque	Volume	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique du taux d'échec du cache du volume dépassé(ocumVolumeCacheMissRatioIncident)	Incident	Volume	Primordial
Seuil d'alerte de taux d'échec du cache de volume dépassé(ocumVolumeCacheMissRatioWarning)	Risque	Volume	Avertissement
Seuil critique de latence et d'IOPS du volume dépassé(ocumVolumeLatencyIopsIncident)	Incident	Volume	Primordial
Le seuil d'alerte de latence du volume et d'IOPS a été dépassé(ocumVolumeLatencyIopsWarning)	Risque	Volume	Avertissement
Latence du volume et seuil critique en MB/s dépassés(ocumVolumeLatencyMbpsIncident)	Incident	Volume	Primordial
Seuil d'avertissement de latence du volume et de MB/s dépassé(ocumVolumeLatencyMbpsWarning)	Risque	Volume	Avertissement
Latence du volume et capacité de performance utilisée de l'agrégat : seuil critique dépassé(ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incident	Volume	Primordial
Latence du volume et capacité de performance de l'agrégat utilisée : seuil d'alerte dépassé(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risque	Volume	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Le seuil critique de latence du volume et d'utilisation de l'agrégat est dépassé(ocumVolumeLatencyAggregateUtilizationIncident)	Incident	Volume	Primordial
Seuil d'alerte de latence du volume et d'utilisation de l'agrégat dépassé(ocumVolumeLatencyAggregateUtilizationWarning)	Risque	Volume	Avertissement
Latence du volume et capacité de performance du nœud utilisées : seuil critique dépassé (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incident	Volume	Primordial
Latence du volume et capacité de performance du nœud utilisée : seuil d'avertissement dépassé (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risque	Volume	Avertissement
Latence du volume et capacité de performance du nœud utilisée - Seuil critique de prise de contrôle dépassé(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incident	Volume	Primordial
Latence du volume et capacité de performance des nœuds utilisée - Seuil d'alerte de prise de contrôle dépassé(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risque	Volume	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Seuil critique de latence du volume et d'utilisation du nœud dépassé(ocumVolumeLatencyNodeUtilizationIncident)	Incident	Volume	Primordial
Seuil d'alerte de latence du volume et d'utilisation du nœud dépassé(ocumVolumeLatencyNodeUtilizationWarning)	Risque	Volume	Avertissement

Domaine d'impact : sécurité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
La surveillance anti-ransomware du volume est activée (mode actif) (antiRansomwareVolumeStateEnabled)	Événement	Volume	Informations
La surveillance anti-ransomware du volume est désactivée (antiRansomwareVolumeStateDisabled)	Risque	Volume	Avertissement
La surveillance anti-ransomware du volume est activée (mode d'apprentissage) (antiRansomwareVolumeStateDryrun)	Événement	Volume	Informations
La surveillance anti-ransomware du volume est suspendue (mode d'apprentissage) (antiRansomwareVolumeStateDryrunPaused)	Risque	Volume	Avertissement
La surveillance anti-ransomware du volume est suspendue (mode actif) (antiRansomwareVolumeStateEnablePaused)	Risque	Volume	Avertissement

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
La surveillance anti-ransomware du volume est en cours de désactivation (antiRansomwareVolumeStateDisableInProgress)	Risque	Volume	Avertissement
Activité de ransomware détectée (callHomeRansomwareActivitySeen)	Incident	Volume	Primordial
Volume adapté à la surveillance anti-ransomware (mode d'apprentissage) (ocumEvtVolumeArwCandidate)	Événement	Volume	Informations
Volume adapté à la surveillance anti-ransomware (mode actif) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risque	Volume	Avertissement
Le volume présente des alertes anti-ransomware bruyantes (antiRansomwareFeatureNoisyVolume)	Risque	Volume	Avertissement

Domaine d'impact : protection des données

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
Le volume ne dispose pas d'une protection locale Snapshot suffisante (volumeLacksLocalProtectionWarning)	Risque	Volume	Avertissement
Le volume ne dispose pas d'une protection locale suffisante des snapshots (volumeLacksLocalProtectionCleared)	Risque	Volume	Avertissement

Découvrez les événements liés à l'état des transferts de volume dans Active IQ Unified Manager

Les événements d'état du déplacement de volume vous informent de l'état de votre déplacement de volume afin que vous puissiez surveiller d'éventuels problèmes. Les

événements sont regroupés par zone d'impact et comprennent le nom de l'événement et du piège, le niveau d'impact, le type de source et la gravité.

Domaine d'impact : capacité

Nom de l'événement (nom du trap)	Niveau d'impact	Type de source	Gravité
État du déplacement de volume : En cours(Non applicable)	Événement	Volume	Informations
État du déplacement de volume - Échec(ocumEvtVolumeMoveFailed)	Risque	Volume	Erreur
État du déplacement de volume : Terminé(Non applicable)	Événement	Volume	Informations
Déplacement de volume - Basculement différé(ocumEvtVolumeMoveCutoverDeferred)	Risque	Volume	Avertissement

Description des fenêtres d'événements et des boîtes de dialogue

Découvrez la page Notifications dans Active IQ Unified Manager

Vous pouvez configurer le serveur Unified Manager pour qu'il envoie des notifications lorsqu'un événement est généré ou lorsqu'il est attribué à un utilisateur. Vous pouvez également configurer les mécanismes de notification. Par exemple, les notifications peuvent être envoyées sous forme d'e-mails ou de traps SNMP.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Messagerie électronique

Cette section vous permet de configurer les paramètres de messagerie suivants pour les notifications d'alerte :

- **Adresse de l'expéditeur**

  Indique l'adresse e-mail à partir de laquelle la notification d'alerte est envoyée. Cette valeur est également utilisée comme adresse de l'expéditeur pour un rapport lorsqu'il est partagé. Si l'adresse de l'expéditeur est préremplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la remplacer par une adresse e-mail réelle et valide pour vous assurer que toutes les notifications par e-mail sont remises correctement.

Serveur SMTP

Cette zone vous permet de configurer les paramètres suivants du serveur SMTP :

- **Nom de l'hôte ou adresse IP**

Spécifie le nom de l'hôte de votre serveur hôte SMTP, qui est utilisé pour envoyer la notification d'alerte aux destinataires spécifiés.

- **Nom d'utilisateur**

  Spécifie le nom d'utilisateur SMTP. Le nom d'utilisateur SMTP est requis uniquement lorsque SMTPAUTH est activé sur le serveur SMTP.

- **Mot de passe**

  Spécifie le mot de passe SMTP. Le nom d'utilisateur SMTP est requis uniquement lorsque SMTPAUTH est activé sur le serveur SMTP.

- **Port**

  Spécifie le port utilisé par le serveur hôte SMTP pour envoyer les notifications d'alerte.

  La valeur par défaut est 25.

- **Utilisez START/TLS**

  Cocher cette case permet une communication sécurisée entre le serveur SMTP et le serveur de gestion grâce aux protocoles TLS/SSL (également connus sous les noms de start_tls et StartTLS).

- **Utilisez SSL**

  Cocher cette case permet une communication sécurisée entre le serveur SMTP et le serveur de gestion grâce au protocole SSL.

SNMP

Cette zone vous permet de configurer les paramètres de trap SNMP suivants:

- **Version**

  Indique la version SNMP que vous souhaitez utiliser en fonction du type de sécurité requis. Les options incluent la version 1, la version 3, la version 3 avec authentification et la version 3 avec authentification et chiffrement. La valeur par défaut est la version 1.

- **Hôte de destination du trap**

  Spécifie le nom de l'hôte ou l'adresse IP (IPv4 ou IPv6) qui reçoit les traps SNMP envoyés par le serveur de gestion. Pour spécifier plusieurs destinations de traps, 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 trap sortant**

  Spécifie le port par lequel le serveur SNMP reçoit les traps envoyés par le serveur de gestion.

  La valeur par défaut est 162.

- **Communauté**

La chaîne de communauté pour accéder à l'hôte.

- **Identifiant du moteur**

  Spécifie l'identifiant unique de l'agent SNMP et est généré automatiquement 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 pour authentifier 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 chiffrer 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 chiffrement.

- **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 chiffrement.

Pour plus d'informations sur les objets et les traps SNMP, vous pouvez télécharger le "MIB d'Active IQ Unified Manager" sur le site de support NetApp.

Découvrez la page d'inventaire de gestion des événements dans Active IQ Unified Manager

La page d'inventaire de la gestion des événements vous permet de consulter la liste des événements en cours et leurs propriétés. Vous pouvez effectuer des tâches telles qu'accuser réception, résoudre et attribuer des événements. Vous pouvez également configurer une alerte pour certains événements.

Les informations de cette page sont actualisées automatiquement toutes les 5 minutes afin que les nouveaux événements les plus récents s'affichent.

Composants du filtre

Vous pouvez 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 sélectionner une option dans une liste prédéfinie de filtres.

  Cela inclut des éléments tels que tous les événements actifs (nouveaux et acquittés), les événements de performance actifs, les événements qui me sont attribués (l'utilisateur connecté) et tous les événements générés pendant toutes les fenêtres de maintenance.

- Volet de recherche pour affiner la liste des événements en saisissant des termes complets ou partiels.
- Le bouton Filtre ouvre le volet Filtres afin que vous puissiez sélectionner parmi tous les champs et attributs de champ disponibles pour affiner la liste des événements.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Attribuer à**

  Permet de sélectionner l'utilisateur auquel l'événement est attribué. Lorsque vous attribuez un événement à un utilisateur, son nom et l'heure à laquelle vous avez attribué 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 le propriétaire », qui vous permet d'attribuer ou de réattribuer l'événement à d'autres utilisateurs. Vous pouvez également annuler l'attribution d'événements en laissant le champ « Propriétaire » vide.

- **Acquitter**

  Reconnaît les événements sélectionnés.

  Lorsque vous accusez réception d'un événement, votre nom d'utilisateur et l'heure à laquelle vous avez accusé réception de l'événement sont ajoutés à la liste des événements pour les événements sélectionnés. Lorsque vous accusez réception d'un événement, vous êtes responsable de sa gestion.

  Vous ne pouvez pas acquitter les événements d'information.

- **Marquer comme résolu**

  Permet de modifier 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 une mesure corrective pour l'événement, vous devez marquer l'événement comme résolu.

- **Ajouter une alte**

  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 actuelle vers un fichier de valeurs séparées par des virgules (.csv) ou un document PDF.

- **Afficher/Masquer le sélecteur de colonnes**

  Permet de choisir les colonnes affichées sur la page et de sélectionner l'ordre dans lequel elles sont affichées.

Liste des événements

Affiche les détails de tous les événements classés par heure de déclenchement.

Par défaut, la vue « Tous les événements actifs » affiche les événements nouveaux et acquittés des sept derniers jours ayant un niveau d'impact « Incident » ou « Risque ».

- **Heure de déclenchement**

  L'heure à laquelle l'événement a été généré.

- **Gravité**

  La gravité de l'événement : Critique (), Erreur (), Avertissement () et Information ().

- **État**

  État de l'événement : Nouveau, acquitté, résolu ou obsolète.

- **Niveau d'impact**

  Niveau d'impact de l'événement : Incident, Risque, Événement ou Mise à niveau.

- **Zone d'impact**

  Le domaine d'impact de l'événement : disponibilité, capacité, performance, protection, configuration ou sécurité.

- **Nom**

  Nom de l'événement. Vous pouvez sélectionner ce nom pour afficher la page Détails de l'événement correspondant.

- **Source**

  Le nom de l'objet sur lequel l'événement s'est produit. Vous pouvez sélectionner ce nom pour afficher la page de détails relative à l'état ou aux performances de cet objet.

  En cas de violation d'une politique QoS partagée, seul l'objet de workload qui consomme le plus d'IOPS ou de Mo/s est affiché dans ce champ. Les autres workloads qui utilisent cette politique sont affichés sur la page Détails de l'événement.

- **Type de source**

  Le type d'objet (par exemple, Storage VM, Volume ou Qtree) auquel l'événement est associé.

- **Attribué à**

Le nom de l’utilisateur auquel l’événement est attribué.

- **Origine de l’événement**

  Que l’événement provienne de « Active IQ Portal » ou directement de « Active IQ Unified Manager ».

- **Nom de l’annotation**

  Le nom de l’annotation attribuée à l’objet de stockage.

- **Remarques**

  Le nombre de notes ajoutées pour un événement.

- **Jours restants**

  Le nombre de jours écoulés depuis la génération initiale de l’événement.

- **Temps attribué**

  Le temps écoulé depuis l’attribution de l’événement à un utilisateur. Si le temps écoulé dépasse une semaine, l’horodatage de l’attribution de l’événement à un utilisateur s’affiche.

- **Reconnu par**

  Nom de l’utilisateur ayant accusé réception de l’événement. Ce champ est vide si l’événement n’a pas été acquitté.

- **Heure d’accusé de réception**

  Le temps écoulé depuis l’acquittement de l’événement. Si le temps écoulé dépasse une semaine, l’horodatage auquel l’événement a été acquitté s’affiche.

- **Résolu par**

  Nom de l’utilisateur ayant résolu l’événement. Ce champ est vide si l’événement n’a pas été résolu.

- **Heure de résolution**

  Le temps écoulé depuis la résolution de l’événement. Si ce temps dépasse une semaine, l’horodatage de la résolution de l’événement est affiché.

- **Temps obsolète**

  L’heure à laquelle l’état de l’événement est devenu obsolète.

Page de détails de l’événement

Découvrez la page de détails de l’événement dans Active IQ Unified Manager

Sur la page de détails de l’événement, vous pouvez consulter les détails d’un événement sélectionné, tels que sa gravité, son niveau d’impact, sa zone d’impact et sa source d’événement. Vous pouvez également consulter des informations complémentaires sur les solutions possibles pour résoudre le problème.

- **Nom de l’événement**

  Le nom de l’événement et l’heure à laquelle il a été vu pour la dernière fois.

  Pour les événements non liés aux performances, tant que l’événement est à l’état Nouveau ou Reconnu, les informations de dernière observation ne sont pas disponibles et sont donc masquées.

- **Description de l’événement**

  Une brève description de l’événement.

  Dans certains cas une raison du déclenchement de l’événement est indiquée dans la description de l’événement.

- **Composant en conflit**

  Pour les événements de performance dynamiques, cette section affiche des icônes représentant les composants logiques et physiques du cluster. Si un composant est en situation de contention, son icône est entourée et surlignée en rouge.

  Consultez la section *Composants du cluster et raisons pour lesquelles ils peuvent être en conflit* pour obtenir une description des composants affichés ici.

Les sections Informations sur l’événement, Diagnostic du système et Actions suggérées sont décrites dans d’autres rubriques.

Boutons de commande

Les boutons de commande vous permettent d’effectuer les tâches suivantes :

- **Icône Notes**

  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

- **M’attribuer**

  Vous assigne l’événement.

- **Attribuer à d’autres**

  Ouvre la boîte de dialogue « Attribuer le propriétaire », qui vous permet d’attribuer ou de réattribuer l’événement à d’autres utilisateurs.

  Lorsque vous attribuez un événement à un utilisateur, le nom de l’utilisateur et l’heure à laquelle l’événement a été attribué sont ajoutés dans la liste des événements pour les événements sélectionnés.

  Vous pouvez également retirer l’attribution d’événements en laissant le champ de propriétaire vide.

- **Acquitter**

  Acquitte les événements sélectionnés afin que vous ne continuiez pas à recevoir des notifications d’alerte répétées.

Lorsque vous accusez réception d'un événement, votre nom d'utilisateur et l'heure à laquelle vous avez accusé réception de l'événement sont ajoutés à la liste des événements (Accusé de réception par) pour les événements sélectionnés. Lorsque vous accusez réception d'un événement, vous assumez la responsabilité de sa gestion.

- **Marquer comme résolu**

  Permet de modifier l'état de l'événement en Résolu.

  Lorsque vous résolvez un événement, votre nom d'utilisateur et l'heure de résolution sont ajoutés à la liste des événements (Résolu par) pour les événements sélectionnés. Une fois l'action corrective effectuée, vous devez marquer l'événement comme résolu.

- **Ajouter une alte**

  Affiche la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter une alerte pour l'événement sélectionné.

Découvrez la section Informations sur l'événement dans Active IQ Unified Manager

Vous utilisez la section Informations sur l'événement sur la page Détails de l'événement pour consulter les détails concernant un événement sélectionné, tels que la gravité de l'événement, son niveau d'impact, sa zone d'impact et sa source.

Les champs qui ne s'appliquent pas au type d'événement sont masqués. Vous pouvez consulter les détails suivants de l'événement :

- **Heure de déclenchement de l'événement**

  L'heure à laquelle l'événement a été généré.

- **État**

  État de l'événement : Nouveau, acquitté, résolu ou obsolète.

- **Cause obsolète**

  Les actions qui ont rendu l'événement obsolète, par exemple, le problème a été résolu.

- **Durée de l'événement**

  Pour les événements actifs (nouveaux et reconnus), il s'agit du délai entre leur détection et leur dernière analyse. Pour les événements obsolètes, il s'agit du délai entre leur détection et leur résolution.

  Ce champ s'affiche pour tous les événements de performance, et pour les autres types d'événements uniquement après leur résolution ou leur obsolescence.

- **Vu pour la dernière fois**

  La date et l'heure auxquelles l'événement a été vu pour la dernière fois comme étant actif.

  Pour les événements de performance, cette valeur peut être plus récente que l'heure de déclenchement de l'événement, car ce champ est mis à jour après chaque nouvelle collecte de données de performance tant que l'événement est actif. Pour les autres types d'événements, lorsqu'ils sont à l'état « Nouveau » ou « Accusé de réception », ce contenu n'est pas mis à jour et le champ est donc masqué.

- **Gravité**

  La gravité de l'événement : Critique (), Erreur (), Avertissement () et Information ().

- **Niveau d'impact**

  Niveau d'impact de l'événement : Incident, Risque, Événement ou Mise à niveau.

- **Zone d'impact**

  Le domaine d'impact de l'événement : disponibilité, capacité, performance, protection, configuration ou sécurité.

- **Source**

  Le nom de l'objet sur lequel l'événement s'est produit.

  Lorsque vous consultez les détails d'un événement de stratégie QoS partagée, jusqu'à trois des objets workload qui consomment le plus d'IOPS ou de MBps sont répertoriés dans ce champ.

  Vous pouvez cliquer sur le lien du nom de la source pour afficher la page de détails sur l'état ou les performances de cet objet.

- **Annotations de la source**

  Affiche le nom et la valeur de l'annotation pour l'objet auquel l'événement est associé.

  Ce champ s'affiche uniquement pour les événements liés à l'état de santé des clusters, des SVM et des volumes.

- **Groupes sources**

  Affiche les noms de tous les groupes auxquels appartient l'objet concerné.

  Ce champ s'affiche uniquement pour les événements liés à l'état de santé des clusters, des SVM et des volumes.

- **Type de source**

  Le type d'objet (par exemple, SVM, Volume ou Qtree) auquel l'événement est associé.

- **Sur le cluster**

  Le nom du cluster sur lequel l'événement s'est produit.

  Vous pouvez cliquer sur le lien du nom du cluster pour afficher la page de détails sur l'état ou les performances de ce cluster.

- **Nombre d'objets affectés**

  Le nombre d'objets affectés par l'événement.

  Vous pouvez cliquer sur le lien de l'objet pour afficher la page d'inventaire contenant les objets actuellement affectés par cet événement.

  Ce champ s'affiche uniquement pour les événements de performance.

- **Volumes concernés**

  Le nombre de volumes concernés par cet événement.

  Ce champ s'affiche uniquement pour les événements de performance sur les nœuds ou les agrégats.

- **Politique déclenchée**

  Le nom de la politique de seuil qui a déclenché l'événement.

  Vous pouvez survoler le nom de la stratégie avec le curseur pour afficher les détails de la stratégie de seuil. Pour les stratégies QoS adaptatives, la stratégie définie, la taille des blocs et le type d'allocation (espace alloué ou espace utilisé) sont également affichés.

  Ce champ s'affiche uniquement pour les événements de performance.

- **Identifiant de la règle**

  Pour les événements de la plateforme Active IQ, il s'agit du numéro de la règle qui a été déclenchée pour générer l'événement.

- **Reconnu par**

  Le nom de la personne qui a pris acte de l'événement et l'heure à laquelle l'événement a été confirmé.

- **Résolu par**

  Le nom de la personne qui a résolu l'événement et l'heure à laquelle l'événement a été résolu.

- **Attribué à**

  Le nom de la personne chargée de travailler sur l'événement.

- **Paramètres d'alerte**

  Les informations suivantes concernant les alertes sont affichées :

  - S'il n'existe aucune alerte associée à l'événement sélectionné, un lien **Ajouter une alerte** s'affiche.

    Vous pouvez ouvrir la boîte de dialogue Ajouter une alerte en cliquant sur le lien.

  - Si une alte est associée à l'événement sélectionné, son nom s'affiche.

    Vous pouvez ouvrir la boîte de dialogue Modifier l'alerte en cliquant sur le lien.

  - S'il existe plusieurs alertes associées à l'événement sélectionné, le nombre d'alertes s'affiche.

    Vous pouvez ouvrir la page de configuration des alertes en cliquant sur le lien pour consulter plus de détails sur ces alertes.

  Les alertes désactivées ne sont pas affichées.

- **Dernière notification envoyée**

  Date et heure d'envoi de la dernière notification d'alerte.

- **Envoyer avant**

  Le mécanisme utilisé pour envoyer la notification d'alerte : courriel ou trap SNMP.

- **Exécution précédente du script**

  Le nom du script qui a été exécuté lors de la génération de l'alerte.

Découvrez les actions suggérées dans Active IQ Unified Manager

La section « Actions suggérées » de la page Détails de l'événement présente les causes possibles de l'événement et suggère quelques actions afin que vous puissiez essayer de résoudre l'événement vous-même. Les actions suggérées sont personnalisées en fonction du type d'événement ou du type de seuil qui a été dépassé.

Cette zone n'est affichée que pour certains types d'événements.

Dans certains cas, des liens **Aide** sont disponibles sur la page et renvoient à des informations complémentaires pour de nombreuses actions suggérées, notamment des instructions pour effectuer une action spécifique. Certaines de ces actions peuvent nécessiter l'utilisation de Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, de commandes ONTAP CLI ou d'une combinaison de ces outils.

Les actions suggérées ici ne constituent qu'une orientation pour la résolution de cet événement. La solution que vous entreprendrez devra être adaptée à votre environnement.

Pour analyser l'objet et l'événement plus en détail, cliquez sur le bouton **Analyser la charge de travail** pour afficher la page d'analyse de la charge de travail.

Unified Manager peut diagnostiquer certains événements en détail et proposer une solution unique. Le cas échéant, ces solutions sont affichées avec un bouton **Fix It**. Cliquez sur ce bouton pour qu'Unified Manager résolve le problème à l'origine de l'événement.

Pour les événements de la plateforme Active IQ, cette section peut contenir, le cas échéant, 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 s'ouvre localement ; ce PDF fait partie du fichier de règles que vous téléchargez manuellement sur l'instance Unified Manager.

Découvrez le diagnostic système dans Active IQ Unified Manager

La section « Diagnostic système » de la page « Détails de l'événement » fournit des informations qui peuvent vous aider à diagnostiquer les problèmes susceptibles d'être à l'origine de l'événement.

Cette zone n'est affichée que pour certains événements.

Certains événements de performance fournissent des graphiques pertinents pour l'événement particulier qui a été déclenché. En général, cela comprend un graphique des IOPS ou des MBps et un graphique de latence pour les dix jours précédents. Lorsqu'ils sont présentés de cette manière, vous pouvez voir quels composants de stockage affectent le plus la latence, ou sont affectés par la latence, lorsque l'événement est actif.

Pour les événements de performance dynamiques, les graphiques suivants s'affichent :

- Latence du workload - Affiche l'historique de la latence des principaux workloads victim, bully ou shark au niveau du composant en conflit.

- Activité du workload - Affiche des détails sur l'utilisation du workload du composant de cluster en contention.
- Activité des ressources - Afficher les statistiques de performance historiques du composant du cluster en contention.

D'autres graphiques s'affichent lorsque certains composants du cluster sont en situation de contention.

D'autres événements fournissent une brève description du type d'analyse effectuée par le système sur l'objet de stockage. Dans certains cas, une ou plusieurs lignes s'affichent, une pour chaque composant analysé, pour les politiques de performances définies par le système qui analysent plusieurs compteurs de performances. Dans ce scénario, une icône verte ou rouge apparaît à côté du diagnostic pour indiquer si un problème a été détecté, ou non, dans ce diagnostic particulier.

Découvrez la page de configuration des événements dans Active IQ Unified Manager

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 activer ou désactiver des événements globalement.

Vous pouvez accéder à cette page uniquement si vous avez le rôle Application Administrator ou Storage Administrator.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour les événements sélectionnés :

- **Désactiver**

  Ouvre la boîte de dialogue Désactiver les événements, que vous pouvez utiliser pour désactiver des événements.

- **Activer**

  Active les événements sélectionnés que vous aviez choisis de désactiver précédemment.

- **Règles de téléchargement**

  Ouvre la boîte de dialogue « Charger les règles », qui permet aux sites sans accès réseau externe de charger manuellement le fichier de règles Active IQ dans Unified Manager. Les règles sont appliquées aux messages AutoSupport du cluster afin de générer des événements relatifs à la configuration système, au câblage, à la bonne pratique et à la disponibilité, telles que définies par la plateforme Active IQ.

- **Abonnez-vous aux événements EMS**

  Ouvre la boîte de dialogue « S'abonner aux événements EMS », qui vous permet de vous abonner pour recevoir des événements spécifiques du système de gestion des événements (EMS) provenant des clusters que vous surveillez. L'EMS collecte des informations sur les événements qui se produisent sur le cluster. Lorsqu'une notification est reçue pour un événement EMS auquel vous êtes abonné, un événement Unified Manager est généré avec le niveau de gravité approprié.

Vue de liste

La vue Liste affiche (sous forme de tableau) les informations relatives aux événements désactivés. Vous

pouvez utiliser les filtres de colonnes pour personnaliser les données affichées.

- **Événement**

  Affiche le nom de l'événement désactivé.

- **Gravité**

  Affiche la gravité de l'événement. La gravité peut être Critique, Erreur, Avertissement ou Information.

- **Type de source**

  Affiche le type de source pour lequel l'événement est généré.

Désactivez la boîte de dialogue Événements dans Active IQ Unified Manager

La boîte de dialogue « Désactiver les événements » affiche la liste des types d'événements pour lesquels vous pouvez désactiver des événements. Vous pouvez désactiver des événements pour un type d'événement donné en fonction d'un niveau de gravité particulier ou pour un ensemble d'événements.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Zone Propriétés de l'événement

La zone Propriétés de l'événement spécifie les propriétés de l'événement suivantes :

- **Gravité de l'événement**

  Permet de sélectionner les événements en fonction de leur niveau 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 associés**

  Affiche la liste des événements correspondant au type de gravité de l'événement et à la chaîne de texte que vous spécifiez.

- **Désactiver les événements**

  Affiche la liste des événements que vous avez sélectionnés pour la désactivation.

  La gravité de l'événement est également affichée avec le nom de l'événement.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour les événements sélectionnés :

- **Enregistrer et fermer**

  Désactive le type d'événement et ferme la boîte de dialogue.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue.

Gérer les alertes

Découvrez les alertes dans Active IQ Unified Manager

Bien que les événements se produisent en continu, Unified Manager génère une alerte uniquement lorsqu'un événement répond à des critères de filtrage 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 qui s'exécute lorsqu'une alerte est déclenchée.

Les critères de filtrage incluent la classe d'objet, le nom ou la gravité de l'événement.

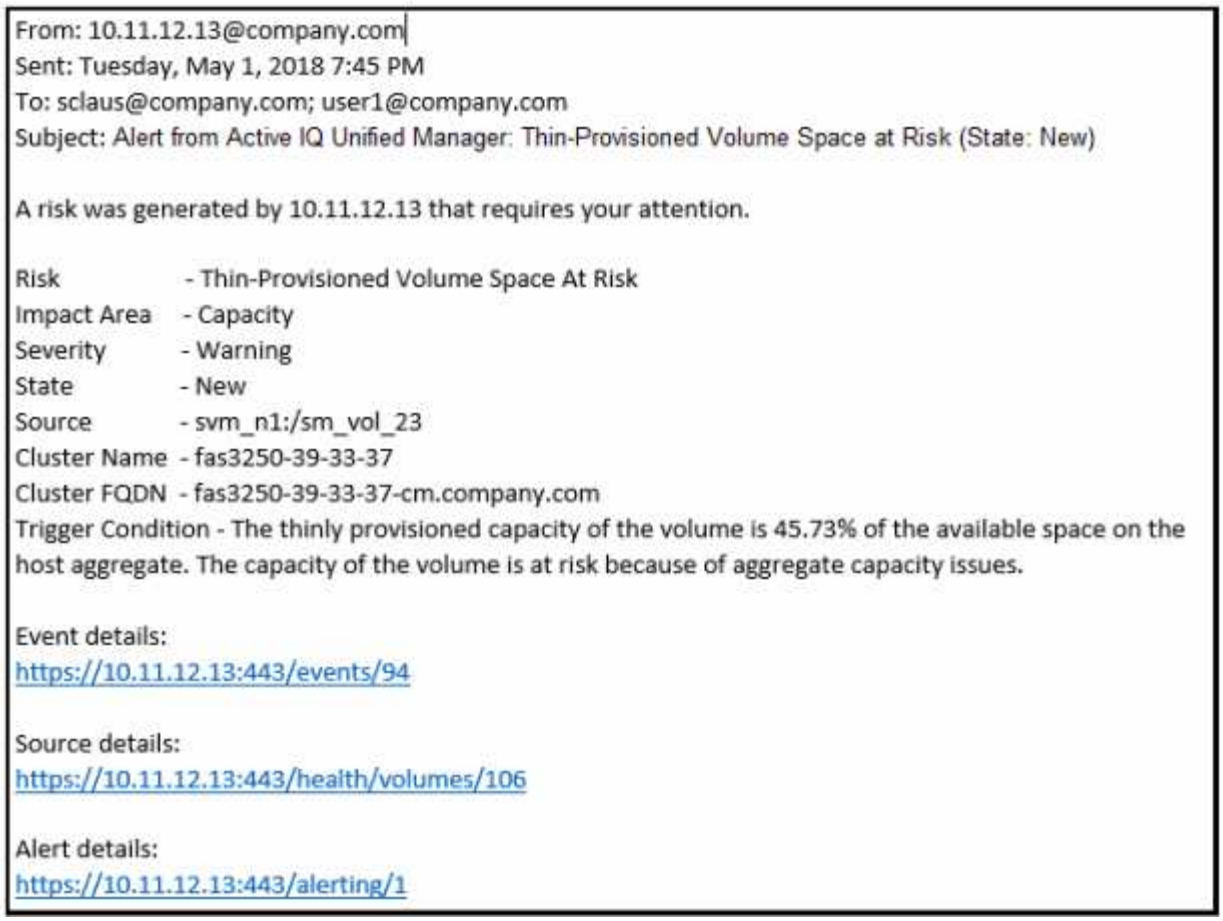
Informations contenues dans un e-mail d'alerte Active IQ Unified Manager

Les alertes par e-mail d'Unified Manager indiquent le type d'événement, sa gravité, le nom de la politique ou du seuil enfreint, ainsi qu'une description de l'événement. Le message électronique fournit également un lien hypertexte pour chaque événement qui vous permet d'afficher la page de détails de l'événement dans l'interface utilisateur.

Tous les utilisateurs qui se sont abonnés pour recevoir des alertes reçoivent des courriels d'alerte.

Si une valeur de compteur de performances ou de capacité subit une variation importante pendant une période de collecte, cela peut déclencher simultanément un événement critique et un événement d'avertissement pour une 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 de dépassement des seuils d'avertissement et critiques.

Un exemple d'e-mail d'alerte est présenté ci-dessous :



Ajouter des alertes

Ajouter des alertes dans Active IQ Unified Manager

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

Avant de commencer

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

Vous pouvez créer une alerte directement depuis la page de détails de l'événement après avoir reçu un événement, en plus de la possibilité de créer une alerte depuis la page de configuration des alertes, comme décrit ici.

Étapes

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

   Vous pouvez définir un filtre en saisissant une chaîne de caractères dans le champ « Le nom contient » afin de sélectionner un groupe de ressources. En fonction de la chaîne de caractères que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtrage. La chaîne de caractères que vous spécifiez est sensible à la casse.

   Si une ressource correspond à la fois aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion prévaut sur la règle d'inclusion, et aucune alerte n'est générée pour les événements liés à la ressource exclue.

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

   Pour sélectionner plusieurs événements, maintenez la touche Ctrl enfoncée pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions**, puis sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence des notifications, indiquez si un trap SNMP doit être envoyé au récepteur de traps, et attribuez un script à exécuter lorsqu'une alerte est générée.

   Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour la modifier, le champ Nom apparaît vide, car l'adresse e-mail modifiée n'est plus associée à l'utilisateur précédemment sélectionné. De même, si vous modifiez l'adresse e-mail de l'utilisateur sélectionné depuis la page Users, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

   Vous pouvez également choisir d'informer les utilisateurs via des traps SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

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

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

Dans la boîte de dialogue Ajouter une alerte, procédez comme suit :

1. Cliquez sur **Nom**, et saisissez **`HealthTest`** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources**, puis dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.

a. Saisissez **`abc`** dans le champ **Name contains** pour afficher les volumes dont le nom contient "abc".

b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles et déplacez-le vers la zone Ressources sélectionnées.

c. Cliquez sur **Exclure**, saisissez **`xyz`** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.

3. Cliquez sur **Événements**, puis sélectionnez **Critique** dans le champ Gravité de l'événement.
4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants, et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions**, et saisissez **`sample@domain.com`** dans le champ Alerter ces utilisateurs.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour notifier l'utilisateur toutes les 15 minutes.

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

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

Instructions pour l'ajout d'alertes dans Active IQ Unified Manager

Vous pouvez ajouter des alertes en fonction d'une ressource, telle qu'un cluster, un nœud, un agrégat ou un volume, et d'événements d'un type de gravité particulier. Comme bonne pratique, vous pouvez ajouter une alerte pour chacun de vos objets critiques après avoir ajouté le cluster auquel l'objet appartient.

Vous pouvez utiliser les directives et considérations suivantes pour créer des alertes et gérer efficacement vos systèmes :

- Description de l'alerte

  Vous devriez fournir une description de l'alerte afin de vous aider à suivre efficacement vos alertes.

- Ressources

  Vous devez déterminer quelle ressource physique ou logique nécessite une alerte. Vous pouvez inclure ou exclure des ressources selon vos besoins. Par exemple, si vous souhaitez surveiller de près vos agrégats en configurant une alerte, vous devez sélectionner les agrégats concernés 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 au sein de ce cluster. Par exemple, si vous créez une alerte pour tous les événements critiques de tous les clusters, vous ne recevrez d'alertes que pour les événements critiques du cluster. Vous ne recevrez pas d'alertes pour les événements critiques sur les nœuds, les agrégats, etc.

- Gravité de l'événement

  Vous devez décider si un événement d'un niveau de gravité spécifié (Critique, Erreur, Avertissement) doit déclencher l'alerte et, le cas échéant, quel niveau de gravité.

- Événements sélectionnés

  Si vous ajoutez une alte basée sur le type d'événement généré, vous devez déterminer quels événements nécessitent une alerte.

  Si vous sélectionnez un niveau de gravité d'événement, mais que vous ne sélectionnez aucun événement individuel (si vous laissez la colonne « Événements sélectionnés » vide), vous recevrez des alertes pour tous les événements de la catégorie.

- Actions

  Vous devez fournir les noms d'utilisateur et les adresses électroniques 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 de notification

  Vous pouvez configurer une alerte pour envoyer de façon répétée une notification aux destinataires pendant une durée spécifiée. Vous devez déterminer à partir de quand la notification d'événement est active pour l'alerte. Si vous souhaitez que la notification d'événement soit répétée jusqu'à ce que l'événement soit reconnu, vous devez déterminer à quelle fréquence vous voulez 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.

Ajoutez des alertes pour les événements de performance dans Active IQ Unified Manager

Vous pouvez configurer des alertes pour chaque événement de performance, comme pour tout autre événement reçu par Unified Manager. De plus, si vous souhaitez traiter tous les événements de performance de la même manière et envoyer un e-mail à la même personne, vous pouvez créer une alerte unique pour être notifié lorsque des événements de performance critiques ou d'avertissement sont déclenchés.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

L'exemple ci-dessous montre comment créer un événement pour tous les événements critiques de latence, d'IOPS et de MBps. Vous pouvez utiliser cette même méthode pour sélectionner des événements parmi tous les compteurs de performance, ainsi que pour tous les événements d'avertissement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis saisissez un nom et une description pour l'alerte.
4. Ne sélectionnez aucune ressource sur la page **Ressources**.

   Comme aucune ressource n'est sélectionnée, l'alerte s'applique à tous les clusters, agrégats, volumes, etc. pour lesquels ces événements sont reçus.

5. Cliquez sur **Événements** et effectuez les actions suivantes :
   a. Dans la liste Gravité de l'événement, sélectionnez **Critique**.
   b. Dans le champ « Le nom de l'événement contient », saisissez `latency` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
   c. Dans le champ « Le nom de l'événement contient », saisissez `iops` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
   d. Dans le champ « Le nom de l'événement contient », saisissez `mbps` puis cliquez sur la flèche pour sélectionner tous les événements correspondants.
6. Cliquez sur **Actions**, puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
7. Configurez les autres options sur cette page pour l'émission de traps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Tester les alertes dans Active IQ Unified Manager

Vous pouvez tester une alerte pour vérifier qu'elle est 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 en utilisant le test d'alerte.

Avant de commencer

- Vous devez avoir configuré les paramètres de notification tels que l'adresse e-mail 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 attribué un script et configuré ce script pour qu'il s'exécute lors de la génération de l'alerte.
- Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page **Configuration des alertes**, sélectionnez l'alerte que vous souhaitez tester, puis cliquez sur **Tester**.

   Un courriel d'alerte de test est envoyé aux adresses électroniques que vous avez spécifiées lors de la création de l'alerte.

Désactiver les alertes pour les événements résolus et obsolètes dans Active IQ Unified Manager

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, Résolu et Obsolète. Si vous ne souhaitez pas recevoir d'alertes pour les événements lorsqu'ils passent aux états Résolu et Obsolète, vous pouvez configurer un paramètre global pour supprimer ces alertes.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Par défaut, aucune alerte n'est envoyée pour les événements lorsqu'ils passent aux états Résolu et Obsolète.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page **Configuration des alertes**, effectuez l'une des actions suivantes à l'aide du curseur situé en regard de l'élément **Alertes pour les événements résolus et obsolètes** :

À…	Faites ceci…
Cessez d'envoyer des alertes lorsque les événements sont résolus ou deviennent obsolètes	Déplacez le curseur vers la gauche
Commencez à envoyer des alertes lorsque des événements sont résolus ou rendus obsolètes	Déplacez le curseur vers la droite

Exclure les volumes de destination de reprise après sinistre de la génération d'alertes dans Active IQ Unified Manager

Lors de la configuration des alertes de volume, vous pouvez spécifier une chaîne de caractères dans la boîte de dialogue Alerte pour identifier un volume ou un groupe de volumes. Toutefois, si vous avez configuré la reprise après sinistre pour les SVM, les volumes source et de destination portent le même nom ; vous recevrez donc des alertes pour les deux volumes.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez désactiver les alertes pour les volumes de destination de reprise après sinistre en excluant les volumes portant le nom de la SVM de destination. Cela est possible, car l'identifiant des événements de volume contient à la fois le nom de la SVM et le nom du volume au format «<svm_name>:/<volume_name>».

L'exemple ci-dessous montre comment créer des alertes pour le volume « vol1 » sur la SVM principale « vs1 », mais exclure la génération de l'alerte sur un volume portant le même nom sur la SVM « vs1-dr ».

Dans la boîte de dialogue Ajouter une alerte, procédez comme suit :

Étapes

1. Cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
2. Cliquez sur **Ressources**, puis sélectionnez l'onglet **Inclure**.
   a. Sélectionnez **Volume** dans la liste déroulante, puis saisissez **`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-le vers la zone **Ressources sélectionnées**.
3. Sélectionnez l'onglet **Exclude**, sélectionnez **Volume**, saisissez **`vs1-dr`** dans le champ **Name contains**, puis cliquez sur **Add**.

   Cela empêche la génération de l'alerte pour le volume « vol1 » sur la SVM « vs1-dr ».

4. Cliquez sur **Événements** et sélectionnez le ou les événements que vous souhaitez appliquer au volume ou aux volumes.
5. Cliquez sur **Actions**, puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
6. Configurez les autres options sur cette page pour l'émission de traps SNMP et l'exécution d'un script, puis cliquez sur **Enregistrer**.

Consultez les alertes dans Active IQ Unified Manager

Vous pouvez consulter la liste des alertes créées pour différents événements à partir de la page Configuration des alertes. Vous pouvez également consulter les propriétés des alertes, telles que la description de l'alerte, la méthode et la fréquence de notification, les événements qui déclenchent l'alerte, les destinataires des alertes par e-mail et les ressources concernées, telles que les clusters, les agrégats et les volumes.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.

   La liste des alertes est affichée sur la page Configuration des alertes.

Modifier les alertes dans Active IQ Unified Manager

Vous pouvez modifier les propriétés de l'alerte, telles que la ressource à laquelle l'alerte est associée, les événements, les destinataires, les options de notification, la fréquence de notification et les scripts associés.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page **Configuration des alertes**, sélectionnez l'alerte que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier l'alerte**, modifiez les sections Nom, Ressources, Événements et Actions, selon vos besoins.

   Vous pouvez modifier ou supprimer le script associé à l'alerte.

4. Cliquez sur **Enregistrer**.

Supprimer les alertes dans Active IQ Unified Manager

Vous pouvez supprimer une alerte lorsqu'elle n'est plus nécessaire. Par exemple, vous pouvez supprimer une alerte créée pour une ressource particulière lorsque cette ressource n'est plus surveillée par Unified Manager.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page **Configuration des alertes**, sélectionnez les alertes que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la demande de suppression.

Description des fenêtres d'alerte et des boîtes de dialogue

Découvrez la page de configuration des alertes dans Active IQ Unified Manager

La page « Configuration des alertes » affiche une liste d'alertes et fournit des informations sur le nom de l'alerte, son statut, la méthode de notification et la fréquence de notification. Vous pouvez également ajouter, modifier, supprimer, activer ou désactiver des alertes depuis cette page.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Boutons de commande

- **Ajouter**

  Affiche la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter de nouvelles alertes.

- **Modifier**

  Affiche la boîte de dialogue Modifier l'alerte, qui vous permet de modifier les alertes sélectionnées.

- **Supprimer**

  Supprime les alertes sélectionnées.

- **Activer**

  Permet aux alertes sélectionnées d'envoyer des notifications.

- **Désactiver**

  Désactive les alertes sélectionnées lorsque vous souhaitez interrompre temporairement l'envoi de notifications.

- **Test**

  Tester les alertes sélectionnées pour vérifier leur configuration après leur ajout ou leur modification.

- **Alertes concernant les événements résolus et obsolètes**

  Permet d'activer ou de désactiver l'envoi d'alertes lorsque des événements passent à l'état Résolu ou Obsolète. Cela peut aider à éviter aux utilisateurs de recevoir des notifications inutiles.

Vue de liste

La vue Liste affiche, sous forme de tableau, les informations relatives aux alertes créées. Vous pouvez utiliser les filtres de colonnes pour personnaliser les données affichées. Vous pouvez également sélectionner une alerte pour afficher plus d'informations la concernant 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 le mode de notification sélectionné pour l'alerte. Vous pouvez avertir les utilisateurs par e-mail ou par traps SNMP.

- **Fréquence de notification**

  Spécifie la fréquence (en minutes) à laquelle le serveur de gestion continue d'envoyer des notifications jusqu'à ce que l'événement soit acquitté, résolu ou déplacé vers l'état Obsolète.

Zone de détails

La zone de détails fournit plus d'informations sur l'alerte sélectionnée.

- **Nom de l'alerte**

  Affiche le nom de l'alerte.

- **Description de l'alerte**

  Affiche une description de l'alerte.

- **Événements**

  Affiche les événements pour lesquels vous souhaitez déclencher l'alerte.

- **Ressources**

  Affiche les ressources pour lesquelles vous souhaitez déclencher l'alerte.

- **Comprend**

  Affiche le groupe de ressources pour lequel vous souhaitez déclencher l'alerte.

- **Exclut**

  Affiche le groupe de ressources pour lequel vous ne souhaitez pas déclencher l'alerte.

- **Méthode de notification**

  Affiche le mode 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 acquitté, résolu ou déplacé vers l'état Obsolete.

- **Nom du script**

  Affiche le nom du script associé à l'alerte sélectionnée. Ce script est exécuté lorsqu'une alerte est générée.

- **Destinataires du courriel**

  Affiche les adresses électroniques des utilisateurs qui reçoivent la notification d'alerte.

Découvrez la boîte de dialogue Ajouter une alerte dans Active IQ Unified Manager

Vous pouvez créer des alertes pour être informé lorsqu'un événement particulier est généré, afin de résoudre rapidement le problème et de minimiser ainsi l'impact sur votre environnement. Vous pouvez créer des alertes pour une ressource unique ou un ensemble de ressources, ainsi que pour des événements d'un niveau de gravité particulier. Vous pouvez également spécifier la méthode et la fréquence de notification des alertes.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Nom

Cette zone vous permet de spécifier un nom et une description pour l'alerte :

- **Nom de l'alerte**

  Permet de spécifier un nom d'alerte.

- **Description de l'alerte**

  Permet de spécifier une description pour l'alerte.

Ressources

Cette zone vous permet de sélectionner une ressource individuelle ou de regrouper les ressources selon une règle dynamique pour laquelle vous souhaitez déclencher l'alerte. Une règle dynamique correspond à un ensemble de ressources filtrées selon la chaîne de texte que vous spécifiez. Vous pouvez rechercher des ressources en sélectionnant un type de ressource dans la liste déroulante ou en indiquant le nom exact d'une ressource pour afficher une ressource spécifique.

Si vous créez une alerte à partir de l'une des pages de détails d'un objet de stockage, cet objet est automatiquement inclus dans l'alerte.

- **Inclure**

  Permet d'inclure les ressources pour lesquelles vous souhaitez déclencher des alertes. Vous pouvez

spécifier une chaîne de caractères pour regrouper les ressources qui correspondent à cette chaîne et sélectionner ce groupe pour l'inclure dans l'alerte. Par exemple, vous pouvez regrouper tous les volumes dont le nom contient la chaîne « abc ».

- **Exclure**

  Permet d'exclure les ressources pour lesquelles vous ne souhaitez pas déclencher d'alertes. Par exemple, vous pouvez exclure tous les volumes dont le nom contient la chaîne « xyz ».

  L'onglet Exclure s'affiche uniquement lorsque vous sélectionnez toutes les ressources d'un type de ressource particulier : par exemple, <<All Volumes>> ou <<All Volumes whose name contains 'xyz'>>.

  Si une ressource correspond à la fois aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion prévaut sur la règle d'inclusion et cet événement ne génère aucune alerte.

Événements

Cette section vous permet de sélectionner les événements pour lesquels vous souhaitez créer des alertes. Vous pouvez créer des alertes pour des événements en fonction de leur niveau de gravité ou pour un ensemble d'événements.

Pour sélectionner plusieurs événements, vous devez maintenir la touche Ctrl enfoncée pendant que vous effectuez vos sélections.

- **Gravité de l'événement**

  Permet de sélectionner les événements en fonction du type de gravité, qui peut être Critique, Erreur ou Avertissement.

- **Le nom de l'événement contient**

  Permet de sélectionner les événements dont le nom contient les caractères spécifiés.

Actions

Cette section vous permet de spécifier les utilisateurs à notifier lorsqu'une alerte est déclenchée. Vous pouvez également y définir le mode et la fréquence de notification.

- **Alertez ces utilisateurs**

  Permet de spécifier l'adresse e-mail ou le nom d'utilisateur de l'utilisateur qui doit recevoir les notifications.

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

- **Fréquence de notification**

  Permet de spécifier la fréquence à laquelle le serveur de gestion envoie des notifications jusqu'à ce que l'événement soit acquitté, résolu ou déplacé vers l'état obsolète.

  Vous pouvez choisir les méthodes de notification suivantes :

  - Notifier une seule fois

- Notifier à la fréquence spécifiée
- Notifier à une fréquence spécifiée dans la plage horaire spécifiée

- **Émettre un trap SNMP**

  Cocher cette case vous permet de spécifier si les traps SNMP doivent être envoyés à l'hôte SNMP configuré globalement.

- **Exécuter le script**

  Permet d'ajouter votre script personnalisé à l'alerte. Ce script est exécuté lorsqu'une alerte est générée.

> Si cette fonctionnalité n'apparaît pas dans l'interface utilisateur, c'est parce qu'elle a été désactivée par votre administrateur. Si nécessaire, vous pouvez activer cette fonctionnalité dans **Gestion du stockage** > **Paramètres des fonctionnalités**.

Boutons de commande

- **Sauvegarder**

  Génère une alerte et ferme la boîte de dialogue.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue.

Modifier les propriétés des alertes dans Active IQ Unified Manager

Vous pouvez modifier les propriétés de l'alerte, telles que la ressource à laquelle elle 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**

  Permet de spécifier une description pour l'alerte.

- **État d'alerte**

  Permet d'activer ou de désactiver l'alerte.

Ressources

Cette zone vous permet de sélectionner une ressource individuelle ou de regrouper les ressources selon 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 en spécifiant le nom exact de la ressource pour afficher une ressource spécifique.

- **Inclure**

  Permet d'inclure les ressources pour lesquelles vous souhaitez déclencher des alertes. Vous pouvez spécifier une chaîne de texte pour regrouper les ressources qui correspondent à cette chaîne et sélectionner ce groupe pour l'inclure dans l'alerte. Par exemple, vous pouvez regrouper tous les volumes dont le nom contient la chaîne "vol0".

- **Exclure**

  Permet d'exclure les ressources pour lesquelles vous ne souhaitez pas déclencher d'alertes. Par exemple, vous pouvez exclure tous les volumes dont le nom contient la chaîne « `xyz` ».

> L'onglet Exclure s'affiche uniquement lorsque vous sélectionnez toutes les ressources d'un type de ressource particulier, par exemple, <<All Volumes>> ou <<All Volumes whose name contains 'xyz'>>.

Événements

Cette section vous permet de sélectionner les événements pour lesquels vous souhaitez déclencher les alertes. Vous pouvez déclencher une alerte pour des événements d'un certain niveau de gravité ou pour un ensemble d'événements.

- **Gravité de l'événement**

  Permet de sélectionner les événements en fonction du type de gravité, qui peut être Critique, Erreur ou Avertissement.

- **Le nom de l'événement contient**

  Permet de sélectionner les événements dont le nom contient les caractères spécifiés.

Actions

Cette zone vous permet de spécifier le mode de notification et la fréquence des notifications.

- **Alertez ces utilisateurs**

  Permet de modifier l'adresse électronique ou le nom d'utilisateur, ou de spécifier une nouvelle adresse électronique 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 reconnu, résolu ou déplacé vers l'état obsolète.

  Vous pouvez choisir les méthodes de notification suivantes :

  - Notifier une seule fois
  - Notifier à la fréquence spécifiée
  - Notifier à une fréquence spécifiée dans la plage horaire spécifiée

- **Émettre un trap SNMP**

  Permet de spécifier si les traps SNMP doivent être envoyés à l'hôte SNMP configuré globalement.

- **Exécuter le script**

  Permet d'associer un script à l'alerte. Ce script est exécuté lorsqu'une alerte est générée.

Boutons de commande

- **Sauvegarder**

  Enregistre les modifications et ferme la boîte de dialogue.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue.

Gérer les scripts

Gérer les scripts dans Active IQ Unified Manager

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 importer des scripts personnalisés et tester leur exécution lorsqu'une alerte est générée.

La possibilité de charger des scripts dans Unified Manager et de les exécuter est activée par défaut. Si votre organisation ne souhaite pas autoriser cette fonctionnalité pour des raisons de sécurité, vous pouvez la désactiver dans **Gestion du stockage** > **Paramètres des fonctionnalités**.

Informations connexes

"Activer et désactiver la possibilité de téléverser des scripts"

Fonctionnement des scripts avec les alertes dans Active IQ Unified Manager

Vous pouvez associer une alerte à votre script afin que celui-ci s'exécute lorsqu'une alerte est déclenchée par 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 à l'origine des 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 alte à un script, ce dernier est exécuté. Vous trouverez dans l'e-mail d'alerte le détail des arguments transmis au script.

> Si vous avez créé un script personnalisé et l'avez associé à une alerte pour un type d'événement spécifique, les actions sont effectuées en fonction de votre script personnalisé pour ce type d'événement, et les actions **Corriger** ne sont pas disponibles par défaut sur la page Actions de gestion ou sur le tableau de bord Unified Manager.

Le script utilise les arguments suivants pour son exécution :

- `-eventID`
- `-eventName`

- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Vous pouvez utiliser les arguments dans vos scripts et recueillir des informations sur les événements associés ou modifier les objets de stockage.

Exemple d'obtention d'arguments à partir de scripts

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Lorsqu'une alerte est générée, le système exécute ce script et affiche le résultat suivant :

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Ajouter des scripts dans Active IQ Unified Manager

Vous pouvez ajouter des scripts dans Unified Manager et associer les scripts à des alertes. Ces scripts s'exécutent automatiquement lorsqu'une alerte est générée et vous permettent d'obtenir des informations sur les objets de stockage pour lesquels l'événement est généré.

Avant de commencer

- Vous devez avoir créé et enregistré les scripts que vous souhaitez ajouter au serveur Unified Manager.
- Les formats de fichiers pris en charge pour les scripts sont Perl, Shell, PowerShell, Python et `.bat` fichiers.

Plateforme sur laquelle Unified Manager est installé	Langues prises en charge
VMware	Scripts Perl et Shell
Linux	Scripts Perl, Python et Shell
Windows	PowerShell, Perl, Python et scripts .bat

  - Pour les scripts Perl, Perl doit être installé sur le serveur Unified Manager. Sur les installations VMware, Perl 5 est installé par défaut et les scripts ne prendront en charge que les fonctionnalités de Perl 5. 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 ces fichiers journaux ne sont créés nulle part dans le dossier d'installation d'Unified Manager.

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez télécharger des scripts personnalisés et recueillir des détails sur l'événement lié à l'alerte.

Si cette fonctionnalité n'apparaît pas dans l'interface utilisateur, c'est parce qu'elle a été désactivée par votre administrateur. Si nécessaire, vous pouvez activer cette fonctionnalité dans **Gestion du stockage** > **Paramètres des fonctionnalités**.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Scripts**.
2. Sur 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 **Add**.

Informations connexes

"Activer et désactiver la possibilité de téléverser des scripts"

Supprimer les scripts dans Active IQ Unified Manager

Vous pouvez supprimer un script de Unified Manager lorsque celui-ci n'est plus nécessaire ou n'est plus valide.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Le script ne doit pas être associé à une alerte.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Scripts**.
2. Sur 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 dans Active IQ Unified Manager

Vous pouvez vérifier que votre script s'exécute correctement lorsqu'une alerte est générée pour un objet de stockage.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir téléchargé un script dans le format de fichier pris en charge vers Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Scripts**.
2. Sur la page **Scripts**, ajoutez votre script de test.
3. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
4. Sur la page **Configuration des alertes**, effectuez l'une des actions suivantes :

À…	Faites ceci…
Ajouter une alerte	a. Cliquez sur **Add**. 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. Sur la page **Configuration des alertes**, sélectionnez l'alerte que vous avez ajoutée ou modifiée, puis cliquez sur **Tester**.

   Le script est exécuté avec l'argument « -test », et une alerte de notification est envoyée aux adresses électroniques spécifiées lors de la création de l'alerte.

Découvrez les commandes CLI prises en charge par Active IQ Unified Manager

En tant qu'administrateur du stockage, vous pouvez utiliser les commandes CLI pour effectuer des requêtes sur les objets de stockage, par exemple sur les clusters, les agrégats, les volumes, les qtrees et les LUN. Vous pouvez utiliser les commandes CLI pour interroger la base de données interne d'Unified Manager et la base de données ONTAP. Vous pouvez également utiliser des commandes CLI dans des scripts 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` et 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 à l'application *console*.

Commande CLI	Description	Sortie
`um cli login -u <username> [-p <password>]`	Permet de se connecter à l'interface de ligne de commande (CLI). Pour des raisons de sécurité, vous devez saisir uniquement le nom d'utilisateur après l'option « -u ». De cette manière, le système vous demandera le mot de passe, et celui-ci ne sera enregistré ni dans l'historique ni dans la table des processus. La session expire trois heures après la connexion, après quoi l'utilisateur doit se reconnecter.	Affiche le message correspondant.
`um cli logout`	Se déconnecter de l'interface de ligne de commande.	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>`	La méthode la plus simple pour exécuter une commande sur un ou plusieurs hôtes. Principalement utilisée pour les scripts d'alerte afin d'obtenir ou d'effectuer une opération sur ONTAP. L'argument optionnel « timeout » définit une durée maximale (en secondes) pour l'exécution de la commande sur le client. La valeur par défaut est 0 (attente indéfinie).	Tel que reçu d'ONTAP.
`um run query <sql command>`	Exécute une requête SQL. Seules les requêtes qui lisent dans la base de données sont autorisées. 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. En cas de résultat vide, d'erreur de syntaxe ou de requête incorrecte, le message d'erreur approprié s'affiche.

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 la manière dont les connexions aux systèmes de stockage sont établies. Les options -u (nom d'utilisateur) et -P (mot de passe) doivent être spécifiées lors de l'ajout d'une source de données. L'option -t (protocole) spécifie le protocole utilisé pour communiquer avec le cluster (http ou https). Si le protocole n'est pas spécifié, les deux protocoles seront essayés L'option -p (port) spécifie le port utilisé pour communiquer avec le cluster. Si le port n'est pas spécifié, la valeur par défaut du protocole approprié sera utilisée. Cette commande ne peut être exécutée que par l'administrateur du stockage.	Invite l'utilisateur à accepter le certificat et affiche 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> .. ]`	Liste toutes les options que vous pouvez configurer à l'aide de la commande set.	Affiche les valeurs suivantes sous forme de tableau : `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Définit une ou plusieurs options. Cette 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")`

Commande CLI	Description	Sortie
`um lun list [-q] [ -ObjectType <object-id>]`	Répertorie les LUN après filtrage sur l'objet spécifié. -q s'applique à toutes les commandes pour n'afficher aucun en-tête. ObjectType peut être lun, qtree, cluster, volume, quota ou svm. Par exemple : **`um lun list -cluster 1`** Dans cet exemple, « -cluster » est objectType et « 1 » est objectId. La commande répertorie tous les LUN du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Affiche la liste des machines virtuelles 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 l'objectType et « 1 » est l'objectId. La commande répertorie toutes les machines virtuelles de stockage du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : `Name and Cluster ID.`
`um qtree list [-q] [ -ObjectType <object-id>]`	Répertorie les qtrees après filtrage sur l'objet spécifié. -q s'applique à toutes les commandes pour ne pas afficher d'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 avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau : `Qtree ID and Qtree Name.`

Commande CLI	Description	Sortie
`um disk list [-q] [-ObjectType <object-id>]`	Affiche la liste des disques après filtrage sur l'objet spécifié. ObjectType peut être disk, aggr, node ou cluster. Par exemple : **`um disk list -cluster 1`** Dans cet exemple, « -cluster » est le objectType et « 1 » est le 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>]`	Liste les clusters après filtrage sur l'objet spécifié. ObjectType peut être disk, aggr, node, cluster, lun, qtree, volume, quota ou svm. Par exemple : **`um cluster list -aggr 1`** Dans cet exemple, « -aggr » est objectType et « 1 » est objectId. La commande répertorie le cluster auquel appartient l'agrégat d'ID 1.	Affiche les valeurs suivantes sous forme de tableau `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`.
`um cluster node list [-q] [-ObjectType <object-id>]`	Liste les nœuds du cluster après 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 le objectId. La commande répertorie tous les nœuds du cluster dont l'ID est 1.	Affiche les valeurs suivantes sous forme de tableau `Name and Cluster ID`.

Commande CLI	Description	Sortie
`um volume list [-q] [-ObjectType <object-id>]`	Affiche la liste des volumes après filtrage sur l'objet spécifié. ObjectType peut être lun, qtree, cluster, volume, quota, svm ou aggregate. Par exemple : **`um volume list -cluster 1`** Dans cet exemple, « -cluster » est objectType et « 1 » est objectId. La commande répertorie tous les volumes du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Affiche la liste des utilisateurs disposant d'un quota après 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 le objectId. La commande répertorie tous les utilisateurs de quota au sein du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau `ID, Name, SID and Email`.
`um aggr list [-q] [-ObjectType <object-id>]`	Affiche la liste des agrégats après 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 objectType et « 1 » est objectId. La commande répertorie tous les agrégats du cluster avec l'ID 1.	Affiche les valeurs suivantes sous forme de tableau `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Reconnaît un ou plusieurs événements.	Affiche le message correspondant.
`um event resolve <event-ids>`	Résout un ou plusieurs événements.	Affiche le message correspondant.
`um event assign -u <username> <event-id>`	Attribue un événement à un utilisateur.	Affiche le message correspondant.

Commande CLI	Description	Sortie
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Affiche la liste des événements générés par le système ou l'utilisateur. Filtre les événements selon leur source, leur état et leurs identifiants.	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

Découvrez la page Scripts dans Active IQ Unified Manager

La page Scripts vous permet d'ajouter vos scripts personnalisés à Unified Manager. Vous pouvez associer ces scripts à des alertes pour permettre la reconfiguration automatique des objets de stockage.

La page Scripts vous permet d'ajouter ou de supprimer des scripts dans Unified Manager.

Boutons de commande

- **Ajouter**

  Affiche la boîte de dialogue Ajouter un script, qui vous permet d'ajouter des scripts.

- **Supprimer**

  Supprime le script sélectionné.

Vue de liste

La vue liste affiche, sous forme de tableau, les scripts que vous avez ajoutés à Unified Manager.

- **Nom**

  Affiche le nom du script.

- **Description**

  Affiche la description du script.

Boîte de dialogue Ajouter un script dans Active IQ Unified Manager

La boîte de dialogue Ajouter un script vous permet d'ajouter des scripts à Unified Manager. Vous pouvez configurer des alertes avec vos scripts afin de résoudre automatiquement les événements générés pour les objets de stockage.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

- **Sélectionnez le fichier de script**

Permet de sélectionner un script pour l’alerte.

- **Description**

  Vous permet de spécifier une description pour le script.

Surveiller et gérer les performances du cluster

Introduction à la surveillance des performances d'Active IQ Unified Manager

Découvrez la surveillance des performances dans Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) offre des fonctionnalités de surveillance des performances et d'analyse des causes profondes des événements pour les systèmes exécutant le logiciel ONTAP de NetApp.

Unified Manager vous aide à identifier les workloads qui sollicitent excessivement les composants du cluster et dégradent les performances des autres workloads sur le cluster. En définissant des politiques de seuil de performance, vous pouvez également spécifier des valeurs maximales pour certains compteurs de performance afin que des événements soient générés lorsque le seuil est dépassé. Unified Manager vous alerte de ces événements de performance afin que vous puissiez prendre des mesures correctives et rétablir les performances à un niveau de fonctionnement normal. Vous pouvez consulter et analyser les événements dans l'interface utilisateur de Unified Manager.

Unified Manager surveille les performances de deux types de workloads :

- Workloads définis par l'utilisateur

  Ces workloads se composent de volumes FlexVol et de volumes FlexGroup que vous avez créés dans votre cluster.

- Charges de travail définies par le système

  Ces charges de travail se composent d'une activité interne au système.

Explorez les fonctionnalités de surveillance des performances d'Active IQ Unified Manager

Unified Manager collecte et analyse les statistiques de performance des systèmes exécutant le logiciel ONTAP. Il utilise des seuils de performance dynamiques et des seuils de performance définis par l'utilisateur pour surveiller divers compteurs de performance 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 que d'habitude. Ce problème indique également que les performances des applications clientes qui utilisent le volume ont diminué. Unified Manager identifie le composant de stockage à l'origine du problème de performances et fournit une liste des actions suggérées que vous pouvez entreprendre pour y remédier.

Unified Manager inclut les fonctionnalités suivantes :

- Surveille et analyse les statistiques de performance du workload d'un système exécutant le logiciel ONTAP.
- Suit les compteurs de performance pour les clusters, les nœuds, les agrégats, les ports, les SVMs, les volumes, les LUNs, les espaces de noms NVMe et les interfaces réseau (LIFs).
- Affiche des graphiques détaillés qui représentent l'activité du workload au fil du temps, notamment les

IOPS (opérations), le MB/s (débit), la latence (temps de réponse), l'utilisation, la capacité de performance et le taux de cache.

- Permet de créer des politiques de seuil de performance définies par l'utilisateur qui déclenchent des événements et envoient des alertes par e-mail lorsque les seuils sont dépassés.
- Utilise des seuils définis par le système et des seuils de performance dynamiques qui apprennent l'activité de votre workload afin d'identifier les problèmes de performance et de vous alerter.
- Identifie les règles de qualité de service (QoS) et les règles de niveau de service de performance (PSL) appliquées à vos volumes et LUNs.
- Identifie clairement le composant du cluster qui fait l'objet d'un conflit.
- Identifie les workloads qui utilisent excessivement les composants du cluster et ceux dont les performances sont affectées par l'augmentation de l'activité.

Utilisez les interfaces d'Active IQ Unified Manager pour gérer les performances du système de stockage

Ces sections contiennent des informations sur les deux interfaces utilisateur qu'Active IQ Unified Manager fournit pour résoudre les problèmes de capacité, de disponibilité et de protection du stockage des données. Les deux interfaces utilisateur sont l'interface utilisateur web Unified Manager et la console de maintenance.

Si vous souhaitez utiliser les fonctionnalités de protection d'Unified Manager, vous devez également installer et configurer OnCommand Workflow Automation (WFA).

interface utilisateur Web de Unified Manager

L'interface utilisateur Web de Unified Manager permet à un administrateur de surveiller et de résoudre les problèmes de cluster liés à la capacité, à la disponibilité et à la protection du stockage des données.

Ces sections décrivent certains workflows 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 de Unified Manager.

Console de maintenance

La console de maintenance Unified Manager permet à un administrateur de surveiller, de diagnostiquer et de résoudre les problèmes liés au système d'exploitation, aux mises à niveau de version, aux accès utilisateurs et au réseau du serveur Unified Manager lui-même. Si l'interface utilisateur web de Unified Manager est indisponible, la console de maintenance est le seul moyen d'accéder 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.

Consultez la configuration du cluster et les données de performance dans Active IQ Unified Manager

L'intervalle de collecte des *données de configuration du cluster* est de 15 minutes. Par exemple, après avoir ajouté un cluster, il faut 15 minutes pour afficher les détails du cluster dans l'interface utilisateur de Unified Manager. Cet intervalle s'applique également lorsque vous apportez des modifications à un cluster.

Par exemple, si vous ajoutez deux nouveaux volumes à une SVM dans un cluster, vous verrez ces nouveaux objets dans l'interface utilisateur après le prochain intervalle d'interrogation, qui peut aller jusqu'à 15 minutes.

Unified Manager collecte les *statistiques de performance* actuelles de tous les clusters surveillés toutes les cinq minutes. Il analyse ces données afin d'identifier les événements de performance et les problèmes potentiels. Il conserve 30 jours de données historiques de performance par tranches de cinq minutes et 180 jours de données historiques de performance par tranches d'une heure. Vous pouvez ainsi consulter des détails de performance très précis pour le mois en cours et les tendances générales de performance sur une période allant jusqu'à un an.

Les requêtes de collecte sont décalées de quelques minutes afin 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 effectuées par Unified Manager :

Activité	Intervalle de temps	Description
Interrogation des statistiques de performance	Toutes les 5 minutes	Collecte les données de performance en temps réel de chaque cluster.
Analyse statistique	Toutes les 5 minutes	Après chaque collecte de statistiques, Unified Manager compare les données recueillies aux seuils définis par l'utilisateur, par le système et dynamiques. Si des seuils de performance ont été dépassés, Unified Manager génère des événements et envoie un e-mail aux utilisateurs spécifiés, si cette option a été configurée.
Interrogation de configuration	Toutes les 15 minutes	Collecte des informations d'inventaire détaillées de chaque cluster afin d'identifier tous les objets de stockage (nœuds, SVM, volumes, etc.).
Synthèse	Toutes les heures	Résume les 12 dernières collectes de données de performance de cinq minutes en moyennes horaires. Les valeurs moyennes horaires sont utilisées dans certaines pages de l'interface utilisateur et sont conservées pendant 180 jours.

Activité	Intervalle de temps	Description
Analyse prévisionnelle et élagage des données	Chaque jour après minuit	Analyse les données du cluster pour établir des seuils dynamiques de latence des volumes et d'IOPS pour les prochaines 24 heures. Supprime de la base de données toutes les données de performance par tranches de cinq minutes datant de plus de 30 jours.
Élagage des données	Tous les jours après 2 h du matin	Supprime de la base de données tous les événements datant de plus de 180 jours et les seuils dynamiques datant de plus de 180 jours.
Élagage des données	Tous les jours après 3 h 30 du matin	Supprime de la base de données toutes les données de performance d'une heure datant de plus de 180 jours.

Comprendre les cycles de collecte de continuité des données dans Active IQ Unified Manager

Un cycle de collecte de continuité des données récupère les données de performance en dehors du cycle de collecte des performances du cluster en temps réel qui s'exécute, par défaut, toutes les cinq minutes. Les collectes de continuité des données permettent à Unified Manager de combler les lacunes dans les données statistiques qui se produisent lorsqu'il n'a pas été possible de collecter les données en temps réel.

Unified Manager effectue des interrogations de collecte de continuité des données de performances historiques lorsque les événements suivants se produisent :

- Un cluster est initialement ajouté à Unified Manager.

  Unified Manager collecte les données de performance historiques des 15 derniers jours. Cela vous permet de consulter deux semaines d'informations sur les performances d'un cluster quelques heures seulement après son ajout.

  De plus, les événements de seuil définis par le système sont signalés pour la période précédente, le cas échéant.

- Le cycle actuel de collecte des données de performance ne se termine pas à temps.

  Si l'interrogation des performances en temps réel dépasse la période de collecte de cinq minutes, un cycle de collecte de données de continuité est lancé afin de recueillir les informations manquantes. Sans cette collecte de données de continuité, la période de collecte suivante est ignorée.

- Unified Manager est inaccessible pendant un certain temps, puis il se remet en ligne, comme dans les situations suivantes :
  - Il a été redémarré.

    - Il s’est arrêté lors d’une mise à jour logicielle ou lors de la création d’un fichier de sauvegarde.
    - Une panne réseau est résolue.
- Un cluster est inaccessible pendant un certain temps, puis il se remet en ligne, comme dans les situations suivantes :
    - Une panne réseau est résolue.
    - Une connexion lente au réseau étendu a retardé la collecte normale des données de performances.

Un cycle de collecte de données de continuité des données peut recueillir un maximum de 24 heures de données historiques. Si Unified Manager est indisponible pendant plus de 24 heures, une interruption dans les données de performances apparaît dans les pages de l’interface utilisateur.

Un cycle de collecte de données de continuité des données et un cycle de collecte de données en temps réel ne peuvent pas s’exécuter en même temps. Le cycle de collecte de données de continuité des données doit se terminer avant le lancement de la collecte de données de performance en temps réel. Lorsque la collecte de données de continuité des données doit collecter plus d’une heure de données historiques, un message de bannière s’affiche en haut du volet Notifications pour ce cluster.

Découvrez les horodatages des données collectées et des événements dans Active IQ Unified Manager

L’horodatage qui apparaît dans les données de santé et de performance collectées, ou qui apparaît comme heure de détection d’un événement, est basé sur l’heure du cluster ONTAP, ajustée au fuseau horaire défini dans le navigateur web.

Il est fortement recommandé d’utiliser un serveur NTP (Network Time Protocol) pour synchroniser l’heure sur vos serveurs Unified Manager, vos clusters ONTAP et vos navigateurs Web.

Si vous constatez des horodatages qui semblent incorrects pour un cluster particulier, vous devriez vérifier que l’heure du cluster est correctement réglée.

Navigation dans les flux de travail de performance de l’interface graphique d’Unified Manager

Naviguez dans les flux de travail de performance dans l’interface graphique Active IQ Unified Manager

L’interface Unified Manager propose de nombreuses pages pour la collecte et l’affichage des informations de performance. Vous utilisez le panneau de navigation de gauche pour naviguer entre les pages de l’interface graphique, et vous utilisez les onglets et les liens sur les pages pour consulter et configurer les informations.

Vous utilisez toutes les pages suivantes pour surveiller et dépanner les informations sur les performances du cluster :

- page du tableau de bord
- pages d’inventaire des objets de stockage et de réseau
- pages de détails des objets de stockage (y compris l’explorateur de performances)

- pages de configuration et d'installation
- pages d'événements

Connectez-vous à l'interface utilisateur Active IQ Unified Manager

Vous pouvez vous connecter à l'interface utilisateur de Unified Manager à l'aide d'un navigateur Web compatible.

Avant de commencer

- Le navigateur web doit répondre aux exigences minimales.

  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 dans **Général** > **Paramètres des fonctionnalités**.

Étapes

1. Saisissez 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, votre navigateur peut afficher un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez alors accepter le risque et poursuivre l'accès, ou installer un certificat numérique signé par une autorité de certification (AC) pour authentifier le serveur. . Sur l'écran de connexion, saisissez votre nom d'utilisateur et votre mot de passe.

Si la connexion à l'interface utilisateur d'Unified Manager est protégée par l'authentification SAML, vous devrez saisir vos identifiants sur la page de connexion du fournisseur d'identité (IdP) au lieu de la page de connexion d'Unified Manager.

La page du tableau de bord s'affiche.

Si le serveur Unified Manager n'est pas initialisé, une nouvelle fenêtre de navigateur affiche l'assistant de première utilisation. Vous devez saisir un premier destinataire d'e-mail auquel les alertes par e-mail seront envoyées, le serveur SMTP qui gérera les communications par e-mail, et indiquer si AutoSupport est activé pour envoyer des informations sur votre installation Unified Manager au support technique. L'interface utilisateur de Unified Manager s'affiche une fois ces informations renseignées.

Interface graphique et chemins de navigation

Explorez l'interface graphique et les chemins de navigation dans Active IQ Unified Manager

Unified Manager offre une grande flexibilité et vous permet d'accomplir de multiples tâches de différentes manières. Vous découvrirez de nombreux chemins de navigation en travaillant avec Unified Manager. Bien que toutes les combinaisons possibles ne puissent

être présentées ici, vous devriez vous familiariser avec quelques-uns des scénarios les plus courants.

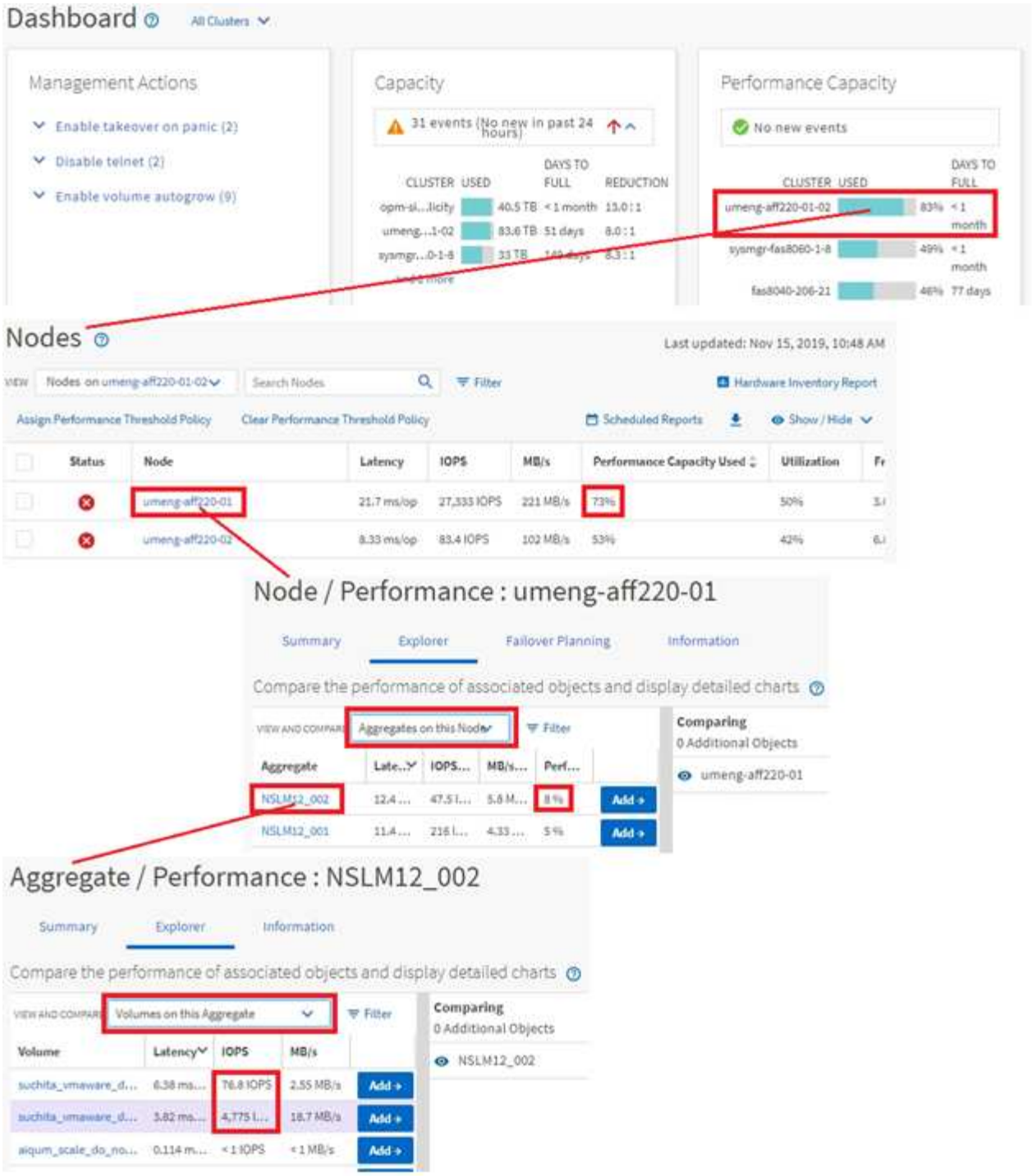
Surveiller la navigation des objets du cluster dans Active IQ Unified Manager

Vous pouvez surveiller les performances de tous les objets de tout cluster géré par Unified Manager. La surveillance de vos objets de stockage vous offre une vue d'ensemble des performances du cluster et des objets, et inclut la surveillance des événements de performance. Vous pouvez consulter les performances et les événements de manière générale, ou examiner plus en détail les performances des objets et les événements de performance.

Voici un exemple parmi tant d'autres de navigations possibles entre les objets d'un cluster:

1. Depuis la page Dashboard, consultez les détails dans le panneau Performance Capacity pour identifier le cluster qui utilise le plus de capacité de performance, puis cliquez sur l'histogramme pour accéder à la liste des nœuds de ce cluster.
2. Identifiez le nœud présentant la valeur de capacité de performance utilisée la plus élevée et cliquez sur ce nœud.
3. Depuis la page Node / Performance Explorer, cliquez sur **Aggregates on this Node** dans le menu View and Compare.
4. Identifiez l'agrégat qui utilise le plus de capacité de performances et cliquez dessus.
5. Dans la page Aggregate / Performance Explorer, cliquez sur **Volumes on this Aggregate** dans le menu View and Compare.
6. Identifiez les volumes qui utilisent le plus d'IOPS.

Vous devriez examiner ces volumes pour voir s'il convient d'appliquer une politique QoS ou une politique de niveau de service des performances, ou de modifier les paramètres de la politique, afin que ces volumes n'utilisent pas un pourcentage aussi élevé d'IOPS sur le cluster.



Surveillez la navigation des performances du cluster dans Active IQ Unified Manager

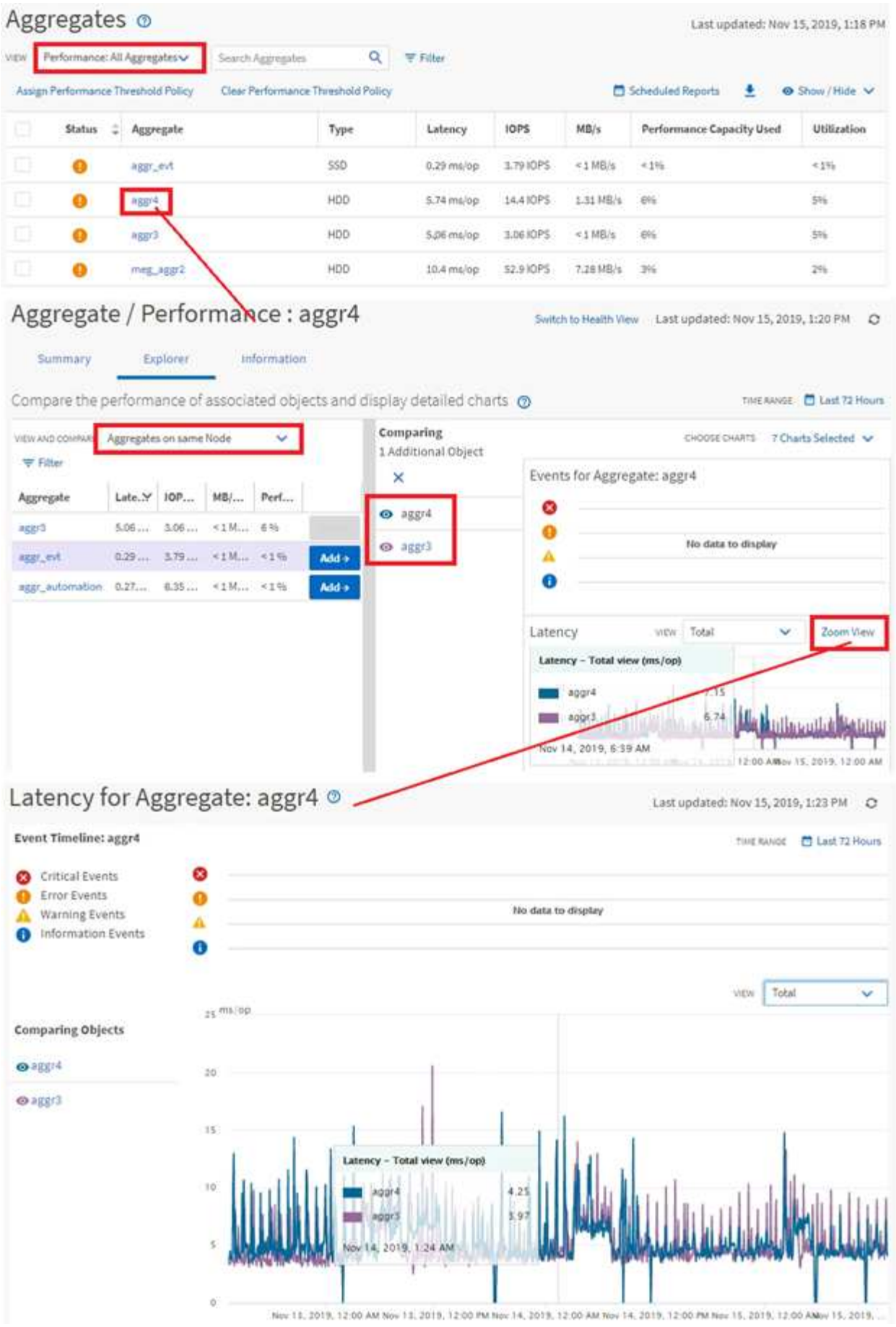
Vous pouvez surveiller les performances de tous les clusters gérés par Unified Manager. Cette surveillance vous offre une vue d'ensemble des performances des clusters et des objets, et inclut le suivi des événements de performance. Vous pouvez consulter les performances et les événements de manière générale, ou examiner plus en détail les performances des clusters et des objets, ainsi que les événements de performance.

Voici un exemple parmi les nombreux chemins de navigation possibles pour les performances d'un cluster :

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Pour consulter des informations sur les performances de ces agrégats, sélectionnez la vue Performance: All Aggregates.
3. Identifiez l'agrégat que vous souhaitez examiner et cliquez sur le nom de cet agrégat pour accéder à la page Aggregate / Performance Explorer.
4. Vous pouvez également sélectionner d'autres objets à comparer avec cet agrégat dans le menu Afficher et comparer, puis ajouter l'un de ces objets au volet de comparaison.

   Les statistiques des deux objets apparaîtront dans les graphiques des compteurs à des fins de comparaison.

5. Dans le volet Comparaison situé à droite de la page Explorateur, cliquez sur **Zoom View** dans l'un des graphiques de compteurs 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%
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
12:00 AM
Nov 15, 2019, 12:00 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
Nov 15, 2019,

Analyser les événements de performance dans Active IQ Unified Manager

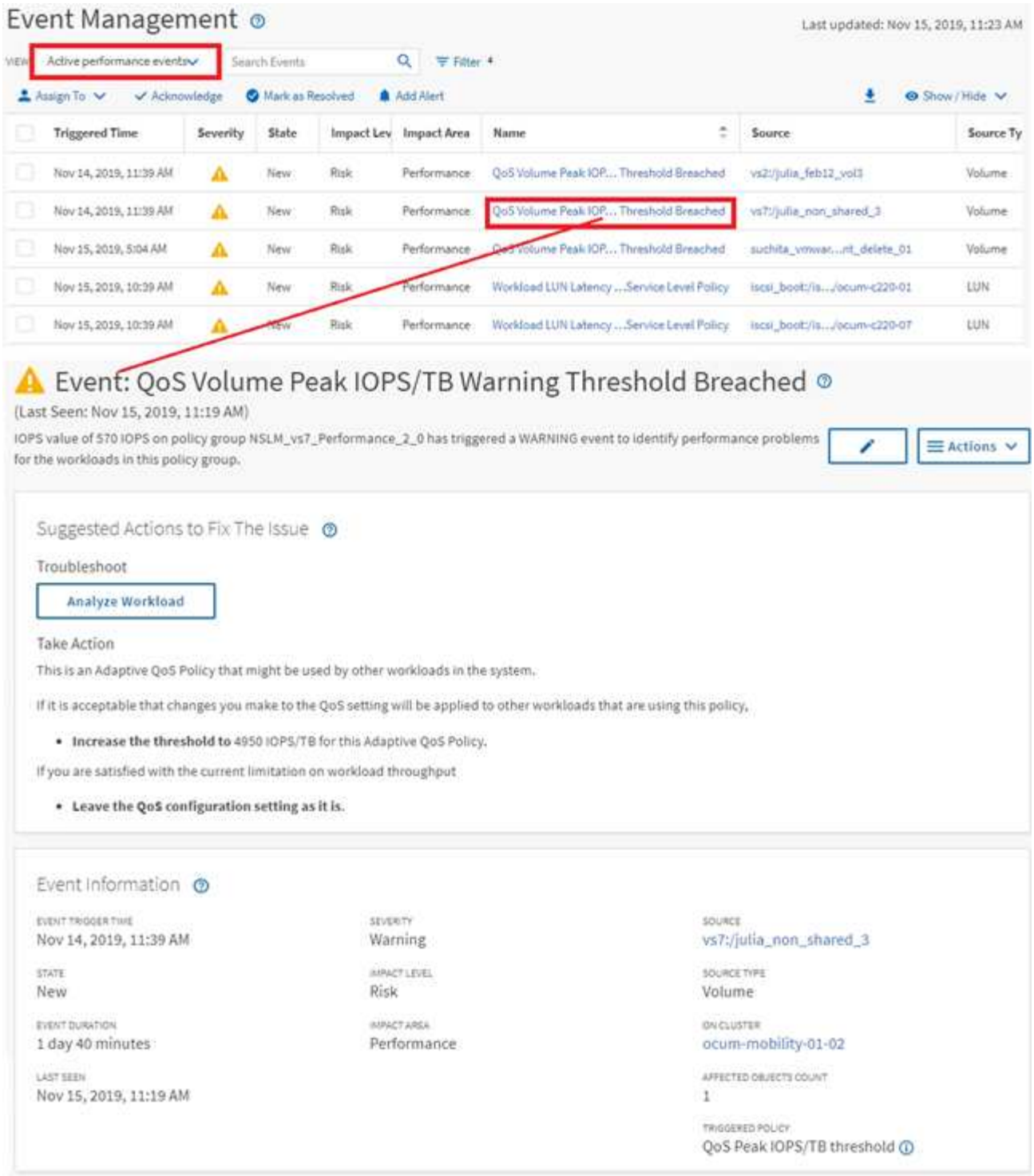
Les pages de détails des événements d'Unified Manager offrent une analyse approfondie de chaque événement de performance. Ceci s'avère utile pour analyser les événements de performance, résoudre les problèmes et optimiser les performances du système.

Selon le type d'événement de performance, vous pourriez voir l'un des deux types de pages de détails de l'événement :

- Page de détails des événements de stratégie de seuil définis par l'utilisateur et par le système
- Page de détails des événements relatifs aux politiques de seuil dynamique

Voici un exemple de navigation dans une enquête sur un événement.

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans le menu Affichage, cliquez sur **Événements de performance actifs**.
3. Cliquez sur le nom de l'événement que vous souhaitez examiner pour afficher la page de détails de l'événement.
4. Consultez la Description de l'événement et passez en revue les Actions suggérées (le cas échéant) pour afficher plus de détails sur l'événement qui peuvent vous aider à résoudre le problème. Vous pouvez cliquer sur le bouton **Analyze Workload** pour afficher des graphiques de performance détaillés afin de vous aider à approfondir l'analyse du problème.



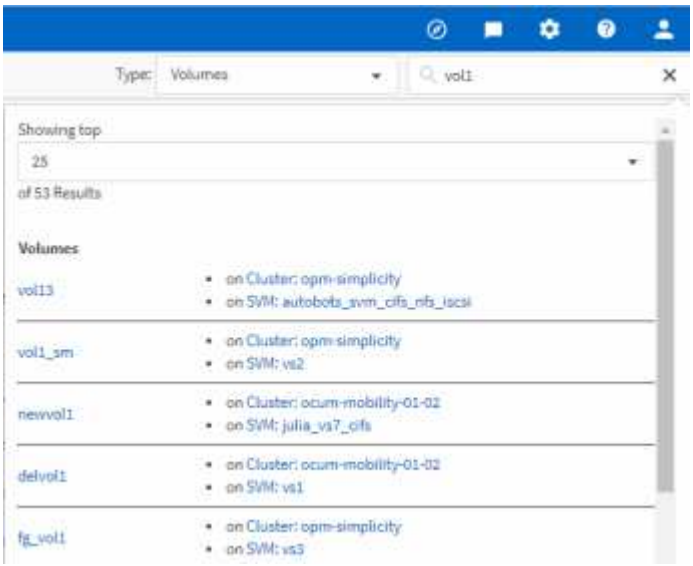
Rechercher des objets de stockage dans Active IQ Unified Manager

Pour accéder rapidement à un objet spécifique, vous pouvez utiliser le champ **Rechercher dans tous les objets de stockage** situé en haut de la barre de menu. Cette méthode de recherche globale dans tous les objets vous permet de localiser rapidement des objets spécifiques par type. Les résultats de recherche sont triés par type d'objet de stockage et vous pouvez les filtrer à l'aide du menu déroulant. Une recherche valide doit contenir au moins trois caractères.

La recherche globale affiche le nombre total de résultats, mais seuls les 25 premiers résultats de recherche sont accessibles. De ce fait, la fonctionnalité de recherche globale peut être considérée comme un outil de raccourci pour trouver des éléments spécifiques si vous savez quels éléments vous souhaitez localiser rapidement. Pour obtenir des résultats de recherche complets, vous pouvez utiliser la fonction de recherche dans les pages d'inventaire des objets et la 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 dans tous les objets de stockage**, puis appuyez sur **Entrée** pour afficher les résultats de la recherche, par exemple :

- Clusters : noms des clusters
- Nœuds : noms des nœuds
- Agrégats : noms des agrégats
- SVMs: noms des SVM
- Volumes: noms de volumes
- LUN : chemins d'accès aux LUN



Les LIF et les ports ne peuvent pas faire l'objet d'une recherche dans la barre de recherche globale.

Dans cet exemple, la liste déroulante a le type d'objet Volume sélectionné. La saisie de « `vol` » dans le champ **Search all Storage Objects** affiche une liste de tous les volumes dont le nom contient ces caractères. Pour les recherches d'objets, vous pouvez cliquer sur n'importe quel résultat de recherche pour accéder à la page Performance Explorer de cet objet. Pour les recherches d'événements, si vous cliquez sur un élément dans le résultat de recherche, vous accédez à la page Event Details.

Filtrer le contenu de la page d'inventaire dans Active IQ Unified Manager

Dans Unified Manager, vous pouvez filtrer les données des pages d'inventaire pour localiser rapidement les données selon des critères spécifiques. Le filtrage vous permet d'affiner le contenu des pages d'Unified Manager et de n'afficher que les résultats qui

vous intéressent. C’est une méthode très efficace pour afficher uniquement les données qui vous intéressent.

Utilisez **Filtering** pour personnaliser la vue de la grille selon vos préférences. Les options de filtre disponibles dépendent du type d’objet affiché dans la grille. Si des filtres sont actuellement appliqués, le nombre de filtres appliqués s’affiche à droite du bouton Filter.

Trois types de paramètres de filtrage sont pris en charge.

Paramètre	Validation
Chaîne (texte)	Les opérateurs sont **contient**, **commence par**, **se termine par** et **ne contient pas**.
Nombre maximum	Les opérateurs sont **supérieur à**, **inférieur à**, **au cours des derniers** et **entre**.
Énumération (texte)	Les opérateurs sont **is** et **is not**.

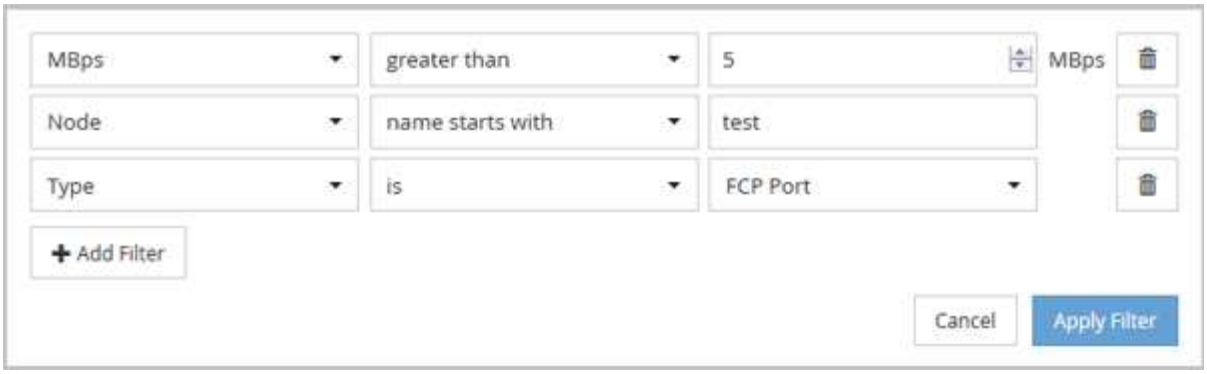
Les champs Colonne, Opérateur et Valeur sont obligatoires pour chaque filtre ; les filtres disponibles correspondent aux colonnes filtrables de la page actuelle. Vous pouvez appliquer jusqu’à quatre filtres. Les résultats filtrés sont basés sur la combinaison des paramètres de filtrage. Les résultats filtrés s’appliquent à toutes les pages de votre recherche filtrée, et pas seulement à la page actuellement affichée.

Vous pouvez ajouter des filtres à l’aide du panneau de filtrage.

1. En haut de la page, cliquez sur le bouton **Filtrer**. Le panneau de filtrage s’affiche.
2. Cliquez sur la liste déroulante de gauche et sélectionnez un objet; par exemple, *Cluster*, ou un compteur de performances.
3. Cliquez sur la liste déroulante centrale et sélectionnez l’opérateur que vous souhaitez utiliser.
4. Dans la dernière liste, sélectionnez ou saisissez une valeur pour compléter le filtre pour cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Add Filter**. Un champ de filtre supplémentaire s’affiche. Complétez ce filtre en suivant la procédure décrite dans les étapes précédentes. Notez qu’après l’ajout de votre quatrième filtre, le bouton **+Add Filter** 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 de filtrage pour supprimer des filtres individuels en cliquant sur l’icône de la 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 de filtrage avec trois filtres. Le bouton **+Ajouter un filtre** s’affiche lorsque vous avez moins du maximum de quatre filtres.



Après avoir cliqué sur **Appliquer le filtre**, le panneau de filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Surveillez les performances du cluster depuis le tableau de bord

Surveillez les performances du cluster depuis le tableau de bord dans Active IQ Unified Manager

Le tableau de bord Unified Manager propose plusieurs panneaux affichant l'état global des performances de tous les clusters surveillés par cette instance d'Unified Manager. Il vous permet d'évaluer les performances globales des clusters gérés et de repérer, localiser ou attribuer rapidement en vue de leur résolution tout événement spécifique identifié.

Consultez les panneaux de performance sur le tableau de bord Active IQ Unified Manager

Le tableau de bord Unified Manager propose plusieurs panneaux affichant l'état de performance global de tous les clusters surveillés dans votre environnement. Vous pouvez choisir d'afficher l'état de tous les clusters ou celui d'un cluster en particulier.

Outre les informations de performance, la plupart des panneaux affichent également le nombre d'événements actifs dans cette catégorie, ainsi que le nombre de nouveaux événements ajoutés au cours des 24 dernières heures. Ces informations vous aident à déterminer quels clusters vous devrez peut-être analyser plus en détail pour résoudre les événements signalés. Le fait de cliquer sur les événements affiche les quelques principaux événements et fournit un lien vers la page d'inventaire Event Management filtrée pour afficher les événements de cette catégorie.

Les panneaux suivants indiquent l'état des performances.

- **Panneau de capacité de performance**

  Lorsque vous consultez tous les clusters, ce panneau affiche la valeur de capacité de performance de chaque cluster (moyenne sur l'heure précédente) et le nombre de jours avant que la capacité de performance n'atteigne la limite supérieure (en fonction du taux de croissance quotidien). Le fait de cliquer sur l'histogramme vous amène 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 Dashboard.

Lors de l'affichage d'un seul cluster, ce panneau affiche les valeurs de capacité de performances du cluster, d'IOPS totales et de débit total.

- **Panneau IOPS du workload**

  Lorsque la gestion active des workloads est activée et que vous affichez un seul cluster, ce panneau indique le nombre total de workloads actuellement exécutés dans une certaine plage d'IOPS.

- **Panneau de performances du workload**

  Lorsque la gestion active des workloads est activée, ce panneau affiche le nombre total de workloads conformes et non conformes affectés à chaque niveau de service de performance défini. En cliquant sur un graphique à barres, vous accédez aux workloads affectés à cette stratégie dans la page Workloads.

- **Panneau d'aperçu de l'utilisation**

  Lorsque vous affichez tous les clusters, vous pouvez choisir de les afficher triés par nombre d'IOPS ou par débit (MB/s) le plus élevé.

  Lorsque vous consultez un seul cluster, vous pouvez choisir d'afficher les workloads de ce cluster classés selon le plus grand nombre d'IOPS ou le débit le plus élevé (MB/s).

Interpréter les messages de bannière de performance dans Active IQ Unified Manager

Unified Manager peut afficher des bannières sur la page Notifications (à partir de la cloche de notification) pour vous alerter de problèmes d'état concernant un cluster particulier.

Message de bannière	Description	Résolution
`No performance data is being collected from cluster` *`cluster_name`*`. Restart Unified Manager to correct this issue.`	Le service de collecte Unified Manager est arrêté et aucune donnée de performance n'est collectée depuis les clusters.	Redémarrez Unified Manager pour résoudre ce problème. Si cela ne résout pas le problème, contactez le support technique.
`More than x hour(s) of historical data is being collected from cluster` *`cluster_name`*`. Current data collections will start after all historical data is collected.`	Un cycle de collecte pour la continuité des données est actuellement en cours afin de récupérer les données de performance en dehors du cycle de collecte des performances du cluster en temps réel.	Aucune action n'est requise. Les données de performance actuelles seront collectées une fois le cycle de collecte des données de continuité terminé. Un cycle de collecte pour la continuité des données s'exécute lorsqu'un nouveau cluster est ajouté ou lorsque Unified Manager n'a pas pu collecter les données de performances actuelles pour une raison quelconque.

Modifiez l'intervalle de collecte des statistiques de performance dans Active IQ Unified Manager

L'intervalle de collecte par défaut des statistiques de performance est de 5 minutes. Vous pouvez le modifier à 10 ou 15 minutes si la collecte des données provenant de grands clusters ne se termine pas dans le délai par défaut. Ce paramètre affecte la collecte des statistiques de tous les clusters surveillés par cette instance d'Unified Manager.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

Le problème de la collecte des statistiques de performance qui ne se termine pas à temps est indiqué par les messages de bannière `Unable to consistently collect from cluster <cluster_name>` ou `Data collection is taking too long on cluster <cluster_name>`.

Vous ne devez modifier l'intervalle de collecte que si cela s'avère nécessaire en raison d'un problème lié à la collecte de statistiques. Ne modifiez pas ce paramètre pour toute autre raison.

> Modifier cette valeur par rapport au paramètre par défaut de 5 minutes peut affecter le nombre et la fréquence des événements de performance signalés par Unified Manager. Par exemple, les seuils de performance définis par le système déclenchent des événements lorsque la règle est dépassée pendant 30 minutes. Avec des collectes toutes les 5 minutes, la règle doit être dépassée pendant six collectes consécutives. Avec des collectes toutes les 15 minutes, la règle doit être dépassée pendant seulement deux périodes de collecte.

Un message en bas de la page de configuration du cluster indique l'intervalle actuel de collecte des données statistiques.

Étapes

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

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

2. Saisissez le numéro de l'option de menu intitulée **Configuration de l'intervalle d'interrogation des performances**, puis appuyez sur Entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe de l'utilisateur de maintenance.
4. Saisissez le numéro du nouvel intervalle d'interrogation que vous souhaitez définir, puis appuyez sur Entrée.

Si vous avez modifié l'intervalle de collecte d'Unified Manager à 10 ou 15 minutes et que vous disposez d'une connexion actuelle à un fournisseur de données externe (tel que Graphite), vous devez modifier l'intervalle de transmission du fournisseur de données afin qu'il soit égal ou supérieur à l'intervalle de collecte d'Unified Manager.

Dépanner les workloads à l'aide de l'analyseur de workload

Dépannez les charges de travail avec l'analyseur de charge de travail dans Active IQ Unified Manager

L'analyseur de workload permet de visualiser sur une seule page les principaux critères d'état et de performance d'un workload afin de faciliter le dépannage. En consultant tous les événements actuels et passés d'un workload, vous pouvez mieux comprendre pourquoi le workload rencontre actuellement un problème de performance ou de capacité.

Cet outil peut également vous aider à déterminer si le stockage est à l'origine des problèmes de performance d'une application ou si le problème est dû à un problème de réseau ou à un autre problème connexe.

Vous pouvez activer cette fonctionnalité à partir de différents endroits de l'interface utilisateur :

- À partir de la sélection Analyse du workload dans le menu de navigation de gauche
- Depuis la page de détails de l'événement en cliquant sur le bouton **Analyze Workload**
- Depuis n'importe quelle page d'inventaire des workloads (volume, LUN, workload, partage NFS ou partage SMB/CIFS), en cliquant sur l'icône Plus , puis sur **Analyser le workload**
- Depuis la page Machines virtuelles, cliquez sur le bouton **Analyser le workload** à partir de n'importe quel objet Datastore.

Lorsque vous lancez l'outil depuis le menu de navigation de gauche, vous pouvez saisir le nom de n'importe quel workload que vous souhaitez analyser et sélectionner la période pour laquelle vous souhaitez effectuer le dépannage. Lorsque vous lancez l'outil depuis l'une des pages d'inventaire des workloads ou des machines virtuelles, le nom du workload est renseigné automatiquement, et les données du workload sont présentées avec la période par défaut de 2 heures. Lorsque vous lancez l'outil depuis la page Event details, le nom du workload est renseigné automatiquement, et les données de 10 jours sont affichées.

Comprendre les données de l'analyseur de charge de travail dans Active IQ Unified Manager

La page de l'analyseur de workload affiche des informations sur les événements en cours susceptibles d'affecter le workload, des recommandations pour résoudre le problème à l'origine de l'événement, ainsi que des graphiques permettant d'analyser l'historique des performances et de la capacité.

En haut de la page, vous indiquez le nom du workload (volume ou LUN) que vous souhaitez analyser ainsi que la période pour laquelle vous souhaitez consulter les statistiques. Vous pouvez modifier cette période à tout moment si vous souhaitez afficher une période plus courte ou plus longue.

Les autres zones de la page affichent les résultats de l'analyse ainsi que les graphiques de performance et de capacité.

> Les graphiques de workload pour les LUN ne fournissent pas le même niveau de statistiques que ceux des volumes ; vous constaterez donc des différences lors de l'analyse de ces deux types de workloads.

- **Résumé des événements**

  Affiche un aperçu du nombre et des types d'événements survenus durant la période considérée. En cas

d'événements relevant de différents domaines d'impact (par exemple, performance et capacité), ces informations sont affichées afin que vous puissiez sélectionner les détails du type d'événement qui vous intéresse. Cliquez sur le type d'événement pour afficher la liste des noms d'événements.

S'il n'y a qu'un seul événement pendant la période concernée, une liste de recommandations pour résoudre le problème est fournie pour certains événements.

- **Chronologie de l'événement**

  Affiche tous les événements survenus pendant la période spécifiée. Survolez chaque événement avec votre curseur pour afficher son nom.

  Si vous avez accédé à cette page en cliquant sur le bouton **Analyze Workload** depuis la page de détails de l'événement, l'icône de l'événement sélectionné apparaît en plus grand afin que vous puissiez identifier l'événement.

- **Zone des graphiques de performance**

  Affiche des graphiques de latence, de débit (IOPS et Mo/s) et d'utilisation (pour le nœud et l'agrégat) en fonction de la période sélectionnée. Vous pouvez cliquer sur le lien « Afficher les détails des performances » pour afficher la page Performance Explorer du workload si vous souhaitez effectuer une analyse plus approfondie.

  - **Latency** affiche la latence du workload sur la période sélectionnée. Le graphique propose trois vues permettant de visualiser :
    - Latence **totale**
    - **Décomposition** de la latence (décomposée en lectures, écritures et autres processus)
    - Latence des **composants du cluster** (décomposée par composant du cluster)

Consultez "Composants du cluster et raisons pour lesquelles ils peuvent être en conflit" pour obtenir une description des composants du cluster affichés ici. **Débit affiche à la fois les IOPS et le débit en Mo/s du workload sur la période sélectionnée. Le graphique comporte quatre vues qui vous permettent d'afficher :** * le débit **Total * le débit Breakdown (ventilé par lectures, écritures et autres processus)** * le **Cloud Throughput** (les Mo/s utilisés pour écrire des données dans le cloud et en lire à partir du cloud, pour les workloads qui hiérarchisent de la capacité vers le cloud) *** les IOPS with Forecast (une prévision des valeurs supérieure et inférieure du débit en IOPS attendues sur la période) Ce graphique affiche également les paramètres de seuil de débit maximal et minimal de la qualité de service (QoS), s'ils sont configurés, afin que vous puissiez voir où le système peut limiter intentionnellement le débit à l'aide de règles QoS. Utilisation** affiche l'utilisation de l'agrégat et du nœud sur lesquels le workload s'exécute sur la période sélectionnée. Vous pouvez voir ici si votre agrégat ou votre nœud est surutilisé, ce qui peut entraîner une latence élevée. Lors de l'analyse des volumes FlexGroup, plusieurs nœuds et plusieurs agrégats sont répertoriés dans les graphiques d'utilisation.

- **Zone du graphique de capacité**

  Affiche des graphiques de la capacité des données et de la capacité Snapshot pour le workload au cours du dernier mois.

  Pour les volumes, vous pouvez cliquer sur le lien « Afficher les détails de capacité » afin d'afficher la page « Détails de l'état » du workload si vous souhaitez effectuer une analyse plus approfondie. Les LUN ne fournissent pas ce lien, car il n'existe pas de page « Détails de l'état » pour les LUN.

  - **Vue Capacité** affiche l'espace total disponible alloué au workload et l'espace logique utilisé (après toutes les optimisations NetApp).

- **Snapshot View** affiche l'espace total réservé aux copies Snapshot, ainsi que l'espace actuellement utilisé. Notez que les LUN ne fournissent pas de Snapshot View.
- **Cloud Tier View** affiche la capacité utilisée dans le tier de performance local et dans le tier cloud. Ces graphiques incluent une estimation du temps restant avant que la capacité soit pleine pour ce workload. 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 "almost full".

Comprendre quand utiliser l'analyseur de charge de travail dans Active IQ Unified Manager

Vous utiliseriez généralement l'analyseur de workload pour résoudre un problème de latence signalé par un utilisateur, pour analyser plus en détail un événement ou une alerte signalé, ou pour explorer un workload que vous constatez comme fonctionnant anormalement.

Si des utilisateurs vous signalent que l'application qu'ils utilisent fonctionne très lentement, vous pouvez consulter les graphiques de latence, de débit et d'utilisation du workload sur lequel l'application s'exécute pour voir si le stockage est la cause du problème de performance. Vous pouvez également utiliser le graphique de capacité pour vérifier si la capacité est faible, car un système ONTAP dont la capacité est utilisée à plus de 85 % peut entraîner des problèmes de performance. Ces graphiques vous aideront à déterminer si le problème est causé par le stockage, ou par le réseau ou un autre problème connexe.

Dans le cas où Unified Manager a généré un événement de performance et que vous souhaitez examiner plus en détail la cause du problème, vous pouvez lancer l'analyseur de workload depuis la page Détails de l'événement en cliquant sur le bouton **Analyze Workload** afin d'étudier certaines tendances de latence, de débit et de capacité pour le workload.

Si vous remarquez un workload qui semble fonctionner de manière anormale lors de la consultation de n'importe quelle page d'inventaire des workloads (volume, LUN, workload, partage NFS ou partage CIFS), vous pouvez cliquer sur l'icône Plus , puis sur **Analyze Workload** pour ouvrir la page Workload Analysis afin d'examiner plus en détail le workload.

Utilisez l'analyseur de charge de travail dans Active IQ Unified Manager

Il existe plusieurs façons de lancer l'analyseur de workload depuis l'interface utilisateur. Nous décrivons ici le lancement de l'outil depuis le volet de navigation de gauche.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Workload Analysis**.

   La page d'analyse de la charge de travail s'affiche.

2. Si vous connaissez le nom du workload, saisissez-le. Si vous n'êtes pas sûr du nom complet, saisissez au moins 3 caractères et le système affiche une liste de workloads correspondant à la chaîne.
3. Sélectionnez la plage horaire si vous souhaitez consulter les statistiques sur une période supérieure aux 2 heures par défaut, puis cliquez sur **Appliquer**.
4. Consultez la section Résumé pour voir les événements qui se sont produits pendant la période considérée.
5. Consultez les graphiques de performance et de capacité pour voir quand l'une des métriques est anormale et vérifiez si des événements correspondent à l'entrée anormale.

Surveillez les performances du cluster depuis la page de destination du cluster de performances

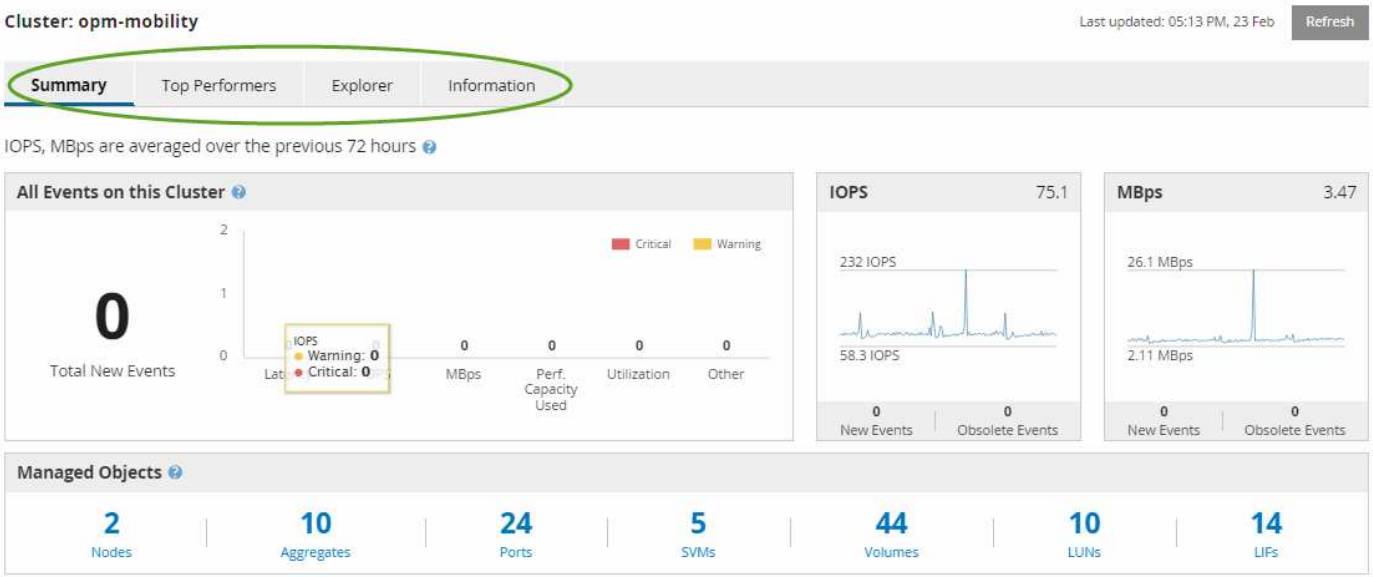
Surveillez les performances du cluster depuis la page d'accueil « Performances du cluster » dans Active IQ Unified Manager

La page d'accueil du cluster de performances affiche l'état général des performances d'un cluster sélectionné surveillé par une instance de Unified Manager. Cette page vous permet d'évaluer les performances globales d'un cluster spécifique et de repérer, localiser ou attribuer rapidement pour résolution tout événement spécifique au cluster qui est identifié.

Comprendre la page d'accueil du cluster de performance dans Active IQ Unified Manager

La page de destination du cluster de performances fournit une vue d'ensemble des performances de haut niveau d'un cluster sélectionné, en mettant l'accent sur l'état des performances des 10 principaux objets du cluster. Les problèmes de performances sont affichés en haut de la page, dans le panneau « Tous les événements de ce cluster ».

La page d'accueil du cluster de performances offre une vue d'ensemble de chaque cluster géré par une instance de Unified Manager. Cette page vous fournit des informations sur les événements et les performances, et vous permet de surveiller et de dépanner les clusters. L'image suivante illustre un exemple de la page d'accueil du cluster de performances pour le cluster nommé opm-mobility :



Le nombre d'événements figurant sur la page Résumé du cluster peut ne pas correspondre au nombre d'événements figurant sur la page Inventaire des événements de performance. En effet, la page Résumé du cluster peut afficher un événement dans chacune des barres Latence et Utilisation lorsque des stratégies de seuil combiné ont été enfreintes, alors que la page Inventaire des événements de performance n'affiche qu'un seul événement lorsqu'une stratégie combinée a été enfreinte.

Si un cluster a été retiré de la gestion par Unified Manager, le statut **Removed** s'affiche à droite

du nom du cluster en haut de la page.

Page d’accueil du cluster de performance

Consultez la page d’accueil du cluster de performance dans Active IQ Unified Manager

La page d’accueil du cluster de performances affiche un aperçu général de l’état des performances du cluster sélectionné. La page vous permet d’accéder aux détails complets de chaque compteur de performances des objets de stockage du cluster sélectionné.

La page d’accueil du cluster de performance comprend quatre onglets qui répartissent les détails du cluster en quatre domaines d’information :

- Page récapitulative
  - volet Événements du cluster
  - Graphiques de performance MB/s et IOPS
  - Volet des objets gérés
- page des meilleures performances
- page Explorer
- Page d’information

Page de résumé du cluster de performances

Consultez la page Résumé du cluster de performances dans Active IQ Unified Manager

La page « Résumé des performances du cluster » présente un récapitulatif des événements actifs, des performances IOPS et des performances en Mo/s du cluster. Elle indique également le nombre total d’objets de stockage dans le cluster.

Consultez le volet des événements de performance du cluster dans Active IQ Unified Manager

Le volet « Événements de performance du cluster » affiche les statistiques de performance et tous les événements actifs du cluster. Il est particulièrement utile pour surveiller vos clusters ainsi que toutes les performances et tous les événements qui leur sont liés.

Volet Tous les événements sur ce cluster

Le volet « Tous les événements sur ce cluster » affiche tous les événements de performance actifs du cluster des 72 dernières heures. Le nombre total d’événements actifs, affiché à l’extrême gauche, représente la somme de tous les événements nouveaux et acquittés pour tous les objets de stockage de ce cluster. Vous pouvez cliquer sur le lien « Nombre total d’événements actifs » pour accéder à la page « Inventaire des événements », qui est filtrée pour afficher ces événements.

Le graphique à barres « Nombre total d’événements actifs » du cluster affiche le nombre total d’événements actifs critiques et d’avertissement :

- Latence (totale pour les nœuds, les agrégats, les SVM, les volumes, les LUN et les namespaces)
- IOPS (total pour les clusters, les nœuds, les agrégats, les SVMs, les volumes, les LUNs et les namespace)
- Mo/s (total pour les clusters, les nœuds, les agrégats, les SVMs, les volumes, les LUNs, les namespaces, les ports et les LIFs)
- Capacité de performance utilisée (totale pour les nœuds et les agrégats)
- Utilisation (total pour les nœuds, les agrégats et les ports)
- Autre (taux de défaut du cache pour les volumes)

La liste contient les événements de performance actifs déclenchés par des politiques de seuil définies par l'utilisateur, des politiques de seuil définies par le système et des seuils dynamiques.

Les données du graphique (barres de comptage verticales) s'affichent en rouge () pour les événements critiques, et en jaune () pour les événements d'avertissement. Placez votre curseur sur chaque barre de comptage verticale pour afficher le type et le nombre réels d'événements. Vous pouvez cliquer sur **Refresh** pour mettre à jour les données du panneau de comptage.

Vous pouvez afficher ou masquer les événements critiques et d'avertissement dans le graphique de performances Total Active Events en cliquant sur les icônes **Critical** et **Warning** dans la légende. Si vous masquez certains types d'événements, les icônes de la légende apparaissent en gris.

Panneaux de compteur

Les panneaux de compteurs affichent l'activité du cluster et les événements de performances des 72 dernières heures, et comprennent les compteurs suivants :

- **Panneau du compteur d'IOPS**

  Les IOPS indiquent la vitesse de fonctionnement du cluster en nombre d'opérations d'entrée/sortie par seconde. Ce panneau de compteur fournit une vue d'ensemble générale de l'état des IOPS du cluster pour la période précédente de 72 heures. Vous pouvez placer votre curseur sur la courbe de tendance du graphique pour afficher la valeur des IOPS à un moment précis.

- **Panneau du compteur MB/s**

  MB/s indique la quantité de données transférées vers et depuis le cluster, exprimée en mégaoctets par seconde. Ce panneau de compteur fournit une vue d'ensemble de l'état MB/s du cluster au cours des 72 heures précédentes. Vous pouvez placer votre curseur sur la courbe de tendance du graphique pour afficher la valeur MB/s à un moment précis.

Le chiffre en haut à droite du graphique, dans la barre grise, correspond à la valeur moyenne des dernières 72 heures. Les chiffres affichés en bas et en haut de la courbe de tendance représentent les valeurs minimale et maximale des dernières 72 heures. La barre grise située sous le graphique indique le nombre d'événements actifs (nouveaux et acquittés) et d'événements obsolètes des dernières 72 heures.

Les panneaux de comptage contiennent deux types d'événements :

- **Actif**

  Indique que l'événement de performance est actuellement actif (nouveau ou confirmé). Le problème à l'origine de l'événement ne s'est pas corrigé ou n'a pas été résolu. Le compteur de performance de l'objet de stockage reste supérieur au seuil de performance.

- **Obsolète**

Indique que l'événement n'est plus actif. Le problème à l'origine de l'événement s'est résolu de lui-même ou a été résolu. Le compteur de performances de l'objet de stockage ne dépasse plus le seuil de performance.

Pour les **Événements actifs**, s'il n'y a qu'un seul événement, vous pouvez placer votre curseur sur l'icône de l'événement et cliquer sur son numéro pour accéder à la page Détails de l'événement appropriée. S'il y a plusieurs événements, vous pouvez cliquer sur **Voir tous les événements** pour afficher la page d'inventaire des événements, qui est filtrée pour afficher tous les événements correspondant au type de compteur d'objet sélectionné.

Consultez le volet Objets gérés dans Active IQ Unified Manager

Le volet Objets gérés de l'onglet Résumé des performances offre une vue d'ensemble des types et du nombre d'objets de stockage du cluster. Ce volet permet de suivre l'état des objets dans chaque cluster.

Le nombre d'objets gérés correspond aux données à un instant donné de la dernière période de collecte. De nouveaux objets sont découverts toutes les 15 minutes.

Le fait de cliquer sur le numéro lié pour tout type d'objet affiche la page d'inventaire des performances des objets pour ce type d'objet. La page d'inventaire des objets est filtrée pour n'afficher que les objets de ce cluster.

Les objets gérés sont :

- **Nœuds**

  Un système physique au sein d'un cluster.

- **Agrégats**

  Un ensemble de plusieurs groupes RAID (Redundant Array of Independent Disks) pouvant être gérés comme une seule unité pour la protection et le provisionnement.

- **Ports**

  Un point de connexion physique sur les nœuds utilisé pour connecter d'autres appareils sur un réseau.

- **Machines virtuelles de stockage**

  Une machine virtuelle fournissant un accès réseau via des adresses réseau uniques. Une SVM peut fournir des données à partir d'un namespace distinct et être administrée séparément du reste du cluster.

- **Volumes**

  Entité logique contenant des données utilisateur accessibles via un ou plusieurs protocoles d'accès pris en charge. Le nombre comprend à la fois les volumes FlexVol et les volumes FlexGroup ; il n'inclut pas les constituants FlexGroup.

- **LUN**

  L'identifiant d'une unité logique Fibre Channel (FC) ou d'une unité logique iSCSI. Une unité logique correspond généralement à un volume de stockage et est représentée au sein d'un système d'exploitation sous la forme d'un périphérique.

- **Interfaces réseau**

  Une interface réseau logique représentant un point d'accès réseau à un nœud. Ce nombre inclut tous les types d'interfaces.

Affichez la page Top Performers dans Active IQ Unified Manager

La page « Meilleures performances » affiche les objets de stockage présentant les performances les plus élevées ou les plus faibles, selon le compteur de performances que vous sélectionnez. Par exemple, dans la catégorie « Machines virtuelles de stockage », vous pouvez afficher les SVM qui ont le plus grand nombre d'IOPS, la latence la plus élevée ou le débit en MB/s le plus faible. Cette page indique également si certains des éléments les plus performants ont des événements de performances actifs (New ou Acknowledged).

La page « Meilleures performances » affiche un maximum de 10 de chaque objet. Notez que l'objet « Volume » inclut à la fois les volumes FlexVol et les volumes FlexGroup.

- **Plage de temps**

  Vous pouvez sélectionner une période pour afficher les objets les plus performants ; la période sélectionnée s'applique à tous les objets de stockage. Périodes disponibles :

  - Dernière heure
  - 24 dernières heures
  - Dernières 72 heures (par défaut)
  - 7 derniers jours
- **Métrique**

  Cliquez sur le menu **Métrique** pour sélectionner un autre compteur. Les options de compteur sont spécifiques à chaque type d'objet. Par exemple, pour l'objet **Volumes**, les compteurs disponibles sont **Latence**, **IOPS** et **Mo/s**. La modification du compteur recharge les données du panneau avec les éléments les plus performants selon le compteur sélectionné.

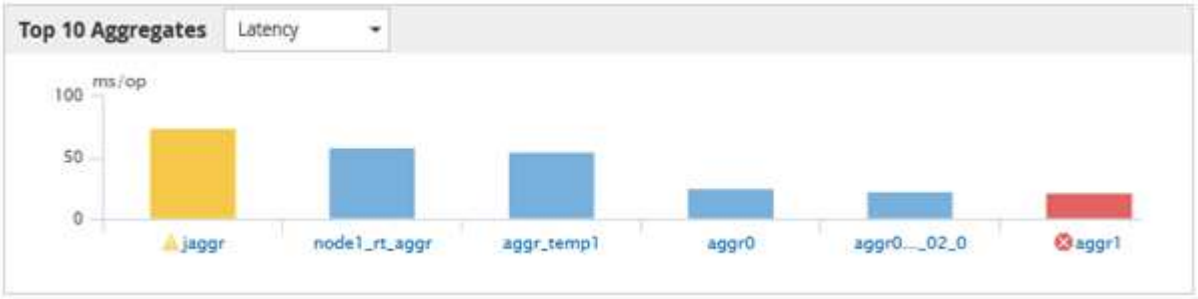
  Compteurs disponibles :

  - Latence
  - Op E/S par sec
  - Mo/s
  - Capacité de performance utilisée (pour les nœuds et les agrégats)
  - Utilisation (pour les nœuds et les agrégats)
- **Trier**

  Cliquez sur le menu **Trier** pour sélectionner un tri ascendant ou descendant pour l'objet et le compteur sélectionnés. Les options sont **Du plus élevé au plus faible** et **Du plus faible au plus élevé**. Ces options vous permettent d'afficher les objets présentant les performances les plus élevées ou les plus faibles.

- **Barre de compteur**

La barre de compteur du graphique affiche les statistiques de performance pour chaque objet, représenté par une barre pour cet élément. Les graphiques à barres sont codés par couleur. Si le compteur ne dépasse pas un seuil de performance, la barre de compteur s'affiche en bleu. Si un dépassement de seuil est actif (événement nouveau ou reconnu), la barre s'affiche dans la couleur de l'événement : les événements d'avertissement s'affichent en jaune ( ), et les événements critiques s'affichent en rouge ( ). Les dépassements de seuil sont en outre indiqués par des icônes d'indicateur de gravité pour les événements d'avertissement et les événements critiques.



Pour chaque graphique, l'axe des abscisses affiche les objets les plus performants pour le type d'objet sélectionné. L'axe des ordonnées affiche les unités applicables au compteur sélectionné. En cliquant sur le lien du nom de l'objet sous chaque élément du graphique à barres verticales, vous accédez à la page Performance Landing de l'objet sélectionné.

- **Indicateur de gravité de l'événement**

  L'icône d'indicateur **Événement de gravité** s'affiche à gauche du nom d'un objet pour les événements critiques actifs ( ) ou d'avertissement actifs ( ) dans les graphiques des meilleurs performeurs. Cliquez sur l'icône d'indicateur **Événement de gravité** pour afficher :

  - **Un événement**

    Permet d'accéder à la page de détails de cet événement.

  - **Deux événements ou plus**

    Permet d'accéder à la page d'inventaire des événements, filtrée pour afficher tous les événements relatifs à l'objet sélectionné.

- **Bouton Exporter**

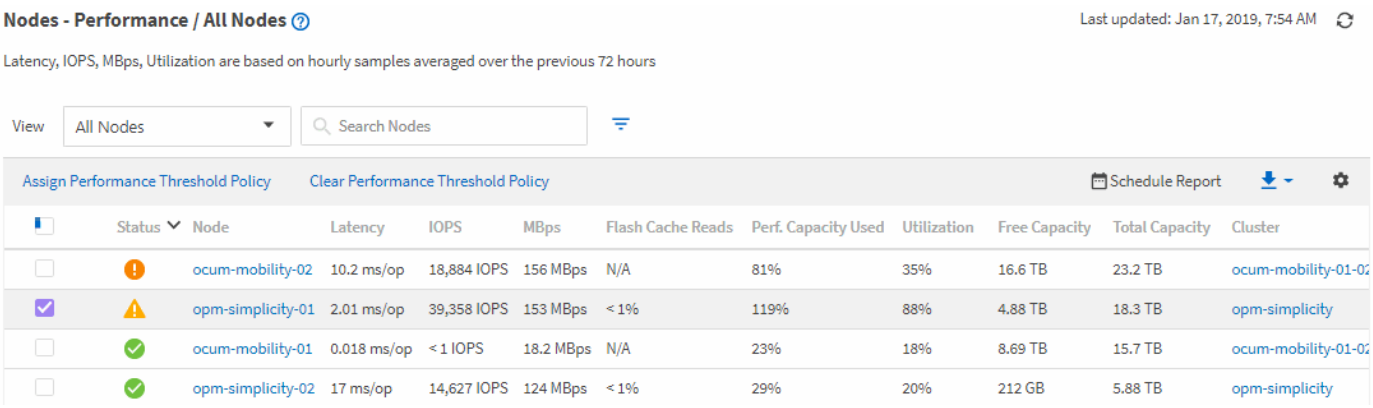
  Crée un `.csv` fichier contenant les données affichées dans la barre de compteur. Vous pouvez choisir de créer le fichier pour le cluster que vous consultez ou pour tous les clusters du centre de données.

Surveillez les performances à l'aide des pages d'inventaire des performances

Surveillez les performances des objets à l'aide des pages d'inventaire des performances dans Active IQ Unified Manager

Les pages d'inventaire des objets affichent les informations de performance, les événements de performance et l'état de santé de tous les objets d'une catégorie de type d'objet. Vous obtenez ainsi un aperçu rapide de l'état des performances de chaque objet au sein d'un cluster, par exemple pour tous les nœuds ou tous les volumes.

Les pages d'inventaire des objets offrent une vue d'ensemble de l'état des objets, vous permettant d'évaluer les performances globales de tous les objets et de comparer les données de performance des objets. Vous pouvez affiner le contenu des pages d'inventaire des objets en effectuant des recherches et en appliquant un tri et des filtres. Cela est utile lors de la surveillance et de la gestion des performances des objets, car cela vous permet de localiser rapidement les objets présentant des problèmes de performances et de commencer le processus de dépannage.



Par défaut, les objets des pages d'inventaire des performances sont triés en fonction de la criticité des performances des objets. Les objets présentant de nouveaux événements de performance critiques apparaissent en premier, suivis des objets présentant des événements d'avertissement. Cela permet d'identifier immédiatement les problèmes qui doivent être résolus. Toutes les données de performance sont basées sur une moyenne sur 72 heures.

Vous pouvez facilement accéder à une page de détails d'objet à partir de la page d'inventaire des performances des objets en cliquant sur le nom de l'objet dans la colonne des noms d'objet. Par exemple, sur la page d'inventaire Performance/All Nodes, vous cliqueriez sur un objet nœud dans la colonne **Nodes**. La page de détails de l'objet fournit des informations détaillées et approfondies sur l'objet sélectionné, notamment une comparaison côte à côte des événements actifs.

Consultez les pages d'inventaire des performances pour tous les objets de stockage dans Active IQ Unified Manager

Les pages d'inventaire des performances permettent de consulter un résumé des informations de performance de chaque objet de stockage disponible, comme les clusters, les agrégats, les volumes, etc. Vous pouvez accéder aux pages de détail des objets de performance pour consulter des informations détaillées sur un objet particulier.

Par défaut, les objets affichés sur les pages de visualisation sont triés selon la criticité des événements. Les objets présentant des événements critiques apparaissent en premier, suivis de ceux présentant des événements d'avertissement. Ceci permet d'identifier immédiatement les problèmes à résoudre.

Vous pouvez exporter les données de ces pages vers un fichier de valeurs séparées par des virgules (`.csv`), un fichier Microsoft Excel (`.xlsx`), ou un document (`.pdf`) en utilisant le bouton **Reports**, puis utiliser les données exportées pour créer des rapports. De plus, vous pouvez personnaliser la page, puis planifier la création et l'envoi réguliers d'un rapport par courriel en utilisant le bouton **Scheduled Reports**.

Tous les champs sur ces pages peuvent être utilisés dans les vues personnalisées et dans les rapports. Certains champs sont liés à des pages associées, ce qui permet un affichage plus détaillé.

Performances: Vue de tous les clusters

La vue « Performances : Tous les clusters » présente 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 surveiller les performances de vos clusters et de résoudre les problèmes de performance et les événements de seuil.

Vous pouvez attribuer des politiques de seuil de performance à n'importe quel objet des pages d'inventaire des objets, ou en supprimer, à l'aide des boutons **Attribuer une politique de seuil de performance** et **Supprimer une politique de seuil de performance**.

Voici quelques champs importants de la vue Performance : All Clusters.

- FQDN du cluster : le nom de domaine complet (FQDN) du cluster.
- IOPS : le nombre d'opérations d'entrée/sortie par seconde sur le cluster.
- MB/s : Le débit sur le cluster, mesuré en Mio par seconde.
- Champs de capacité : capacité libre et capacité totale en GiB.
- Nom de l'hôte ou adresse IP : nom de l'hôte ou adresse IP (IPv4 ou IPv6) de la LIF de gestion du cluster.
- Version du système d'exploitation : version du logiciel ONTAP installée sur le cluster.

> Si différentes versions du logiciel ONTAP sont installées sur les nœuds du cluster, le numéro de version le plus bas est indiqué. Vous pouvez afficher la version de ONTAP installée sur chaque nœud dans la vue « Performances : Tous les nœuds ».

- Politique de seuil : la ou les politiques de seuil de performance définies par l'utilisateur et actives sur cet objet de stockage. Placez votre curseur sur les noms de politique contenant des points de suspension (…) pour afficher le nom complet de la politique ou la liste des politiques attribuées. Les boutons « Attribuer une politique de seuil de performance » et « Supprimer la politique de seuil de performance » restent désactivés tant que vous n'avez pas sélectionné un ou plusieurs objets en cochant les cases situées à l'extrême gauche.

Performance : vue de tous les volumes

La vue « Performances : Tous les volumes » présente un aperçu des événements de performance, des données de compteur et des informations de configuration de chaque volume FlexVol et volume FlexGroup surveillé par une instance d'Unified Manager. Vous pouvez ainsi surveiller rapidement les performances de vos volumes et résoudre les problèmes de performance et les événements de seuil.

Si vous souhaitez analyser la latence et le débit d'un objet spécifique, cliquez sur le bouton Plus d'options ⋮, puis sur **Analyze Workload**, et vous pourrez afficher les graphiques de performances et de capacité sur la page Analyse du workload. Vous pouvez afficher les détails dans System Manager, à condition de disposer d'identifiants valides pour System Manager.

> Pour les volumes de protection des données (DP), seules les valeurs des compteurs relatives au trafic généré par l'utilisateur sont affichées. Les volumes racine ne sont pas affichés sur cette page.

Voici quelques champs importants de la vue Performances : Tous les volumes.

- Style : soit FlexVol, soit FlexGroup.
- Latence : pour les volumes FlexVol, il s'agit du temps de réponse moyen du volume pour toutes les

requêtes d'E/S, exprimé en millisecondes par opération. Pour les volumes FlexGroup, il s'agit de la latence moyenne de tous les volumes qui les composent.

- IOPS/To : nombre d'opérations d'entrée/sortie traitées par seconde en fonction de l'espace total consommé par le workload, en téraoctets. Ce compteur mesure le niveau de performance pouvant être fourni par une quantité donnée de capacité de stockage.
- IOPS : Pour les volumes FlexVol, il s'agit du nombre d'opérations d'entrée/sortie par seconde pour le volume. Pour les volumes FlexGroup, il s'agit de la somme des IOPS de tous les volumes constituants.
- Mo/s : Pour les volumes FlexVol, il s'agit du débit sur le volume, mesuré en mégaoctets par seconde. Pour les volumes FlexGroup, il s'agit de la somme des Mo/s de tous les volumes constitutifs.
- Champs de capacité : capacité libre et capacité totale en GiB.

Consultez les liens suivants pour plus d'informations :

- "Attribution de stratégies de seuil de performance aux objets de stockage"
- "Suppression des politiques de seuil de performance des objets de stockage"
- "Types de workloads surveillés par Unified Manager"
- "Affichage des paramètres du groupe de règles QoS appliqués à des volumes ou LUN spécifiques"
- "Comprendre les recommandations de Unified Manager concernant la hiérarchisation des données vers le cloud"
- "Affichage des graphiques de performance pour comparer les volumes ou les LUN appartenant au même groupe de stratégie QoS"

Performances: Vue de tous les agrégats

La vue « Performances : Tous les agrégats » présente un aperçu des événements de performance, des données et des informations de configuration de chaque agrégat surveillé par une instance d'Unified Manager. Cette page vous permet de surveiller les performances de vos agrégats et de résoudre les problèmes de performance et les événements de seuil.

Voici quelques champs importants dans la vue Performance: All Aggregates.

- Type : Le type d'agrégat :
  - disque dur
  - Hybride. Combine des disques durs et des SSD, mais Flash Pool n'a pas été activé.
  - Hybride (Flash Pool). Combine des HDD et des SSD, et Flash Pool est activé.
  - SSD
  - SSD (FabricPool). Associe des disques SSD et un niveau cloud
  - Disque dur (FabricPool). Associe des disques durs et un niveau cloud
  - VMDisk (SDS). Disques virtuels au sein d'une machine virtuelle
  - VMDisk (FabricPool). Associe des disques virtuels et un niveau cloud
  - LUN
- Rapports de données inactives : indique si la fonctionnalité de rapport de données inactives est activée ou désactivée pour cet agrégat. Lorsqu'elle est activée, les volumes de cet agrégat affichent la quantité de données froides dans la vue « Performances : Tous les volumes ». La valeur de ce champ est « N/A » si la version d'ONTAP ne prend pas en charge les rapports de données inactives.

- Politique de seuil : la ou les politiques de seuil de performance définies par l'utilisateur et actives sur cet objet de stockage. Placez votre curseur sur les noms de politique contenant des points de suspension (…) pour afficher le nom complet de la politique ou la liste des noms de politique attribués. Les boutons « Attribuer une politique de seuil de performance » et « Effacer la politique de seuil de performance » restent désactivés tant que vous n'avez pas sélectionné un ou plusieurs objets en cochant les cases situées à l'extrême gauche. Consultez les liens suivants pour plus d'informations :
- "Attribution de stratégies de seuil de performance aux objets de stockage"
- "Suppression des politiques de seuil de performance des objets de stockage"

Performances: vue de tous les nœuds

La vue « Performances : Tous les nœuds » présente un aperçu des événements de performance, des données et des informations de configuration de chaque nœud surveillé par une instance d'Unified Manager. Vous pouvez ainsi suivre rapidement les performances de vos nœuds et résoudre les problèmes de performance et les dépassements de seuil.

Le rapport « Lectures Flash Cache » indique le pourcentage d'opérations de lecture sur le nœud qui sont prises en charge par le cache, au lieu d'être lues sur le disque. Les données Flash Cache ne sont affichées que pour les nœuds, et uniquement lorsqu'un module Flash Cache est installé sur le nœud.

Dans le menu **Rapports**, l'option **Rapport d'inventaire matériel** est 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 contenant une liste complète des informations sur les clusters et les nœuds, telles que les numéros de modèle et de série du matériel, les types et le nombre de disques, les licences installées, etc. Cette fonctionnalité de génération de rapports est utile pour le renouvellement des contrats dans des sites sécurisés qui ne sont pas connectés à la plateforme NetApp Active IQ. Vous pouvez attribuer des politiques de seuil de performance à n'importe quel objet des pages d'inventaire des objets, ou en supprimer, à l'aide des boutons **Attribuer une politique de seuil de performance** et **Supprimer une politique de seuil de performance**.

Consultez les liens suivants pour plus d'informations :

- "Attribution de stratégies de seuil de performance aux objets de stockage"
- "Suppression des politiques de seuil de performance des objets de stockage"
- "Génération d'un rapport d'inventaire du matériel pour le renouvellement du contrat"

Performances : vue de toutes les machines virtuelles de stockage

La vue « Performances : Toutes les machines virtuelles de stockage » présente un aperçu des événements de performance, des données et des informations de configuration de chaque machine virtuelle de stockage (SVM) surveillée par une instance d'Unified Manager. Vous pouvez ainsi surveiller rapidement les performances de vos SVM et résoudre les problèmes de performance et les dépassements de seuil. Le champ « Latence » de cette page indique le temps de réponse moyen pour toutes les requêtes d'E/S, exprimé en millisecondes par opération.

Les SVM listées sur cette page incluent uniquement les SVM de données et de cluster. Unified Manager n'utilise ni n'affiche les SVM d'administration ou de nœud.

Consultez les liens suivants pour plus d'informations :

- "Attribution de stratégies de seuil de performance aux objets de stockage"

- "Suppression des politiques de seuil de performance des objets de stockage"

Performances : vue de toutes les LUN

La vue « Performances : toutes les LUN » affiche un aperçu des événements de performance, des données et des informations de configuration de chaque LUN surveillé par une instance de Unified Manager. Vous pouvez ainsi surveiller rapidement les performances de vos LUN et résoudre les problèmes de performance et les événements de dépassement de seuil.

Si vous souhaitez analyser la latence et le débit d'un objet spécifique, cliquez sur l'icône Plus ⋮, puis sur **Analyze Workload** et vous pourrez consulter les graphiques de performance et de capacité sur la page **Workload Analysis**.

Consultez les liens suivants pour plus d'informations :

- "Surveillance des LUN dans le cadre d'une relation de groupe de cohérence"
- "Provisionnement des LUN"
- "Attribution de stratégies de seuil de performance aux objets de stockage"
- "Suppression des politiques de seuil de performance des objets de stockage"
- "Affichage des volumes ou LUN appartenant au même groupe de stratégie QoS".
- "Affichage des paramètres du groupe de règles 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 « Performances : Tous les espaces de noms NVMe » présente un aperçu des événements de performance, des données et des informations de configuration de chaque espace de noms NVMe surveillé par une instance de Unified Manager. Vous pouvez ainsi contrôler rapidement les performances et l'état de vos espaces de noms, et résoudre les problèmes ainsi que les événements de seuil.

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 n'a plus d'espace disponible.

Consultez les liens suivants pour plus d'informations :

- "Attribution de stratégies de seuil de performance aux objets de stockage"
- "Suppression des politiques de seuil de performance des objets de stockage"

Performance : vue de toutes les interfaces réseau

La vue « Performances : Toutes les interfaces réseau » présente un aperçu des événements de performance, des données et des informations de configuration de chaque interface réseau (LIF) surveillée par cette instance d'Unified Manager. Cette page vous permet de surveiller rapidement les performances de vos interfaces et de résoudre les problèmes de performance et les dépassements de seuil. Voici quelques champs importants de la vue « Performances : Toutes les interfaces réseau ».

- IOPS : opérations d'entrée/sortie par seconde. La valeur IOPS ne s'applique pas aux LIF NFS et aux LIF CIFS, et s'affiche sous la forme N/A pour ces types.
- Latence : le temps de réponse moyen pour toutes les requêtes d'E/S, exprimé en millisecondes par

opération. La latence ne s'applique pas aux LIF NFS et aux LIF CIFS, et s'affiche comme N/A pour ces types.

- Emplacement principal : l'emplacement principal de l'interface, affiché sous la forme du nom du nœud et du nom du port, séparés par deux points (:). Si l'emplacement est affiché avec des points de suspension (…), vous pouvez placer votre curseur sur le nom de l'emplacement pour afficher l'emplacement complet.
- Emplacement actuel : emplacement actuel de l'interface, affiché sous la forme du nom du nœud et du nom du port, séparés par deux points (:). Si l'emplacement est affiché avec des points de suspension (…), vous pouvez placer votre curseur sur le nom de l'emplacement pour afficher l'emplacement complet.
- Rôle : rôle de l'interface : données, cluster, gestion des nœuds ou intercluster.

Les interfaces répertoriées sur cette page comprennent les LIF de données, les LIF de cluster, les LIF de gestion de nœud et les LIF intercluster. Unified Manager n'utilise ni n'affiche les LIF système.

Performances : Vue de tous les ports

La vue « Performance : All Ports » affiche une vue d'ensemble des événements de performance, des données et des informations de configuration de chaque port surveillé par une instance de Unified Manager. Cela vous permet de surveiller rapidement les performances de vos ports et de résoudre les problèmes de performance et les événements de seuil. Pour le rôle d'un port, la fonction du port réseau affichée est Data ou Cluster. Les ports FCP ne peuvent pas avoir de rôle, et le rôle est affiché comme N/A.

Les valeurs des compteurs de performance sont affichées uniquement pour les ports physiques. Elles ne sont pas affichées pour les VLAN ou les groupes d'interfaces.

Consultez les liens suivants pour plus d'informations :

- "Attribution de stratégies de seuil de performance aux objets de stockage"
- "Suppression des politiques de seuil de performance des objets de stockage"

Performances: vue des groupes de stratégies QoS

La vue Groupes de stratégies QoS affiche les groupes de stratégies QoS disponibles sur les clusters surveillés par Unified Manager. Cela inclut les stratégies QoS traditionnelles, les stratégies QoS adaptatives et les stratégies QoS attribuées à l'aide de Performance Service Levels.

Voici quelques champs importants de la vue « Performances : Groupes de stratégies QoS ».

- Groupe de stratégies QoS : Le nom du groupe de stratégies QoS. Pour les stratégies NetApp Service Level Manager (NSLM) 1.3 qui ont été importées dans Unified Manager 9.7 ou version ultérieure, le nom affiché ici inclut le nom du SVM et d'autres informations qui ne figurent pas dans le nom lorsque le Performance Service Level a été défini dans NSLM. Par exemple, le nom « NSLM_vs6_Performance_2_0 » signifie qu'il s'agit de la stratégie PSL « Performance » définie par le système NSLM et créée sur le SVM « vs6 » avec une latence attendue de « 2 ms/op ».
- SVM : la machine virtuelle de stockage (SVM) à laquelle appartient le groupe de règles QoS. Vous pouvez cliquer sur le nom de la machine virtuelle de stockage pour accéder à sa page de détails. Notez que ce champ est vide si la règle QoS a été créée sur la machine virtuelle de stockage Admin, car ce type de machine virtuelle de stockage représente le cluster.
- Débit minimal : débit minimal, en IOPS, que le groupe de règles garantit de fournir. Pour les stratégies adaptatives, il s'agit du nombre minimal d'IOPS attendus par To alloué au volume ou au LUN, en fonction de la taille allouée à l'objet de stockage.

- Débit maximal : débit, exprimé en IOPS et/ou Mo/s, que le groupe de stratégies ne doit pas dépasser. Si ce champ est vide, le débit maximal défini dans ONTAP est infini. Pour les stratégies adaptatives, il s'agit du nombre maximal (de pointe) d'IOPS possibles par To alloué au volume ou au LUN, calculé en fonction de la taille allouée ou de la taille utilisée de l'objet de stockage.
- IOPS minimales absolues : pour les politiques adaptatives, il s'agit de la valeur minimale absolue d'IOPS utilisée comme valeur de remplacement lorsque les IOPS attendues sont inférieures à cette valeur.
- Taille des blocs : taille des blocs spécifiée pour la politique adaptative de QoS.
- Allocation minimale : indique si l'« espace alloué » ou l'« espace utilisé » sert à déterminer le débit maximal (pic) en IOPS.
- Latence attendue : Latence moyenne attendue pour les opérations d'entrée/sortie de stockage.
- Partagé : Pour les politiques QoS traditionnelles, indique si les valeurs de débit définies dans le groupe de politiques sont partagées entre plusieurs objets.
- Objets associés : nombre de workloads affectés au groupe de stratégie QoS. Cliquez sur le bouton Développer ( ) à côté du nom du groupe de stratégie QoS pour afficher plus de détails sur le groupe de stratégie.
- Capacité allouée : quantité d'espace actuellement utilisée par les objets appartenant au groupe de stratégie QoS.
- Objets associés : nombre de workloads affectés au groupe de stratégies QoS, répartis entre volumes et LUN. Vous pouvez cliquer sur le nombre pour accéder à une page contenant des informations détaillées sur les volumes ou LUN sélectionnés.

Pour plus d'informations, consultez les rubriques sous "Gestion des performances à l'aide des informations sur les groupes de règles QoS".

Affiner le contenu de la page d'inventaire des performances

Affinez le contenu de la page d'inventaire des performances dans Active IQ Unified Manager

Les pages d'inventaire des objets de performance contiennent des outils pour vous aider à affiner le contenu des données d'inventaire des objets, ce qui vous permet de localiser rapidement et facilement des données spécifiques.

Les pages d'inventaire des objets de performance contiennent des informations très volumineuses, souvent réparties sur plusieurs pages. Ces données complètes sont idéales pour le suivi et l'amélioration des performances ; cependant, la recherche de données spécifiques nécessite des outils permettant de les localiser rapidement. C'est pourquoi les pages d'inventaire des objets de performance intègrent des fonctionnalités de recherche, de tri et de filtrage. De plus, la recherche et le filtrage peuvent être combinés pour affiner vos résultats.

Recherche sur les pages de performances de l'inventaire des objets dans Active IQ Unified Manager

Vous pouvez rechercher des chaînes sur les pages de performances de l'inventaire des objets. Utilisez le champ **Rechercher** situé en haut à droite de la page pour localiser rapidement des données par nom d'objet ou par nom de stratégie. Cela vous permet de localiser rapidement des objets spécifiques et leurs données associées, ou de localiser rapidement des stratégies et d'afficher les données des objets de stratégie associés.

Étape

1. Choisissez l’une des options suivantes, en fonction de vos critères de recherche :

Pour localiser cela…	Tapez ceci…
Un objet spécifique	Saisissez le nom de l’objet dans le champ **Rechercher**, puis cliquez sur **Rechercher**. L’objet recherché et ses données associées s’affichent.
Une politique de seuil de performance définie par l’utilisateur	Saisissez tout ou partie du nom de la politique dans le champ **Rechercher**, puis cliquez sur **Rechercher**. Les objets associés à la politique recherchée s’affichent.

Triez les données sur les pages de performances de l’inventaire des objets dans Active IQ Unified Manager

Vous pouvez trier toutes les données des pages « Performances de l’inventaire des objets » selon n’importe quelle colonne, par ordre croissant ou décroissant. Cela vous permet de localiser rapidement les données d’inventaire des objets, ce qui est utile pour analyser les performances ou entamer 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 en forme de flèche indiquant le sens du tri à droite du nom. Une flèche vers le haut indique un ordre croissant ; une flèche vers le bas indique un ordre décroissant. Par défaut, le tri s’effectue par **Status** (criticité de l’événement) en ordre décroissant, les événements de performance les plus critiques étant répertoriés en premier.

Étape

1. Vous pouvez cliquer sur le nom d’une colonne pour basculer l’ordre de tri de la colonne en ordre croissant ou décroissant.

   Le contenu de la page « Performances de l’inventaire des objets » est trié par ordre croissant ou décroissant, en fonction de la colonne sélectionnée.

Filtrer les données sur les pages de performance de l’inventaire des objets dans Active IQ Unified Manager

Vous pouvez filtrer les données dans les pages « Performances de l’inventaire des objets » pour localiser rapidement des 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 de filtrage pour personnaliser l’affichage en grille selon vos préférences. Les options de filtrage disponibles dépendent du type d’objet affiché dans la grille. Si des filtres sont actuellement appliqués, leur nombre s’affiche à droite du bouton Filtrer.

Trois types de paramètres de filtrage sont pris en charge.

Paramètre	Validation
Chaîne (texte)	Les opérateurs sont **contient**, **commence par**, **se termine par** et **ne contient pas**.
Nombre maximum	Les opérateurs sont **supérieur à**, **inférieur à**, **au cours des derniers** et **entre**.
Énumération (texte)	Les opérateurs sont **is** et **is not**.

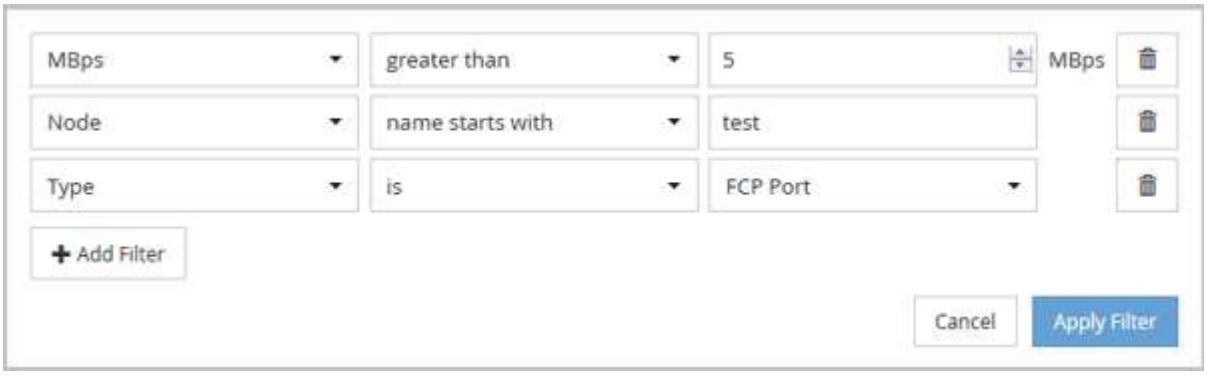
Les champs Colonne, Opérateur et Valeur sont obligatoires pour chaque filtre ; les filtres disponibles correspondent aux colonnes filtrables de la page actuelle. Vous pouvez appliquer jusqu'à quatre filtres. Les résultats filtrés sont basés sur la combinaison des paramètres de filtrage. Les résultats filtrés s'appliquent à toutes les pages de votre recherche filtrée, et pas seulement à la page actuellement affichée.

Vous pouvez ajouter des filtres à l'aide du panneau de filtrage.

1. En haut de la page, cliquez sur le bouton **Filtrer**. Le panneau de filtrage s'affiche.
2. Cliquez sur la liste déroulante de gauche et sélectionnez un objet; par exemple, *Cluster*, ou un compteur de performances.
3. Cliquez sur la liste déroulante centrale et sélectionnez l'opérateur que vous souhaitez utiliser.
4. Dans la dernière liste, sélectionnez ou saisissez une valeur pour compléter le filtre pour cet objet.
5. Pour ajouter un autre filtre, cliquez sur **+Add Filter**. Un champ de filtre supplémentaire s'affiche. Complétez ce filtre en suivant la procédure décrite dans les étapes précédentes. Notez qu'après l'ajout de votre quatrième filtre, le bouton **+Add Filter** 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 de filtrage pour supprimer des filtres individuels en cliquant sur l'icône de la 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 de filtrage avec trois filtres. Le bouton **+Ajouter un filtre** s'affiche lorsque vous avez moins du maximum de quatre filtres.



Après avoir cliqué sur **Appliquer le filtre**, le panneau de filtrage se ferme, applique vos filtres et affiche le nombre de filtres appliqués (3).

Consultez les recommandations d'Active IQ Unified Manager concernant la hiérarchisation des données vers le cloud

La vue « Performances : Tous les volumes » affiche des informations relatives à la taille des données utilisateur stockées sur le volume qui est inactif (froid). Dans certains cas, Unified Manager identifie certains volumes pour lesquels il serait avantageux de hiérarchiser les données inactives vers le niveau cloud (fournisseur de cloud ou StorageGRID) d'un agrégat compatible avec FabricPool.

> FabricPool a été introduit dans ONTAP 9.2. Par conséquent, si vous utilisez une version du logiciel ONTAP antérieure à 9.2, la recommandation de Unified Manager de hiérarchiser les données exige une mise à niveau de votre logiciel ONTAP. De plus, la stratégie de hiérarchisation **`auto`** a été introduite dans ONTAP 9.4, et la stratégie de hiérarchisation **`all`** a été introduite dans ONTAP 9.6. Par conséquent, si la recommandation consiste à utiliser la stratégie de hiérarchisation auto, vous devez effectuer une mise à niveau vers ONTAP 9.4 ou une version ultérieure.

Les trois champs suivants de la vue Performance : All Volumes fournissent des informations indiquant si vous pouvez améliorer l'utilisation des disques de votre système de stockage et gagner de l'espace sur le niveau de performance en déplaçant les données inactives vers le niveau cloud.

- **Stratégie de tiering**

  La politique de hiérarchisation détermine si les données du volume restent sur le niveau de performance ou si certaines données sont déplacées du niveau de performance vers le niveau cloud.

  La valeur de ce champ indique la stratégie de hiérarchisation définie sur le volume, même si le volume ne réside pas actuellement sur un agrégat FabricPool. La stratégie de hiérarchisation ne prend effet que lorsque le volume se trouve sur un agrégat FabricPool.

- **Données froides**

  Les données froides indiquent la taille des données utilisateur inactives (froides) stockées sur le volume.

  Cette valeur s'affiche ici uniquement lorsque vous utilisez ONTAP 9.4 ou une version ultérieure, car cela exige que l'agrégat sur lequel le volume est déployé ait le **`inactive data reporting parameter`** défini sur **`enabled`**, et que le seuil minimal du nombre de jours de refroidissement ait été atteint (pour les volumes qui utilisent la stratégie de hiérarchisation **`snapshot-only`** ou **`auto`**). Sinon, la valeur est indiquée comme "N/A".

- **Recommandation cloud**

  Une fois que suffisamment d'informations ont été collectées sur l'activité des données sur le volume, Unified Manager peut déterminer qu'aucune action n'est requise ou que vous pourriez économiser de l'espace sur le niveau de performance en déplaçant les données inactives vers le niveau cloud.

> Le champ « Données froides » est mis à jour toutes les 15 minutes, tandis que le champ « Recommandation cloud » est mis à jour tous les 7 jours lors de l'analyse des données froides du volume. Par conséquent, la quantité exacte de données froides peut différer entre les deux champs. Le champ « Recommandation cloud » affiche la date d'exécution de l'analyse.

Lorsque la fonctionnalité de création de rapports sur les données inactives est activée, le champ « Données froides » affiche la quantité exacte de données inactives. Sans la fonctionnalité de création de rapports sur les

données inactives, Unified Manager utilise les statistiques de performance pour déterminer si des données sont inactives sur un volume. Dans ce cas, la quantité de données inactives n'est pas affichée dans le champ « Données froides », mais elle s'affiche lorsque vous placez le curseur sur le mot **Tier** pour consulter la recommandation cloud.

Les recommandations cloud que vous verrez sont :

- **En cours d'apprentissage**. Les données recueillies sont insuffisantes pour formuler une recommandation.
- **Niveau**. L'analyse a déterminé que le volume contient des données inactives (froides) et que vous devez le configurer pour déplacer ces données vers le niveau cloud. Dans certains cas, cela peut nécessiter de déplacer le volume vers un agrégat sur lequel FabricPool est activé. Dans d'autres cas, lorsque le volume se trouve déjà sur un agrégat FabricPool, il vous suffit de modifier la stratégie de hiérarchisation.
- **Aucune action**. Soit le volume contient très peu de données inactives, soit le volume est déjà défini sur la stratégie de hiérarchisation "auto" sur un agrégat FabricPool, soit le volume est un volume de protection des données. Cette valeur s'affiche également lorsque le volume est hors ligne ou lorsqu'il est utilisé dans une configuration MetroCluster.

Pour déplacer un volume ou pour modifier la politique de hiérarchisation du volume ou les paramètres de rapport des données inactives de l'agrégat, utilisez ONTAP System Manager, les commandes ONTAP CLI ou une combinaison de ces outils.

Si vous êtes connecté à Unified Manager avec le rôle Application Administrator ou Storage Administrator, le lien **Configure Volume** est disponible dans la recommandation cloud lorsque vous survolez le mot **Tier** avec votre curseur. Cliquez sur ce bouton pour ouvrir la page Volumes dans System Manager et effectuer la modification recommandée.

Surveillez les performances à l'aide des pages Performance Explorer

Surveillez les performances à l'aide des pages Performance Explorer dans Active IQ Unified Manager

Les pages de l'Explorateur de performances affichent des informations détaillées sur les performances de chaque objet d'un cluster. Elles offrent une vue détaillée des performances de tous les objets du cluster, permettant ainsi de sélectionner et de comparer les données de performances d'objets spécifiques sur différentes périodes.

Vous pouvez également évaluer les performances globales de tous les objets et comparer les données de performance des objets côte à côte.

Utilisez les objets racine pour la surveillance des performances dans Active IQ Unified Manager

L'objet racine sert de référence par rapport à laquelle les autres objets sont comparés. Cela vous permet d'afficher et de comparer les données des autres objets à l'objet racine, en fournissant une analyse des performances qui vous aide à dépanner et à améliorer les performances des objets.

Le nom de l'objet racine s'affiche en haut du volet Comparaison. Les 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 Comparaison, un seul objet racine est autorisé. Les données de l'objet racine s'affichent automatiquement dans les graphiques du volet Graphiques des compteurs.

Vous ne pouvez pas modifier l'objet racine ; il est toujours défini sur la page de l'objet que vous consultez. Par exemple, si vous ouvrez la page Explorateur de performances du volume Volume1, Volume1 est l'objet racine et ne peut pas être modifié. Si vous souhaitez effectuer une comparaison avec un autre objet racine, vous devez cliquer sur le lien d'un objet et ouvrir sa page de destination.

Les événements et les seuils sont affichés uniquement pour les objets racine.

Filtrer les objets corrélés dans la grille Active IQ Unified Manager

Le filtrage vous permet d'afficher un sous-ensemble plus restreint et mieux défini d'objets dans la grille. Par exemple, si vous avez 25 volumes dans la grille, le filtrage vous permet de visualiser uniquement ceux dont le débit est inférieur à 90 Mo/s ou dont la latence est supérieure à 1 ms/op.

Spécifiez une plage horaire pour les objets corrélés

Spécifiez une plage horaire pour les objets corrélés dans Active IQ Unified Manager

Le sélecteur de plage horaire de la page Performance Explorer vous permet de spécifier la plage horaire pour la comparaison des données d'objet. La spécification d'une plage horaire affine le contenu des pages Performance Explorer afin d'afficher uniquement les données d'objet comprises dans la plage horaire que vous avez spécifiée.

Le filtrage temporel permet d'afficher efficacement uniquement les données de performance qui vous intéressent. Vous pouvez sélectionner une plage horaire prédéfinie ou en spécifier une personnalisée. La plage horaire par défaut correspond aux 72 dernières heures.

Sélectionnez une plage horaire prédéfinie dans Active IQ Unified Manager

Sélectionner une période prédéfinie est un moyen rapide et efficace de personnaliser et de cibler les données affichées lors de la consultation des données de performance des objets du cluster. Lors de la sélection d'une période prédéfinie, des données sur une période allant jusqu'à 13 mois sont disponibles.

Étapes

1. En haut à droite de la page **Performance Explorer**, cliquez sur **Time Range**.
2. Dans le panneau **Time Range Selection**, à droite, sélectionnez une plage horaire prédéfinie.
3. Cliquez sur **Apply Range**.

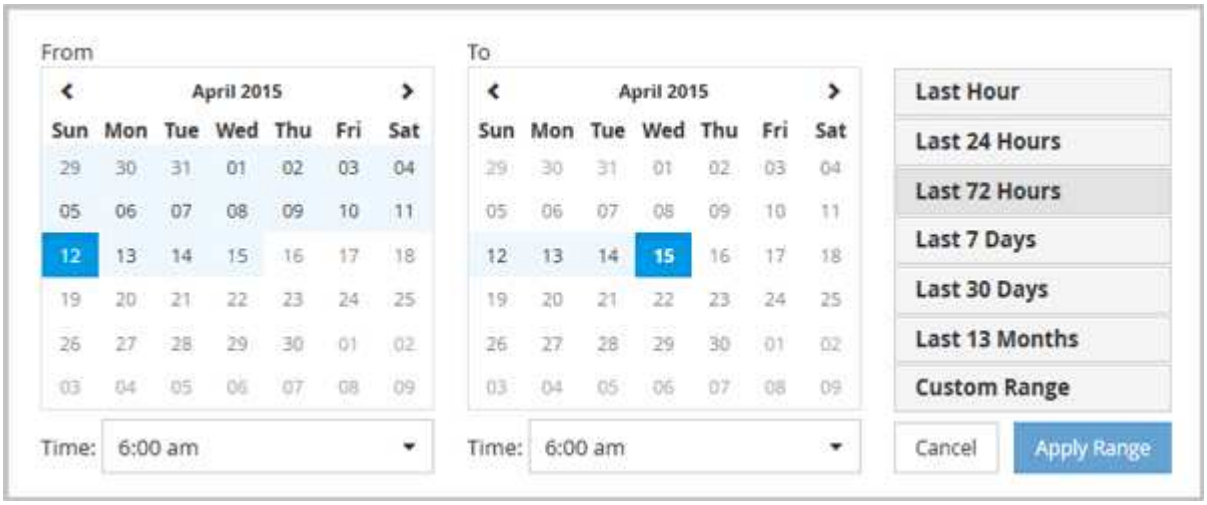
Spécifiez une plage horaire personnalisée dans Active IQ Unified Manager

La page Explorateur de performances vous permet de spécifier la plage de dates et d'heures de vos données de performances. La spécification d'une plage horaire personnalisée offre une plus grande flexibilité que l'utilisation de plages horaires prédéfinies lors de l'affinage des données d'objets de cluster.

Vous pouvez sélectionner une plage horaire comprise entre une heure et 390 jours. 13 mois correspondent à 390 jours, car chaque mois est compté comme 30 jours. Le fait de spécifier une plage de dates et d'heures fournit davantage de détails et vous permet de zoomer sur des événements de performance spécifiques ou des séries d'événements. Le fait de spécifier une plage horaire facilite également le dépannage de problèmes de performance potentiels, car la spécification d'une plage de dates et d'heures affiche avec plus de précision les données entourant l'événement de performance. Utilisez la commande **Time Range** pour sélectionner des plages de dates et d'heures prédéfinies, ou spécifiez votre propre plage de dates et d'heures personnalisée, jusqu'à 390 jours. Les boutons des plages horaires prédéfinies vont de **Last Hour** à **Last 13 Months**.

La sélection de l'option « 13 derniers mois » ou la spécification d'une plage de dates personnalisée supérieure à 30 jours affiche une boîte de dialogue vous avertissant que les données de performance affichées pour une période supérieure à 30 jours sont représentées sous forme de graphiques à l'aide de moyennes horaires et non de données collectées toutes les 5 minutes. Par conséquent, une perte de granularité visuelle de la chronologie peut se produire. Si vous cliquez sur l'option « Ne plus afficher » dans la boîte de dialogue, le message n'apparaît pas lorsque vous sélectionnez l'option « 13 derniers mois » ou spécifiez une plage de dates personnalisée supérieure à 30 jours. Les données récapitulatives s'appliquent également à une plage de temps plus réduite si celle-ci inclut une heure/date remontant à plus de 30 jours par rapport à aujourd'hui.

Lors de la sélection d'une période (personnalisée ou prédéfinie), les périodes de 30 jours ou moins sont basées sur des échantillons de données à intervalles de 5 minutes. Les périodes supérieures à 30 jours sont basées sur des échantillons de données à intervalles d'une heure.



1. Cliquez sur la liste déroulante **Plage horaire** pour afficher le panneau Plage horaire.
2. Pour sélectionner une plage de temps prédéfinie, cliquez sur l'un des boutons **Last…** à droite du panneau **Time Range**. Lorsque vous sélectionnez une plage de temps prédéfinie, les données sur une période pouvant aller jusqu'à 13 mois sont disponibles. Le bouton de plage de temps prédéfinie que vous avez sélectionné est mis en surbrillance, et les jours et l'heure correspondants s'affichent dans les calendriers et les sélecteurs d'heure.
3. Pour sélectionner une plage de dates personnalisée, cliquez sur la date de début dans le calendrier **De** à gauche. Cliquez sur **<** or **>** pour avancer ou reculer 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** à droite du panneau Plage de dates est mis en surbrillance, ce qui indique que vous avez sélectionné une plage de dates personnalisée.
4. Pour sélectionner une plage horaire personnalisée, cliquez sur la commande **Heure** sous le calendrier **De** et sélectionnez l'heure de début. Pour spécifier l'heure de fin, cliquez sur la commande **Heure** sous le calendrier **À** situé à droite et sélectionnez l'heure de fin. Le bouton **Plage personnalisée** à droite du panneau Plage horaire est mis en surbrillance, ce qui indique que vous avez sélectionné une plage horaire 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 indiqué précédemment, puis sélectionnez les heures de début et de fin comme indiqué précédemment. Les dates sélectionnées sont mises en surbrillance dans les calendriers, les heures de début et de fin que vous avez spécifiées s'affichent dans les commandes **Heure**, et le bouton **Plage personnalisée** est mis en surbrillance.
6. Après avoir sélectionné la plage de dates et d'heures, cliquez sur **Appliquer la plage**. Les statistiques de performance pour cette plage horaire s'affichent dans les graphiques et dans la chronologie des événements.

Définissez des objets corrélés pour la création de graphiques de comparaison dans Active IQ Unified Manager

Dans le volet Graphique de compteurs, vous pouvez définir une liste d'objets corrélés pour comparer les données et les performances. Par exemple, si votre machine virtuelle de stockage (SVM) rencontre un problème de performances, vous pouvez comparer tous les volumes de la SVM afin d'identifier celui qui pourrait être à l'origine du problème.

Vous pouvez ajouter n'importe quel objet de la grille des objets corrélés aux volets Comparing et Counter Chart. Cela vous permet d'afficher et de comparer les données de plusieurs objets ainsi qu'avec l'objet racine. Vous pouvez ajouter et supprimer des objets dans la grille des objets corrélés ; toutefois, l'objet racine du volet Comparing ne peut pas être supprimé.

L'ajout de nombreux objets au volet de comparaison peut nuire aux 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, repérez l'objet que vous souhaitez ajouter, puis cliquez sur le bouton **Ajouter**.

   Le bouton **Add** devient gris et l'objet est ajouté à la liste des objets supplémentaires dans le volet Comparing. Les données de l'objet sont ajoutées aux graphiques dans les volets Counter Charts. La couleur de l'icône en forme d'œil ( ) de l'objet correspond à la couleur de la courbe de tendance des données de l'objet dans les graphiques.

2. **Facultatif:** Masquer ou afficher les données pour les objets sélectionnés:

Pour ce faire…	Prenez cette mesure…
Masquer un objet sélectionné	Cliquez sur l'icône en forme d'œil ( ) de l'objet sélectionné dans le volet Comparaison. Les données de l'objet sont masquées et l'icône en forme d'œil de cet objet devient grise.
Afficher un objet caché	Cliquez sur l'icône en forme d'œil gris de l'objet sélectionné dans le volet Comparaison. L'icône en forme d'œil reprend sa couleur d'origine et les données de l'objet sont réintégrées dans les graphiques du volet Graphiques de compteurs.

3. **Facultatif :** Supprimez les objets sélectionnés du volet **Comparaison**:

Pour ce faire…	Prenez cette mesure…
Supprimer un objet sélectionné	Dans le volet de comparaison, survolez le nom de l'objet sélectionné pour afficher le bouton Supprimer l'objet (**X**), puis cliquez dessus. L'objet est alors supprimé du volet de comparaison et ses données sont effacées des graphiques de compteurs.
Supprimer tous les objets sélectionnés	Cliquez sur le bouton Supprimer tous les objets (**X**) en haut du volet Comparaison. Tous les objets sélectionnés et leurs données sont supprimés, ne laissant que l'objet racine.

Comprendre les graphiques de compteurs dans Active IQ Unified Manager

Les graphiques du volet « Graphiques de compteurs » vous permettent de visualiser et de comparer les données de performance de l'objet racine et des objets que vous avez ajoutés à partir de la grille des objets corrélés. Cela peut vous aider à comprendre les tendances de performance et à isoler et résoudre les problèmes de performance.

Les graphiques de compteur affichés par défaut sont Events, Latency, IOPS et MBps. Les graphiques facultatifs que vous pouvez choisir d'afficher sont Utilization, Performance Capacity Used, Available IOPS, IOPS/TB et Cache Miss Ratio. De plus, vous pouvez choisir d'afficher les valeurs totales ou les valeurs de répartition pour les graphiques Latency, IOPS, MBps et Performance Capacity Used.

L'explorateur de performances affiche par défaut certains graphiques de compteurs, que l'objet de stockage les prenne tous en charge ou non. Lorsqu'un compteur n'est pas pris en charge, le graphique de compteur est vide et le message `Not applicable for <object>`s'affiche.

Les graphiques affichent les tendances de performance de l'objet racine et de tous les objets sélectionnés dans le volet Comparaison. Les données de chaque graphique sont organisées comme suit :

- **Axe X**

  Affiche la période spécifiée. Si vous n'avez pas spécifié de plage horaire, la valeur par défaut est la période de 72 heures précédente.

- **Axe Y**

  Affiche les unités de comptage propres à l'objet ou aux objets sélectionnés.

La couleur des courbes de tendance correspond à celle du nom de l'objet affiché dans le volet Comparaison. Vous pouvez placer votre curseur sur un point d'une courbe de tendance pour afficher les détails temporels et de valeur de ce point.

Si vous souhaitez étudier une période spécifique au sein d'un graphique, vous pouvez utiliser l'une des méthodes suivantes :

- Utilisez le bouton **<** pour étendre le volet Graphiques de compteurs sur toute la largeur de la page.
- Utilisez le curseur (lorsqu'il se transforme en loupe) pour sélectionner une portion de la période sur le graphique afin de vous concentrer sur cette zone et de l'agrandir. Vous pouvez cliquer sur « Réinitialiser le zoom du graphique » pour rétablir la période par défaut.
- Utilisez le bouton **Zoom View** pour afficher un grand graphique d'un seul compteur contenant des détails

étendus et des indicateurs de seuil.

Il arrive que des interruptions apparaissent dans les courbes de tendance. Ces interruptions indiquent soit que Unified Manager n'a pas pu collecter les données de performance du système de stockage, soit que Unified Manager était hors service.

Comprendre les types de graphiques de compteurs de performance dans Active IQ Unified Manager

Des graphiques de performance standard affichent les valeurs des compteurs pour l'objet de stockage sélectionné. Chaque graphique de compteur détaillé présente les valeurs totales ventilées par catégories : lecture, écriture et autres. De plus, certains graphiques de compteur détaillés affichent des informations supplémentaires lorsque le graphique est affiché en mode Zoom.

Le tableau suivant présente les graphiques des compteurs de performance disponibles.

Graphiques disponibles	Description du graphique
Événements	Affiche les événements critiques, d'erreur, d'avertissement et d'information en corrélation avec les graphiques statistiques de l'objet racine. Les événements de santé s'affichent en plus des événements de performance afin de fournir une vue d'ensemble complète des raisons pour lesquelles les performances peuvent être affectées.
Latence - Totale	Nombre de millisecondes nécessaires pour répondre aux requêtes de l'application. Notez que les valeurs de latence moyennes sont pondérées par les E/S.
Latence - Répartition	Les mêmes informations sont affichées dans Latency Total, mais les données de performance sont ventilées en latence de lecture, d'écriture et autres latences. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est une SVM, un nœud, un agrégat, un volume, un LUN ou un namespace.
Latence - Composants du cluster	Les mêmes informations que celles affichées dans Latency Total, mais avec les données de performance ventilées par composant de cluster. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un volume.
IOPS - Total	Nombre d'opérations d'entrée/sortie traitées par seconde. Lorsqu'elles sont affichées pour un nœud, la sélection de "Total" affiche les IOPS des données transitant par ce nœud, qui peuvent résider sur le nœud local ou sur le nœud distant, et la sélection de "Total (Local)" affiche les IOPS des données qui résident uniquement sur le nœud actuel.

Graphiques disponibles	Description du graphique
IOPS - Répartition	Les mêmes informations sont affichées dans IOPS Total, mais les données de performance sont ventilées en IOPS de lecture, d'écriture et autres. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est une SVM, un nœud, un agrégat, un volume, un LUN ou un namespace. Lorsqu'il est affiché en mode Zoom, le graphique des volumes affiche les valeurs de débit minimum et maximum de la QoS, si elles sont configurées dans ONTAP. Lorsqu'elle est affichée pour un nœud, la sélection de « `Répartition` » affiche la répartition des IOPS pour les données transitant par ce nœud et pouvant résider sur le nœud local ou sur le nœud distant, et la sélection de « `Répartition (Local)` » affiche la répartition des IOPS pour les données résidant uniquement sur le nœud actuel.
IOPS - Protocoles	Les mêmes informations sont affichées dans IOPS Total, mais les données de performance sont présentées dans des graphiques distincts pour le trafic des protocoles CIFS, NFS, FCP, NVMe et iSCSI. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est une SVM.
IOPS/To - Total	Nombre d'opérations d'entrée/sortie traitées par seconde, en fonction de l'espace total consommé par le workload, en téraoctets. Également appelé densité d'E/S, ce compteur mesure le niveau de performances pouvant être fourni par une capacité de stockage donnée. Lorsqu'il est affiché en vue Zoom, le graphique des volumes affiche les valeurs de débit attendues et de débit de pointe, si elles sont configurées dans ONTAP. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un volume.
Mo/s - Total	Nombre de mégaoctets de données transférés vers et depuis l'objet par seconde.

Graphiques disponibles	Description du graphique
MB/s - Détail	Les mêmes informations sont affichées que dans le graphique en MB/s, mais les données de débit sont ventilées en lectures sur disque, lectures de Flash Cache, écritures et autres. En mode Zoom, le graphique des volumes affiche les valeurs de débit maximal QoS, si elles sont configurées dans ONTAP. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un SVM, un nœud, un agrégat, un volume, un LUN ou un namespace. Les données Flash Cache sont affichées uniquement pour les nœuds, et uniquement lorsqu'un module Flash Cache est installé sur le nœud.
Capacité de performances utilisée - Total	Pourcentage de capacité de performance consommée par le nœud ou l'agrégat.
Capacité de performance utilisée - Détail	Les données relatives à la capacité de performance utilisée sont ventilées entre les protocoles utilisateur et les processus système en arrière-plan. En outre, la quantité de capacité de performance libre est indiquée.
IOPS disponibles - Total	Nombre d'opérations d'entrée/sortie par seconde actuellement disponibles (libres) sur cet objet. Ce nombre résulte de la soustraction des IOPS actuellement utilisées du total des IOPS que Unified Manager calcule que l'objet peut effectuer. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un nœud ou un agrégat.
Utilisation - Totale	Pourcentage des ressources disponibles de l'objet en cours d'utilisation. L'utilisation indique l'utilisation des nœuds pour les nœuds, l'utilisation des disques pour les agrégats et l'utilisation de la bande passante pour les ports. Cette option de graphique s'applique uniquement lorsque l'objet sélectionné est un nœud, un agrégat ou un port.
Taux de défaut du cache - Total	Pourcentage de requêtes de lecture provenant d'applications clientes renvoyées depuis le disque plutôt que depuis le cache. Cette option du graphique s'applique uniquement lorsque l'objet sélectionné est un volume.

Sélectionnez les graphiques de performance à afficher dans Active IQ Unified Manager

La liste déroulante « Choisir les graphiques » vous permet de sélectionner les types de graphiques de compteurs de performances à afficher dans le volet « Graphiques de compteurs ». Vous pouvez ainsi visualiser des données et des compteurs spécifiques, en

fonction de vos besoins en matière de performances.

Étapes

1. Dans le volet **Graphiques de compteur**, cliquez sur la liste déroulante **Choisir les graphiques**.
2. Ajouter ou supprimer des graphiques :

À…	Faites ceci…
Ajouter ou supprimer des graphiques individuels	Cochez les cases en regard des graphiques que vous souhaitez afficher ou masquer
Ajouter tous les graphiques	Cliquez sur **Tout sélectionner**
Supprimer tous les graphiques	Cliquez sur **Tout désélectionner**

Vos sélections de graphiques s'affichent dans le volet Counter Charts. Notez que lorsque vous ajoutez des graphiques, les nouveaux graphiques sont insérés dans le volet Counter Charts pour correspondre à l'ordre des graphiques répertoriés dans la liste déroulante Choose charts. La sélection de graphiques supplémentaires peut nécessiter un défilement supplémentaire.

Développez le volet Graphiques de compteurs dans Active IQ Unified Manager

Vous pouvez agrandir le volet Graphiques des compteurs 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 « Graphiques des compteurs » plus grand. Utilisez le bouton **<** au centre de la fenêtre Performance Explorer pour développer le volet.

Étape

1. Développez ou réduisez le volet **Counter Charts**.

À…	Faites ceci…
Agrandissez le volet Counter Charts pour qu'il occupe toute la largeur de la page	Cliquez sur le bouton **<**
Réduisez le volet Graphiques de compteur à la moitié droite de la page	Cliquez sur le bouton **>**

Modifiez la période des graphiques de compteurs pour une période plus courte dans Active IQ Unified Manager

Vous pouvez utiliser votre souris pour réduire la plage temporelle afin de vous concentrer sur une période spécifique dans le volet Graphique de compteurs ou dans la fenêtre Vue zoom des graphiques de compteurs. Cela vous permet d'obtenir une vue plus granulaire et microscopique de n'importe quelle partie de la chronologie des données de performance, des événements et des seuils.

Avant de commencer

Le curseur doit s'être transformé en loupe pour indiquer que cette fonctionnalité est active.

Lorsque vous utilisez cette fonctionnalité, qui modifie la chronologie pour afficher des valeurs correspondant à l'affichage plus précis, la plage de dates et d'heures du sélecteur **Plage de dates** ne change pas par rapport aux 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 que vous souhaitez voir en détail.

   Les valeurs du compteur pour la période que vous sélectionnez alimentent le graphique du compteur.

2. Pour revenir à la période initiale définie dans le sélecteur **Plage de temps**, cliquez sur le bouton **Réinitialiser le zoom du graphique**.

   Le graphique du compteur s'affiche dans son état d'origine.

Consultez les détails de l'événement dans la chronologie des événements d'Active IQ Unified Manager.

Vous pouvez consulter tous les événements et leurs détails associés dans le volet Chronologie des événements de Performance Explorer. Cette méthode rapide et efficace permet de visualiser tous les événements liés à l'état et aux performances de l'objet racine pendant une période donnée, ce qui peut s'avérer utile pour résoudre les problèmes de performances.

Le volet Chronologie des événements affiche les événements critiques, d'erreur, d'avertissement et d'information survenus sur l'objet racine pendant la période sélectionnée. Chaque niveau de gravité d'événement possède sa propre chronologie. Les événements uniques et multiples sont représentés par un point d'événement sur la chronologie. Vous pouvez placer votre curseur sur un point d'événement pour afficher les détails de l'événement. Pour augmenter la granularité visuelle des événements multiples, vous pouvez réduire la période. Cela répartit les événements multiples en événements individuels, ce qui vous permet d'afficher et d'examiner séparément chaque événement.

Chaque point d'événement de performance sur la chronologie des événements s'aligne verticalement avec un pic correspondant sur les courbes de tendance des graphiques des compteurs affichés sous la chronologie des événements. Cela fournit une corrélation visuelle directe entre les événements et les performances globales. Les événements de santé sont également affichés sur la chronologie, mais ces types d'événements ne correspondent pas nécessairement à un pic dans l'un des graphiques de performance.

Étapes

1. Dans le volet **Chronologie des événements**, placez le curseur sur un point d'événement de la chronologie pour afficher un résumé de l'événement ou des événements à ce point précis.

   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 ce faire…	Cliquez ici…
Afficher les détails d'un seul événement	**Afficher les détails de l'événement** dans la boîte de dialogue contextuelle.

Pour ce faire…	Cliquez ici…
Afficher les détails de plusieurs événements	**Consultez les détails de l'événement** dans la fenêtre contextuelle. Lorsque vous cliquez sur un seul événement dans la boîte de dialogue « Événements multiples », la page Détails de l'événement correspondante s'affiche.

Vue agrandie des graphiques de compteur

Découvrez la vue zoom dans les graphiques de compteurs dans Active IQ Unified Manager

Les graphiques de compteurs offrent une vue zoomée qui vous permet d'examiner en détail les performances sur la période spécifiée. Vous pouvez ainsi visualiser les détails des performances et les événements avec une granularité beaucoup plus fine, ce qui est particulièrement utile pour le dépannage des problèmes de performance.

En mode Zoom, certains graphiques de répartition fournissent des informations supplémentaires par rapport à leur affichage normal. Par exemple, les pages en mode Zoom des graphiques de répartition IOPS, IOPS/TB et MBps affichent les valeurs de stratégie QoS pour les volumes et les LUN si elles ont été définies dans ONTAP.

Pour les politiques de seuil de performance définies par le système, seules les politiques "Node resources over-utilized" et "QoS throughput limit breached" sont disponibles dans la liste **Policies**. Les autres politiques de seuil définies par le système ne sont pas disponibles pour le moment.

Afficher la vue zoom des graphiques de compteurs dans Active IQ Unified Manager

L'affichage zoom des graphiques de compteur offre un niveau de détail plus fin pour le graphique de compteur sélectionné et sa chronologie associée. Ce zoom permet d'agrandir les données du graphique de compteur, offrant ainsi une vision plus précise des événements de performance et de leurs causes sous-jacentes.

Vous pouvez afficher la vue de zoom des graphiques de compteur pour n'importe quel graphique de compteur.

Étapes

1. Cliquez sur **Zoom View** pour ouvrir le graphique sélectionné dans une nouvelle fenêtre de navigateur.
2. Si vous consultez un graphique de répartition puis cliquez sur **Zoom View**, le graphique de répartition s'affiche dans **Zoom View**. Vous pouvez sélectionner **Total** dans **Zoom View** si vous souhaitez modifier l'option d'affichage.

Spécifiez la plage horaire dans la vue Zoom dans Active IQ Unified Manager

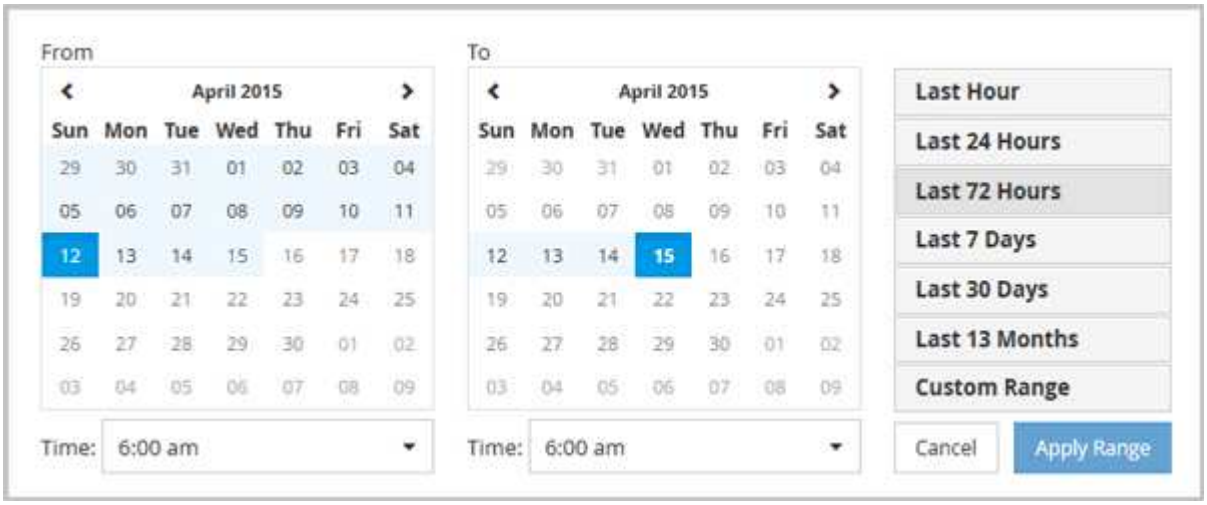
La commande **Time Range** de la fenêtre Counter Charts Zoom View vous permet de spécifier une plage de dates et d'heures pour le graphique sélectionné. Vous pouvez ainsi localiser rapidement des données spécifiques en fonction d'une plage horaire

prédéfinie ou d'une plage horaire personnalisée.

Vous pouvez sélectionner une plage horaire comprise entre une heure et 390 jours. 13 mois correspondent à 390 jours, car chaque mois est compté comme 30 jours. Le fait de spécifier une plage de dates et d'heures fournit davantage de détails et vous permet de zoomer sur des événements de performance spécifiques ou des séries d'événements. Le fait de spécifier une plage horaire facilite également le dépannage de problèmes de performance potentiels, car la spécification d'une plage de dates et d'heures affiche avec plus de précision les données entourant l'événement de performance. Utilisez la commande **Time Range** pour sélectionner des plages de dates et d'heures prédéfinies, ou spécifiez votre propre plage de dates et d'heures personnalisée, jusqu'à 390 jours. Les boutons des plages horaires prédéfinies vont de **Last Hour** à **Last 13 Months**.

La sélection de l'option « 13 derniers mois » ou la spécification d'une plage de dates personnalisée supérieure à 30 jours affiche une boîte de dialogue vous avertissant que les données de performance affichées pour une période supérieure à 30 jours sont représentées sous forme de graphiques à l'aide de moyennes horaires et non de données collectées toutes les 5 minutes. Par conséquent, une perte de granularité visuelle de la chronologie peut se produire. Si vous cliquez sur l'option « Ne plus afficher » dans la boîte de dialogue, le message n'apparaît pas lorsque vous sélectionnez l'option « 13 derniers mois » ou spécifiez une plage de dates personnalisée supérieure à 30 jours. Les données récapitulatives s'appliquent également à une plage de temps plus réduite si celle-ci inclut une heure/date remontant à plus de 30 jours par rapport à aujourd'hui.

Lors de la sélection d'une période (personnalisée ou prédéfinie), les périodes de 30 jours ou moins sont basées sur des échantillons de données à intervalles de 5 minutes. Les périodes supérieures à 30 jours sont basées sur des échantillons de données à intervalles d'une heure.



1. Cliquez sur la liste déroulante **Plage horaire** pour afficher le panneau Plage horaire.
2. Pour sélectionner une plage de temps prédéfinie, cliquez sur l'un des boutons **Last…** à droite du panneau **Time Range**. Lorsque vous sélectionnez une plage de temps prédéfinie, les données sur une période pouvant aller jusqu'à 13 mois sont disponibles. Le bouton de plage de temps prédéfinie que vous avez sélectionné est mis en surbrillance, et les jours et l'heure correspondants s'affichent dans les calendriers et les sélecteurs d'heure.
3. Pour sélectionner une plage de dates personnalisée, cliquez sur la date de début dans le calendrier **De** à gauche. Cliquez sur **<** or **>** pour avancer ou reculer 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** à droite du panneau Plage de dates est mis en surbrillance, ce qui indique que vous avez sélectionné une plage de dates personnalisée.
4. Pour sélectionner une plage horaire personnalisée, cliquez sur la commande **Heure** sous le calendrier **De** et sélectionnez l'heure de début. Pour spécifier l'heure de fin, cliquez sur la commande **Heure** sous le calendrier **À** situé à droite et sélectionnez l'heure de fin. Le bouton **Plage personnalisée** à droite du

panneau Plage horaire est mis en surbrillance, ce qui indique que vous avez sélectionné une plage horaire 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 indiqué précédemment, puis sélectionnez les heures de début et de fin comme indiqué précédemment. Les dates sélectionnées sont mises en surbrillance dans les calendriers, les heures de début et de fin que vous avez spécifiées s'affichent dans les commandes **Heure**, et le bouton **Plage personnalisée** est mis en surbrillance.
6. Après avoir sélectionné la plage de dates et d'heures, cliquez sur **Appliquer la plage**. Les statistiques de performance pour cette plage horaire s'affichent dans les graphiques et dans la chronologie des événements.

Sélectionnez les seuils de performance dans la vue Zoom des graphiques de compteurs dans Active IQ Unified Manager

L'application de seuils dans la vue Zoom des graphiques de compteurs offre une vue détaillée des occurrences d'événements de seuil de performance. Vous pouvez ainsi appliquer ou supprimer des seuils et visualiser immédiatement les résultats, ce qui peut s'avérer utile pour déterminer si le dépannage doit être votre prochaine étape.

La sélection de seuils dans la vue agrandie des graphiques de compteurs vous permet de visualiser des données précises sur les événements de seuil de performance. Vous pouvez appliquer n'importe quel seuil figurant dans la zone **Policies** de la vue agrandie des graphiques de compteurs.

Dans la vue zoom des graphiques de compteurs, une seule politique peut être appliquée à la fois à l'objet.

Étape

1. Sélectionnez ou désélectionnez l'  associé à une politique.

   Le seuil sélectionné est appliqué à la vue de zoom des graphiques de compteurs. Les seuils critiques sont affichés sous forme de ligne rouge ; les seuils d'alerte sont affichés sous forme de ligne jaune.

Afficher la latence du volume par composant de cluster dans Active IQ Unified Manager

Vous pouvez consulter des informations détaillées sur la latence d'un volume via la page Explorateur de performances des volumes. Le graphique « Latence totale » affiche la latence totale du volume, tandis que le graphique « Latence détaillée » permet d'évaluer l'impact des latences de lecture et d'écriture sur ce volume.

De plus, le graphique « Latence - Composants du cluster » présente une comparaison détaillée de la latence de chaque composant du cluster afin de déterminer la contribution de chacun à la latence totale du volume. Les composants du cluster suivants sont affichés :

- Réseau
- Limite maximale de QoS
- Limite QoS min
- Traitement réseau
- Interconnexion de clusters
- Data Processing

- Opérations sur les agrégats
- Activation du volume
- MetroCluster Ressources
- Latence du cloud
- Synchronisation SnapMirror

Étapes

1. Sur la page **Explorateur de performances du volume** de votre volume sélectionné, dans le graphique de latence, sélectionnez **Composants du cluster** dans le menu déroulant.

   Le graphique « Latency - Cluster Components » s'affiche.

2. Pour afficher une version agrandie du graphique, sélectionnez **Zoom View**.

   Le tableau comparatif des composants du cluster s'affiche. Vous pouvez restreindre la comparaison en désélectionnant ou en sélectionnant associé à chaque composant du cluster.

3. Pour afficher les valeurs spécifiques, déplacez votre curseur dans la zone du graphique pour faire apparaître la fenêtre contextuelle.

Affichez le trafic IOPS SVM par protocole dans Active IQ Unified Manager

Vous pouvez consulter des informations détaillées sur les IOPS d'une SVM à l'aide de la page Performance/SVM Explorer. Le graphique de compteur « IOPS - Total » affiche l'utilisation totale des IOPS sur la SVM, tandis que le graphique de compteur « IOPS - Breakdown » est utile pour déterminer l'impact des IOPS de lecture, d'écriture et autres sur la SVM.

De plus, le graphique IOPS - Protocoles présente une comparaison détaillée du trafic IOPS pour chaque protocole utilisé sur la SVM. Les protocoles suivants sont disponibles :

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

Étapes

1. Sur la page **Performance/SVM Explorer** de votre SVM sélectionné, dans le graphique IOPS, sélectionnez **Protocoles** dans le menu déroulant.

   Le graphique IOPS - Protocoles s'affiche.

2. Pour afficher une version agrandie du graphique, sélectionnez **Zoom View**.

   Le tableau comparatif avancé des protocoles IOPS s'affiche. Vous pouvez limiter la comparaison en désélectionnant ou en sélectionnant l' associé à un protocole.

3. Pour afficher les valeurs spécifiques, déplacez votre curseur dans la zone de l'un ou l'autre graphique pour faire apparaître la fenêtre contextuelle.

Consultez les graphiques de volume et de latence LUN pour vérifier la garantie de performance dans Active IQ Unified Manager

Vous pouvez consulter les volumes et les LUN auxquels vous avez souscrit dans le cadre du programme « `Performance Guarantee` » pour vérifier que la latence n'a pas dépassé le niveau qui vous a été garanti.

La garantie de latence est une valeur en millisecondes par opération à ne pas dépasser. Elle est calculée sur la base d'une moyenne horaire, et non sur la période de collecte des performances par défaut de cinq minutes.

Étapes

1. Dans la vue **Performances : Tous les volumes** ou **Performances : Tous les LUN**, sélectionnez le volume ou le LUN qui vous intéresse.
2. Sur la page **Performance Explorer** de votre volume ou de la LUN sélectionné(e), choisissez **Moyenne horaire** dans le sélecteur **Afficher les statistiques dans**.

   La ligne horizontale du graphique de latence sera plus lisse lorsque les relevés par tranches de cinq minutes seront remplacés par la moyenne horaire.

3. Si vous avez d'autres volumes sur le même agrégat qui bénéficient de la garantie de performance, vous pouvez ajouter ces volumes pour visualiser leur valeur de latence dans le même graphique.

Consultez les performances de tous les clusters SAN Array dans Active IQ Unified Manager

Vous pouvez utiliser la vue Performances : Tous les clusters pour afficher l'état des performances de vos clusters All SAN Array.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez consulter des informations générales sur les clusters All SAN Array dans la vue Performance: All Clusters, ainsi que des détails dans la page Cluster / Performance Explorer.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.
2. Assurez-vous que la colonne « `Personality` » est affichée dans la vue **Health: All Clusters**, ou ajoutez-la à l'aide de la commande **Show / Hide**.

   Cette colonne affiche « `All SAN Array` » pour vos clusters All SAN Array.

3. Pour afficher des informations sur les performances de ces clusters, sélectionnez la vue **Performances : Tous les clusters**.

   Consultez les informations de performance 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 **Nœuds sur ce cluster** dans le menu **Afficher et comparer**.

Vous pouvez comparer les statistiques de performance des deux nœuds de ce cluster pour vérifier que la charge est quasiment identique sur les deux nœuds. S'il existe d'importants écarts entre les deux nœuds, vous pouvez ajouter le second nœud aux graphiques et comparer les valeurs sur une période plus longue afin d'identifier d'éventuels problèmes de configuration.

Afficher les IOPS des nœuds en fonction des charges de travail locales dans Active IQ Unified Manager

Le graphique du compteur IOPS du nœud permet de mettre en évidence les opérations qui transitent uniquement par le nœud local via une interface réseau LIF pour effectuer des opérations de lecture/écriture sur des volumes situés sur un nœud distant. Les graphiques IOPS - "Total (Local)" et "Breakdown (Local)" affichent les IOPS des données résidant uniquement dans les volumes locaux du nœud actuel.

Les versions « `Local` » de ces graphiques de compteurs sont similaires aux graphiques de nœuds pour la capacité et l'utilisation des performances, car elles affichent également uniquement les statistiques des données résidant sur des volumes locaux.

En comparant les versions "Local" de ces graphiques de compteurs aux versions "Total" standard de ces graphiques de compteurs, vous pouvez voir si un volume important de trafic passe par le nœud local pour accéder aux volumes sur le nœud distant. Cette situation peut entraîner des problèmes de performance, éventuellement indiqués par une utilisation élevée du nœud, si un trop grand nombre d'opérations passent par le nœud local pour atteindre un volume sur un nœud distant. Dans ce cas, vous pouvez envisager de déplacer un volume vers le nœud local, ou de créer une LIF sur le nœud distant à laquelle le trafic des hôtes accédant à ce volume peut être connecté.

Étapes

1. Sur la page **Performance/Node Explorer** de votre nœud sélectionné, dans le graphique IOPS, sélectionnez **Total** dans le menu déroulant.

   Le graphique IOPS - Total s'affiche.

2. Cliquez sur **Zoom View** pour afficher une version agrandie du graphique dans un nouvel onglet du navigateur.
3. De retour sur la page **Performance/Node Explorer**, dans le graphique IOPS, sélectionnez **Total (Local)** dans le menu déroulant.

   Le graphique IOPS - Total (Local) est affiché.

4. Cliquez sur **Zoom View** pour afficher une version agrandie du graphique dans un nouvel onglet du navigateur.
5. Comparez les deux graphiques côte à côte et identifiez les zones où les valeurs IOPS semblent très différentes.
6. Déplacez votre curseur sur ces zones pour comparer les IOPS locales et totales à un moment précis.

Composants des pages de destination des objets

Examinez les composants des pages de destination des objets dans Active IQ Unified Manager

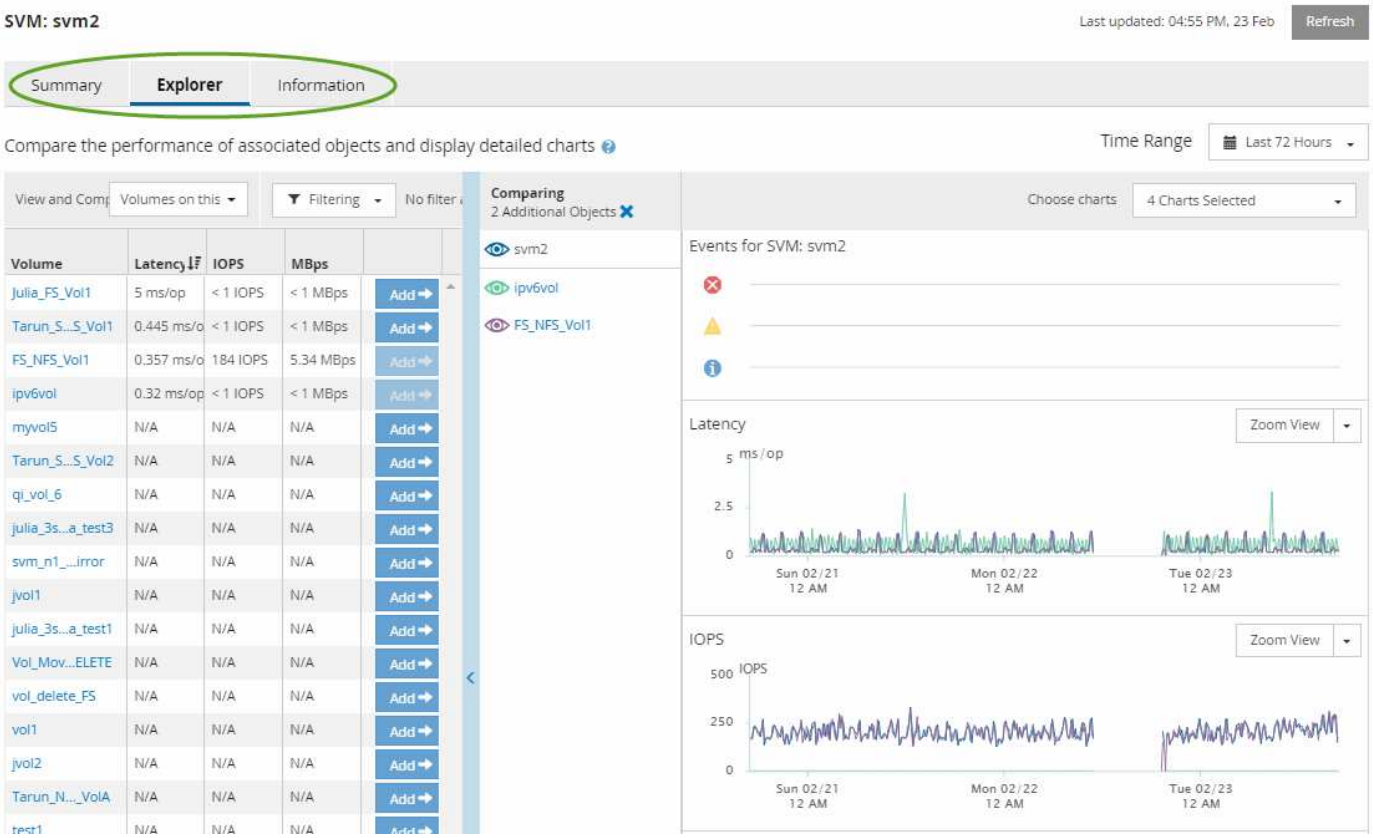
Les pages de destination des objets fournissent des détails sur tous les événements critiques, d'avertissement et d'information. Elles offrent une vue détaillée des

performances de tous les objets du cluster, vous permettant de sélectionner et de comparer des objets individuels sur différentes périodes.

Les pages d'accueil des objets vous permettent d'examiner les performances globales de tous les objets et de comparer les données de performance des objets côte à côte. Cela est utile lors de l'évaluation des performances et du dépannage des événements.

> Les données affichées dans les panneaux récapitulatifs des compteurs et dans les graphiques des compteurs sont basées sur un intervalle d'échantillonnage de cinq minutes. Les données affichées dans la grille d'inventaire des objets située à gauche de la page sont basées sur un intervalle d'échantillonnage d'une heure.

L'image suivante montre un exemple de page de destination d'objet affichant les informations Explorer :



Selon l'objet de stockage consulté, la page d'accueil de l'objet peut comporter les onglets suivants qui fournissent des données de performance sur l'objet :

- Résumé

  Affiche trois ou quatre graphiques de compteurs contenant les événements et les performances par objet pour la période de 72 heures précédente, y compris une ligne de tendance qui montre les valeurs hautes et basses au cours de cette période.

- Explorateur

  Affiche une grille des objets de stockage liés à l'objet actuel, permettant de comparer les valeurs de performances de ce dernier avec celles des objets associés. Cet onglet comprend jusqu'à onze graphiques de compteurs et un sélecteur de plage temporelle, offrant ainsi la possibilité d'effectuer diverses comparaisons.

- Informations

  Affiche les valeurs des attributs de configuration non liés aux performances de l'objet de stockage, notamment la version installée du logiciel ONTAP, le nom du partenaire HA et le nombre de ports et d'interfaces logiques (LIF).

- Éléments les plus performants

  Pour les clusters : affiche les objets de stockage présentant les performances les plus élevées ou les plus faibles, en fonction du compteur de performances que vous sélectionnez.

- Planification du basculement

  Pour les nœuds : Affiche l'estimation de l'impact sur les performances d'un nœud si son partenaire HA tombe en panne.

- Détails

  Pour les volumes : affiche des statistiques de performance détaillées pour toutes les activités et opérations d'E/S du workload de volume sélectionné. Cet onglet est disponible pour les volumes FlexVol, les volumes FlexGroup et les composants de FlexGroups.

Consultez la page Résumé des performances dans Active IQ Unified Manager

La page Résumé affiche des graphiques de compteurs contenant des informations détaillées sur les événements et les performances de chaque objet au cours des 72 dernières heures. Ces données ne sont pas actualisées automatiquement, mais elles sont à jour au moment du dernier chargement de la page. Les graphiques de la page Résumé répondent à la question : « Dois-je consulter d'autres informations ? »

Graphiques et statistiques de compteurs

Les graphiques récapitulatifs offrent un aperçu rapide et global des dernières 72 heures et vous aident à identifier les problèmes potentiels qui nécessitent un examen plus approfondi.

Les statistiques du compteur de la page Summary sont affichées sous forme de graphiques.

Vous pouvez placer votre curseur sur la courbe de tendance d'un graphique pour afficher les valeurs des compteurs à un instant précis. Les graphiques récapitulatifs affichent également le nombre total d'événements critiques et d'alertes actifs au cours des 72 dernières heures pour les compteurs suivants :

- **Latence**

  Temps de réponse moyen pour toutes les requêtes d'E/S; exprimé en millisecondes par opération.

  Affiché pour tous les types d'objets.

- **IOPS**

  Vitesse de fonctionnement moyenne; exprimée en opérations d'entrée/sortie par seconde.

  Affiché pour tous les types d'objets.

- **Mo/s**

Débit moyen; exprimé en mégaoctets par seconde.

Affiché pour tous les types d'objets.

- **Capacité de performance utilisée**

  Pourcentage de capacité de performance consommée par un nœud ou un agrégat.

  Affiché uniquement pour les nœuds et les agrégats.

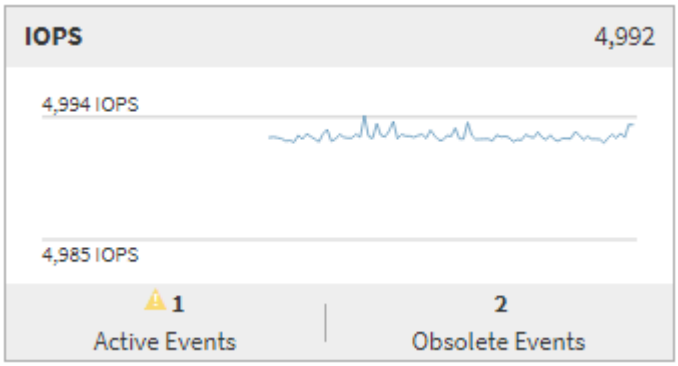
- **Utilisation**

  Pourcentage d'utilisation des objets pour les nœuds et les agrégats, ou utilisation de la bande passante pour les ports.

  Affiché uniquement pour les nœuds, les agrégats et les ports.

En plaçant le curseur sur le nombre d'événements actifs, vous pouvez voir leur type et leur nombre. Les événements critiques sont affichés en rouge (■) et les événements d'avertissement en jaune (■).

Le chiffre en haut à droite du graphique, dans la barre grise, correspond à la valeur moyenne des dernières 72 heures. Les chiffres affichés en bas et en haut de la courbe de tendance représentent les valeurs minimale et maximale des dernières 72 heures. La barre grise située sous le graphique indique le nombre d'événements actifs (nouveaux et acquittés) et d'événements obsolètes des dernières 72 heures.



- **Graphique du compteur de latence**

  Le graphique du compteur de latence offre une vue d'ensemble de la latence des objets au cours des 72 dernières heures. La latence correspond au temps de réponse moyen pour toutes les requêtes d'E/S ; elle est exprimée en millisecondes par opération, soit le temps de service, le temps d'attente, ou les deux, subis par un paquet de données ou un bloc dans le composant de stockage du cluster considéré.

  Haut (valeur du compteur): Le nombre dans l'en-tête affiche la moyenne de la période précédente de 72 heures.

  Partie centrale (graphique de performance) : Le chiffre en bas du graphique indique la latence la plus faible, et celui en haut du graphique indique la latence la plus élevée pour la période précédente de 72 heures. Placez votre curseur sur la courbe de tendance du graphique pour afficher la valeur de latence à un moment précis.

  En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page d'inventaire des événements et consulter les détails complets des événements.

- **Graphique du compteur IOPS**

  Le graphique du compteur IOPS offre une vue d'ensemble de l'état des IOPS de l'objet pour la période précédente de 72 heures. Les IOPS indiquent la vitesse du système de stockage en nombre d'opérations d'entrée/sortie par seconde.

  Haut (valeur du compteur): Le nombre dans l'en-tête affiche la moyenne de la période précédente de 72 heures.

  Partie centrale (graphique de performances) : Le nombre en bas du graphique indique le nombre d'IOPS le plus bas, et le nombre en haut du graphique indique le nombre d'IOPS le plus élevé pour la période précédente de 72 heures. Placez votre curseur sur la courbe de tendance du graphique pour afficher la valeur des IOPS à un moment précis.

  En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page d'inventaire des événements et consulter les détails complets des événements.

- **Graphique du compteur MB/s**

  Le graphique du compteur Mo/s affiche les performances de l'objet en Mo/s et indique la quantité de données transférées vers et depuis l'objet, exprimée en mégaoctets par seconde. Ce graphique offre une vue d'ensemble de l'état de l'objet en Mo/s au cours des 72 dernières heures.

  Haut (valeur du compteur): Le nombre dans l'en-tête affiche le nombre moyen de Mo/s pour les 72 heures précédentes.

  Au milieu (graphique de performance) : La valeur en bas du graphique affiche le nombre le plus faible de Mo/s, et la valeur en haut du graphique affiche le nombre le plus élevé de Mo/s pour la période de 72 heures précédente. Placez votre curseur sur la courbe de tendance du graphique pour afficher la valeur en Mo/s à un moment précis.

  En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page d'inventaire des événements et consulter les détails complets des événements.

- **Graphique du compteur de capacité de performance utilisée**

  Le graphique du compteur « Capacité de performance utilisée » affiche le pourcentage de capacité de performance consommée par l'objet.

  Valeur du compteur (en haut): Le nombre dans l'en-tête affiche la capacité de performance moyenne utilisée au cours des 72 dernières heures.

  Milieu (graphique des performances) : La valeur au bas du graphique affiche le pourcentage le plus faible de capacité de performance utilisée, et la valeur en haut du graphique affiche le pourcentage le plus élevé de capacité de performance utilisée pour la période précédente de 72 heures. Placez votre curseur sur la courbe de tendance du graphique pour afficher la valeur de capacité de performance utilisée à un moment précis.

  En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page d'inventaire des événements et consulter les détails complets des événements.

- **Graphique du compteur d'utilisation**

Le graphique du compteur d'utilisation affiche le pourcentage d'utilisation de l'objet. Le graphique du compteur d'utilisation fournit une vue d'ensemble de haut niveau du pourcentage d'utilisation de l'objet ou de l'utilisation de la bande passante au cours de la période précédente de 72 heures.

Haut (valeur du compteur) : Le nombre dans l'en-tête affiche le pourcentage moyen d'utilisation pour la période précédente de 72 heures.

Milieu (graphique de performance): La valeur en 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 précédente de 72 heures. Placez votre curseur sur la courbe de tendance du graphique pour afficher la valeur d'utilisation à un moment précis.

En bas (événements) : Au survol, la fenêtre contextuelle affiche les détails des événements. Cliquez sur le lien **Événements actifs** sous le graphique pour accéder à la page d'inventaire des événements et consulter les détails complets des événements.

Événements

Le tableau d'historique des événements, le cas échéant, répertorie les événements les plus récents survenus sur cet objet. Lorsque vous cliquez sur le nom d'un événement, ses détails s'affichent sur la page « Détails de l'événement ».

Consultez la page Performance Explorer dans Active IQ Unified Manager

La page Explorateur de performances vous permet de comparer les performances d'objets similaires dans un cluster, par exemple, tous les volumes d'un cluster. Cette fonctionnalité est utile pour le dépannage des événements de performance et l'optimisation des performances des objets. Vous pouvez également comparer des objets avec l'objet racine, qui constitue la référence par rapport à laquelle les autres comparaisons d'objets sont effectuées.

Vous pouvez cliquer sur le bouton **Switch to Health View** pour afficher la page de détails de l'état de santé de cet objet. Dans certains cas, vous pouvez y trouver des informations importantes sur les paramètres de configuration du stockage pour cet objet, qui peuvent vous aider lors du dépannage d'un problème.

La page Explorateur de performances affiche la liste des objets du cluster et leurs données de performance. Elle présente tous les objets du cluster de même type (par exemple, les volumes et leurs statistiques de performance spécifiques) sous forme de tableau. Cette vue offre un aperçu efficace des performances des objets du cluster.

Si « `N/A` » apparaît dans une cellule du tableau, cela signifie qu'aucune valeur n'est disponible pour ce compteur, car il n'y a aucune opération d'E/S sur cet objet à ce moment-là.

La page Performance Explorer contient les composants suivants :

- **Plage de temps**

  Permet de sélectionner une plage horaire pour les données de l'objet.

  Vous pouvez choisir une plage prédéfinie ou spécifier votre propre plage horaire personnalisée.

- **Voir et comparer**

Permet de sélectionner le type d'objet corrélé affiché dans la grille.

Les options disponibles dépendent du type d'objet racine et des données associées. Vous pouvez cliquer sur la liste déroulante « Afficher et comparer » pour sélectionner un type d'objet. Le type d'objet sélectionné s'affiche dans la liste.

- **Filtrage**

  Vous permet de limiter la quantité de données que vous recevez, 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 comparaison avec l'objet racine.

  Les données des objets du volet Comparaison sont affichées dans les graphiques de compteurs.

- **Afficher les statistiques dans**

  Pour les volumes et les LUN, vous pouvez choisir si les statistiques sont affichées après chaque cycle de collecte (5 minutes par défaut) ou si les statistiques sont présentées sous forme de moyenne horaire. Cette fonctionnalité vous permet de consulter le graphique de latence dans le cadre du programme « Performance Guarantee » de NetApp.

- **Graphiques de compteurs**

  Affiche des données graphiques pour chaque catégorie de performance d'objet.

  En général, seuls trois ou quatre graphiques sont affichés par défaut. Le composant Choose charts vous permet d'afficher des graphiques supplémentaires ou de masquer certains d'entre eux. Vous pouvez également choisir d'afficher ou de masquer Events Timeline.

- **Chronologie des événements**

  Affiche les événements de performance et de santé survenus pendant la période sélectionnée dans le composant Plage de temps.

Gérer les performances à l'aide des informations du groupe de règles QoS

Gérez les performances à l'aide des informations des groupes de stratégies QoS dans Active IQ Unified Manager

Unified Manager vous permet d'afficher les groupes de règles de qualité de service (QoS) disponibles sur tous les clusters que vous surveillez. Ces règles peuvent avoir été définies à l'aide du logiciel ONTAP (System Manager ou ONTAP CLI) ou par les règles de niveau de service de performance de Unified Manager. Unified Manager affiche également les volumes et les LUN auxquels un groupe de règles QoS est attribué.

Pour plus d'informations sur le réglage des paramètres QoS, consultez "Aperçu de la gestion des performances"

Contrôlez le débit des charges de travail grâce à la QoS de stockage dans Active IQ Unified Manager

Vous pouvez créer un groupe de règles de qualité de service (QoS) pour contrôler la limite d'E/S par seconde (IOPS) ou de débit (MB/s) des workloads qu'il contient. Si les workloads se trouvent dans un groupe de règles sans limite définie, comme le groupe de règles par défaut, ou si la limite définie ne répond pas à vos besoins, vous pouvez l'augmenter ou déplacer les workloads vers un groupe de règles nouveau ou existant disposant de la limite souhaitée.

Les groupes de stratégies QoS « traditionnels » peuvent être attribués à des workloads individuels, par exemple un seul volume ou LUN. Dans ce cas, le workload peut utiliser la totalité de la limite de débit. Les groupes de stratégies QoS peuvent également être attribués à plusieurs workloads ; dans ce cas, la limite de débit est « partagée » entre les workloads. Par exemple, une limite QoS de 9 000 IOPS attribuée à trois workloads empêcherait le total des IOPS de dépasser 9 000 IOPS.

Les groupes de règles de QoS « Adaptive » peuvent également être attribués à des workloads individuels ou à plusieurs workloads. Cependant, même lorsqu'ils sont attribués à plusieurs workloads, chaque workload bénéficie de l'intégralité de la limite de débit au lieu de partager cette valeur de débit avec les autres workloads. De plus, les règles de QoS adaptative ajustent automatiquement le paramètre de débit en fonction de la taille du volume, par workload, maintenant ainsi le ratio d'IOPS par téraoctet à mesure que la taille du volume change. Par exemple, si le pic est défini sur 5 000 IOPS/To dans une règle de QoS adaptative, un volume de 10 To aura un débit maximal de 50 000 IOPS. Si le volume est ensuite redimensionné à 20 To, la QoS adaptative ajuste le maximum à 100 000 IOPS.

À partir d'ONTAP 9.5, vous pouvez inclure la taille de bloc lors de la définition d'une politique QoS adaptative. Cela convertit effectivement la politique d'un seuil d'IOPS/To en un seuil de Mo/s lorsque les workloads utilisent des tailles de bloc très importantes et finissent par consommer un pourcentage élevé du débit.

Pour les règles QoS de groupe partagées, lorsque les IOPS ou le débit en Mo/s de toutes les charges de travail d'un groupe de règles dépassent la limite définie, le groupe de règles limite les charges de travail afin de restreindre leur activité, ce qui peut dégrader les performances de toutes les charges de travail du groupe de règles. Si un événement de performance dynamique est généré par la limitation d'un groupe de règles, la description de l'événement affiche le nom du groupe de règles concerné.

Dans la vue Performance: All Volumes, vous pouvez trier les volumes concernés par IOPS et Mo/s afin de voir quels workloads présentent l'utilisation la plus élevée et ont pu contribuer à l'événement. Dans la page Performance/Volumes Explorer, vous pouvez sélectionner d'autres volumes, ou des LUN sur le volume, pour les comparer à l'utilisation des IOPS ou du débit en MBps du workload concerné.

En attribuant les workloads qui consomment excessivement les ressources du nœud à un groupe de stratégies plus restrictif, ce groupe de stratégies limite leur activité, ce qui peut réduire l'utilisation des ressources sur ce nœud. Toutefois, si vous souhaitez qu'un workload puisse utiliser davantage de ressources du nœud, vous pouvez augmenter la valeur du groupe de stratégies.

Vous pouvez utiliser System Manager, les commandes ONTAP ou Unified Manager Performance Service Levels pour gérer les groupes de stratégies, notamment les tâches suivantes :

- Création d'un groupe de règles
- Ajout ou suppression de workloads dans un groupe de stratégies
- Déplacer un workload entre des groupes de stratégie
- Modification de la limite de débit d'un groupe de stratégies

- Déplacement d'une workload vers un autre agrégat et/ou nœud

Consultez les groupes de règles QoS disponibles sur tous les clusters dans Active IQ Unified Manager

Vous pouvez afficher une liste de tous les groupes de stratégies QoS disponibles sur les clusters surveillés par Unified Manager. Cela inclut les stratégies QoS traditionnelles, les stratégies QoS adaptatives et les stratégies QoS gérées par les stratégies de niveau de service de performances de Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Groupes de stratégies QoS**.

   La vue Performance: Traditional QoS Policy Groups s'affiche par défaut.

2. Consultez les paramètres de configuration détaillés de chaque groupe de stratégie QoS traditionnelle disponible.
3. Cliquez sur le bouton d'extension ( ) à côté du nom du groupe de stratégie QoS pour afficher plus de détails sur ce groupe de stratégie.
4. Dans le menu Affichage, sélectionnez l'une des options supplémentaires pour afficher tous les groupes de stratégies QoS adaptatifs ou pour afficher tous les groupes de stratégies QoS créés à l'aide de Unified Manager Performance Service Levels.

Afficher les volumes ou les LUN appartenant au même groupe de stratégie QoS dans Active IQ Unified Manager

Vous pouvez afficher la liste des volumes et des LUN attribués au même groupe de stratégie QoS.

Dans le cas des groupes de règles QoS traditionnels qui sont "shared" entre plusieurs volumes, cela peut être utile pour vérifier si certains volumes utilisent de façon excessive le débit défini pour le groupe de règles. Cela peut également vous aider à déterminer si vous pouvez ajouter d'autres volumes au groupe de règles sans impact négatif sur les autres volumes.

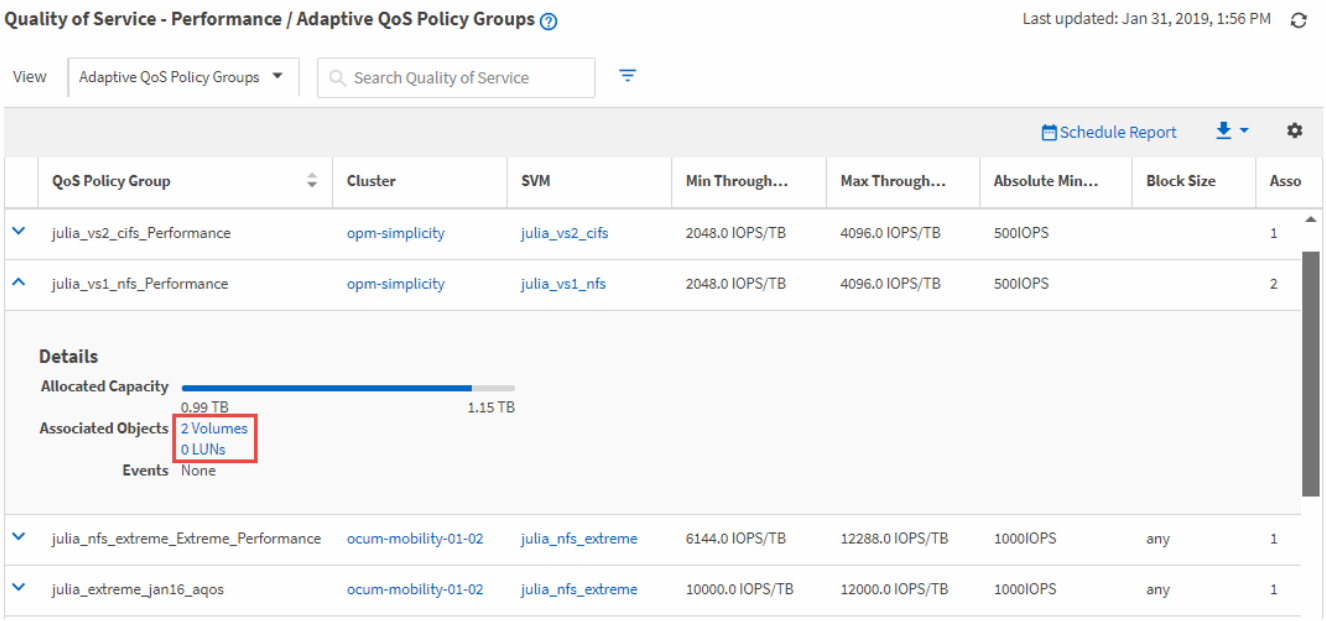
Dans le cas des règles de QoS adaptatives et des règles Unified Manager Performance Service Levels, il peut être utile d'afficher tous les volumes ou LUN qui utilisent un groupe de règles afin de voir quels objets seraient affectés si vous modifiiez les paramètres de configuration de la règle de QoS.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Groupes de stratégies QoS**.

   La vue Performance: Traditional QoS Policy Groups s'affiche par défaut.

2. Si vous vous intéressez au groupe de stratégies traditionnel, restez sur cette page. Sinon, sélectionnez l'une des options d'affichage supplémentaires pour afficher tous les groupes de stratégies QoS adaptatifs ou tous les groupes de stratégies QoS créés par Unified Manager Performance Service Levels.
3. Dans la politique QoS qui vous intéresse, cliquez sur le bouton d'extension ( ) à côté du nom du groupe de politiques QoS pour afficher plus de
   détails.



4. Cliquez sur le lien Volumes ou LUNs pour afficher les objets utilisant cette politique QoS.

   La page d'inventaire des performances pour les volumes ou les LUN affiche la liste triée des objets qui utilisent la politique QoS.

Affichez les paramètres des groupes de règles QoS pour les volumes ou les LUN dans Active IQ Unified Manager

Vous pouvez consulter les groupes de stratégies QoS qui ont été appliqués à vos volumes et LUNs, et vous pouvez accéder à la vue Performance/QoS Policy Groups pour afficher les paramètres de configuration détaillés de chaque stratégie QoS.

Les étapes permettant de consulter la politique QoS appliquée à un volume sont indiquées ci-dessous. La procédure est similaire pour un LUN.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.

   La vue « Santé : Tous les volumes » s'affiche par défaut.

2. Dans le menu Affichage, sélectionnez **Performance: volumes dans le groupe de règles QoS**.
3. Repérez le volume que vous souhaitez examiner et faites défiler vers la droite jusqu'à ce que vous voyiez la colonne **Groupe de stratégie QoS**.
4. Cliquez sur le nom du groupe de stratégies QoS.

   La page Quality of Service correspondante s'affiche selon qu'il s'agit d'une politique QoS traditionnelle, d'une politique QoS adaptative ou d'une politique QoS créée à l'aide de Unified Manager Performance Service Levels.

5. Consultez les paramètres de configuration détaillés du groupe de stratégies QoS.
6. Cliquez sur le bouton d'extension ( ) à côté du nom du groupe de stratégie QoS pour afficher plus de détails sur ce groupe de stratégie.

Comparez les volumes ou les LUN au sein du même groupe de règles QoS dans Active IQ Unified Manager

Vous pouvez visualiser les volumes et les LUN qui se trouvent dans les mêmes groupes de stratégie QoS, puis comparer les performances sur un seul graphique IOPS, MB/s ou IOPS/TB pour identifier les éventuels problèmes.

Les étapes permettant de comparer les performances des volumes appartenant au même groupe de règles QoS sont décrites ci-dessous. La procédure pour consulter ces informations pour un LUN est similaire.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.

   La vue « Santé : Tous les volumes » s'affiche par défaut.

2. Dans le menu Affichage, sélectionnez **Performance: volumes dans le groupe de règles QoS**.
3. Cliquez sur le nom du volume que vous souhaitez consulter.

   La page Performance Explorer s'affiche pour le volume.

4. Dans le menu Afficher et comparer, sélectionnez **Volumes dans le même groupe de stratégie QoS**.

   Les autres volumes qui partagent la même politique QoS sont répertoriés dans le tableau ci-dessous.

5. Cliquez sur le bouton **Ajouter** pour ajouter ces volumes aux graphiques afin de pouvoir comparer les IOPS, les MB/s, les IOPS/TB et autres compteurs de performance pour tous les volumes sélectionnés dans les graphiques.

   Vous pouvez modifier la plage horaire pour visualiser les performances sur différents intervalles de temps autres que l'intervalle par défaut de 72 heures.

Affichez les politiques QoS dans les graphiques de débit avec Active IQ Unified Manager

Vous pouvez consulter les paramètres de stratégie de qualité de service (QoS) définis par ONTAP et appliqués à un volume ou un LUN dans l'Explorateur de performances et les graphiques IOPS, IOPS/TB et Mo/s de l'analyse du workload. Les informations affichées dans les graphiques diffèrent selon le type de stratégie de QoS appliquée au workload.

Le paramètre de débit maximal (ou « `peak` ») définit le débit maximal que le workload peut consommer, et limite ainsi l'impact des workloads concurrents sur les ressources système. Le paramètre de débit minimal (ou « `expected` ») définit le débit minimal qui doit être disponible pour le workload, afin qu'un workload critique atteigne ses objectifs de débit minimal, quelle que soit la demande des workloads concurrents.

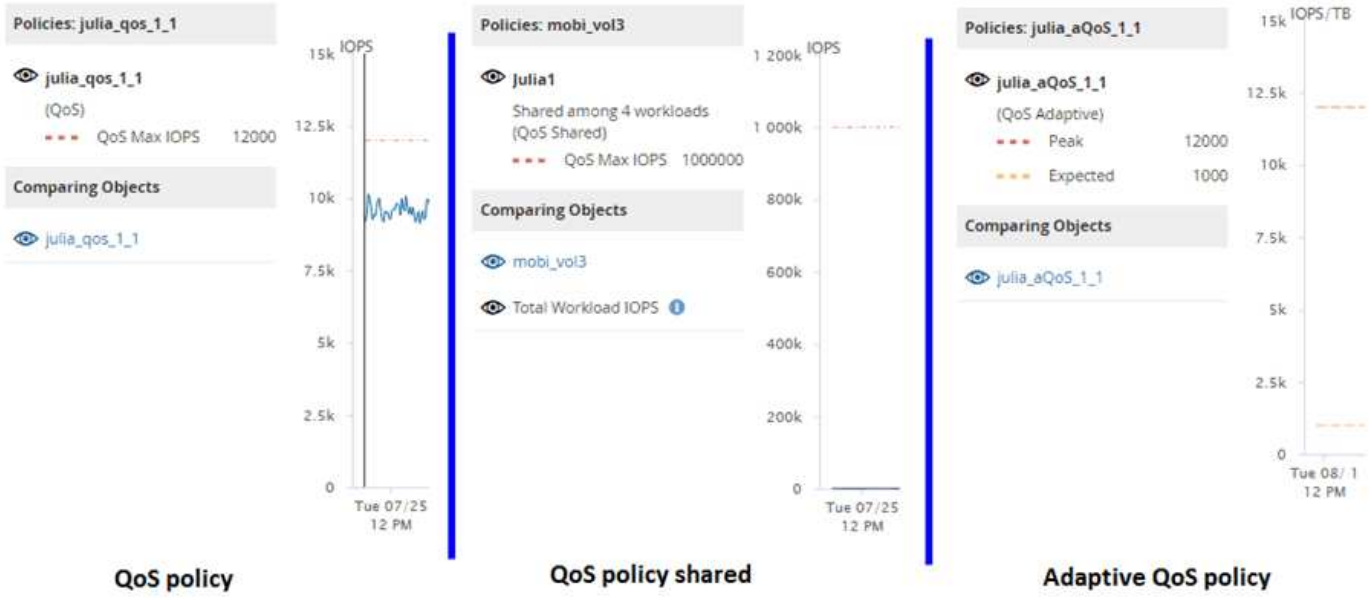
Les politiques QoS partagées et non partagées pour les IOPS et les Mo/s utilisent les termes « `minimum` » et « `maximum` » pour définir les valeurs plancher et plafond. Les politiques QoS adaptatives pour les IOPS/To, introduites dans ONTAP 9.3, utilisent les termes « `expected` » et « `peak` » pour définir les valeurs plancher et plafond.

Bien que ONTAP vous permette de créer ces deux types de politiques QoS, selon la manière dont elles sont appliquées aux workloads, la politique QoS s'affichera de trois manières différentes dans les graphiques de

performance.

Type de politique	Fonctionnalité	Indicateur dans l'interface Unified Manager
Politique QoS partagée attribuée à un seul workload, ou politique QoS non partagée attribuée à un seul workload ou à plusieurs workloads	Chaque workload peut consommer le paramètre de débit spécifié	Affiche « `(QoS)` »
Politique QoS partagée attribuée à plusieurs workloads	Tous les workloads partagent le paramètre de débit spécifié	Affiche « `(QoS Shared)` »
Politique QoS adaptative attribuée à un seul workload ou à plusieurs workloads	Chaque workload peut consommer le paramètre de débit spécifié	Affiche « `(QoS Adaptive)` »

La figure suivante illustre un exemple de la manière dont les trois options sont affichées dans les graphiques de compteurs.



Lorsqu'une politique QoS normale définie en IOPS apparaît dans le graphique IOPS/TB d'une workload, ONTAP convertit la valeur IOPS en une valeur IOPS/TB et Unified Manager affiche cette politique dans le graphique IOPS/TB avec le texte « `QoS, defined in IOPS` ».

Lorsqu'une stratégie QoS adaptative définie en IOPS/TB apparaît dans le graphique des IOPS d'un workload, ONTAP convertit la valeur IOPS/TB en une valeur IOPS et Unified Manager affiche cette stratégie dans le graphique des IOPS avec le texte « `QoS Adaptive - Used, defined in IOPS/TB` » ou « `QoS Adaptive - Allocated, defined in IOPS/TB` », selon la configuration du paramètre d'allocation des IOPS maximales. Lorsque le paramètre d'allocation est défini sur « `allocated-space` », les IOPS maximales sont calculées en fonction de la taille du volume. Lorsque le paramètre d'allocation est défini sur « `used-space` », les IOPS maximales sont calculées en fonction de la quantité de données stockées dans le volume, en tenant compte des efficacités de stockage.

Le graphique IOPS/TB affiche les données de performance uniquement lorsque la capacité logique utilisée par le volume est supérieure ou égale à 128 Go. Des lacunes s'affichent dans le graphique lorsque la capacité utilisée passe en dessous de 128 Go pendant la période

sélectionnée.

Affichez les paramètres QoS minimum et maximum de la charge de travail dans Active IQ Unified Manager

Vous pouvez consulter les paramètres de stratégie de qualité de service (QoS) définis par ONTAP pour un volume ou un LUN dans les graphiques de l'Explorateur de performances. Un paramètre de débit maximal limite l'impact des workloads concurrents sur les ressources système. Un paramètre de débit minimal garantit qu'un workload critique atteint les objectifs de débit minimaux, quelle que soit la demande des workloads concurrents.

Les paramètres de débit QoS « `minimum` » et « `maximum` » (IOPS et MB/s) ne s'affichent dans les graphiques de compteurs que s'ils ont été configurés dans ONTAP. Les paramètres de débit minimum sont disponibles uniquement sur les systèmes exécutant ONTAP 9.2 ou une version ultérieure, uniquement sur les systèmes AFF, et ne peuvent être définis que pour les IOPS pour le moment.

Les politiques QoS adaptatives sont disponibles à partir de ONTAP 9.3 et sont exprimées en IOPS/TB au lieu d'IOPS. Ces politiques ajustent automatiquement la valeur de la politique QoS en fonction de la taille du volume, par workload, maintenant ainsi le ratio d'IOPS par téraoctet à mesure que la taille du volume change. Vous pouvez appliquer un groupe de politiques QoS adaptatives aux volumes uniquement. La terminologie QoS « `expected` » et « `peak` » est utilisée pour les politiques QoS adaptatives au lieu de minimum et maximum.

Unified Manager génère des événements d'avertissement en cas de violation des règles de QoS lorsque le débit du workload a dépassé le paramètre maximal défini par la règle de QoS au cours de chaque période de collecte des performances de l'heure précédente. Le débit du workload peut dépasser le seuil de QoS 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. C'est pourquoi vous pouvez voir des événements de QoS alors que le débit d'un workload n'a peut-être pas dépassé le seuil de règle indiqué sur le graphique.

Étapes

1. Dans la page **Performance Explorer** du volume ou du LUN sélectionné, effectuez les actions suivantes pour afficher les paramètres de plafond et de plancher QoS :

Si vous voulez…	Faites ceci…
Afficher le plafond des IOPS (le maximum de QoS)	Dans le graphique IOPS total ou détaillé, cliquez sur **Zoom View**.
Afficher le plafond en MB/s (le maximum QoS)	Dans le graphique MB/s Total ou Breakdown, cliquez sur **Zoom View**.
Afficher le plancher d'IOPS (le minimum QoS)	Dans le graphique IOPS total ou détaillé, cliquez sur **Zoom View**.
Afficher le plafond IOPS/TB (le pic de QoS)	Pour les volumes, dans le graphique IOPS/TB, cliquez sur **Zoom View**.
Afficher le plancher IOPS/TB (la QoS attendue)	Pour les volumes, dans le graphique IOPS/TB, cliquez sur **Zoom View**.

La ligne horizontale en pointillés indique la valeur de débit maximale ou minimale définie dans ONTAP. Vous pouvez également consulter la date d'application des modifications apportées aux valeurs QoS.

2. Pour afficher les valeurs IOPS et MB/s spécifiques par rapport au paramètre QoS, déplacez votre curseur dans la zone du graphique pour faire apparaître la fenêtre contextuelle.

Si vous constatez que certains volumes ou LUN présentent des IOPS ou des MB/s très élevés et sollicitent fortement les ressources système, vous pouvez utiliser System Manager ou l'ONTAP CLI pour ajuster les paramètres QoS afin que ces workloads n'affectent pas les performances des autres workloads.

Pour plus d'informations sur le réglage des paramètres QoS, consultez "Aperçu de la gestion des performances"

Gérez les performances à l'aide de la capacité de performance et des informations sur les IOPS disponibles

Gérez la capacité de performance et les IOPS disponibles dans Active IQ Unified Manager

La capacité de performance indique le débit maximal que vous pouvez obtenir d'une ressource sans dépasser ses performances utiles. En utilisant les compteurs de performance existants, la capacité de performance correspond au seuil d'utilisation maximale d'un nœud ou d'un agrégat avant que la latence ne devienne problématique.

Unified Manager collecte les statistiques de capacité de performance des nœuds et les agrège dans chaque cluster. La *capacité de performance utilisée* correspond au pourcentage de capacité de performance actuellement utilisée, et la *capacité de performance libre* correspond au pourcentage de capacité de performance encore disponible.

Alors que la capacité de performance libre indique le pourcentage de la ressource encore disponible, les IOPS disponibles vous indiquent le nombre d'IOPS pouvant être ajoutés à la ressource avant d'atteindre sa capacité de performance maximale. Grâce à cette métrique, vous avez la garantie de pouvoir ajouter des charges de travail d'un nombre prédéterminé d'IOPS à une ressource.

Le suivi des informations relatives aux capacités de performance présente les avantages suivants :

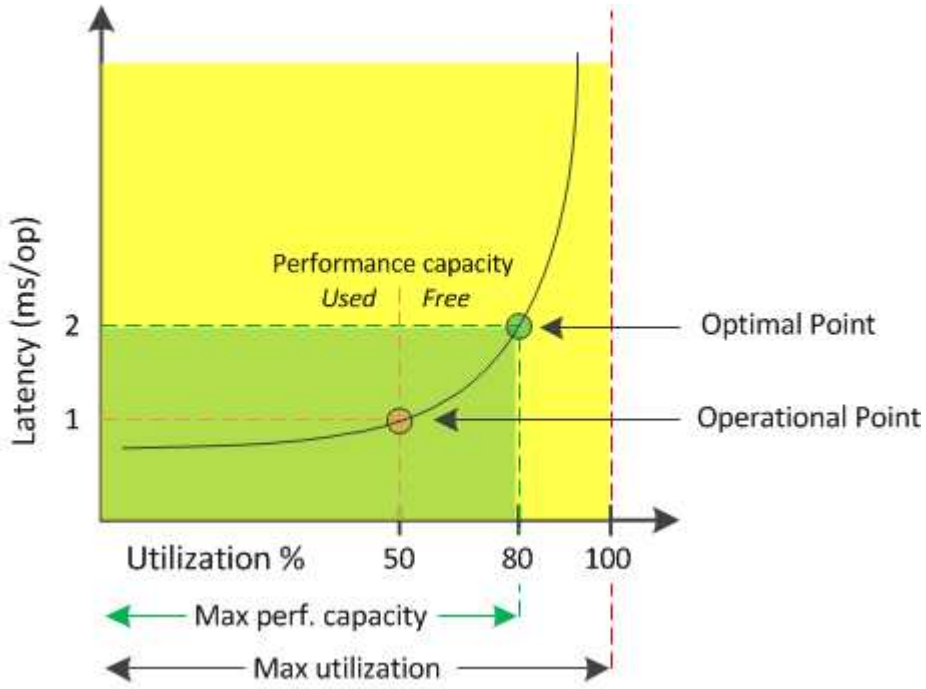
- Contribue au provisionnement et à l'équilibrage des workflows.
- Permet d'éviter la surcharge d'un nœud ou la sollicitation excessive de ses ressources, réduisant ainsi le besoin de dépannage.
- Vous aide à déterminer avec plus de précision où des équipements de stockage supplémentaires pourraient être nécessaires.

Comprendre le compteur de capacité de performance utilisée dans Active IQ Unified Manager

Le compteur de capacité de performance utilisée permet d'identifier si les performances d'un nœud ou d'un agrégat atteignent un point où elles risquent de se dégrader si les workloads augmentent. Il peut également indiquer si un nœud ou un agrégat est actuellement surutilisé pendant certaines périodes. La capacité de performance utilisée est similaire à l'utilisation, mais elle fournit davantage d'informations sur les capacités de performance disponibles d'une ressource physique pour un workload spécifique.

La capacité de performance utilisée optimale correspond au point où un nœud ou un agrégat présente une

utilisation et une latence (temps de réponse) optimales, et est utilisé efficacement. La figure suivante illustre un exemple de courbe de latence en fonction de l'utilisation pour un agrégat.



Dans cet exemple, le *point opérationnel* indique que l'agrégat fonctionne actuellement à 50 % d'utilisation avec une latence de 1,0 ms/op. D'après les statistiques collectées à partir de l'agrégat, Unified Manager détermine qu'une capacité de performance supplémentaire est disponible pour cet agrégat. Dans cet exemple, le *point optimal* correspond au moment 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 d'utiliser vos systèmes plus efficacement.

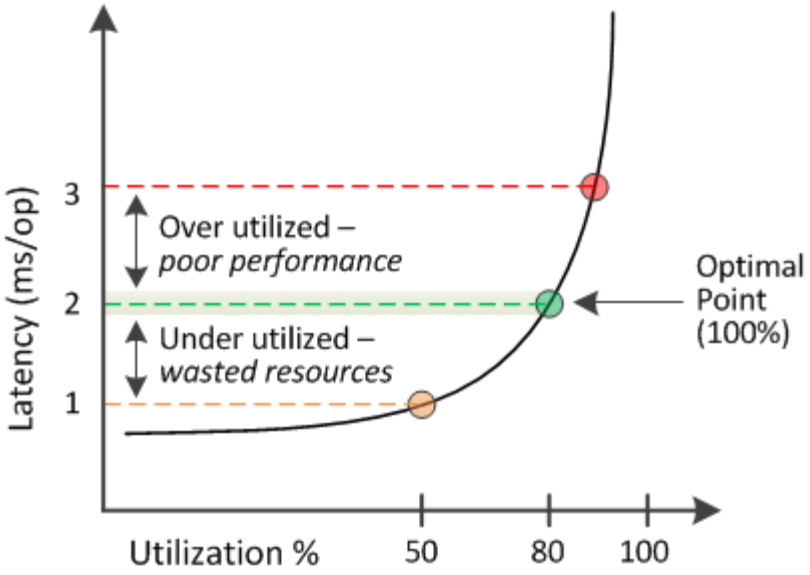
Le compteur de capacité de performance utilisée devrait afficher une valeur supérieure au compteur "utilization", car la capacité de performance prend en compte l'impact sur la latence. Par exemple, si un nœud ou un agrégat est utilisé à 70 %, la valeur de capacité de performance peut se situer entre 80 % et 100 %, selon la latence.

Dans certains cas, toutefois, le compteur d'utilisation peut être plus élevé sur la page Dashboard. Cela est normal, car le tableau de bord actualise les valeurs actuelles du compteur à chaque période de collecte ; il n'affiche pas de moyennes sur une période donnée comme le font les autres pages de l'interface utilisateur Unified Manager. Le compteur de capacité de performance utilisée est préférable comme indicateur des performances moyennées sur une période donnée, tandis que le compteur d'utilisation est préférable pour déterminer l'utilisation instantanée d'une ressource.

Utilisez la valeur de capacité de performance utilisée dans Active IQ Unified Manager

L'indicateur de capacité de performance utilisée vous aide à identifier les nœuds et les agrégats actuellement surutilisés ou sous-utilisés. Vous pouvez ainsi redistribuer les charges de travail afin d'optimiser l'utilisation de vos ressources de stockage.

La figure suivante illustre la courbe de latence en fonction de l'utilisation d'une ressource et identifie, par des points colorés, trois zones où pourrait se situer le point de fonctionnement actuel.



- Un pourcentage d'utilisation de la capacité de performance égal à 100 correspond au point optimal.

  Les ressources sont utilisées efficacement à ce stade.

- Un pourcentage de capacité de performances utilisée supérieur à 100 indique que le nœud ou l'agrégat est surutilisé et que les workloads bénéficient de performances sous-optimales.

  Aucun nouveau workload ne doit être ajouté à la ressource, et les workloads existants pourraient devoir être redistribués.

- Un pourcentage de capacité de performance utilisée inférieur à 100 indique que le nœud ou l'agrégat est sous-utilisé et que les ressources ne sont pas utilisées efficacement.

  D'autres workloads peuvent être ajoutés à la ressource.

Contrairement au taux d'utilisation, le pourcentage de capacité de performance utilisée peut dépasser 100 %. Il n'y a pas de pourcentage maximal, mais les ressources se situent généralement entre 110 % et 140 % lorsqu'elles sont surutilisées. Des pourcentages plus élevés indiquent qu'une ressource présente de graves problèmes.

Comprendre les IOPS disponibles dans Active IQ Unified Manager

Le compteur d'IOPS disponibles indique le nombre d'IOPS restants pouvant être ajoutés à un nœud ou à un agrégat avant que la ressource n'atteigne sa limite.

Le nombre total d'IOPS qu'un nœud peut fournir est basé sur les caractéristiques physiques du nœud, par exemple le nombre de processeurs, la vitesse du processeur et la quantité de RAM. Le nombre total d'IOPS qu'un agrégat peut fournir est basé sur les propriétés physiques des disques, par exemple un disque SATA, SAS ou SSD.

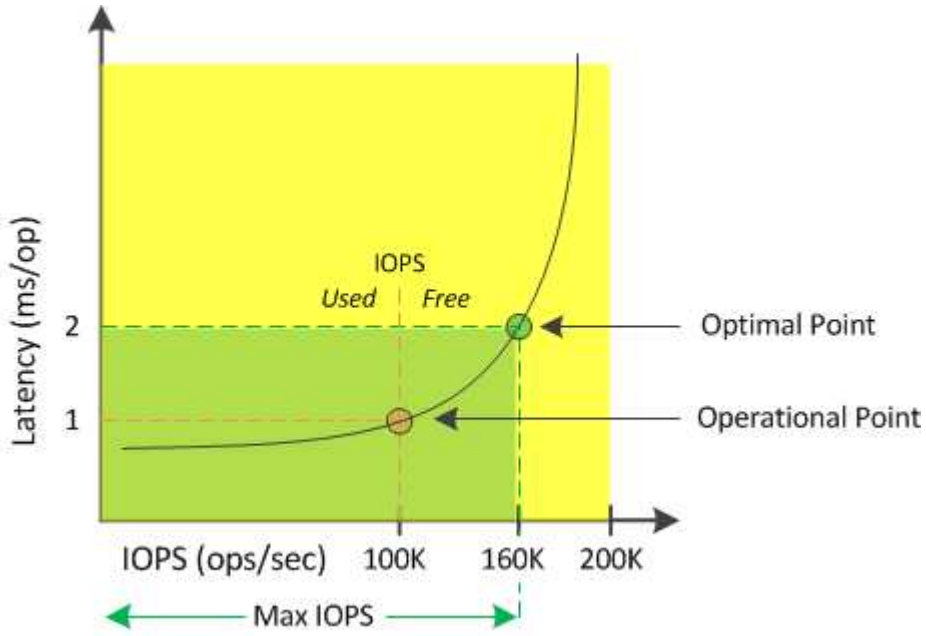
Le total des IOPS de tous les volumes d'un agrégat peut ne pas correspondre au total des IOPS de l'agrégat. Ce point est abordé dans l'article suivant de la base de connaissances : KB "Pourquoi la somme de tous les IOPs de volume dans un agrégat ne correspond-elle pas aux IOPs de l'agrégat ?"

Alors que le compteur de capacité de performances disponible indique le pourcentage d'une ressource encore disponible, le compteur d'IOPS disponibles vous indique le nombre exact d'IOPS (workloads) qui peuvent être

ajoutées à une ressource avant d'atteindre la capacité de performances maximale.

Par exemple, si vous utilisez une paire de systèmes de stockage FAS2520 et FAS8060, une valeur de capacité de performances disponible de 30 % signifie que vous disposez d'une certaine capacité de performances libre. Cependant, cette valeur n'indique pas combien de workloads supplémentaires vous pouvez déployer sur ces nœuds. Le compteur d'IOPS disponibles peut indiquer que vous disposez de 500 IOPS disponibles sur le FAS8060, mais de seulement 100 IOPS disponibles sur le FAS2520.

La figure suivante présente un exemple de courbe de latence en fonction des IOPS pour un nœud.



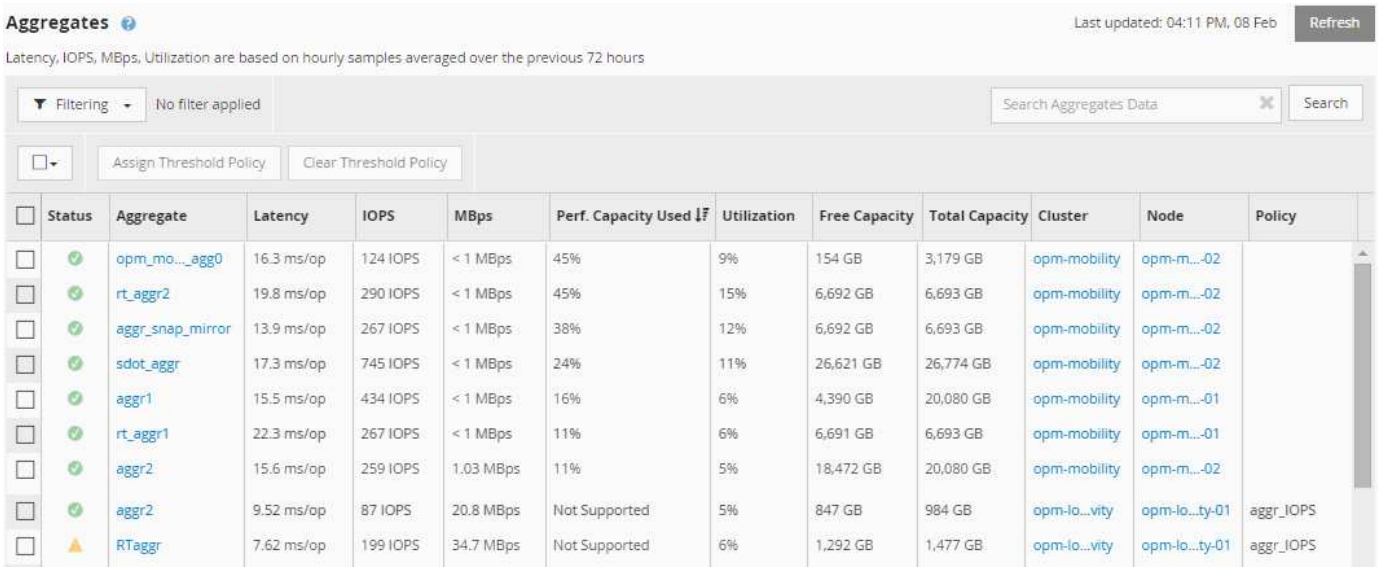
Le nombre maximal d'IOPS qu'une ressource peut fournir est le nombre d'IOPS lorsque le compteur de capacité de performance utilisée est à 100 % (le point optimal). Le point de fonctionnement indique que le nœud fonctionne actuellement à 100K IOPS avec une latence de 1.0 ms/op. D'après les statistiques capturées à partir du nœud, Unified Manager détermine que le nombre maximal d'IOPS pour le nœud est de 160K, ce qui signifie qu'il y a 60K IOPS libres ou disponibles. Par conséquent, vous pouvez ajouter davantage de workloads à ce nœud afin que vos systèmes soient utilisés plus efficacement.

En cas d'activité utilisateur minimale sur la ressource, la valeur des IOPS disponibles est calculée sur la base d'un workload générique d'environ 4 500 IOPS par cœur de processeur. En effet, Unified Manager ne dispose pas des données nécessaires pour estimer précisément les caractéristiques du workload pris en charge.

Afficher les valeurs de capacité de performance utilisées des nœuds et des agrégats dans Active IQ Unified Manager

Vous pouvez surveiller les valeurs de capacité de performance utilisées pour tous les nœuds ou pour tous les agrégats d'un cluster, ou consulter les détails d'un seul nœud ou agrégat.

Les valeurs de capacité de performance utilisée apparaissent dans le Dashboard, les pages Performance Inventory, la page Top Performers, la page Create Threshold Policy, les pages Performance Explorer et dans les graphiques détaillés. Par exemple, la page Performance: All Aggregates comporte une colonne Performance Capacity Used permettant d'afficher la valeur de capacité 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

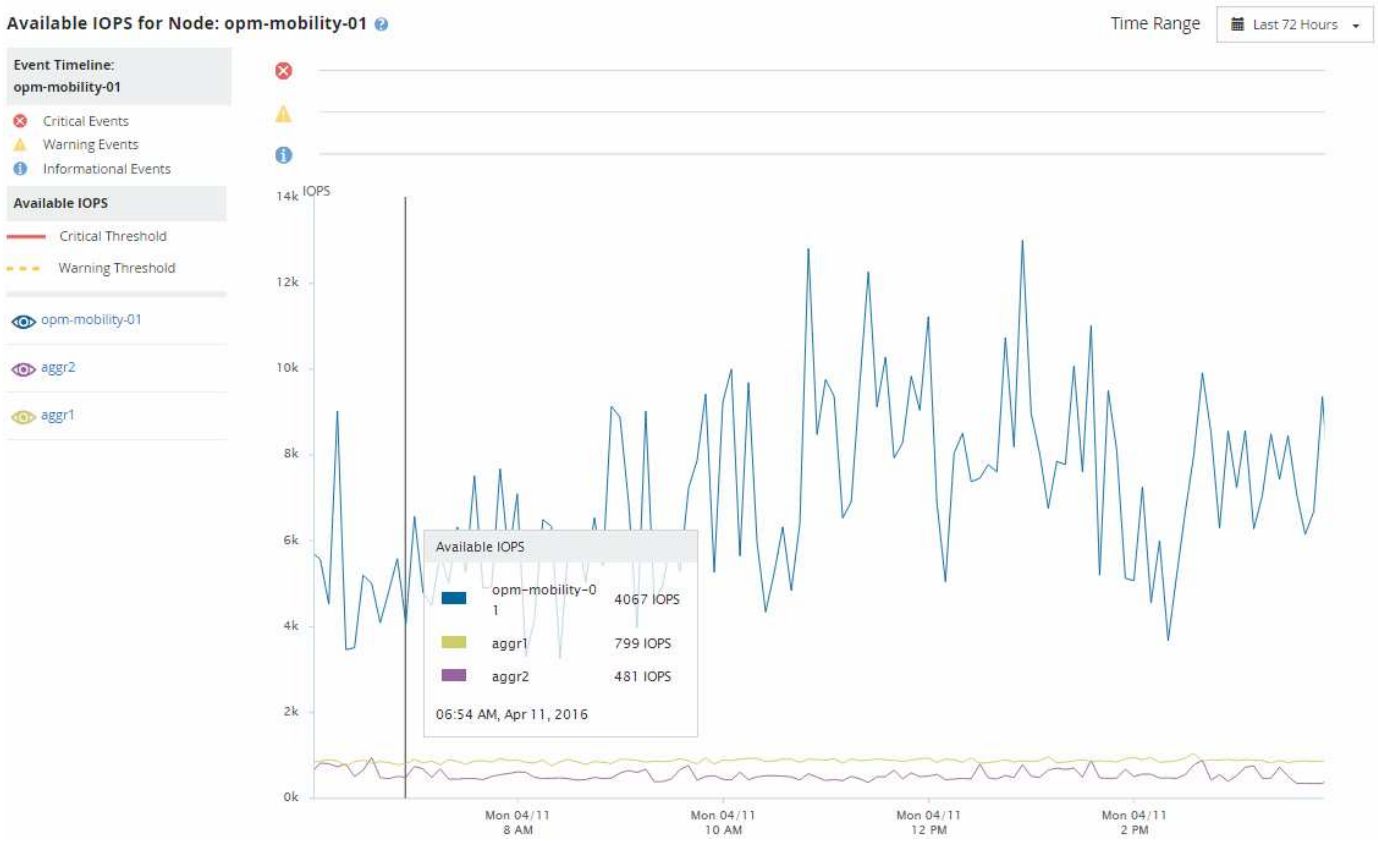
Le compteur de capacité de performance utilisée vous permet d'identifier les éléments suivants :

- Si des nœuds ou des agrégats de clusters ont une valeur élevée de capacité de performance utilisée
- Si des nœuds ou des agrégats sur un cluster présentent des événements actifs d'utilisation de la capacité de performance
- Les nœuds et les agrégats qui présentent la valeur de capacité de performances utilisée la plus élevée et la plus faible dans un cluster
- Valeurs des compteurs de latence et d'utilisation associées aux nœuds ou agrégats présentant des valeurs d'utilisation de capacité de performance élevées
- Comment les valeurs de capacité de performance utilisées pour les nœuds d'une paire haute disponibilité seront affectées si l'un des nœuds tombe en panne
- Les volumes et les LUN les plus sollicités sur un agrégat ayant une valeur élevée de capacité de performance utilisée

Consultez les valeurs IOPS disponibles pour les nœuds et les agrégats dans Active IQ Unified Manager

Vous pouvez surveiller les valeurs IOPS disponibles pour tous les nœuds ou pour tous les agrégats d'un cluster, ou vous pouvez consulter les détails d'un seul nœud ou agrégat.

Les valeurs d'IOPS disponibles apparaissent dans les pages d'inventaire des performances 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 Node/Performance Explorer, vous pouvez sélectionner le graphique du compteur « `Available IOPS` » dans la liste afin de comparer les valeurs d'IOPS disponibles pour le nœud et plusieurs agrégats sur ce nœud.



La surveillance du compteur des IOPS disponibles vous permet d'identifier :

- Les nœuds ou agrégats présentant les valeurs d'IOPS disponibles les plus élevées permettent de déterminer où les futurs workloads peuvent être déployés.
- Les nœuds ou agrégats présentant les valeurs IOPS disponibles les plus faibles permettent d'identifier les ressources à surveiller afin de déceler d'éventuels problèmes de performance futurs.
- Les volumes et LUN les plus sollicités sur un agrégat ayant une faible valeur d'IOPS disponible.

Consultez les graphiques des compteurs de capacité de performance dans Active IQ Unified Manager

Vous pouvez afficher les graphiques de capacité de performance utilisée pour les nœuds et les agrégats sur la page Explorateur de performances. Cela vous permet d'afficher des données détaillées sur la capacité de performance des nœuds et des agrégats sélectionnés pour une période donnée.

Le graphique de compteur standard affiche les valeurs de capacité de performances utilisées pour les nœuds ou agrégats sélectionnés. Le graphique de compteur détaillé affiche les valeurs totales de capacité de performances de l'objet racine, ventilées selon l'utilisation par les protocoles utilisateur et les processus système en arrière-plan. En outre, la quantité de capacité de performances libre est également indiquée.

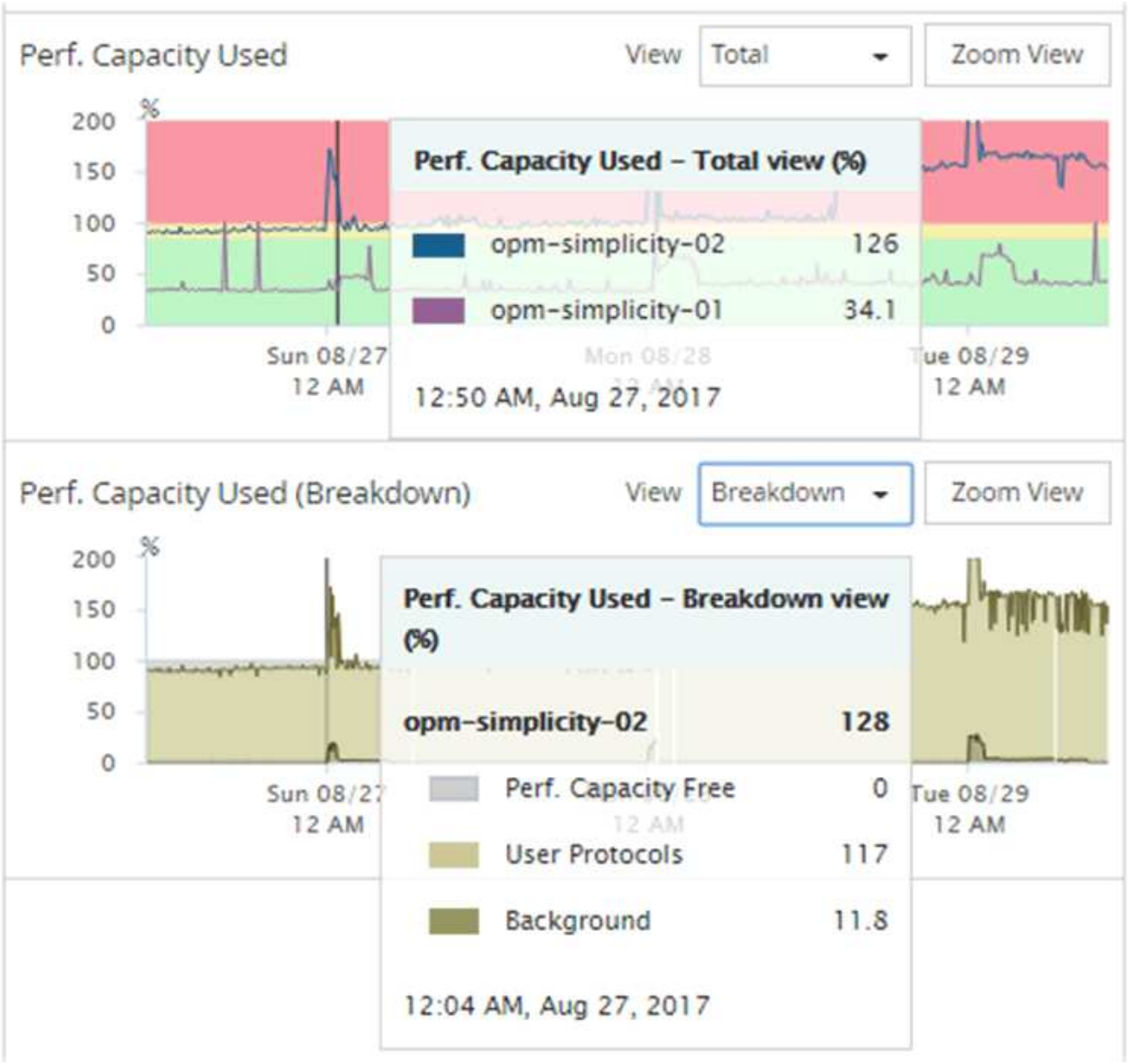
Étant donné que certaines activités en arrière-plan liées à la gestion du système et des données sont identifiées comme des workloads utilisateur et catégorisées comme des protocoles utilisateur, le pourcentage de protocoles utilisateur peut paraître artificiellement élevé lorsque ces processus s'exécutent. Ces processus s'exécutent généralement aux alentours de minuit, lorsque l'utilisation du cluster est faible. Si vous constatez un pic d'activité des protocoles utilisateur aux alentours de minuit, vérifiez si des 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** dans une page **Landing** de nœud ou d'agrégat.
2. Dans le volet **Graphiques de compteurs**, cliquez sur **Choisir les graphiques**, puis sélectionnez le graphique **Perf. Capacité utilisée**.
3. Faites défiler vers le bas jusqu'à ce que vous puissiez voir le graphique.

   Les couleurs du graphique standard indiquent si l'objet se trouve dans la plage optimale (jaune), s'il est sous-utilisé (vert) ou s'il est surutilisé (rouge). Le graphique de répartition affiche des informations détaillées sur la capacité de performance de l'objet racine uniquement.



4. Si vous souhaitez afficher l'un ou l'autre graphique en taille réelle, cliquez sur **Zoom View**.

   De cette manière, vous pouvez ouvrir plusieurs graphiques de compteur dans des fenêtres distinctes pour comparer les valeurs de capacité de performance utilisée aux valeurs d'IOPS ou de MBps sur la même

période.

Configurez les seuils de capacité de performance utilisés dans Active IQ Unified Manager

Vous pouvez créer des règles de seuil de performance définies par l'utilisateur afin que des événements soient déclenchés lorsque la valeur de capacité de performance utilisée pour un nœud ou un agrégat dépasse le paramètre de seuil de capacité de performance utilisée défini.

De plus, les nœuds peuvent être configurés avec une politique de seuil « `Performance capacity used takeover` ». Cette politique de seuil totalise les statistiques de capacité de performance utilisée pour les deux nœuds d'une paire haute disponibilité afin de déterminer si l'un des nœuds manquerait de capacité suffisante en cas de défaillance de l'autre nœud. Étant donné que la workload lors d'un basculement est la combinaison des workloads des deux nœuds partenaires, la même politique « Performance capacity used takeover » peut être appliquée aux deux nœuds.



Cette équivalence de capacité de performance utilisée est généralement vérifiée entre les nœuds. Cependant, si le trafic inter-nœuds destiné à l'un des nœuds via son partenaire de basculement est nettement plus important, la capacité de performance totale utilisée lors de l'exécution de tous les workloads sur un nœud partenaire par rapport à l'autre pourrait être légèrement différente selon le nœud défaillant.

Les conditions de capacité de performance utilisée peuvent également servir de paramètres de seuil de performance secondaires pour créer une stratégie de seuil combinée lors de la définition des seuils pour les LUN et les volumes. La condition de capacité de performance utilisée s'applique à l'agrégat ou au nœud sur lequel se trouvent le volume ou le LUN. Par exemple, vous pouvez créer une stratégie de seuil combinée à l'aide des critères suivants :

Objet de stockage	Compteur de performances	Seuil d'alerte	Seuil critique	Durée
Volume	Latence	15 ms/op	25 ms/op	20 minutes
Agrégat	Capacité de performance utilisée	80%	95%	

Les politiques de seuil combiné ne génèrent un événement que lorsque les deux conditions sont dépassées pendant toute la durée.

Utilisez le compteur de capacité de performance utilisée dans Active IQ Unified Manager

En règle générale, les organisations souhaitent fonctionner avec un pourcentage de capacité de performance utilisée inférieur à 100 afin que les ressources soient utilisées efficacement tout en réservant une capacité de performance supplémentaire pour répondre aux demandes des périodes de pointe. Vous pouvez utiliser des politiques de seuil pour personnaliser le moment où des alertes sont envoyées en cas de valeurs élevées de capacité de performance utilisée.

Vous pouvez définir des objectifs précis en fonction de vos exigences de performance. Par exemple, les entreprises de services financiers peuvent réserver une capacité de performance plus importante afin de

garantir l'exécution rapide des transactions. Elles peuvent fixer des seuils d'utilisation de la capacité de performance compris entre 70 et 80 %. Les entreprises manufacturières aux marges plus faibles peuvent choisir de réserver une capacité de performance moindre si elles sont prêtes à accepter un certain risque de performance afin de mieux maîtriser leurs coûts IT. Ces entreprises peuvent fixer des seuils d'utilisation de la capacité de performance compris entre 85 et 95 %.

Lorsque la valeur de capacité de performance utilisée dépasse le pourcentage défini dans une règle de seuil définie par l'utilisateur, Unified Manager envoie un e-mail d'alerte et ajoute l'événement à la page Event Inventory. Vous pouvez ainsi gérer les problèmes potentiels avant qu'ils n'affectent les performances. Ces événements peuvent également indiquer que vous devez déplacer des workloads et effectuer des modifications au sein de vos nœuds et agrégats.

Comprendre et utiliser la page de planification du basculement de nœud

Utilisez la page Node Failover Planning dans Active IQ Unified Manager

La page « Planification des performances/basculement de nœud » estime l'impact sur les performances d'un nœud en cas de défaillance de son nœud partenaire haute disponibilité (HA). Unified Manager fonde ces estimations sur les performances historiques des nœuds de la paire haute disponibilité.

L'estimation de l'impact d'un basculement sur les performances vous aide à planifier les scénarios suivants :

- Si un basculement dégrade systématiquement les performances estimées du nœud de reprise à un niveau inacceptable, vous pouvez envisager de prendre des mesures correctives pour réduire l'impact du basculement sur les performances.
- Avant d'initier un basculement manuel pour effectuer des tâches de maintenance matérielle, vous pouvez estimer l'impact du basculement sur les performances du nœud de prise de contrôle afin de déterminer le meilleur moment pour effectuer cette tâche.

Déterminez les actions correctives à partir de la page Performance/Node Failover Planning dans Active IQ Unified Manager

En vous basant sur les informations affichées sur la page « Planification des performances/basculement des nœuds », vous pouvez prendre des mesures pour éviter qu'un basculement n'entraîne une baisse des performances d'une paire haute disponibilité en dessous d'un niveau acceptable.

Par exemple, pour réduire l'impact estimé d'un basculement sur les performances, vous pouvez déplacer certains volumes ou LUN d'un nœud de la paire haute disponibilité vers d'autres nœuds du cluster. Cela garantit que le nœud principal peut continuer à fournir des performances acceptables après un basculement.

Examinez les composants de la page Planification du basculement des performances/nœuds dans Active IQ Unified Manager

Les éléments de la page « Planification des performances/basculement de nœud » sont affichés sous forme de grille et dans le volet Comparaison. Ces sections vous permettent d'évaluer l'impact d'un basculement de nœud sur les performances du nœud de reprise.

Grille de statistiques de performance

La page de planification du basculement des performances/nœuds affiche une grille contenant des statistiques sur la latence, les IOPS, l'utilisation et la capacité de performance utilisée.

> Les valeurs de latence et d'IOPS affichées sur cette page et sur la page Performance/Explorateur de performances des nœuds peuvent ne pas correspondre, car différents compteurs de performances sont utilisés pour calculer les valeurs afin de prédire le basculement du nœud.

Dans la grille, chaque nœud se voit attribuer l'un des rôles suivants :

- Primaire

  Le nœud qui prend le relais du partenaire HA en cas de défaillance de ce dernier. L'objet racine est toujours le nœud principal.

- Partenaire

  Le nœud qui tombe en panne dans le scénario de basculement.

- Acquisition estimée

  Identique au nœud principal. Les statistiques de performance affichées pour ce nœud indiquent les performances du nœud de reprise après la prise de relais du partenaire défaillant.

> Bien que le workload du nœud de reprise soit équivalent aux workloads combinés des deux nœuds après un basculement, les statistiques du nœud de reprise 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 la latence du nœud partenaire de 3 ms/op, le nœud de reprise estimé peut avoir une latence de 4 ms/op. Cette valeur est un calcul effectué par Unified Manager.

Vous pouvez cliquer sur le nom du nœud Partner si vous souhaitez qu'il devienne l'objet racine. Une fois la page Performance/Node Performance Explorer affichée, vous pouvez cliquer sur l'onglet **Failover Planning** pour voir comment les performances changent dans ce scénario de panne de nœud. Par exemple, si Node1 est le nœud Primary et Node2 le nœud Partner, vous pouvez cliquer sur Node2 pour en faire le nœud Primary. De cette manière, vous pouvez voir comment les performances estimées changent selon le nœud qui tombe en panne.

Volet de comparaison

La liste suivante décrit les composants affichés par défaut dans le volet Comparaison :

- **Graphiques des événements**

  Elles sont affichées dans le même format que celles de la page Performance/Node Performance Explorer. Elles concernent uniquement le nœud principal.

- **Graphiques de compteurs**

  Ils affichent des statistiques historiques pour le compteur de performance indiqué dans la grille. Dans chaque graphique, celui du nœud « Prise de contrôle estimée » illustre les performances estimées si un basculement s'était produit à un moment donné.

Par exemple, supposons que le graphique d'utilisation indique 73 % pour le nœud de reprise estimé à 11 h le 8 février. Si un basculement s'était produit à ce moment-là, l'utilisation du nœud de reprise aurait été de 73 %.

Les statistiques historiques vous aident à déterminer le moment optimal pour déclencher un basculement, minimisant ainsi le risque de surcharge du nœud de secours. Vous pouvez planifier un basculement uniquement lorsque les performances prévues du nœud de secours sont acceptables.

Par défaut, les statistiques de l'objet racine et du nœud partenaire sont affichées dans le volet Comparaison. Contrairement à la page Performances/Explorateur de performances des nœuds, cette page ne comporte pas le bouton **Ajouter** permettant d'ajouter des objets à comparer.

Vous pouvez personnaliser le volet Comparing de la même manière que sur la page Performance/Node Performance Explorer. La liste suivante présente des exemples de personnalisation des graphiques :

- Cliquez sur le nom d'un nœud pour afficher ou masquer ses statistiques dans les graphiques des compteurs.
- Cliquez sur **Zoom View** pour afficher un graphique détaillé pour un compteur particulier dans une nouvelle fenêtre.

Créez des politiques de seuil pour la planification du basculement des nœuds dans Active IQ Unified Manager

Vous pouvez créer une politique de seuil de nœud afin de recevoir une notification sur la page Performance/Node Failover Planning lorsqu'un basculement potentiel dégraderait les performances du nœud de prise en charge à un niveau inacceptable.

La stratégie de seuil de performance définie par le système, nommée « `Node HA pair over-utilized` », génère un événement d'avertissement si le seuil est dépassé pendant six périodes de collecte consécutives (30 minutes). Le seuil est considéré comme dépassé si la capacité de performance combinée utilisée des nœuds d'une paire haute disponibilité dépasse 200 %.

L'événement généré par la politique de seuil définie par le système vous avertit qu'un basculement entraînera une augmentation inacceptable de la latence du nœud de takeover. Lorsqu'un tel événement est généré pour un nœud donné, vous pouvez accéder à la page Performance/Node Failover Planning de ce nœud afin d'afficher la valeur de latence prévue due à un basculement.

Outre l'utilisation de cette stratégie de seuil définie par le système, vous pouvez créer des stratégies de seuil à l'aide du compteur « `Performance Capacity Used - Takeover` », puis appliquer la stratégie aux nœuds sélectionnés. Le fait de spécifier un seuil inférieur à 200 % vous permet de recevoir un événement avant que le seuil de la stratégie définie par le système ne soit dépassé. Vous pouvez également spécifier une durée minimale de dépassement du seuil inférieure à 30 minutes si vous souhaitez être averti avant que l'événement de la stratégie définie par le système ne soit généré.

Par exemple, vous pouvez définir une politique de seuil pour générer un événement d'avertissement si la capacité de performance combinée utilisée des nœuds d'une paire haute disponibilité dépasse 175 % pendant plus de 10 minutes. Vous pouvez appliquer cette politique à Node1 et Node2, qui forment une paire haute disponibilité. Après avoir reçu une notification d'événement d'avertissement pour Node1 ou Node2, vous pouvez afficher la page Performance/Node Failover Planning de ce nœud pour évaluer l'impact estimé sur les performances du nœud de reprise. Vous pouvez prendre des mesures correctives pour éviter de surcharger le nœud de reprise si un basculement se produit. Si vous intervenez lorsque la capacité de performance combinée utilisée des nœuds est inférieure à 200 %, la latence du nœud de reprise n'atteint pas un niveau inacceptable, même si un basculement se produit pendant cette période.

Utilisez le graphique de répartition de la capacité de performance utilisée pour la planification du basculement dans Active IQ Unified Manager

Le graphique détaillé « Capacité de performance utilisée - ventilation » montre la capacité de performance utilisée pour le nœud principal et le nœud partenaire. Il montre également la quantité de capacité de performance disponible sur le nœud de basculement estimé. Ces informations vous aident à déterminer si vous risquez d'avoir un problème de performance en cas de défaillance du nœud partenaire.

En plus d'afficher la capacité de performance totale utilisée pour les nœuds, le graphique de répartition ventile les valeurs de chaque nœud en protocoles utilisateur et processus d'arrière-plan.

- Les protocoles utilisateur correspondent aux opérations d'entrée/sortie des applications utilisateur vers et depuis le cluster.
- Les processus d'arrière-plan sont les processus internes du système liés à l'efficacité du stockage, à la réplication des données et à l'état de santé 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 des processus système en arrière-plan, tels que la déduplication, la reconstruction RAID, le nettoyage du disque et les copies SnapMirror.

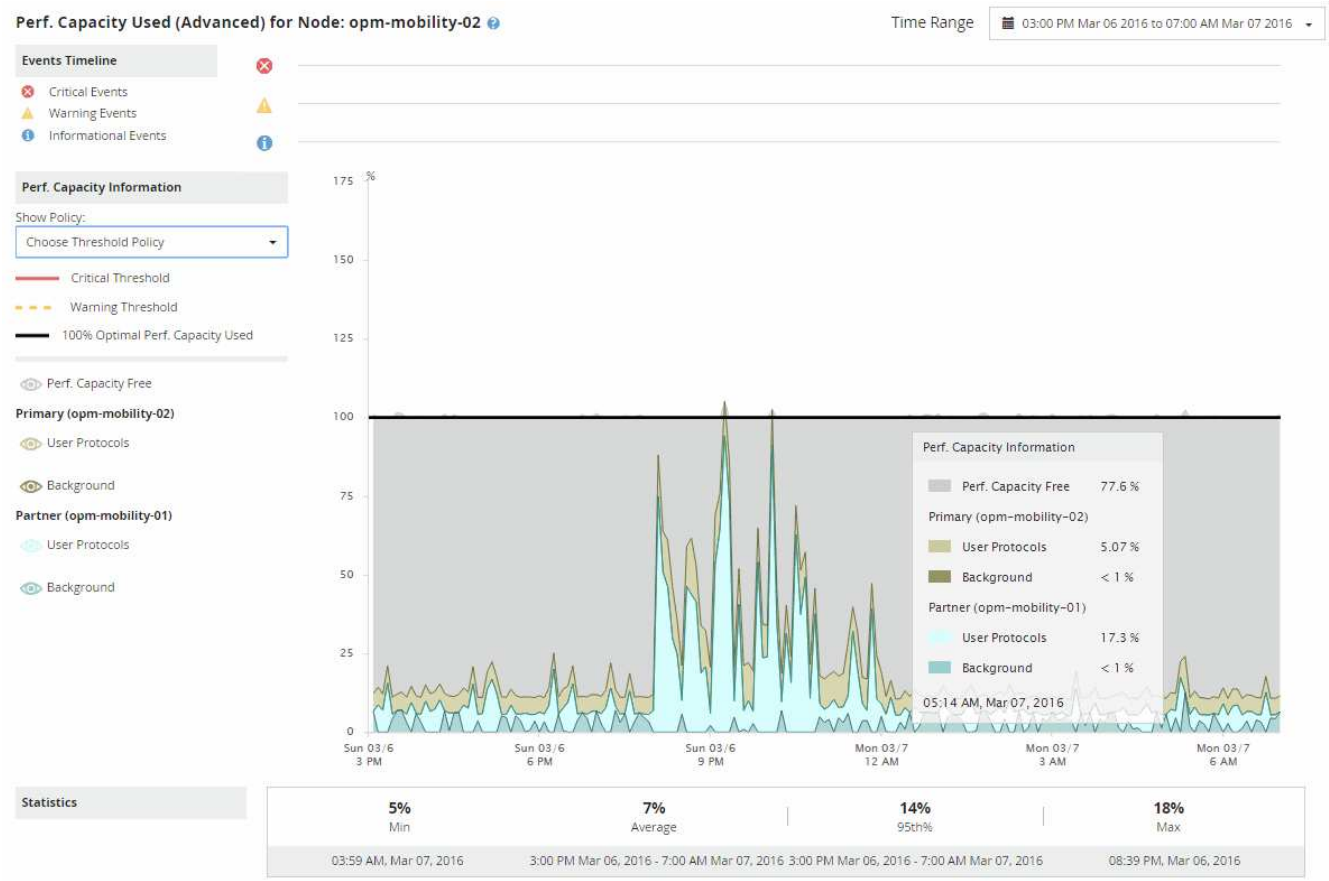
Étapes

1. Accédez à la page **Performance/Node Failover Planning** pour le nœud qui fera office de nœud de reprise estimé.
2. À partir du sélecteur **Plage de temps**, choisissez la période pour laquelle les statistiques historiques sont affichées dans la grille des compteurs et les graphiques des compteurs.

   Les graphiques de compteurs affichant les statistiques du nœud principal, du nœud partenaire et du nœud de reprise estimé sont affichés.

3. Dans la liste **Choisir les graphiques**, sélectionnez **Perf. Capacité utilisée**.
4. Dans le graphique **Perf. Capacité utilisée**, sélectionnez **Détail** et cliquez sur **Vue agrandie**.

   Le graphique détaillé de Perf. Capacity Used s'affiche.



5. Déplacez le curseur sur le graphique détaillé pour afficher les informations relatives à la capacité de performance utilisée dans la fenêtre contextuelle.

   Le pourcentage de capacité de performance disponible représente la capacité de performance disponible sur le nœud de reprise estimé. Il indique la capacité de performance restante sur le nœud de reprise après un basculement. S'il est de 0 %, un basculement entraînera une augmentation de la latence à un niveau inacceptable sur le nœud de reprise.

6. Envisagez de prendre des mesures correctives pour éviter un faible pourcentage libre de capacité de performance.

   Si vous prévoyez de déclencher un basculement pour la maintenance d'un nœud, choisissez un moment pour faire basculer le nœud partenaire lorsque le pourcentage de capacité de performance disponible n'est pas à 0.

Collecter des données et surveiller les performances du workload

Collectez des données et surveillez les performances de la charge de travail dans Active IQ Unified Manager

Unified Manager collecte et analyse l'activité des workloads toutes les 5 minutes afin d'identifier les événements de performance, et détecte les modifications de configuration toutes les 15 minutes. Il conserve au maximum 30 jours de données historiques de performance et d'événements par tranches de 5 minutes, et utilise ces données pour

prévoir la plage de latence attendue pour tous les workloads surveillés.

Unified Manager doit collecter au minimum 3 jours d'activité de workload avant de pouvoir commencer son analyse et avant que les prévisions de latence du temps de réponse des E/S puissent être affichées sur la page « Analyse de workload » et sur la page « Détails de l'événement ». Pendant la collecte de cette activité, les prévisions de latence n'affichent pas toutes les modifications résultant de l'activité du workload. Après avoir collecté 3 jours d'activité, Unified Manager ajuste les prévisions de latence toutes les 24 heures à 00:00 afin de refléter les modifications de l'activité du workload et d'établir un seuil de performance dynamique plus précis.

Pendant les 4 premiers jours durant lesquels Unified Manager surveille un workload, si plus de 24 heures se sont écoulées depuis la dernière collecte de données, les graphiques de latence n'afficheront pas les prévisions de latence pour ce workload. Les événements détectés avant la dernière collecte restent disponibles.

Le passage à l'heure d'été modifie l'heure système, ce qui affecte les prévisions de latence des statistiques de performance des workloads surveillés. Unified Manager commence immédiatement à corriger la prévision de latence, ce qui prend environ 15 jours. Pendant cette période, vous pouvez continuer à utiliser Unified Manager, mais comme Unified Manager utilise la prévision de latence pour détecter les événements dynamiques, certains événements peuvent ne pas être exacts. Les événements détectés avant le changement d'heure ne sont pas affectés.

Surveillez les types de charges de travail avec Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour surveiller les performances de deux types de workloads : ceux définis par l'utilisateur et ceux définis par le système.

- ***workloads définis par l'utilisateur***

  Le débit d'E/S des applications vers le cluster. Il s'agit des processus impliqués dans les requêtes de lecture et d'écriture. Un volume, un LUN, un partage NFS, un partage SMB/CIFS et un workload constituent un workload défini par l'utilisateur.

  Unified Manager surveille uniquement l'activité du workload sur le cluster. Il ne surveille pas les applications, les clients ni les chemins d'accès entre les applications et le cluster.

  Si une ou plusieurs des conditions suivantes sont remplies pour une workload, celle-ci ne peut pas être surveillée par Unified Manager :

  - Il s'agit d'une copie de protection des données (DP) en mode lecture seule. (Les volumes DP sont surveillés afin de détecter tout trafic généré par l'utilisateur.)
  - Il s'agit d'un clone de données hors ligne.
  - Il s'agit d'un volume en miroir dans une configuration MetroCluster.

- ***workloads définis par le système***

  Les processus internes liés à l'efficacité du stockage, à la réplication des données et à l'état du système, notamment :

  - l'efficacité du stockage, comme la déduplication
  - L'état du disque, qui comprend la reconstruction RAID, le scrubbing du disque, etc.

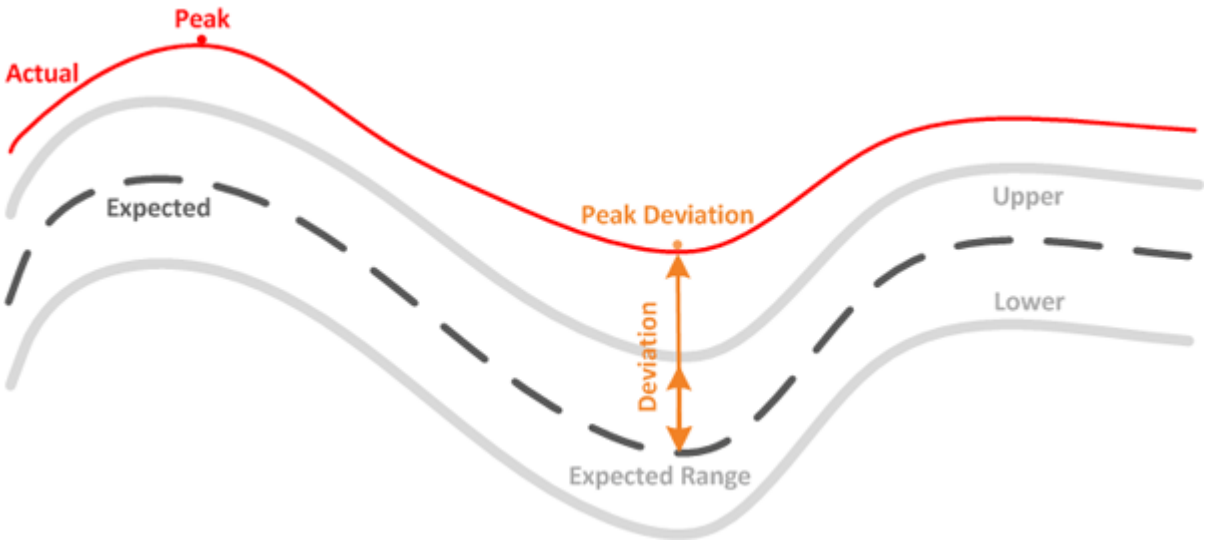
- La réplication des données, comme les copies SnapMirror
- Activités de gestion
- L'état du système de fichiers, qui comprend diverses activités WAFL
- Les analyseurs de systèmes de fichiers, tels que WAFL scan
- Déchargement des copies, par exemple le déchargement des opérations d'efficacité du stockage à partir des hôtes VMware
- L'état de santé du système, notamment les déplacements de volumes, la compression des données, etc.
- Volumes non surveillés

Les données de performance des charges de travail définies par le système ne s'affichent dans l'interface graphique que lorsque le composant du cluster utilisé par ces charges de travail est en contention. Par exemple, il est impossible de rechercher le nom d'une charge de travail définie par le système pour consulter ses données de performance dans l'interface graphique.

Comprendre les valeurs de mesure des performances de la charge de travail dans Active IQ Unified Manager

Unified Manager mesure les performances des workloads sur un cluster en se basant sur des valeurs statistiques historiques et attendues, qui constituent la prévision de latence des valeurs pour les workloads. Il compare les valeurs statistiques réelles des workloads à la prévision de latence afin de déterminer quand les performances des workloads sont trop élevées ou trop faibles. Un workload qui ne fonctionne pas comme prévu déclenche un événement de performance dynamique pour vous en informer.

Dans l'illustration suivante, la valeur réelle, en rouge, représente les statistiques de performance réelles sur la période considérée. Cette valeur a dépassé le seuil de performance, qui correspond à la limite supérieure de la prévision de latence. Le pic représente la valeur réelle la plus élevée enregistrée sur cette période. L'écart mesure la différence entre les valeurs attendues (la prévision) et les valeurs réelles, tandis que l'écart maximal indique la différence la plus importante entre ces deux valeurs.



Le tableau suivant répertorie les valeurs de mesure des performances du workload.

Mesure	Description
Activité	Le pourcentage de la limite QoS utilisée par les workloads du groupe de politiques. Si Unified Manager détecte une modification apportée à un groupe de stratégies, comme l'ajout ou la suppression d'un volume ou la modification de la limite QoS, les valeurs réelles et attendues peuvent dépasser 100 % de la limite définie. Si une valeur dépasse 100 % de la limite définie, elle s'affiche comme >100 %. Si une valeur est inférieure à 1 % de la limite définie, elle s'affiche comme <1 %.
Réel	La valeur de performance mesurée à un moment précis pour un workload donné.
Déviation	L'écart entre les valeurs attendues et les valeurs réelles. Il s'agit du rapport entre la valeur réelle moins la valeur attendue et la valeur supérieure de l'intervalle attendu moins la valeur attendue. Une valeur d'écart négative indique que les performances du workload sont inférieures aux attentes, tandis qu'une valeur d'écart positive indique que les performances du workload sont supérieures aux attentes.
Attendu	Les valeurs attendues sont basées sur l'analyse des données de performance historiques pour un workload donné. Unified Manager analyse ces valeurs statistiques afin de déterminer la plage de valeurs attendue (prévision de latence).
Prévision de latence (plage attendue)	La prévision de latence est une estimation des valeurs de performance minimales et maximales attendues à un instant précis. Pour la latence du workload, les valeurs maximales constituent le seuil de performance. Lorsque la valeur réelle dépasse ce seuil, Unified Manager déclenche un événement de performance dynamique.
Pic	La valeur maximale mesurée sur une période donnée.
Déviation maximale	La valeur maximale de l'écart mesurée sur une période donnée.
Profondeur de la file d'attente	Le nombre de requêtes d'E/S en attente au niveau du composant d'interconnexion.

Mesure	Description
Utilisation	Pour les composants de traitement réseau, de traitement des données et d'agrégat, il s'agit du pourcentage de temps d'activité nécessaire pour effectuer des opérations de workload sur une période donnée. Par exemple, le pourcentage de temps nécessaire aux composants de traitement réseau ou de traitement des données pour traiter une requête d'E/S, ou à un agrégat pour répondre à une requête de lecture ou d'écriture.
Débit d'écriture	Le débit d'écriture, en mégaoctets par seconde (Mo/s), des workloads sur un cluster local vers le cluster partenaire dans une configuration MetroCluster.

Comprendre comment Active IQ Unified Manager calcule la plage de performances attendue

La prévision de latence est une estimation des valeurs de performance minimales et maximales attendues à un instant précis. Pour la latence du workload, les valeurs maximales constituent le seuil de performance. Lorsque la valeur réelle dépasse ce seuil, Unified Manager déclenche un événement de performance dynamique.

Par exemple, pendant les heures de bureau normales, entre 9 h et 17 h, la plupart des employés consultent leurs courriels entre 9 h et 10 h 30. L'augmentation de la demande sur les serveurs de messagerie entraîne une hausse de l'activité du workload sur le stockage back-end pendant cette période. Les employés peuvent alors constater un temps de réponse lent de leurs clients de messagerie.

Pendant la pause déjeuner, entre 12 h 00 et 13 h 00, et en fin de journée après 17 h 00, la plupart des employés sont généralement loin de leur ordinateur. La charge sur les serveurs de messagerie diminue alors généralement, ce qui réduit aussi la demande sur le stockage back-end. Il peut également y avoir des opérations de workload planifiées, telles que des sauvegardes de stockage ou des analyses antivirus, qui démarrent après 17 h 00 et augmentent l'activité sur le stockage back-end.

Sur plusieurs jours, l'augmentation et la diminution de l'activité du workload déterminent la plage attendue d'activité (prévision de latence), avec des limites supérieure et inférieure pour un workload. Lorsque l'activité réelle du workload d'un objet se situe en dehors des limites supérieure ou inférieure et reste en dehors de ces limites pendant un certain temps, cela peut indiquer que l'objet est surutilisé ou sous-utilisé.

Comment la prévision de latence est établie

Unified Manager doit collecter un minimum de 3 jours d'activité de workload avant de pouvoir commencer son analyse et avant que la prévision de latence pour le temps de réponse des E/S puisse être affichée dans la GUI. La collecte de données minimale requise ne tient pas compte de toutes les modifications résultant de l'activité du workload. Après avoir collecté les 3 premiers jours d'activité, Unified Manager ajuste la prévision de latence toutes les 24 heures à 00:00 afin de refléter les modifications de l'activité du workload et d'établir un seuil de performance dynamique plus précis.

Le passage à l'heure d'été modifie l'heure système, ce qui affecte les prévisions de latence des statistiques de performance des workloads surveillés. Unified Manager commence immédiatement à corriger la prévision de latence, ce qui prend environ 15 jours. Pendant cette période, vous pouvez continuer à utiliser Unified Manager, mais comme Unified Manager utilise

la prévision de latence pour détecter les événements dynamiques, certains événements peuvent ne pas être exacts. Les événements détectés avant le changement d'heure ne sont pas affectés.

Utilisez les prévisions de latence pour l'analyse des performances dans Active IQ Unified Manager

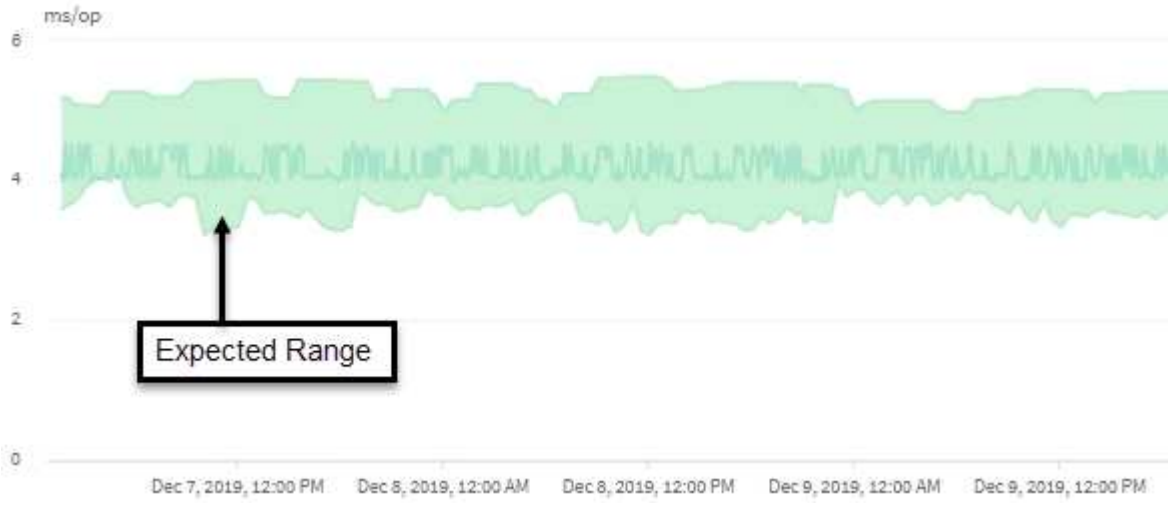
Unified Manager utilise les prévisions de latence pour représenter l'activité de latence d'E/S typique (temps de réponse) de vos workloads surveillés. Il vous alerte lorsque la latence réelle d'un workload dépasse les limites supérieures des prévisions de latence, ce qui déclenche un événement de performance dynamique, afin que vous puissiez analyser le problème de performance et prendre les mesures correctives nécessaires pour le résoudre.

La prévision de latence définit la performance de référence pour le workload. Au fil du temps, Unified Manager s'appuie sur les mesures de performance passées pour prévoir les niveaux de performance et d'activité attendus pour le workload. La limite supérieure de la plage attendue établit le seuil de performance dynamique. Unified Manager utilise cette référence pour déterminer si la latence réelle est supérieure ou inférieure à un seuil, ou si elle se situe en dehors des limites de sa plage attendue. La comparaison entre les valeurs réelles et les valeurs attendues crée un profil de performance pour le workload.

Lorsque la latence réelle d'un workload dépasse le seuil de performance dynamique en raison d'une contention sur un composant du cluster, la latence est élevée et le workload s'exécute plus lentement que prévu. Les performances des autres workloads partageant les mêmes composants du cluster peuvent également être plus lentes que prévu.

Unified Manager analyse le franchissement de seuil et détermine s'il s'agit d'un événement de performance. Si l'activité de workload élevée reste constante pendant une longue période, par exemple plusieurs heures, Unified Manager considère l'activité comme normale et ajuste dynamiquement les prévisions de latence afin de définir le nouveau seuil de performance dynamique.

Certaines charges de travail peuvent présenter une activité constamment faible, lorsque les prévisions de latence n'affichent pas un taux élevé de variation au fil du temps. Afin de minimiser le nombre d'événements lors de l'analyse des événements de performance, Unified Manager ne déclenche un événement que pour les volumes à faible activité dont les opérations et les latences sont nettement supérieures aux prévisions.



Dans cet exemple, la latence d'un volume fait l'objet d'une prévision de latence, en gris, de 3,5 millisecondes

par opération (ms/op) au plus bas et de 5,5 ms/op au plus haut. Si la latence réelle, en bleu, augmente soudainement jusqu'à 10 ms/op, en raison d'un pic intermittent du trafic réseau ou d'une contention sur un composant du cluster, elle est alors supérieure à la prévision de latence et a dépassé le seuil de performance dynamique.

Lorsque le trafic réseau a diminué ou que le composant du cluster n'est plus en situation de contention, la latence revient dans les prévisions de latence. Si la latence reste supérieure ou égale à 10 ms/op pendant une période prolongée, vous devrez peut-être prendre des mesures correctives pour résoudre l'événement.

Utilisez la latence de la charge de travail pour identifier les problèmes de performance dans Active IQ Unified Manager

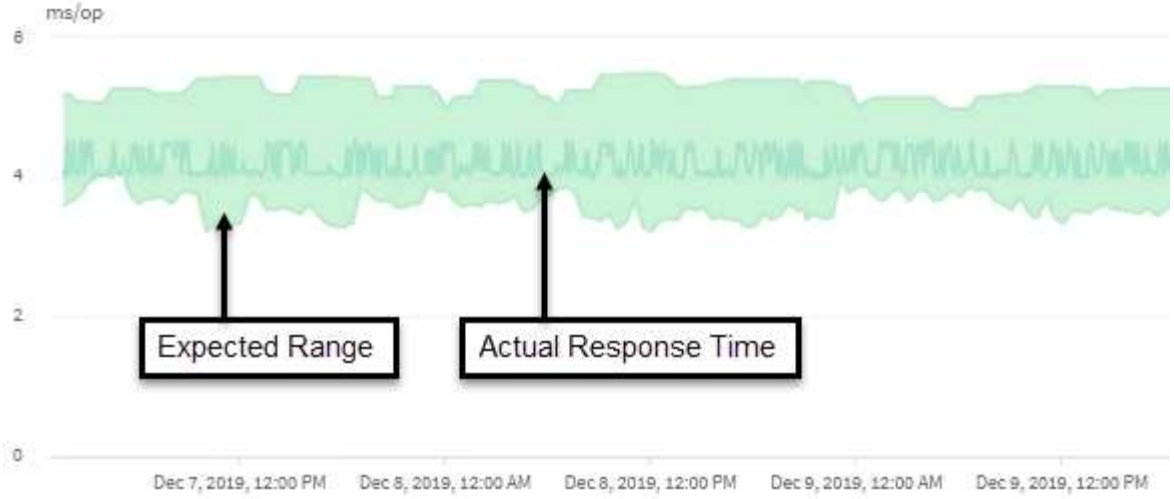
La latence du workload (temps de réponse) correspond au temps nécessaire à un volume d'un cluster pour répondre aux requêtes d'E/S des applications clientes. Unified Manager utilise cette latence pour détecter les événements de performance et vous alerter.

Une latence élevée signifie que les requêtes des applications vers un volume sur un cluster prennent plus de temps que d'habitude. Cette latence élevée peut provenir du cluster lui-même, en raison d'une contention sur un ou plusieurs de ses composants. Elle peut également être causée par des problèmes externes au cluster, tels que des goulots d'étranglement réseau, des problèmes avec le client hébergeant les applications ou des problèmes avec les applications elles-mêmes.

Unified Manager surveille uniquement l'activité du workload sur le cluster. Il ne surveille pas les applications, les clients ni les chemins d'accès entre les applications et le cluster.

Les opérations sur le cluster, telles que l'exécution de sauvegardes ou de la déduplication, qui augmentent leur demande en composants du cluster partagés par d'autres workloads peuvent également contribuer à une latence élevée. Si la latence réelle dépasse le seuil de performance dynamique de la plage attendue (prévision de latence), Unified Manager analyse l'événement afin de déterminer s'il s'agit d'un événement de performance que vous devrez peut-être résoudre. La latence est mesurée en millisecondes par opération (ms/op).

Sur le graphique « Latence totale » de la page « Analyse du workload », vous pouvez consulter une analyse des statistiques de latence afin de voir comment l'activité des processus individuels, tels que les requêtes de lecture et d'écriture, se compare aux statistiques de latence globales. Cette comparaison vous aide à déterminer quelles opérations présentent l'activité la plus élevée ou si certaines opérations présentent une activité anormale qui a un impact sur la latence d'un volume. Lors de l'analyse des événements de performance, vous pouvez utiliser les statistiques de latence pour déterminer si un événement a été causé par un problème sur le cluster. Vous pouvez également identifier les activités de workload spécifiques ou les composants du cluster impliqués dans l'événement.



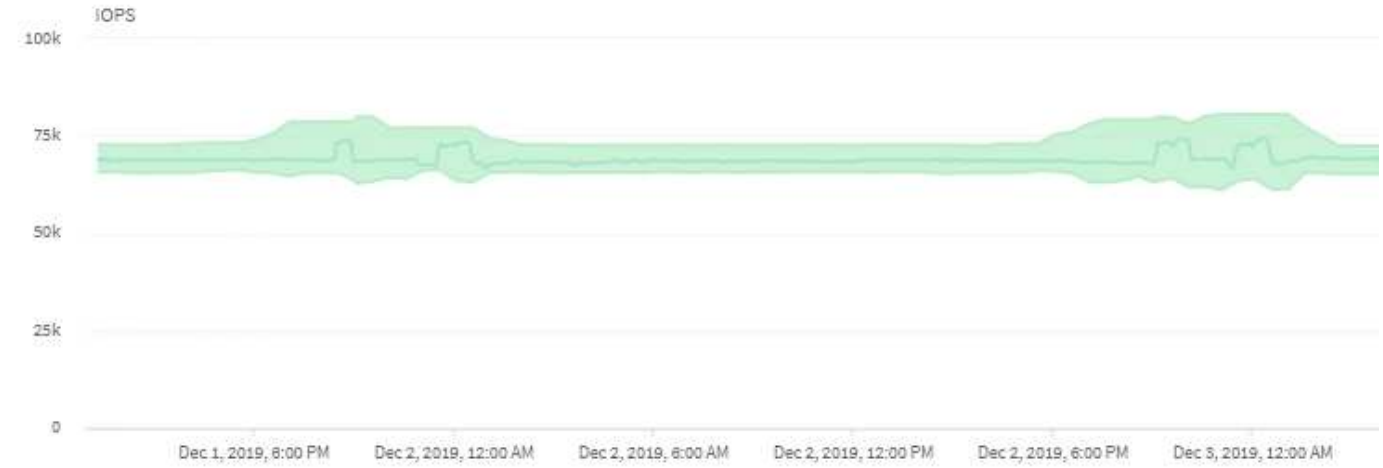
Cet exemple illustre le graphique de latence. Le temps de réponse réel (latence) est représenté par une ligne bleue et la prévision de latence (plage attendue) par une ligne verte.

Des interruptions peuvent apparaître sur la ligne bleue si Unified Manager n'a pas pu collecter les données. Cela peut se produire si le cluster ou le volume était inaccessible, si Unified Manager était arrêté pendant cette période ou si la collecte prenait plus de temps que la période de collecte de 5 minutes.

Évaluez comment les opérations de cluster peuvent affecter la latence des charges de travail dans Active IQ Unified Manager

Les opérations (IOPS) représentent l'activité de tous les workloads définis par l'utilisateur et par le système sur un cluster. Les statistiques d'IOPS vous aident à déterminer si les processus du cluster, tels que les sauvegardes ou l'exécution de la déduplication, ont un impact sur la latence du workload (temps de réponse) ou s'ils ont pu provoquer, ou contribuer à, un incident de performance.

Lors de l'analyse des incidents de performance, vous pouvez utiliser les statistiques d'IOPS pour déterminer si un incident de performance a été causé par un problème sur le cluster. Vous pouvez identifier les activités de workload spécifiques qui ont pu contribuer principalement à l'incident de performance. Les IOPS sont mesurées en opérations par seconde (ops/sec).



Cet exemple illustre le graphique IOPS. Les statistiques d'opérations réelles sont représentées par une ligne bleue et les prévisions IOPS des statistiques d'opérations sont en vert.

Dans certains cas où un cluster est surchargé, Unified Manager peut afficher le message `Data collection is taking too long on Cluster` *`cluster_name`*. Cela signifie qu'Unified Manager n'a pas collecté suffisamment de statistiques pour effectuer une analyse. Vous devez réduire les ressources utilisées par le cluster afin que des statistiques puissent être collectées.

Surveillez les performances de MetroCluster avec Active IQ Unified Manager

Unified Manager vous permet de surveiller le débit d'écriture entre les clusters dans une configuration MetroCluster afin d'identifier les workloads présentant un débit d'écriture élevé.

Si ces workloads hautes performances entraînent des temps de réponse d'E/S élevés pour d'autres volumes du cluster local, Unified Manager déclenche des événements de performance pour vous en informer.

Unified Manager traite les clusters d'une configuration MetroCluster comme des clusters individuels. Il ne fait pas de distinction entre les clusters partenaires et ne corrèle pas le débit d'écriture de chaque cluster.

Lorsqu'un cluster local dans une configuration MetroCluster réplique ses données vers son cluster partenaire, les données sont écrites dans la NVRAM, puis transférées via les liaisons intercommutateurs (ISL) vers les agrégats distants. Unified Manager analyse la NVRAM afin d'identifier les workloads dont le débit d'écriture élevé entraîne une surutilisation de la NVRAM, provoquant ainsi une contention au niveau de la NVRAM.

Les workloads dont l'écart du temps de réponse a dépassé le seuil de performance sont appelés « victimes », et les workloads dont l'écart du débit d'écriture vers la NVRAM est plus élevé que d'habitude, provoquant la contention, sont appelés « bullies ». Étant donné que seules les requêtes d'écriture sont mises en miroir vers le cluster partenaire, Unified Manager n'analyse pas le débit de lecture.

Vous pouvez visualiser le débit de n'importe lequel des clusters d'une configuration MetroCluster en analysant les workloads des LUN et des volumes correspondants à partir des écrans suivants. Vous pouvez filtrer les résultats par cluster. Dans le volet de navigation de gauche :

- **Stockage > Clusters > Performances : Tous les clusters** Voir
- vue **Stockage > Volumes > Performance : Tous les volumes**.
- **Stockage > LUN > Performances: vue de toutes les LUN**.
- **Analyse des workloads > Tous les workloads**

Informations connexes

"Analyse et notification des événements de performance"

"Analyse des événements de performances pour une configuration MetroCluster"

"Rôles des workloads impliqués dans un événement de performance"

"Identification des workloads victimes impliqués dans un événement de performance"

"Identifier les workloads perturbateurs impliqués dans un événement de performance"

"Identification des charges de travail shark impliquées dans un événement de performance"

Comprendre les événements et alertes de performance

Comprendre les événements et alertes de performance dans Active IQ Unified Manager

Les événements de performance sont des incidents liés aux performances des workloads sur un cluster. Ils vous aident à identifier les workloads dont les temps de réponse sont lents. Associés aux événements de santé survenus au même moment, ils vous permettent de déterminer les problèmes qui ont pu causer ces temps de réponse lents ou y contribuer.

Lorsque Unified Manager détecte plusieurs occurrences de la même condition d'événement pour le même composant du cluster, il traite toutes les occurrences comme un seul événement, et non comme des événements distincts.

Vous pouvez configurer des alertes pour envoyer automatiquement des notifications par e-mail lorsque des événements de performance d'un certain niveau de gravité se produisent.

Identifier les sources des événements de performance dans Active IQ Unified Manager

Les événements de performance sont des problèmes liés aux performances des workloads sur un cluster. Ils vous aident à identifier les objets de stockage présentant des temps de réponse lents, également appelés latence élevée. Associés à d'autres événements d'intégrité survenus au même moment, ils vous permettent de déterminer les problèmes susceptibles d'avoir causé, ou contribué à, les temps de réponse lents.

Unified Manager reçoit les événements de performance des sources suivantes :

- **Événements de politique de seuil de performance définis par l'utilisateur**

  Problèmes de performance liés aux valeurs de seuil personnalisées que vous avez définies. Vous configurez des politiques de seuil de performance pour les objets de stockage, par exemple les agrégats et les volumes, afin que des événements soient générés lorsqu'une valeur de seuil d'un compteur de performance est dépassée.

  Vous devez définir une politique de seuil de performance et l'affecter à un objet de stockage pour recevoir ces événements.

- **Événements liés à la politique de seuil de performance définie par le système**

  Les problèmes de performance sont basés sur des valeurs seuils définies par le système. Ces politiques de seuil sont incluses dans l'installation d'Unified Manager afin de couvrir les problèmes de performance courants.

  Ces politiques de seuil sont activées par défaut, et vous pourriez voir des événements peu de temps après l'ajout d'un cluster.

- **Événements de seuil de performance dynamique**

Les problèmes de performance résultent de défaillances ou d'erreurs dans l'infrastructure informatique, ou de workloads qui surutilisent les ressources du cluster. La cause de ces événements peut être un simple problème qui se corrige de lui-même avec le temps ou auquel il peut être remédié par une réparation ou une modification de la configuration. Un événement de seuil dynamique indique que les workloads sur un système ONTAP sont lents en raison d'autres workloads qui utilisent fortement les composants partagés du cluster.

Ces seuils sont activés par défaut, et vous pourriez observer des événements après trois jours de collecte de données à partir d'un nouveau cluster.

Priorisez les événements de performance par niveau de gravité dans Active IQ Unified Manager

Chaque événement de performance est associé à un niveau de gravité afin de vous aider à prioriser les événements qui nécessitent une action corrective immédiate.

- **Critique**

  Un incident de performance s'est produit et pourrait entraîner une interruption de service si des mesures correctives ne sont pas prises immédiatement.

  Les événements critiques sont envoyés uniquement à partir des seuils définis par l'utilisateur.

- **Avertissement**

  Un compteur de performance d'un objet de cluster présente une valeur anormale et doit être surveillé afin d'éviter qu'il n'atteigne le seuil critique. Les événements de cette gravité n'entraînent pas d'interruption de service et ne nécessitent généralement pas d'intervention immédiate.

  Les événements d'avertissement sont envoyés à partir de seuils définis par l'utilisateur, par le système ou dynamiques.

- **Informations**

  Cet événement se produit lorsqu'un nouvel objet est découvert ou lorsqu'une action utilisateur est effectuée. Par exemple, lorsqu'un objet de stockage est supprimé ou que des modifications de configuration sont apportées, un événement de type de gravité Information est généré.

  Les événements d'information sont envoyés directement par 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"
- "Quelles informations contient un courriel d'alerte"
- "Ajout d'alertes"
- "Ajout d'alertes pour les événements de performance"

Surveillez les modifications de configuration détectées par Active IQ Unified Manager

Unified Manager surveille vos clusters pour détecter les modifications de configuration

afin de vous aider à déterminer si une modification a pu provoquer ou contribuer à un événement de performances. Les pages de l'Explorateur de performances affichent une icône d'événement de modification (●) pour indiquer la date et l'heure à laquelle la modification a été détectée.

Vous pouvez consulter les graphiques de performance dans les pages de l'Explorateur de performances et dans la page Analyse de la charge de travail pour déterminer si l'événement de modification a eu un impact sur les performances de l'objet de cluster sélectionné. Si la modification a été détectée simultanément ou presque à un événement de performance, elle a pu contribuer au problème et déclencher l'alerte d'événement.

Unified Manager peut détecter les événements de changement suivants, qui sont catégorisés comme événements d'information :

- Un volume se déplace entre les agrégats.

  Unified Manager peut détecter l'état d'avancement, la fin ou l'échec d'un déplacement de volume. En cas d'indisponibilité d'Unified Manager pendant un déplacement de volume, une fois remis en service, il détecte le déplacement et affiche un événement de modification.

- La limite de débit (Mo/s ou IOPS) d'un groupe de stratégies QoS contenant une ou plusieurs charges de travail surveillées change.

  La modification d'une limite de groupe de règles peut entraîner des pics intermittents de latence (temps de réponse), susceptibles de déclencher des événements pour ce groupe. La latence revient progressivement à la normale et les événements provoqués par ces pics deviennent caducs.

- Un nœud d'une paire haute disponibilité prend le relais du stockage de son nœud partenaire ou le lui restitue.

  Unified Manager peut détecter la fin d'une prise de contrôle, d'une prise de contrôle partielle ou d'une restitution. En revanche, si la prise de contrôle est due à un nœud défaillant, Unified Manager ne détecte pas l'événement.

- Une opération de mise à niveau ou de rétablissement d'ONTAP s'est terminée avec succès.

  La version précédente et la nouvelle version sont affichées.

Comprendre les politiques de seuil de performance définies par le système dans Active IQ Unified Manager

Unified Manager fournit des politiques de seuil standard qui surveillent les performances du cluster et génèrent automatiquement des événements. Ces politiques sont activées par défaut et génèrent des événements d'avertissement ou d'information lorsque les seuils de performance surveillés sont dépassés.

ⓘ Les politiques 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 politiques de seuil de performance définies par le système, vous pouvez désactiver les événements pour chaque politique individuellement à partir de la page Configuration des événements.

Politiques de seuil du cluster

Les politiques de seuil de performance de cluster définies par le système sont attribuées, par défaut, à chaque cluster surveillé par Unified Manager :

- **Déséquilibre de charge du cluster**

  Identifie les situations dans lesquelles un nœud fonctionne avec une charge bien plus élevée que les autres nœuds du cluster et peut donc potentiellement affecter les latences du workload.

  Pour ce faire, il compare la valeur de capacité de performance utilisée pour tous les nœuds d'un cluster afin de déterminer si l'un d'eux a dépassé le seuil de 30 % pendant plus de 24 heures. Il s'agit d'un événement d'alerte.

- **Déséquilibre de capacité du cluster**

  Identifie les situations dans lesquelles un agrégat a une capacité utilisée beaucoup plus élevée que les autres agrégats du cluster et peut donc potentiellement affecter l'espace requis pour les opérations.

  Il procède en comparant la capacité utilisée de tous les agrégats du cluster afin de détecter une éventuelle différence de 70 % entre eux. Il s'agit d'un événement d'alerte.

Politiques de seuil de nœud

Les politiques de seuil de performance des nœuds définies par le système sont attribuées, par défaut, à chaque nœud des clusters surveillés par Unified Manager :

- **Seuil de capacité de performance utilisée dépassé**

  Identifie les situations dans lesquelles un seul nœud fonctionne au-delà des limites de son efficacité opérationnelle et peut donc potentiellement affecter les latences des workloads.

  Il détecte les nœuds qui utilisent plus de 100 % de leur capacité de performance pendant plus de 12 heures. Il s'agit d'un événement d'alerte.

- **Paire haute disponibilité de nœuds surutilisée**

  Identifie les situations dans lesquelles les nœuds d'une paire haute disponibilité fonctionnent au-delà des limites d'efficacité opérationnelle de la paire haute disponibilité.

  Le système effectue cela en examinant la valeur de capacité de performance utilisée pour les deux nœuds de la paire haute disponibilité. Si la capacité de performance utilisée combinée des deux nœuds dépasse 200 % pendant plus de 12 heures, un basculement du contrôleur aura un impact sur la latence des workloads. Cet événement est informatif.

- **Fragmentation du disque du nœud**

  Identifie les situations dans lesquelles un ou plusieurs disques d'un agrégat sont fragmentés, ce qui ralentit les services système essentiels et peut potentiellement affecter les latences des workload sur un nœud.

  Il le fait en examinant certains ratios d'opérations de lecture et d'écriture sur l'ensemble des agrégats d'un nœud. Cette politique peut également être déclenchée lors d'une resynchronisation SyncMirror ou lorsque des erreurs sont détectées lors d'opérations de nettoyage de disque. Il s'agit d'un événement d'avertissement.

La politique « Fragmentation du disque du nœud » analyse uniquement les agrégats HDD ; les agrégats Flash Pool, SSD et FabricPool ne sont pas analysés.

Politiques de seuil d'agrégat

La politique de seuil de performance d'agrégat définie par le système est attribuée par défaut à chaque agrégat des clusters surveillés par Unified Manager :

- **Disques d'agrégat surutilisés**

  Ce système identifie les situations dans lesquelles un agrégat fonctionne au-delà des limites de son efficacité opérationnelle, ce qui peut affecter les latences de workload. Il repère ces situations en recherchant les agrégats dont les disques sont utilisés à plus de 95 % pendant plus de 30 minutes. Cette politique multiconditionnelle effectue ensuite l'analyse suivante pour aider à déterminer la cause du problème :

  - Un disque de l'agrégat fait-il actuellement l'objet d'une activité de maintenance en arrière-plan ?

    Parmi les activités de maintenance en arrière-plan qu'un disque peut subir figurent la reconstruction du disque, le nettoyage du disque, la resynchronisation de SyncMirror et la réparation de la parité.

  - Existe-t-il un goulot d'étranglement des communications au niveau de l'interconnexion Fibre Channel du tiroir disque ?
  - L'espace libre est-il insuffisant dans l'agrégat ? Un événement d'avertissement est émis pour cette stratégie uniquement si une (ou plusieurs) des trois stratégies subordonnées est également considérée comme non respectée. Aucun événement de performance n'est déclenché si seuls les disques de l'agrégat sont utilisés à plus de 95 %.

La politique « Surutilisation des disques d'agrégat » analyse les agrégats composés uniquement de HDD et les agrégats Flash Pool (hybrides) ; les agrégats SSD et FabricPool ne sont pas analysés.

Politiques de seuil de latence du workload

Les politiques de seuil de latence de workload définies par le système sont attribuées à tout workload disposant d'une politique de niveau de service de performance configurée avec une valeur « latence attendue » définie :

- **Seuil de latence du volume/de la LUN du workload dépassé, conformément au niveau de service de performances**

  Identifie les volumes (partages de fichiers) et les LUN qui ont dépassé leur limite de "latence attendue" et qui affectent les performances du workload. Il s'agit d'un événement d'avertissement.

  Pour ce faire, il recherche les workloads qui ont dépassé la valeur de latence attendue pendant 30 % du temps au cours de l'heure précédente.

Politiques de seuil de QoS

Les politiques de seuil de performance QoS définies par le système sont attribuées à tout workload disposant d'une politique ONTAP QoS de débit maximal configurée (IOPS, IOPS/TB ou Mo/s). Unified Manager déclenche un événement lorsque la valeur de débit du workload est inférieure de 15 % à la valeur QoS configurée :

- **Seuil QoS max. en IOPS ou Mo/s**

  Identifie les volumes et les LUN qui ont dépassé leur limite maximale de QoS en IOPS ou en débit (Mo/s) et qui affectent la latence des workloads. Il s'agit d'un événement d'avertissement.

  Lorsqu'une seule workload est affectée à un groupe de stratégies, cela consiste à rechercher les workloads qui ont dépassé le seuil de débit maximal défini dans le groupe de stratégies QoS affecté au cours de chaque période de collecte de l'heure précédente.

  Lorsque plusieurs workloads partagent une seule politique QoS, celle-ci procède en additionnant les IOPS ou les MB/s de tous les workloads de la politique et en comparant ce total au seuil.

- **QoS Peak IOPS/TB ou IOPS/TB avec seuil de taille de bloc**

  Identifie les volumes ayant dépassé leur limite de débit de pointe IOPS/TB de la QoS adaptative (ou leur limite IOPS/TB avec taille de bloc) et qui affectent la latence du workload. Il s'agit d'un événement d'avertissement.

  Il le fait en convertissant le seuil maximal d'IOPS/TB défini dans la politique de QoS adaptative en une valeur maximale d'IOPS QoS basée sur la taille de chaque volume, puis en recherchant les volumes qui ont dépassé le nombre maximal d'IOPS QoS au cours de chaque période de collecte des performances pendant l'heure précédente.

  > Cette politique s'applique aux volumes uniquement lorsque le cluster est installé avec le logiciel ONTAP 9.3 ou une version ultérieure.

  Lorsque l'élément "block size" a été défini dans la politique QoS adaptative, le seuil est converti en une valeur QoS maximale en Mo/s en fonction de la taille de chaque volume. Ensuite, le système recherche les volumes qui ont dépassé la valeur QoS maximale en Mo/s pendant chaque période de collecte des performances de l'heure précédente.

  > Cette politique s'applique aux volumes uniquement lorsque le cluster est installé avec le logiciel ONTAP 9.5 ou une version ultérieure.

Analysez les événements et notifications de performance dans Active IQ Unified Manager

Les événements de performance vous informent des problèmes de performances d'E/S sur un workload causés par une contention sur un composant du cluster. Unified Manager analyse l'événement pour identifier tous les workloads concernés, le composant en contention et déterminer si le problème persiste et nécessite une intervention.

Unified Manager surveille la latence d'E/S (temps de réponse) et les IOPS (opérations) des volumes sur un cluster. Lorsque d'autres workloads sollicitent excessivement un composant du cluster, par exemple, le composant est en contention et ne peut pas fonctionner à un niveau optimal pour répondre aux exigences du workload. Les performances des autres workloads qui utilisent le même composant peuvent être affectées, ce qui entraîne une augmentation de leur latence. Si la latence dépasse le seuil de performance dynamique, Unified Manager déclenche un événement de performance pour vous en informer.

Analyse d'événements

Unified Manager effectue les analyses suivantes, en utilisant les statistiques de performance des 15 derniers jours, afin d'identifier les workloads victimes, les workloads agresseurs et le composant du cluster impliqué

dans un événement :

- Identifie les workloads victimes dont la latence a dépassé le seuil de performance dynamique, qui correspond à la limite supérieure de la prévision de latence :
  - Pour les volumes sur des agrégats hybrides HDD ou Flash Pool (niveau local), les événements ne sont déclenchés que lorsque la latence est supérieure à 5 millisecondes (ms) et que les IOPS sont supérieures à 10 opérations par seconde (ops/sec).
  - Pour les volumes sur des agrégats entièrement SSD ou des agrégats FabricPool (niveau cloud), les événements ne sont déclenchés que lorsque la latence est supérieure à 1 ms et que les IOPS sont supérieures à 100 ops/sec.
- Identifie le composant du cluster en contention.

  Si la latence des workloads victimes au niveau de l'interconnexion de cluster est supérieure à 1 ms, Unified Manager considère cela comme significatif et déclenche un événement pour l'interconnexion de cluster.

- Identifie les workloads perturbateurs qui surutilisent le composant du cluster et provoquent un état de contention.
- Classe les workloads concernés, en fonction de leur écart d'utilisation ou d'activité d'un composant du cluster, afin de déterminer quels bullies présentent la plus forte variation d'utilisation du composant du cluster et quelles victims sont les plus impactées.

Un événement peut ne se produire que pendant un bref instant, puis se corriger de lui-même une fois que le composant qu'il utilise n'est plus en situation de contention. Un événement continu est un événement qui se reproduit pour le même composant du cluster dans un intervalle de cinq minutes et reste à l'état actif. Pour les événements continus, Unified Manager déclenche une alerte après avoir détecté le même événement pendant deux intervalles d'analyse consécutifs.

Lorsqu'un événement est résolu, il reste disponible dans Unified Manager dans l'historique des problèmes de performance passés d'un volume. Chaque événement possède un identifiant unique qui précise son type, ainsi que les volumes, le cluster et les composants du cluster concernés.

Un seul volume peut être impliqué dans plusieurs événements simultanément.

État de l'événement

Les événements peuvent se trouver dans l'un des états suivants :

- **Actif**

  Indique que l'événement de performance est actuellement actif (nouveau ou confirmé). Le problème à l'origine de l'événement ne s'est pas corrigé ou n'a pas été résolu. Le compteur de performance de l'objet de stockage reste supérieur au seuil de performance.

- **Obsolète**

  Indique que l'événement n'est plus actif. Le problème à l'origine de l'événement s'est résolu de lui-même ou a été résolu. Le compteur de performances de l'objet de stockage ne dépasse plus le seuil de performance.

Notification d'événement

Les événements sont affichés sur la page Dashboard et sur de nombreuses autres pages de l'interface utilisateur, et des alertes pour ces événements sont envoyées aux adresses e-mail spécifiées. Vous pouvez consulter des informations d'analyse détaillées sur un événement et obtenir des suggestions pour le résoudre sur la page Event details et sur la page Workload Analysis.

Interaction avec l'événement

Sur la page Détails de l'événement et sur la page Analyse du workload, vous pouvez interagir avec les événements des manières suivantes :

- En déplaçant la souris sur un événement, un message s'affiche indiquant la date et l'heure de sa détection.

  S'il y a plusieurs événements pour la même période, le message affiche le nombre d'événements.

- Lorsque vous cliquez sur un seul événement, une boîte de dialogue s'affiche et présente des informations plus détaillées sur cet événement, notamment les composants du cluster impliqués.

  Le composant en cause est encerclé et surligné en rouge. Cliquez sur **Afficher l'analyse complète** pour consulter l'analyse complète sur la page Détails de l'événement. Si plusieurs événements se produisent pour la même période, la boîte de dialogue affiche les détails des trois événements les plus récents. Cliquez sur un événement pour afficher son analyse sur la page Détails de l'événement.

Comprendre comment Active IQ Unified Manager détermine l'impact sur les performances d'un événement

Unified Manager utilise les variations d'activité, d'utilisation, de débit d'écriture, d'utilisation des composants du cluster ou de latence d'E/S (temps de réponse) d'un workload pour déterminer le niveau d'impact sur les performances du workload. Ces informations déterminent le rôle de chaque workload dans l'événement et leur classement sur la page de détails de l'événement.

Unified Manager compare les dernières valeurs analysées pour un workload à la plage de valeurs attendue (prévision de latence). L'écart entre les dernières valeurs analysées et la plage de valeurs attendue permet d'identifier les workloads dont les performances ont été les plus affectées par l'événement.

Par exemple, supposons qu'un cluster contienne deux charges de travail : la charge de travail A et la charge de travail B. La latence prévue pour la charge de travail A est de 5 à 10 millisecondes par opération (ms/op) et sa latence réelle est généralement d'environ 7 ms/op. La latence prévue pour la charge de travail B est de 10 à 20 ms/op et sa latence réelle est généralement d'environ 15 ms/op. Les deux charges de travail respectent leurs prévisions de latence. En raison d'une contention sur le cluster, la latence des deux charges de travail augmente à 40 ms/op, dépassant ainsi le seuil de performance dynamique, qui correspond à la limite supérieure des prévisions de latence, et déclenchant des événements. L'écart de latence entre les valeurs attendues et les valeurs supérieures au seuil de performance est d'environ 33 ms/op pour la charge de travail A et d'environ 25 ms/op pour la charge de travail B. La latence des deux charges de travail atteint un pic de 40 ms/op, mais la charge de travail A a eu l'impact le plus important sur les performances, car elle présentait l'écart de latence le plus élevé, à 33 ms/op.

Sur la page Détails de l'événement, dans la section Diagnostic système, vous pouvez trier les workloads selon leur écart d'activité, d'utilisation ou de débit pour un composant du cluster. Vous pouvez également trier les workloads par latence. Lorsque vous sélectionnez une option de tri, Unified Manager analyse l'écart d'activité, d'utilisation, de débit ou de latence depuis la détection de l'événement par rapport aux valeurs attendues afin de déterminer l'ordre de tri des workloads. Pour la latence, les points rouges (🔴) indiquent le franchissement

d’un seuil de performance par un workload victime, ainsi que l’impact qui en résulte sur la latence. Chaque point rouge indique un niveau d’écart de latence plus élevé, ce qui vous aide à identifier les workloads victimes dont la latence a été la plus affectée par un événement.

Comprendre les composants du cluster et la contention dans Active IQ Unified Manager

Vous pouvez identifier les problèmes de performance du cluster lorsqu’un composant du cluster est en contention. Les performances des workloads qui utilisent ce composant ralentissent et leur temps de réponse (latence) aux requêtes client augmente, ce qui déclenche un événement dans Unified Manager.

Un composant en situation de contention ne peut pas fonctionner à un niveau optimal. Ses performances ont diminué, et les performances des autres composants du cluster et des workloads, appelés « victimes », peuvent présenter une latence accrue. Pour sortir un composant de la contention, vous devez réduire son workload ou augmenter sa capacité à traiter davantage de travail, afin que les performances puissent revenir à des niveaux normaux. Comme Unified Manager collecte et analyse les performances des workloads à intervalles de cinq minutes, il détecte uniquement lorsqu’un composant du cluster est constamment surutilisé. Les pics transitoires de surutilisation qui ne durent qu’une courte période pendant l’intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être en situation de contention parce qu’une ou plusieurs workloads qu’il contient se disputent le traitement de leurs requêtes d’E/S. D’autres workloads sur l’agrégat peuvent être affectés, ce qui entraîne une baisse de leurs performances. Pour réduire le niveau d’activité sur l’agrégat, vous pouvez prendre différentes mesures, par exemple déplacer une ou plusieurs workloads vers un agrégat ou un nœud moins sollicité, afin de réduire la demande globale de workload sur l’agrégat actuel. Pour un groupe de stratégies QoS, vous pouvez ajuster la limite de débit ou déplacer des workloads vers un autre groupe de stratégies, afin que les workloads ne soient plus limités.

Unified Manager surveille les composants de cluster suivants pour vous alerter lorsqu’ils sont en contention :

- **Réseau**

  Représente le temps d’attente des requêtes d’E/S par les protocoles réseau externes du cluster. Ce temps d’attente correspond au temps nécessaire pour que les transactions « transfer ready » soient terminées avant que le cluster puisse répondre à une requête d’E/S. Si le composant réseau est en contention, cela signifie qu’un temps d’attente élevé au niveau du protocole impacte la latence d’une ou plusieurs charges de travail.

- **Traitement réseau**

  Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre la couche protocolaire et le cluster. Le nœud gérant le traitement réseau a peut-être changé depuis la détection de l’événement. Si le composant de traitement réseau est en contention, cela signifie qu’une utilisation élevée du nœud de traitement réseau impacte la latence d’un ou de plusieurs workloads.

  Lors de l’utilisation d’un cluster All SAN Array en configuration active-active, la valeur de latence de traitement réseau est affichée pour les deux nœuds afin que vous puissiez vérifier que la charge est répartie équitablement entre eux.

- **Limite QoS maximale**

  Représente le paramètre de débit maximal (de pointe) du groupe de règles de qualité de service (QoS) du stockage attribué au workload. Si le composant du groupe de règles est en conflit, cela signifie que tous

les workloads du groupe de règles sont limités par la limite de débit définie, ce qui affecte la latence d'un ou de plusieurs de ces workloads.

- **Limite minimale de QoS**

  Représente la latence d'un workload causée par le paramètre minimal de débit QoS (attendu) attribué à d'autres workloads. Si le minimum QoS défini sur certains workloads utilise la majeure partie de la bande passante pour garantir le débit promis, les autres workloads seront limités et présenteront une latence plus élevée.

- **Interconnexion de cluster**

  Représente les câbles et adaptateurs auxquels les nœuds du cluster sont physiquement connectés. Si le composant d'interconnexion de cluster est saturé, cela signifie qu'un temps d'attente élevé pour les requêtes d'E/S au niveau de l'interconnexion de cluster affecte la latence d'un ou de plusieurs workloads.

- **Data Processing**

  Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient le workload. Le nœud gérant le traitement des données a peut-être changé depuis la détection de l'événement. Si le composant de traitement des données est en contention, cela signifie qu'une utilisation élevée au niveau du nœud de traitement des données affecte la latence d'un ou de plusieurs workloads.

- **Activation du volume**

  Représente le processus qui suit l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1 000 volumes sont actifs, ce processus suit le nombre de volumes critiques qui doivent accéder simultanément aux ressources via le nœud. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques présentent une latence, comme indiqué ici.

- **MetroCluster Ressources**

  Représente les ressources MetroCluster, notamment NVRAM et les liaisons inter-commutateurs (ISL), utilisées pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster est en conflit, cela signifie qu'un débit d'écriture élevé provenant des workloads sur le cluster local ou un problème d'état de la liaison affecte la latence d'un ou de plusieurs workloads sur le cluster local. Si le cluster n'est pas dans une configuration MetroCluster, cette icône n'est pas affichée.

- **Opérations sur des agrégats ou des agrégats SSD**

  Représente l'agrégat de stockage sur lequel les workloads s'exécutent. Si le composant d'agrégat est en contention, cela signifie qu'une utilisation élevée de l'agrégat affecte la latence d'un ou de plusieurs workloads. Un agrégat se compose uniquement de HDD, ou d'un mélange de HDD et de SSD (un agrégat Flash Pool), ou d'un mélange de HDD et d'un niveau cloud (un agrégat FabricPool). Un « `SSD Aggregate` » se compose uniquement de SSD (un agrégat 100 % Flash), ou d'un mélange de SSD et d'un niveau cloud (un agrégat FabricPool).

- **Latence du cloud**

  Ce composant logiciel du cluster gère les entrées/sorties entre le cluster et le niveau cloud où sont stockées les données utilisateur. Si le composant de latence cloud est saturé, cela signifie qu'un grand nombre de lectures sur des volumes hébergés sur le niveau cloud impactent la latence d'un ou plusieurs workloads.

- **Synchronisation SnapMirror**

  Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur du volume principal vers le volume secondaire dans une relation synchrone SnapMirror. Si le composant de synchronisation SnapMirror est en contention, cela signifie que l'activité des opérations synchrones SnapMirror affecte la latence d'un ou de plusieurs workloads.

Identifier les rôles de la charge de travail dans les événements de performance dans Active IQ Unified Manager

Unified Manager utilise des rôles pour identifier l'implication d'un workload dans un événement de performance. Ces rôles incluent les victimes, les agresseurs et les prédateurs. Un workload défini par l'utilisateur peut être à la fois victime, agresseur et prédateur.

Rôle	Description
Victime	Un workload défini par l'utilisateur dont les performances ont diminué en raison d'autres workloads, appelés « agresseurs », qui surutilisent un composant du cluster. Seuls les workloads définis par l'utilisateur sont identifiés comme victimes. Unified Manager identifie les workloads victimes en fonction de leur écart de latence : la latence réelle, lors d'un événement, a considérablement augmenté par rapport à la latence prévue (plage attendue).
Brute	Un workload défini par l'utilisateur ou par le système, dont la surutilisation d'un composant du cluster a entraîné une baisse des performances d'autres workloads, appelés victimes. Unified Manager identifie les workloads accapareurs en fonction de leur écart d'utilisation d'un composant du cluster, lorsque l'utilisation réelle, lors d'un événement, a largement augmenté par rapport à la plage d'utilisation prévue.
Requin	Un workload défini par l'utilisateur présentant l'utilisation la plus élevée d'un composant du cluster par rapport à tous les workloads impliqués dans un événement. Unified Manager identifie les workloads shark en fonction de leur utilisation d'un composant du cluster pendant un événement.

Les workloads sur un cluster peuvent partager de nombreux composants du cluster, tels que les agrégats et le processeur pour le réseau et le traitement des données. Lorsqu'un workload, tel qu'un volume, augmente son utilisation d'un composant du cluster au point que ce composant ne puisse pas répondre efficacement aux demandes du workload, le composant est en contention. Le workload qui surutilise un composant du cluster est un agresseur. Les autres workloads qui partagent ces composants et dont les performances sont affectées par l'agresseur sont les victimes. L'activité de workloads définis par le système, tels que la déduplication ou les copies Snapshot, peut également dégénérer en « bullying ».

Lorsque Unified Manager détecte un événement, il identifie tous les workloads et composants du cluster impliqués, y compris les workloads agressifs qui ont provoqué l'événement, le composant du cluster en conflit

et les workloads victimes dont les performances ont diminué en raison de l'activité accrue des workloads agressifs.

> Si Unified Manager ne parvient pas à identifier les workloads perturbateurs, il génère uniquement des alertes concernant les workloads victimes et le composant du cluster concerné.

Unified Manager peut identifier les workloads victimes de workloads agressifs, et également identifier quand ces mêmes workloads deviennent des workloads agressifs. Un workload peut être agressif envers lui-même. Par exemple, un workload très performant dont les performances sont limitées par une limite de groupe de règles entraîne la limitation des performances de tous les workloads du groupe de règles, y compris le sien. Un workload qui est agressif ou victime dans un incident de performance en cours peut changer de rôle ou ne plus être un participant à l'incident.

Gérer les seuils de performance

Gérez les seuils de performance dans Active IQ Unified Manager

Les politiques de seuil de performance vous permettent de déterminer le moment auquel Unified Manager génère un événement afin d'informer les administrateurs système des problèmes susceptibles d'affecter les performances du workload. Ces politiques de seuil sont appelées seuils de performance *définis par l'utilisateur*.

Cette version prend en charge les seuils de performance définis par l'utilisateur, définis par le système et dynamiques. Avec les seuils de performance dynamiques et définis par le système, Unified Manager analyse l'activité du workload pour déterminer la valeur de seuil appropriée. Avec les seuils définis par l'utilisateur, vous pouvez définir les limites supérieures de performance pour de nombreux compteurs de performance 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 sont pas configurables. Si vous recevez des événements inutiles provenant de l'une des stratégies de seuil de performance définies par le système, vous pouvez désactiver les stratégies individuelles depuis la page Event Setup.

Utilisez des politiques de seuil de performance définies par l'utilisateur dans Active IQ Unified Manager

Vous définissez des politiques de seuil de performance sur les objets de stockage (par exemple, sur les agrégats et les volumes) afin qu'un événement puisse être envoyé à l'administrateur de stockage pour l'informer que le cluster rencontre un problème de performance.

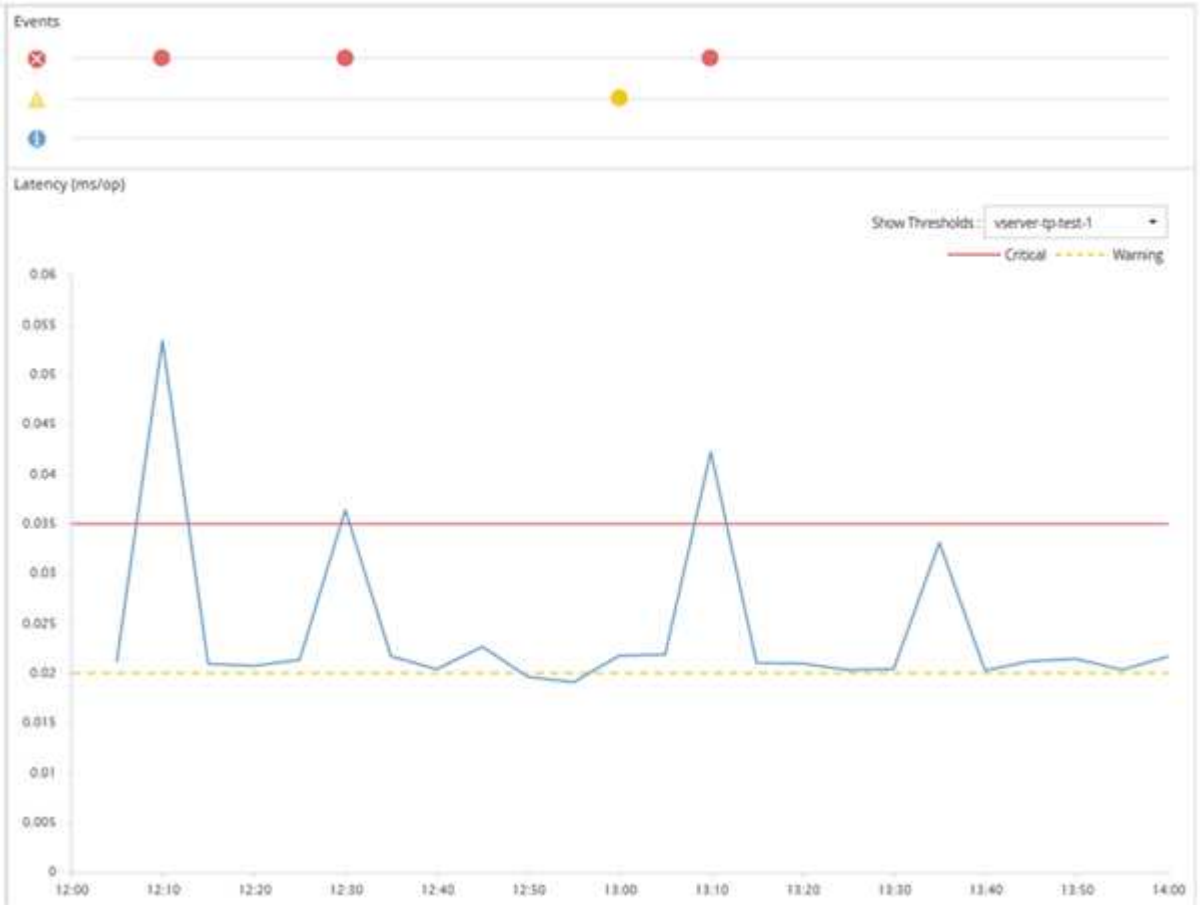
Vous créez une politique de seuil de performance pour un objet de stockage en :

- Sélection d'un objet de stockage
- Sélection d'un compteur de performance associé à cet objet
- Spécifier les valeurs qui définissent les limites supérieures du compteur de performance considérées comme des situations d'avertissement et critiques
- Spécifier une période de temps définissant la durée pendant laquelle le compteur doit dépasser la limite supérieure

Par exemple, vous pouvez définir une politique de seuil de performance pour un volume afin de recevoir une notification d'événement critique lorsque les IOPS de ce volume dépassent 750 opérations par seconde pendant 10 minutes consécutives. Cette même politique de seuil peut également spécifier l'envoi d'un avertissement lorsque les IOPS dépassent 500 opérations par seconde pendant 10 minutes.

La version actuelle permet de définir des seuils qui déclenchent l'envoi d'événements lorsqu'une valeur de compteur dépasse le seuil défini. Il n'est pas possible de définir des seuils qui déclenchent l'envoi d'événements lorsqu'une valeur de compteur passe en dessous d'un seuil défini.

Un exemple de graphique de compteur est présenté ici, indiquant qu'un seuil d'alerte (icône jaune) a été franchi à 1 h 00 et qu'un seuil critique (icône rouge) a été franchi à 12 h 10, 12 h 30 et 1 h 10:



Le dépassement du seuil doit se produire de manière continue pendant la durée spécifiée. Si le seuil descend en dessous des valeurs limites pour quelque raison que ce soit, tout dépassement ultérieur est considéré comme le début d'une nouvelle période.

Certains objets de cluster et des compteurs de performance permettent de créer une stratégie de seuil combinée qui exige que deux compteurs de performance dépassent 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 de cluster	Compteur de performances	Seuil d'alerte	Seuil critique	Durée
Volume	Latence	10 millisecondes	20 millisecondes	15 minutes

Objet de cluster	Compteur de performances	Seuil d'alerte	Seuil critique	Durée
Agrégat	Utilisation	65%	85%	

Les politiques de seuil utilisant deux objets de cluster ne génèrent un événement que lorsque les deux conditions sont dépassées. Par exemple, avec la politique de seuil définie dans le tableau :

Si la latence du volume est en moyenne…	Et l'utilisation du disque de l'agrégat est…	Ensuite…
15 millisecondes	50%	Aucun événement n'est signalé.
15 millisecondes	75%	Un événement d'avertissement a été signalé.
25 millisecondes	75%	Un événement d'avertissement a été signalé.
25 millisecondes	90%	Un événement critique a été signalé.

Répondez aux politiques de seuils de performance dépassés dans Active IQ Unified Manager

Lorsqu'une valeur de compteur dépasse son seuil de performance défini pendant la durée spécifiée, le seuil est franchi et un événement est signalé.

Cet événement déclenche les actions suivantes :

- L'événement est affiché dans le tableau de bord, la page Résumé du cluster de performances, la page Événements et la page Inventaire des performances spécifique à l'objet.
- (facultatif) Une alerte par e-mail concernant l'événement peut être envoyée à un ou plusieurs destinataires, et un trap SNMP peut être envoyé à un récepteur de traps.
- (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 distinctes selon qu'une stratégie de seuil Warning ou Critical est enfreinte.

Après qu'un dépassement de la stratégie de seuil de performances s'est produit sur un objet de stockage, aucun autre événement n'est généré pour cette stratégie tant que la valeur du compteur ne repasse pas en dessous de la valeur de seuil, moment auquel la durée est réinitialisée pour cette limite. Tant que le seuil continue d'être dépassé, l'heure de fin de l'événement est mise à jour en continu pour indiquer que cet événement est toujours en cours.

Un événement de seuil capture, ou fige, les informations relatives à la gravité et à la définition de la politique afin que des informations de seuil propres à l'événement s'affichent avec celui-ci, même si la politique de seuil est modifiée ultérieurement.

Comprendre les compteurs de performance suivis à l'aide de seuils dans Active IQ Unified Manager

Certains compteurs de performance courants, tels que les IOPS et les Mo/s, peuvent avoir des seuils définis pour tous les objets de stockage. D'autres compteurs peuvent avoir des seuils définis uniquement pour certains objets de stockage.

Compteurs de performances disponibles

Objet de stockage	Compteur de performances	Description
Cluster	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le cluster par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis ce cluster par seconde.	Nœud
Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie que le nœud traite par seconde.	Mo/s
Nombre moyen de mégaoctets de données transférés vers et depuis ce nœud par seconde.	Latence	Nombre moyen de millisecondes nécessaires au nœud pour répondre aux requêtes de l'application.
Utilisation	Pourcentage moyen d'utilisation du processeur et de la mémoire vive du nœud.	Capacité de performance utilisée
Pourcentage moyen de capacité de performance consommée par le nœud.	Capacité de performance utilisée - Prise de contrôle	Pourcentage moyen de capacité de performance consommée par le nœud, plus la capacité de performance de son nœud partenaire.
Agrégat	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie que l'agrégat traite par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis cet agrégat par seconde.	Latence
Nombre moyen de millisecondes nécessaires à l'agrégat pour répondre aux requêtes de l'application.	Utilisation	Pourcentage moyen des disques de l'agrégat qui sont utilisés.
Capacité de performance utilisée	Pourcentage moyen de la capacité de performance consommée par l'agrégat.	VM de stockage
Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le SVM par seconde.	Mo/s

Objet de stockage	Compteur de performances	Description
Nombre moyen de mégaoctets de données transférés vers et depuis cette SVM par seconde.	Latence	Nombre moyen de millisecondes nécessaires au SVM pour répondre aux requêtes de l'application.
Volume	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie que le volume traite par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés à destination et en provenance de ce volume par seconde.	Latence
Nombre moyen de millisecondes que le volume met pour répondre aux requêtes de l'application.	Taux de défauts du cache	Pourcentage moyen de requêtes de lecture provenant d'applications clientes qui sont satisfaites par le volume plutôt que par le cache.
LUN	Op E/S par sec	Nombre moyen d'opérations d'entrée/sortie traitées par le LUN par seconde.
Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis ce LUN par seconde.	Latence
Nombre moyen de millisecondes nécessaires au LUN pour répondre aux requêtes de l'application.	Espace de noms	Op E/S par sec
Nombre moyen d'opérations d'entrée/sortie que le namespace traite par seconde.	Mo/s	Nombre moyen de mégaoctets de données transférés vers et depuis ce namespace par seconde.
Latence	Nombre moyen de millisecondes nécessaires au namespace pour répondre aux requêtes de l'application.	Port
Utilisation de la bande passante	Pourcentage moyen de la bande passante disponible du port utilisée.	Mo/s
Nombre moyen de mégaoctets de données transférés vers et depuis ce port par seconde.	Interface réseau (LIF)	Mo/s

Comprendre les objets de stratégie de seuil combinés et les compteurs dans Active IQ Unified Manager

Seuls certains compteurs de performance peuvent être utilisés simultanément dans les stratégies combinées. Lorsque des compteurs de performance principaux et secondaires sont spécifiés, les deux doivent dépasser leurs limites maximales pour qu'un événement soit généré.

Objet et compteur de stockage principaux	Objet de stockage secondaire et compteur
Latence du volume	IOPS du volume
Mo/s du volume	Utilisation de l'agrégat
Capacité de performance de l'agrégat utilisée	Utilisation du nœud
Capacité de performance du nœud utilisée	Capacité de performance du nœud utilisée - Prise de contrôle
Latence LUN	IOPS de la LUN
Mo/s de la LUN	Utilisation de l'agrégat
Capacité de performance de l'agrégat utilisée	Utilisation du nœud
Capacité de performance du nœud utilisée	Capacité de performance du nœud utilisée - Prise de contrôle

Lorsqu'une stratégie de combinaison de volumes est appliquée à un volume FlexGroup, au lieu d'être appliquée à un volume FlexVol, seuls les attributs « Volume IOPS » et « Volume MB/s » peuvent être sélectionnés comme compteur secondaire. Si la stratégie de seuil contient l'un des attributs de nœud ou d'agrégat, la stratégie ne sera pas appliquée au volume FlexGroup, et vous recevrez un message d'erreur décrivant ce cas. Cela s'explique par le fait que les volumes FlexGroup peuvent exister sur plusieurs nœuds ou agrégats.

Créez des politiques de seuil de performance définies par l'utilisateur dans Active IQ Unified Manager

Vous créez des stratégies de seuil de performance pour les objets de stockage afin que des notifications soient envoyées lorsqu'un compteur de performance dépasse une valeur spécifique. La notification d'événement indique que le cluster rencontre un problème de performance.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Vous créez des politiques de seuil de performance en saisissant les valeurs de seuil sur la page « Créer une politique de seuil de performance ». Vous pouvez créer de nouvelles politiques en définissant toutes les valeurs de la politique sur cette page, ou vous pouvez copier une politique existante et modifier les valeurs de la copie (opération appelée « clonage »).

Les valeurs de seuil valides sont de 0,001 à 10 000 000 pour les nombres, de 0,001 à 100 pour les pourcentages et de 0,001 à 200 pour les pourcentages de Performance Capacity Used.

La version actuelle permet de définir des seuils qui déclenchent l'envoi d'événements lorsqu'une valeur de compteur dépasse le seuil défini. Il n'est pas possible de définir des seuils qui déclenchent l'envoi d'événements lorsqu'une valeur de compteur passe en dessous d'un seuil défini.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Seuils d'événements** > **Performance**.

   La page « Seuils de performance » s'affiche.

2. Cliquez sur le bouton approprié selon que vous souhaitez créer une nouvelle stratégie ou cloner une stratégie similaire et modifier la version clonée.

À…	Cliquez…
Créer une nouvelle politique	**Créer**
Cloner une stratégie existante	Sélectionnez une stratégie existante et cliquez sur **Clone**

La page « Créer une stratégie de seuil de performance » ou « Cloner une stratégie de seuil de performance » s'affiche.

3. Définissez la politique de seuil en spécifiant les valeurs de seuil des compteurs de performance 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 stratégie.

   b. Sélectionnez le compteur de performances à suivre et spécifiez les valeurs limites qui définissent les événements d'avertissement et critiques.

      Vous devez définir au moins une limite d'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 d'avertissement et critiques.

      L'ajout d'un compteur secondaire exige que les deux compteurs dépassent les valeurs limites avant que le seuil ne soit franchi et qu'un événement ne soit signalé. Seuls certains objets et compteurs peuvent être configurés à l'aide d'une stratégie combinée.

   d. Sélectionnez la durée pendant laquelle les valeurs limites doivent être dépassées pour qu'un événement soit envoyé.

   Lors du clonage d'une stratégie existante, vous devez saisir un nouveau nom pour la stratégie.

4. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

   Vous êtes redirigé vers la page « Seuils de performance ». Un message de confirmation en haut de la page indique que la stratégie de seuil a bien été créée et fournit un lien vers la page « Inventaire » du type d'objet concerné, vous permettant ainsi d'appliquer immédiatement la nouvelle stratégie aux objets de stockage.

Si vous souhaitez appliquer la nouvelle politique de seuil aux objets de stockage dès maintenant, vous pouvez cliquer sur le lien **Accéder à object_type maintenant** pour accéder à la page Inventory.

Attribuez des politiques de seuil de performance aux objets de stockage dans Active IQ Unified Manager

Vous attribuez une stratégie de seuil de performance définie par l'utilisateur à un objet de stockage afin qu'Unified Manager signale un événement si la valeur du compteur de performance dépasse le paramètre de stratégie.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

La ou les politiques de seuil de performance que vous souhaitez appliquer à l'objet doivent exister.

Vous ne pouvez appliquer qu'une seule politique de performance à la fois à un objet ou à un groupe d'objets.

Vous pouvez attribuer un maximum de trois stratégies de seuil à chaque objet de stockage. Lors de l'attribution de stratégies à plusieurs objets, si l'un d'eux possède déjà le nombre maximal de stratégies attribuées, Unified Manager effectue les actions suivantes :

- Applique la politique à tous les objets sélectionnés qui n'ont pas atteint leur maximum
- Ignore les objets ayant atteint le nombre maximal de stratégies
- Affiche un message indiquant que la stratégie n'a pas été attribuée à tous les objets

Étapes

1. Depuis la page d'inventaire des performances de n'importe quel objet de stockage, sélectionnez le ou les objets auxquels vous souhaitez attribuer une stratégie de seuil :

Pour attribuer des seuils à…	**Cliquez…**
Un seul objet	La case à cocher située à gauche de cet objet.
Objets multiples	La case à cocher située à gauche de chaque objet.
Tous les objets de la page	La liste déroulante ☐▾, puis choisissez **Sélectionner tous les objets de cette page**.
Tous les objets du même type	La ☐▾ liste déroulante, puis choisissez **Sélectionner tous les objets**.

   Vous pouvez utiliser les fonctionnalités de tri et de filtrage pour affiner la liste des objets sur la page d'inventaire afin de faciliter l'application de politiques de seuil à de nombreux objets.

2. Faites votre sélection, puis cliquez sur **Attribuer une politique de seuil de performance**.

   La page « Attribuer une stratégie de seuil de performance » s'affiche, présentant une liste des stratégies de seuil qui existent pour ce type spécifique d'objet de stockage.

3. Cliquez sur chaque règle pour afficher les détails des paramètres de seuil de performance et vérifier que vous avez sélectionné la règle de seuil appropriée.
4. Après avoir sélectionné la politique de seuil appropriée, cliquez sur **Attribuer une politique**.

   Un message de confirmation en haut de la page indique que la politique de seuil a été attribuée à l'objet ou aux objets, et fournit un lien vers la page Alerting afin que vous puissiez configurer les paramètres d'alerte pour cet objet et cette politique.

Si vous souhaitez recevoir des alertes par e-mail ou sous forme de trap SNMP pour être averti de la génération d'un événement de performance particulier, vous devez configurer les paramètres d'alerte sur la page Alert Setup.

Consultez les règles de seuil de performance dans Active IQ Unified Manager

Vous pouvez consulter toutes les politiques de seuil de performance actuellement définies sur la page « Seuils de performance ».

La liste des politiques de seuil est triée par ordre alphabétique selon le nom de la politique et comprend des

politiques pour tous les types d'objets de stockage. Vous pouvez cliquer sur l'en-tête d'une colonne pour trier les politiques selon cette colonne. Si vous recherchez une politique spécifique, utilisez les mécanismes de filtre et de recherche pour affiner la liste des politiques de seuil qui s'affichent dans la liste d'inventaire.

Vous pouvez survoler le nom de la stratégie et le nom de la condition avec votre curseur pour voir les détails de configuration de la stratégie. De plus, vous pouvez utiliser les boutons fournis pour créer, cloner, modifier et supprimer des stratégies de seuil définies par l'utilisateur.

Étape

1. Dans le volet de navigation de gauche, sélectionnez **Seuils d'événements** > **Performance**.

   La page « Seuils de performance » s'affiche.

Modifiez les règles de seuil de performance définies par l'utilisateur dans Active IQ Unified Manager

Vous pouvez modifier les paramètres de seuil des politiques de seuil de performance existantes. Cela peut s'avérer utile si vous recevez trop ou trop peu d'alertes pour certaines conditions de seuil.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Vous ne pouvez pas modifier le nom de la stratégie ni le type d'objet de stockage surveillé pour les stratégies de seuil existantes.

Étapes

1. Dans le volet de navigation de gauche, sélectionnez **Seuils d'événements** > **Performance**.

   La page « Seuils de performance » s'affiche.

2. Sélectionnez la stratégie de seuil que vous souhaitez modifier et cliquez sur **Modifier**.

   La page « Modifier la politique de seuil de performance » s'affiche.

3. Apportez vos modifications à la politique de seuil et cliquez sur **Enregistrer**.

   Vous revenez à la page des seuils de performance.

Une fois enregistrées, les modifications s'appliquent immédiatement à tous les objets de stockage qui utilisent cette stratégie.

Selon le type de modifications apportées à la stratégie, vous pouvez consulter les paramètres d'alerte configurés pour les objets qui utilisent cette stratégie sur la page Configuration des alertes.

Supprimez les stratégies de seuil de performance des objets de stockage dans Active IQ Unified Manager

Vous pouvez supprimer une stratégie de seuil de performance définie par l'utilisateur d'un objet de stockage lorsque vous ne souhaitez plus que Unified Manager surveille la valeur du compteur de performance.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Vous ne pouvez supprimer qu'une seule stratégie à la fois sur un objet sélectionné.

Vous pouvez supprimer une stratégie de seuil de plusieurs objets de stockage en sélectionnant plusieurs objets dans la liste.

Étapes

1. Depuis la page **inventaire** de n'importe quel objet de stockage, sélectionnez un ou plusieurs objets auxquels au moins une politique de seuil de performance est appliquée.

Pour effacer les seuils de…	Faites ceci…
Un seul objet	Sélectionnez la case à cocher à gauche de cet objet.
Objets multiples	Sélectionnez la case à cocher à gauche de chaque objet.
Tous les objets de la page	Cliquez dans l'en-tête de la colonne.

2. Cliquez sur **Effacer la politique de seuil de performance**.

   La page « Effacer la stratégie de seuil » s'affiche et présente la liste des stratégies de seuil actuellement attribuées aux objets de stockage.

3. Sélectionnez la politique de seuil que vous souhaitez supprimer des objets et cliquez sur **Effacer la politique**.

   Lorsque vous sélectionnez une stratégie de seuil, les détails de cette stratégie s'affichent afin que vous puissiez confirmer que vous avez sélectionné la stratégie appropriée.

Comprendre les modifications apportées aux politiques de seuil de performance dans Active IQ Unified Manager

Si vous modifiez la valeur du compteur ou la durée d'une stratégie de seuil de performance existante, la modification de la stratégie est appliquée à tous les objets de stockage qui utilisent cette stratégie. Le nouveau paramètre prend effet immédiatement, et Unified Manager commence à comparer les valeurs du compteur de performance aux nouveaux paramètres de seuil pour toutes les nouvelles données de performance collectées.

S'il existe des événements actifs pour des objets utilisant la politique de seuil modifiée, ces événements sont marqués comme obsolètes, et la politique de seuil commence à surveiller le compteur en tant que politique de seuil nouvellement définie.

Dans la vue détaillée des graphiques de compteurs, lorsque vous consultez le compteur auquel le seuil a été appliqué, les lignes de seuil critique et d'alerte reflètent les paramètres de seuil actuels. Les paramètres de seuil d'origine n'apparaissent pas sur cette page, même si vous consultez les données historiques lorsque les anciens paramètres de seuil étaient en vigueur.

Étant donné que les anciens paramètres de seuil n'apparaissent pas dans la vue détaillée des graphiques de compteurs, il se peut que vous voyiez des événements historiques qui apparaissent sous les lignes de seuil actuelles.

Gérez les politiques de seuil lors du déplacement d'objets dans Active IQ Unified Manager

Étant donné que les politiques de seuil de performance sont attribuées aux objets de stockage, si vous déplacez un objet, toutes les politiques de seuil attribuées restent associées à l'objet une fois le déplacement terminé. Par exemple, si vous déplacez un volume ou un LUN vers un autre agrégat, les politiques de seuil restent actives pour ce volume ou ce LUN sur le nouvel agrégat.

Si une condition de compteur secondaire existe pour la stratégie de seuil (une stratégie combinée), par exemple si une condition supplémentaire est attribuée à un agrégat ou à un nœud, la condition de compteur secondaire est appliquée au nouvel agrégat ou nœud vers lequel le volume ou la LUN a été déplacé.

S'il existe de nouveaux événements actifs pour des objets utilisant la politique de seuil modifiée, ces événements sont marqués comme obsolètes, et la politique de seuil commence à surveiller le compteur comme une politique de seuil nouvellement définie.

Une opération de déplacement de volume amène ONTAP à envoyer un événement de modification informatif. Une icône d'événement de modification apparaît dans la chronologie des événements sur la page Performance Explorer et la page Workload Analysis pour indiquer l'heure à laquelle l'opération de déplacement a été terminée.

> Si vous déplacez un objet vers un autre cluster, la politique de seuil définie par l'utilisateur est supprimée de l'objet. Le cas échéant, vous devez attribuer une politique de seuil à l'objet une fois le déplacement terminé. Les politiques de seuil dynamiques et définies par le système, quant à elles, sont appliquées automatiquement à l'objet après son déplacement vers un nouveau cluster.

Fonctionnalité de la stratégie de seuil lors de la prise de contrôle et de la restitution HA

Lors d'une opération de basculement ou de restitution dans une configuration à haute disponibilité (HA), les objets déplacés d'un nœud à l'autre conservent leurs politiques de seuil, comme lors d'un déplacement manuel. Unified Manager vérifiant les modifications de configuration du cluster toutes les 15 minutes, l'impact du basculement vers le nouveau nœud n'est identifié qu'à la prochaine interrogation de la configuration du cluster.

> Si une opération de prise de contrôle et une opération de restitution ont toutes deux lieu au cours de la période de collecte des modifications de configuration de 15 minutes, il se peut que les statistiques de performances ne passent pas d'un nœud à l'autre.

fonctionnalité de la règle de seuil lors de la relocalisation d'agrégat

Si vous déplacez un agrégat d'un nœud vers un autre à l'aide de la commande `aggregate relocation start`, les politiques de seuil simples et combinées sont conservées sur tous les objets, et la partie nœud de la politique de seuil est appliquée au nouveau nœud.

Fonctionnalité de la stratégie de seuil lors du basculement MetroCluster

Les objets qui se déplacent d'un cluster à un autre dans une configuration MetroCluster ne conservent pas leurs paramètres de stratégie de seuil définis par l'utilisateur. Si nécessaire, vous pouvez appliquer des stratégies de seuil aux volumes et aux LUN qui ont été déplacés vers le cluster partenaire. Une fois qu'un objet est revenu à son cluster d'origine, la stratégie de seuil définie par l'utilisateur est automatiquement

réappliquée.

Pour plus d'informations, consultez "Comportement du volume lors du basculement et du rétablissement".

Analyser les événements de performance

Analysez les événements de performance dans Active IQ Unified Manager

Vous pouvez analyser les événements de performance pour identifier quand ils ont été détectés, s'ils sont actifs (nouveaux ou reconnus) ou obsolètes, les workloads et les composants du cluster concernés, ainsi que les options permettant de résoudre ces événements par vous-même.

Afficher les informations relatives aux événements de performance dans Active IQ Unified Manager

La page d'inventaire de gestion des événements vous permet de consulter la liste de tous les événements de performance sur les clusters surveillés par Unified Manager. Ces informations vous permettent d'identifier les événements les plus critiques, puis d'accéder à des informations détaillées pour en déterminer la cause.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

La liste des événements est triée par date de détection, les plus récents apparaissant en premier. Vous pouvez cliquer sur l'en-tête d'une colonne pour trier les événements selon cette colonne. Par exemple, vous pouvez trier par la colonne « Statut » pour afficher les événements par niveau de gravité. Si vous recherchez un événement spécifique ou un type d'événement particulier, vous pouvez utiliser les filtres et la fonction de recherche pour affiner la liste des événements affichés.

Les événements provenant de toutes les sources sont affichés sur cette page :

- Règle de seuil de performance définie par l'utilisateur
- Politique de seuil de performance définie par le système
- Seuil de performance dynamique

La colonne « Type d'événement » indique la source de l'événement. Vous pouvez sélectionner un événement pour afficher ses détails dans la page Détails de l'événement.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans le menu Affichage, sélectionnez **Événements de performance actifs**.

   Cette page affiche tous les événements de performance nouveaux et acquittés générés au cours des 7 derniers jours.

3. Repérez l'événement que vous souhaitez 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 depuis la page Performance Explorer et depuis un e-mail d'alerte.

Analyser les événements à partir de seuils de performance définis par l'utilisateur

Analysez les événements à partir des seuils de performance définis par l'utilisateur dans Active IQ Unified Manager

Les événements générés par des seuils définis par l'utilisateur indiquent qu'un compteur de performance d'un objet de stockage donné, par exemple un agrégat ou un volume, a dépassé le seuil défini dans la stratégie. Cela signifie que l'objet du cluster rencontre un problème de performance.

Vous utilisez la page de détails de l'événement pour analyser l'événement de performance et prendre les mesures correctives nécessaires afin de rétablir des performances normales.

Répondez aux événements de seuil de performance définis par l'utilisateur dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser les événements de performance provoqués par le franchissement, par un compteur de performances, d'un seuil d'avertissement ou critique défini par l'utilisateur. Vous pouvez également utiliser Unified Manager pour vérifier l'état du composant du cluster afin de déterminer si des événements d'état récents détectés sur ce composant ont contribué à l'événement de performance.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux ou obsolètes.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Veuillez consulter la **Description**, qui décrit le dépassement de seuil ayant provoqué l'événement.

   Par exemple, le message « `La valeur de latence de 456 ms/op a déclenché un événement d'avertissement en fonction du paramètre de seuil de 400 ms/op` » indique qu'un événement d'avertissement de latence s'est produit pour l'objet.

3. Placez votre curseur sur le nom de la politique pour afficher les détails concernant la politique de seuil qui a déclenché l'événement.

   Cela inclut le nom de la stratégie, le compteur de performance évalué, la valeur du compteur qui doit être dépassée pour qu'un événement soit considéré comme critique ou d'avertissement, ainsi que la durée pendant laquelle le compteur doit dépasser cette valeur.

4. Notez l'**Heure de déclenchement de l'événement** afin de pouvoir vérifier si d'autres événements ont pu se produire simultanément et contribuer à cet événement.
5. Suivez l'une des options ci-dessous pour examiner plus en détail l'événement et déterminer si vous devez prendre des mesures pour résoudre le problème de performance :

Option	Actions d'enquête possibles
Cliquez sur le nom de l'objet source pour afficher la page Explorateur de cet objet.	Cette page vous permet de consulter les détails de l'objet et de le comparer à d'autres objets de stockage similaires afin de déterminer si d'autres objets de stockage rencontrent un problème de performance au même moment. Par exemple, vous pouvez vérifier si d'autres volumes du même agrégat présentent également un problème de performance.
Cliquez sur le nom du cluster pour afficher la page Résumé du cluster.	Cette page vous permet de consulter les détails du cluster sur lequel se trouve cet objet afin de vérifier si d'autres problèmes de performance sont survenus à peu près au même moment.

Analyser les événements à partir des seuils de performance définis par le système

Analysez les événements à partir des seuils de performance définis par le système dans Active IQ Unified Manager

Les événements générés à partir de seuils de performance définis par le système indiquent qu'un compteur de performance, ou un ensemble de compteurs de performance, pour un objet de stockage donné a franchi le seuil d'une politique définie par le système. Cela indique que l'objet de stockage, par exemple un agrégat ou un nœud, rencontre un problème de performance.

Vous utilisez la page de détails de l'événement pour analyser l'événement de performance et prendre les mesures correctives nécessaires afin de rétablir des performances normales.

Les politiques de seuil définies par le système ne sont pas activées sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Répondez aux événements de seuil de performance définis par le système dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser les événements de performance provoqués par le franchissement d'un seuil d'avertissement défini par le système par un compteur de performance. Vous pouvez également utiliser Unified Manager pour vérifier l'état du composant du cluster afin de déterminer si des événements récents détectés sur ce composant ont contribué à l'événement de performance.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux ou obsolètes.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Veuillez consulter la **Description**, qui décrit le dépassement de seuil ayant provoqué l'événement.

Par exemple, le message « `La valeur d'utilisation du nœud de 90 % a déclenché un événement AVERTISSEMENT en fonction du paramètre de seuil de 85 %` » indique qu'un événement d'avertissement d'utilisation du nœud s'est produit pour l'objet de cluster.

3. Notez l'**Heure de déclenchement de l'événement** afin de pouvoir vérifier si d'autres événements ont pu se produire simultanément et contribuer à cet événement.
4. Sous **Diagnostic système**, consultez la brève description du type d'analyse que la politique définie par le système effectue sur l'objet de cluster.

   Pour certains événements, une icône verte ou rouge s'affiche à côté du diagnostic pour indiquer si un problème a été détecté dans ce diagnostic particulier. Pour d'autres types d'événements définis par le système, des graphiques de compteurs affichent les performances de l'objet.

5. Sous **Actions suggérées**, cliquez sur le lien **Aidez-moi à faire ceci** pour afficher les actions suggérées que vous pouvez effectuer afin de tenter de résoudre vous-même l'événement de performances.

Répondez aux événements de performance des groupes de règles QoS dans Active IQ Unified Manager

Unified Manager génère des événements d'avertissement de politique QoS lorsque le débit du workload (IOPS, IOPS/TB ou Mo/s) a dépassé le paramètre défini de la politique QoS ONTAP et que la latence du workload commence à être affectée. Ces événements définis par le système offrent la possibilité de corriger des problèmes de performance potentiels avant que de nombreux workloads ne soient affectés par la latence.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Unified Manager génère des événements d'avertissement en cas de non-respect des règles de QoS lorsque le débit du workload a dépassé le paramètre de règle de QoS défini pendant chaque période de collecte des performances de l'heure précédente. Le débit du workload peut dépasser le seuil de QoS pendant une courte période seulement au cours de chaque période de collecte, mais Unified Manager affiche uniquement le débit "average" de la période de collecte sur le graphique. C'est pourquoi vous pouvez recevoir des événements QoS alors que le débit d'un workload n'a peut-être pas dépassé le seuil de règle indiqué sur le graphique.

Vous pouvez utiliser System Manager ou les commandes ONTAP pour gérer les groupes de stratégies, notamment les tâches suivantes :

- Création d'un nouveau groupe de stratégies pour le workload
- Ajout ou suppression de workloads dans un groupe de stratégies
- Déplacer un workload entre des groupes de stratégie
- Modification de la limite de débit d'un groupe de stratégies
- Déplacement d'un workload vers un autre agrégat ou nœud

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Veuillez consulter la **Description**, qui décrit le dépassement de seuil ayant provoqué l'événement.

   Par exemple, le message « `La valeur IOPS de 1 352 IOPS sur vol1_NFS1 a déclenché un événement AVERTISSEMENT afin d'identifier des problèmes de performance`

`potentiels pour le workload` » indique qu'un événement QoS Max IOPS s'est produit sur le volume vol1_NFS1.

3. Consultez la section **Informations sur l'événement** pour obtenir plus de détails sur le moment où l'événement s'est produit et depuis combien de temps l'événement est actif.

   De plus, pour les volumes ou LUN qui partagent le débit d'une politique QoS, vous pouvez voir les noms des trois principaux workloads qui consomment le plus d'IOPS ou de MBps.

4. Dans la section **Diagnostic système**, consultez les deux graphiques : l'un présente le nombre moyen total d'IOPS ou de Mo/s (selon l'événement), et l'autre la latence. Cette présentation permet d'identifier les composants du cluster qui affectent le plus la latence lorsque la workload approche de la limite maximale de la QoS.

   Lors d'un événement de politique QoS partagée, les trois principaux workloads sont affichés dans le graphique de débit. Si plus de trois workloads partagent la politique QoS, les workloads supplémentaires sont alors regroupés dans une catégorie « `Other workloads` ». Par ailleurs, le graphique de latence affiche la latence moyenne de tous les workloads qui font partie de la politique QoS.

   Notez que, pour les événements de politique de QoS adaptative, les graphiques IOPS et MBps affichent des valeurs IOPS ou MBps qu'ONTAP a converties à partir de la politique de seuil IOPS/TB attribuée en fonction de la taille du volume.

5. Dans la section **Actions suggérées**, examinez les suggestions et déterminez les actions que vous devez entreprendre pour éviter une augmentation de la latence du workload.

   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'incident de performance.

Comprendre les événements QoS adaptatifs avec une taille de bloc définie dans Active IQ Unified Manager

Les groupes de stratégies Adaptive QoS ajustent automatiquement un débit maximal ou minimal en fonction de la taille du volume, en maintenant le ratio IOPS/To à mesure que la taille du volume change. À partir de ONTAP 9.5, vous pouvez spécifier la taille de bloc dans la stratégie QoS afin d'appliquer simultanément un seuil en Mo/s.

L'attribution d'un seuil d'IOPS dans une politique QoS adaptative limite uniquement le nombre d'opérations effectuées dans chaque workload. Selon la taille des blocs définie sur le client générant les workloads, certaines IOPS contiennent beaucoup plus de données et imposent donc une charge beaucoup plus importante aux nœuds qui traitent les opérations.

La valeur en MB/s pour un workload est calculée à l'aide de la formule suivante :

```
MB/s = (IOPS * Block Size) / 1000
```

Si un workload atteint en moyenne 3 000 IOPS et que la taille de bloc côté client est définie sur 32 Ko, le débit effectif en Mo/s pour ce workload est de 96. Si ce même workload atteint en moyenne 3 000 IOPS et que la taille de bloc côté client est définie sur 48 Ko, le débit effectif en Mo/s pour ce workload est de 144. Vous pouvez constater que le nœud traite 50 % de données en plus lorsque la taille de bloc est plus grande.

Examinons la politique QoS adaptative suivante, qui possède une taille de bloc définie, et la manière dont les

événements sont déclenchés en fonction de la taille de bloc définie sur le client.

Créez une stratégie et définissez le débit maximal à 2 500 IOPS/To avec une taille de bloc de 32 Ko. Cela définit effectivement le seuil en Mo/s à 80 Mo/s ((2 500 IOPS * 32 Ko) / 1 000) pour un volume dont la capacité utilisée est de 1 To. Notez que Unified Manager génère un événement d'avertissement lorsque la valeur du débit est inférieure de 10 % au seuil défini. Des événements sont générés dans les situations suivantes :

Capacité utilisée	Un événement est généré lorsque le débit dépasse ce nombre de …	
	Op E/S par sec	Mo/s
1 TB	2 250 IOPS	72 Mo/s
2 TB	4 500 IOPS	144 Mo/s
5 To	11 250 IOPS	360 Mo/s

Si le volume utilise 2 To d'espace disponible, que les IOPS sont de 4 000 et que la taille des blocs QoS est de 32 Ko côté client, le débit est de 128 Mo/s ((4 000 IOPS * 32 Ko) / 1 000). Aucun événement n'est généré dans ce cas, car 4 000 IOPS et 128 Mo/s sont tous deux inférieurs au seuil pour un volume utilisant 2 To d'espace.

Si le volume utilise 2 To d'espace disponible, que les IOPS sont de 4 000 et que la taille des blocs QoS est définie à 64 Ko côté client, le débit est de 256 Mo/s ((4 000 IOPS * 64 Ko) / 1 000). Dans ce cas, les 4 000 IOPS ne génèrent pas d'événement, mais la valeur de 256 Mo/s est supérieure au seuil de 144 Mo/s et un événement est généré.

Pour cette raison, lorsqu'un événement est déclenché suite à un dépassement du seuil de débit (MB/s) pour une politique QoS adaptative prenant en compte la taille des blocs, un graphique de débit (MB/s) s'affiche dans la section « Diagnostic système » de la page « Détails de l'événement ». Si l'événement est déclenché suite à un dépassement des IOPS pour la politique QoS adaptative, un graphique des IOPS s'affiche dans la section « Diagnostic système ». En cas de dépassement simultané des IOPS et du débit (MB/s), vous recevrez deux événements.

Pour plus d'informations sur le réglage des paramètres QoS, consultez "Aperçu de la gestion des performances".

Répondez aux événements de surutilisation des ressources des nœuds dans Active IQ Unified Manager

Unified Manager génère des événements d'avertissement de surutilisation des ressources du nœud lorsqu'un seul nœud fonctionne au-delà des limites de son efficacité opérationnelle et risque donc d'affecter les latences des workloads. Ces événements définis par le système permettent de corriger d'éventuels problèmes de performance avant que la latence n'affecte de nombreux workloads.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux ou obsolètes.

Unified Manager génère des événements d'avertissement pour les violations de la politique de surutilisation des ressources des nœuds 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 QoS aux volumes ou LUN qui utilisent excessivement les ressources système
- Réduction de la limite de débit maximal QoS d'un groupe de règles auquel des workloads ont été appliqués
- Déplacement d'un workload vers un autre agrégat ou nœud
- Augmenter la capacité en ajoutant des disques au nœud ou en passant à un nœud doté d'un CPU plus rapide et de plus de RAM

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Veuillez consulter la **Description**, qui décrit le dépassement de seuil ayant provoqué l'événement.

   Par exemple, le message « `Perf. Capacity Used value of 139 % on simplicity-02 has triggered a WARNING event to identify potential performance problems in the data processing unit.` » indique que la capacité de performance du nœud simplicity-02 est surutilisée et affecte les performances du nœud.

3. Dans la section **Diagnostic système**, consultez les trois graphiques : un pour la capacité de performance utilisée sur le nœud, un pour les IOPS de stockage moyennes utilisées par les principaux workloads, et un pour la latence des principaux workloads. Lorsqu'ils sont organisés de cette manière, vous pouvez voir quels workloads sont à l'origine de la latence sur le nœud.

   Vous pouvez voir quels workloads ont des stratégies QoS appliquées, et lesquels n'en ont pas, en déplaçant votre curseur sur le graphique IOPS.

4. Dans la section **Actions suggérées**, examinez les suggestions et déterminez les actions que vous devez entreprendre pour éviter une augmentation de la latence du workload.

   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'incident de performance.

Répondez aux événements de performance liés au déséquilibre des clusters dans Active IQ Unified Manager

Unified Manager génère des alertes d'déséquilibre du cluster lorsqu'un nœud d'un cluster fonctionne à une charge bien plus élevée que les autres nœuds, ce qui peut donc affecter la latence des workloads. Ces alertes définies par le système permettent de corriger les problèmes de performance potentiels avant que de nombreux workloads ne soient affectés par la latence.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Unified Manager génère des événements d'avertissement en cas de violation de la règle de seuil de déséquilibre du cluster en comparant la valeur de capacité de performances utilisée pour tous les nœuds du cluster afin de déterminer s'il existe une différence de charge de 30 % entre deux nœuds.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les workloads les plus performants vers un nœud moins utilisé :

- Les nœuds du même cluster qui sont moins utilisés

- Les agrégats sur le nouveau nœud qui sont les moins utilisés
- Les volumes les plus performants sur le nœud actuel

Étapes

1. Consultez la page de détails **Event** pour afficher des informations sur l'événement.
2. Veuillez consulter la **Description**, qui décrit le dépassement de seuil ayant provoqué l'événement.

   Par exemple, le message « `Le compteur de capacité de performance utilisée indique une différence de charge de 62 % entre les nœuds du cluster Dallas-1-8 et a déclenché un événement WARNING basé sur le seuil système de 30 %` » indique que la capacité de performance de l'un des nœuds est surutilisée et affecte les performances du nœud.

3. Consultez le texte de la section **Actions suggérées** pour déplacer un volume hautes performances du nœud présentant la valeur de capacité de performances utilisée la plus élevée vers un nœud présentant la valeur de capacité de performances utilisée la plus faible.
4. Identifiez les nœuds présentant les valeurs de capacité de performance utilisée les plus élevées et les plus faibles :
   a. Dans la section **Informations sur l'événement**, cliquez sur le nom du cluster source.
   b. Sur la page **Résumé du cluster / des performances**, cliquez sur **Nœuds** dans la zone **Objets gérés**.
   c. Dans la page d'inventaire **Nodes**, triez les nœuds selon la colonne **Performance Capacity Used**.
   d. Identifiez les nœuds présentant les valeurs de capacité de performance utilisée les plus élevées et les plus faibles, et notez leurs noms.
5. Identifiez le volume utilisant le plus d'IOPS sur le nœud présentant la valeur d'utilisation de la capacité de performance la plus élevée :
   a. Cliquez sur le nœud présentant la valeur de capacité de performance utilisée la plus élevée.
   b. Sur la page **Nœud / Explorateur de performances**, sélectionnez **Agrégats sur ce nœud** dans le menu **Afficher et comparer**.
   c. Cliquez sur l'agrégat présentant la valeur de capacité de performance utilisée la plus élevée.
   d. Sur la page **Aggregate / Performance Explorer**, sélectionnez **Volumes on this Aggregate** dans le menu **View and Compare**.
   e. Triez les volumes selon la colonne **IOPS** et notez le nom du volume utilisant le plus grand nombre d'IOPS, ainsi que le nom de l'agrégat dans lequel se trouve ce volume.
6. Identifiez l'agrégat présentant le taux d'utilisation le plus faible sur le nœud dont la valeur de capacité de performance utilisée est la plus faible:
   a. Cliquez sur **Stockage** > **Agrégats** pour afficher la page d'inventaire **Agrégats**.
   b. Sélectionnez la vue **Performances : Tous les agrégats**.
   c. Cliquez sur le bouton **Filter** et ajoutez un filtre où « `Node` » correspond au nom du nœud ayant la valeur de capacité de performance utilisée la plus faible que vous avez notée à l'étape 4.
   d. Notez le nom de l'agrégat dont la valeur de capacité de performance utilisée est la plus faible.
7. Déplacez le volume du nœud surchargé vers l'agrégat que vous avez identifié comme ayant une faible utilisation sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement à l'aide de ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même événement de déséquilibre du cluster provenant de ce cluster.

Analyser les événements à partir de seuils de performance dynamiques

Analysez les événements issus des seuils de performance dynamiques dans Active IQ Unified Manager

Les événements générés par les seuils dynamiques indiquent que le temps de réponse réel (latence) d'un workload est trop élevé ou trop faible par rapport à la plage de temps de réponse attendue. Vous utilisez la page « Détails de l'événement » pour analyser l'événement de performance et prendre les mesures correctives nécessaires afin de rétablir des performances normales.

Les seuils de performance dynamiques ne sont pas activés sur les systèmes Cloud Volumes ONTAP, ONTAP Edge ou ONTAP Select.

Identifier les charges de travail victimes dans les événements de performance dynamiques dans Active IQ Unified Manager

Dans Unified Manager, vous pouvez identifier les workloads de volume qui présentent le plus grand écart de temps de réponse (latence) causé par un composant de stockage en contention. L'identification de ces workloads vous aide à comprendre pourquoi les applications clientes qui y accèdent fonctionnent plus lentement que d'habitude.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance dynamique nouveaux, reconnus ou obsolètes.

La page de détails de l'événement affiche une liste des workloads définis par l'utilisateur et par le système, classés selon l'écart le plus important d'activité ou d'utilisation sur le composant, ou les plus affectés par l'événement. Ces valeurs sont basées sur les pics que Unified Manager a identifiés lorsqu'il a détecté l'événement et l'a analysé pour la dernière fois.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Dans les graphiques Workload Latency et Workload Activity, sélectionnez **Victim Workloads**.
3. Passez votre curseur sur les graphiques pour afficher les principales charges de travail définies par l'utilisateur qui affectent le composant, ainsi que le nom de la workload victime.

Identifier les charges de travail excessives dans les événements de performance dynamiques dans Active IQ Unified Manager

Dans Unified Manager, vous pouvez identifier les workloads qui présentent le plus grand écart d'utilisation pour un composant de cluster en contention. L'identification de ces workloads vous aide à comprendre pourquoi certains volumes du cluster ont des temps de réponse longs (latence).

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance dynamique nouveaux, reconnus ou obsolètes.

La page Détails de l'événement affiche une liste des workloads définis par l'utilisateur et par le système, classés selon l'utilisation la plus élevée du composant ou selon ceux qui sont les plus affectés par l'événement. Ces valeurs sont basées sur les pics que Unified Manager a identifiés lorsqu'il a détecté l'événement et l'a analysé pour la dernière fois.

Étapes

1. Consultez la page de détails de l'événement pour obtenir des informations sur l'événement.
2. Dans les graphiques Latence du workload et Activité du workload, sélectionnez **Bully Workloads**.
3. Passez le curseur sur les graphiques pour afficher les principaux workloads perturbateurs définis par l'utilisateur qui affectent le composant.

Identifier les charges de travail shark lors d'un événement de performance dynamique dans Active IQ Unified Manager

Dans Unified Manager, vous pouvez identifier les charges de travail présentant le plus grand écart d'utilisation pour un composant de stockage en conflit. L'identification de ces charges de travail vous aide à déterminer s'il convient de les déplacer vers un cluster moins sollicité.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il existe des événements dynamiques de performance nouveaux, reconnus ou obsolètes.

La page Détails de l'événement affiche une liste des workloads définis par l'utilisateur et par le système, classés selon l'utilisation la plus élevée du composant ou selon ceux qui sont les plus affectés par l'événement. Ces valeurs sont basées sur les pics que Unified Manager a identifiés lorsqu'il a détecté l'événement et l'a analysé pour la dernière fois.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Dans les graphiques de latence du workload et d'activité du workload, sélectionnez **Shark Workloads**.
3. Passez votre curseur sur les graphiques pour afficher les principales workloads définies par l'utilisateur qui affectent le composant, ainsi que le nom de la workload shark.

Analyse des événements de performances pour une configuration MetroCluster

Analysez les événements de performance MetroCluster avec Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser un incident de performance lié à une configuration MetroCluster. Vous pouvez identifier les workloads impliqués dans l'incident et consulter les actions suggérées pour le résoudre.

MetroCluster Les incidents de performance peuvent être dus à des workloads *bully* qui surutilisent les liaisons intercommutateurs (ISL) entre les clusters, ou à des problèmes d'état des liaisons. Unified Manager surveille chaque cluster d'une configuration MetroCluster indépendamment, sans tenir compte des incidents de performance 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 d'Unified Manager. Vous pouvez aussi consulter les pages d'état d'Unified Manager pour vérifier l'état de chaque cluster et visualiser leur relation.

Analyser un événement de performance MetroCluster sur un cluster dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser le cluster dans une configuration MetroCluster où un événement de performance a été détecté. Vous pouvez identifier le nom du cluster, l'heure de détection de l'événement et les workloads *bully* et *victim* impliqués.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Une configuration MetroCluster doit comporter des événements de performance nouveaux, reconnus ou obsolètes.
- Les deux clusters de la configuration MetroCluster doivent être surveillés par la même instance d'Unified Manager.

Étapes

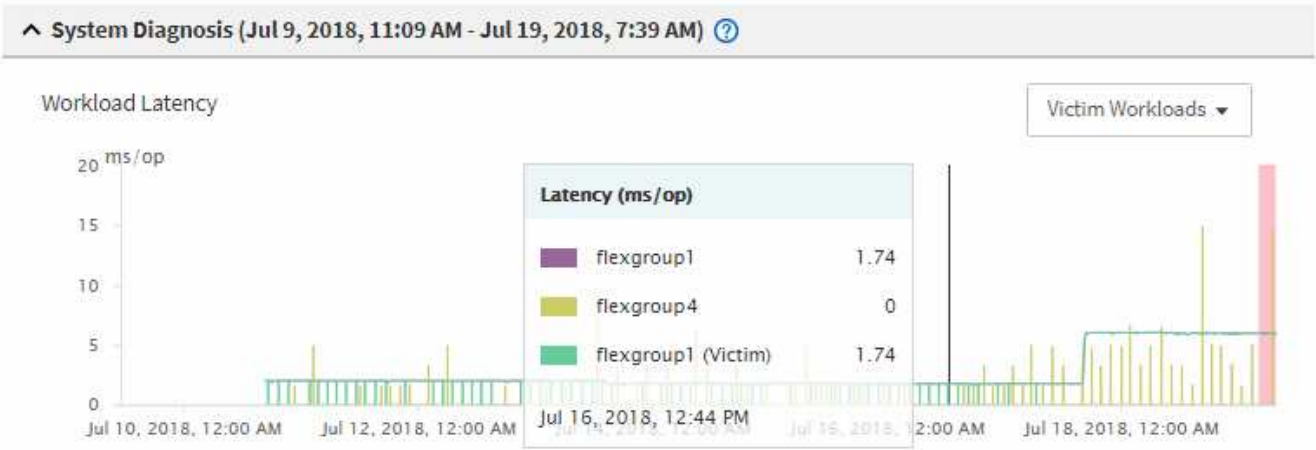
1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Consultez la description de l'événement pour voir les noms des workloads concernés et le nombre de workloads concernés.

   Dans cet exemple, l'icône Ressources MetroCluster est rouge, ce qui indique que les ressources MetroCluster sont en conflit. Vous placez votre curseur sur l'icône pour afficher une description de l'icône.



3. Notez le nom du cluster et l'heure de détection de l'événement, que vous pourrez utiliser pour analyser les événements de performance sur le cluster partenaire.
4. Dans les graphiques, examinez les workloads *victimes* pour confirmer que leurs temps de réponse sont supérieurs au seuil de performance.

   Dans cet exemple, le workload victime s'affiche dans le texte de survol. Les graphiques de latence présentent, à un niveau élevé, un profil de latence cohérent pour les workloads victimes concernés. Bien que la latence anormale des workloads victimes ait déclenché l'événement, un profil de latence cohérent peut indiquer que les workloads fonctionnent dans la plage attendue, 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 workloads de volume et que cette application leur envoie un volume important d'E/S, vous pourriez vous attendre à une augmentation de leur latence. Si la latence des workloads revient dans la plage attendue, que l'état de l'événement passe à « obsolète » et y reste pendant plus de 30 minutes, vous pouvez probablement ignorer l'événement. Si l'événement est toujours en cours et reste dans le nouvel état, vous pouvez approfondir l'analyse afin de déterminer si d'autres problèmes en sont la cause.

5. Dans le graphique de débit du workload, sélectionnez **Bully Workloads** pour afficher les workloads dominants.

   La présence de workloads perturbateurs indique que l'événement pourrait avoir été causé par un ou plusieurs workloads sur le cluster local qui surutilisent les ressources MetroCluster. Les workloads perturbateurs présentent un écart élevé dans le débit d'écriture (Mo/s).

   Ce graphique présente, de manière générale, le profil de débit d'écriture (Mo/s) des workloads. Vous pouvez analyser le profil en Mo/s d'écriture pour identifier un débit anormal, ce qui pourrait indiquer qu'un workload surutilise les ressources MetroCluster.

   Si aucune charge de travail excessive n'est impliquée dans l'événement, celui-ci peut être dû à un problème d'intégrité de la liaison entre les clusters ou à un problème de performance sur le cluster partenaire. Vous pouvez utiliser Unified Manager pour vérifier l'intégrité des deux clusters dans une configuration MetroCluster. Vous pouvez également utiliser Unified Manager pour rechercher et analyser les événements de performance sur le cluster partenaire.

Analysez un événement de performance MetroCluster sur un cluster distant dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser les événements de performance dyniques sur un cluster distant dans une configuration MetroCluster. Cette analyse vous aide à déterminer si un événement sur le cluster distant a provoqué un événement sur son cluster partenaire.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous devez avoir analysé un événement de performance sur un cluster local dans une configuration MetroCluster et obtenu l'heure de détection de l'événement.
- Vous devez avoir vérifié l'état de santé du cluster local et de son cluster partenaire impliqué dans l'événement de performance et avoir obtenu le nom du cluster partenaire.

Étapes

1. Connectez-vous à l'instance Unified Manager qui surveille le cluster partenaire.
2. Dans le volet de navigation de gauche, cliquez sur **Événements** pour afficher la liste des événements.
3. Dans le sélecteur **Plage horaire**, sélectionnez **Dernière heure**, puis cliquez sur **Appliquer la plage**.
4. Dans le sélecteur **Filtering**, sélectionnez **Cluster** dans le menu déroulant de gauche, saisissez le nom du cluster partenaire dans le champ de texte, puis cliquez sur **Apply Filter**.

   Si aucun événement n'a été enregistré pour le cluster sélectionné au cours de la dernière heure, cela indique que le cluster n'a rencontré aucun problème de performance pendant la période où l'événement a été détecté sur son partenaire.

5. Si le cluster sélectionné présente des événements détectés au cours de la dernière heure, comparez l'heure de détection de l'événement à celle de l'événement sur le cluster local.

   Si ces événements impliquent des workloads perturbateurs provoquant une contention sur le composant de traitement des données, un ou plusieurs de ces workloads perturbateurs peuvent avoir causé l'événement sur le cluster local. Vous pouvez cliquer sur l'événement pour l'analyser et consulter les actions suggérées pour le résoudre sur la page de détails de l'événement.

   Si ces événements n'impliquent pas de workloads perturbateurs, ils n'ont pas provoqué l'événement de performances sur le cluster local.

Répondez à un événement de limitation dynamique de la QoS dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser un incident de performance causé par la limitation du débit (Mo/s) des workloads par un groupe de stratégies de qualité de service (QoS). Cette limitation a augmenté les temps de réponse (latence) des workloads de volume du groupe de stratégies. Les informations relatives à cet événement vous permettront de déterminer si de nouvelles limites doivent être définies pour les groupes de stratégies afin de mettre fin à cette limitation.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Lisez la **Description**, qui affiche le nom des workloads affectés par la limitation.

   La description peut afficher le même workload pour la victime et l'agresseur, car la limitation de débit fait du workload une victime de lui-même.

3. Notez 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 de latence du workload et d'utilisation du workload, sélectionnez **Bully Workloads**.
5. Placez votre curseur sur les graphiques pour afficher les principaux workloads définis par l'utilisateur qui affectent le groupe de règles.

   La workload en tête de liste présente l'écart le plus important et a provoqué la limitation de débit. L'activité

correspond au pourcentage de la limite du groupe de stratégies utilisé par chaque workload.

6. Dans la zone **Actions suggérées**, cliquez sur le bouton **Analyser le workload** pour le workload principal.
7. Sur la page Workload Analysis, configurez le graphique Latency pour afficher tous les Cluster Components, et le graphique Throughput pour afficher Breakdown.

   Les graphiques de répartition s'affichent sous le graphique de latence et le graphique des IOPS.

8. Comparez les limites de QoS dans le graphique **Latence** pour voir quel niveau de bridage a eu un impact sur la latence au moment de l'événement.

   Le groupe de règles QoS a un débit maximal de 1 000 opérations par seconde (op/sec), que les workloads qu'il contient ne peuvent pas dépasser collectivement. Au moment de l'incident, les workloads du groupe de règles avaient un débit combiné de plus de 1 200 op/sec, ce qui a amené le groupe de règles à limiter son activité à 1 000 op/sec.

9. Comparez les valeurs de **latence de lecture/écriture** aux valeurs de **lecture/écriture/autres**.

   Les deux graphiques montrent un nombre élevé de requêtes de lecture avec une latence importante, tandis que le nombre de requêtes et la latence des requêtes d'écriture sont faibles. Ces valeurs vous aident à déterminer si c'est un débit élevé ou un grand nombre d'opérations qui a entraîné une augmentation de la latence. Vous pouvez utiliser ces valeurs pour décider d'appliquer une limite de groupe de règles au débit ou au nombre d'opérations.

10. Utilisez ONTAP System Manager pour augmenter la limite actuelle du groupe de stratégies à 1 300 op/sec.
11. Après un jour, retournez dans Unified Manager et saisissez le workload que vous avez enregistré à l'étape 3 dans la page **Analyse de la charge de travail**.
12. Sélectionnez le graphique de répartition du débit.

    Le graphique des lectures/écritures/autres s'affiche.

13. En haut de la page, pointez votre curseur sur l'icône d'événement de modification ( ) pour la modification de la limite du groupe de stratégies.
14. Comparez le graphique **Lectures/écritures/autres** au graphique **Latence**.

    Les requêtes de lecture et d'écriture sont identiques, mais la limitation de débit a cessé et la latence a diminué.

Répondez à un événement de performance causé par une défaillance de disques dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser un incident de performance causé par des workloads qui surutilisent un agrégat. Vous pouvez également utiliser Unified Manager pour vérifier l'état de l'agrégat afin de voir si des incidents d'état récents détectés sur l'agrégat ont contribué à l'incident de performance.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Lisez la **Description**, qui décrit les workloads impliqués dans l'événement et le composant du cluster en conflit.

   Plusieurs volumes victimes ont une latence affectée par le composant de cluster en conflit. L'agrégat, en cours de reconstruction RAID pour remplacer la défaillance de disque par un disque de secours, est le composant de cluster en conflit. Sous « Composant en conflit », l'icône de l'agrégat est surlignée en rouge et le nom de l'agrégat est affiché entre parenthèses.

3. Dans le graphique d'utilisation de la charge de travail, sélectionnez **Bully Workloads**.
4. Passez votre curseur sur le graphique pour afficher les principaux workloads perturbateurs qui affectent le composant.

   Les workloads ayant enregistré les pics d'utilisation les plus élevés depuis la détection de l'événement sont affichés en haut du graphique. L'un des workloads principaux est le workload défini par le système Disk Health, qui indique une reconstruction RAID. Une reconstruction est le processus interne impliqué dans la reconstruction de l'agrégat avec le disque de secours. Le workload Disk Health, ainsi que d'autres workloads sur l'agrégat, a probablement provoqué la contention sur l'agrégat et l'événement associé.

5. Après avoir confirmé que l'activité du workload Disk Health a provoqué l'événement, veuillez patienter environ 30 minutes afin que la reconstruction se termine et que Unified Manager analyse l'événement et détecte si l'agrégat est toujours en conflit.
6. Actualisez les **détails de l'événement**.

   Une fois la reconstruction RAID terminée, vérifiez que l'état est obsolète, ce qui indique que l'événement est résolu.

7. Dans le graphique d'utilisation des workloads, sélectionnez **Bully Workloads** pour afficher les workloads sur l'agrégat en fonction de l'utilisation maximale.
8. Dans la zone **Actions suggérées**, cliquez sur le bouton **Analyser le workload** pour le workload principal.
9. Dans la page **Workload Analysis**, définissez la plage de temps pour afficher les données des dernières 24 heures (1 jour) du volume sélectionné.

   Dans la chronologie des événements, un point rouge (🔴) indique le moment où l'événement de défaillance de disques s'est produit.

10. Dans le graphique d'utilisation des nœuds et des agrégats, masquez la ligne des statistiques des nœuds afin de ne conserver que la ligne des agrégats.
11. Comparez les données de ce graphique aux données au moment de l'événement dans le graphique **Latency**.

    Au moment de l'incident, l'utilisation de l'agrégat montrait une activité de lecture et d'écriture élevée, due aux processus de reconstruction RAID, ce qui a augmenté la latence du volume sélectionné. Quelques heures après l'incident, les lectures, les écritures et la latence avaient diminué, confirmant que l'agrégat n'était plus en contention.

Répondez à un événement de performance provoqué par une prise de contrôle HA dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour analyser un incident de performance dû à un traitement des données élevé sur un nœud de cluster appartenant à une paire haute disponibilité (HA). Vous pouvez également utiliser Unified Manager pour vérifier l'état de

santé des nœuds afin de déterminer si des incidents d'état de santé récents détectés sur les nœuds ont contribué à l'incident de performance.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Il doit y avoir des événements de performance nouveaux, reconnus ou obsolètes.

Étapes

1. Consultez la page **Détails de l'événement** pour obtenir des informations sur l'événement.
2. Lisez la **Description**, qui décrit les workloads impliqués dans l'événement et le composant du cluster en conflit.

   Il existe un volume victime dont la latence a été affectée par le composant du cluster en conflit. Le nœud Data Processing, qui a pris en charge tous les workloads de son nœud partenaire, est le composant du cluster en conflit. Sous « Composant en conflit », l'icône Data Processing est surlignée en rouge et le nom du nœud qui gérait le Data Processing au moment de l'événement est affiché entre parenthèses.

3. Dans la **Description**, cliquez sur le nom du volume.

   La page Explorateur des performances du volume s'affiche. En haut de la page, dans la chronologie des événements, une icône d'événement de modification ( ) indique l'heure à laquelle Unified Manager a détecté le début de la prise de contrôle HA.

4. Placez votre curseur sur l'icône de l'événement de changement pour la prise de contrôle HA, et les détails concernant cette prise de contrôle s'affichent dans le texte au survol.

   Dans le graphique de latence, un événement indique que le volume sélectionné a franchi le seuil de performance en raison d'une latence élevée à peu près au même moment que le basculement HA.

5. Cliquez sur **Zoom View** pour afficher le graphique de latence sur une nouvelle page.
6. Dans le menu Affichage, sélectionnez **Composants du cluster** pour afficher la latence totale par composant du cluster.
7. Pointez le curseur de votre souris sur l'icône d'événement de changement au début du basculement HA et comparez la latence du traitement des données à la latence totale.

   Au moment de la prise de contrôle HA, il y a eu une hausse du traitement des données due à l'augmentation de la demande de workload sur le nœud de traitement des données. L'augmentation du taux d'utilisation du processeur a accru la latence et déclenché l'incident.

8. Après avoir réparé le nœud défaillant, utilisez ONTAP System Manager pour effectuer un retour HA, qui déplace les workloads du nœud partenaire vers le nœud réparé.
9. Une fois le retour HA terminé, après la prochaine découverte de configuration dans Unified Manager (environ 15 minutes), recherchez l'événement et workload déclenchés par la prise de contrôle HA sur la page d'inventaire **Gestion des événements**.

   L'événement déclenché par la prise de contrôle HA a désormais l'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 que le volume sélectionné utilise désormais pour le traitement des données a résolu l'événement.

Résoudre les événements de performance

Résolvez les événements de performance dans Active IQ Unified Manager

Vous pouvez utiliser les actions suggérées pour tenter de résoudre vous-même les problèmes de performance. 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, d'ONTAP System Manager, de OnCommand Workflow Automation, des commandes ONTAP CLI, ou d'une combinaison de ces outils.

Vérifiez que la latence se situe dans la plage attendue dans Active IQ Unified Manager

Lorsqu'un composant du cluster est en conflit, les workloads de volume qui l'utilisent peuvent présenter un temps de réponse (latence) réduit. Vous pouvez examiner la latence de chaque workload victime sur le composant en conflit afin de confirmer que sa latence réelle se situe dans la plage attendue. Vous pouvez également cliquer sur le nom d'un volume pour afficher les données historiques du volume.

Si l'événement de performance est à l'état obsolète, la latence de chaque victime impliquée dans l'événement peut être revenue dans la plage attendue.

Évaluez comment les modifications de configuration affectent les performances de la charge de travail dans Active IQ Unified Manager

Les modifications de configuration sur le cluster, telles qu'une défaillance de disque, un basculement HA ou un déplacement de volume, peuvent avoir un impact négatif sur les performances du volume et entraîner une augmentation de la latence.

Dans Unified Manager, vous pouvez consulter la page d'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 le workload du volume sélectionné.

Les pages de performance d'Unified Manager ne détectent qu'un nombre limité d'événements de modification. Les pages d'état fournissent des alertes pour les autres événements liés aux modifications de configuration. Vous pouvez rechercher le volume dans Unified Manager pour consulter l'historique des événements.

Améliorez les performances de la charge de travail en ajustant les paramètres côté client dans Active IQ Unified Manager

Vous pouvez vérifier les workloads de vos clients, comme les applications ou les bases de données, qui envoient des E/S vers des volumes impliqués dans un événement de performances afin de déterminer si une modification côté client pourrait corriger l'événement.

Lorsque les clients connectés aux volumes d'un cluster augmentent leurs requêtes d'E/S, le cluster doit fournir un effort accru pour répondre à la demande. Si vous identifiez les clients qui génèrent un grand nombre de

requêtes d'E/S vers un volume particulier du cluster, vous pouvez améliorer les performances de ce dernier en ajustant le nombre de clients accédant à ce volume ou en réduisant le volume d'E/S qui lui est adressé. Vous pouvez également appliquer ou augmenter une limite au groupe de règles QoS auquel le volume appartient.

Vous pouvez examiner les clients et leurs applications pour déterminer si les clients envoient plus d'E/S que d'habitude, ce qui pourrait provoquer une contention sur un composant du cluster. Sur la page Détails de l'événement, la section Diagnostic système affiche les principaux workloads de volume utilisant le composant en contention. Si vous savez quel client accède à un volume particulier, vous pouvez consulter le client pour déterminer si le matériel client ou une application ne fonctionne pas comme prévu ou effectue plus de travail que d'habitude.

Dans une configuration MetroCluster, les requêtes d'écriture vers un volume sur un cluster local sont répliquées vers un volume sur le cluster distant. Le maintien de la synchronisation du volume source sur le cluster local avec le volume de destination sur le cluster distant peut également accroître la charge sur les deux clusters dans la configuration MetroCluster. En réduisant les requêtes d'écriture vers ces volumes répliqués, les clusters peuvent effectuer moins d'opérations de synchronisation, ce qui réduit l'impact sur les performances des autres workloads.

Comprendre comment les problèmes liés aux clients ou au réseau affectent les performances d'Active IQ Unified Manager

Lorsque les clients connectés aux volumes d'un cluster augmentent leurs requêtes d'E/S, le cluster doit fournir davantage d'efforts pour répondre à la demande. L'augmentation de la demande sur le cluster peut entraîner une contention au niveau d'un composant, accroître la latence des workloads qui l'utilisent et déclencher un événement dans Unified Manager.

Sur la page Détails de l'événement, la section Diagnostic système affiche les principaux workloads de volume utilisant le composant en contention. Si vous savez quel client accède à un volume particulier, vous pouvez accéder au client pour déterminer si le matériel du client ou une application ne fonctionne pas comme prévu, ou effectue plus de travail que d'habitude. Il se peut que vous deviez contacter l'administrateur du client ou le fournisseur de l'application pour obtenir de l'aide.

Vous pouvez vérifier votre infrastructure réseau afin de déterminer s'il existe des problèmes matériels, des goulots d'étranglement ou des workloads concurrents susceptibles d'avoir ralenti les requêtes d'E/S entre le cluster et les clients connectés. Il se peut que vous deviez contacter votre administrateur réseau pour obtenir de l'aide.

Analysez les volumes à forte activité au sein d'un groupe de politiques QoS dans Active IQ Unified Manager

Vous pouvez examiner les workloads du groupe de règles de qualité de service (QoS) présentant la plus forte variation d'activité afin de déterminer si plusieurs workloads sont à l'origine de l'événement. Vous pouvez également vérifier si d'autres workloads dépassent toujours la limite de débit définie ou s'ils sont revenus dans leur plage d'activité attendue.

Sur la page Détails de l'événement, dans la section Diagnostic système, vous pouvez trier les workloads par écart maximal d'activité afin d'afficher en haut du tableau les workloads présentant la plus forte variation d'activité. Ces workloads peuvent être les « bullies », dont l'activité a dépassé la limite définie et qui peuvent avoir provoqué l'événement.

Vous pouvez accéder à la page d'analyse du workload pour chaque volume afin d'examiner son activité IOPS. Si le workload présente des périodes d'activité des opérations très élevée, il a peut-être contribué à l'événement. Vous pouvez modifier les paramètres du groupe de stratégies du workload ou déplacer le workload vers un autre groupe de stratégies.

Vous pouvez utiliser ONTAP System Manager ou les commandes de l'interface de ligne de commande ONTAP pour gérer les groupes de règles, comme suit :

- Créer un groupe de politiques.
- Ajouter ou supprimer des charges de travail dans un groupe de stratégies.
- Déplacer un workload entre des groupes de règles.
- Modifier la limite de débit d'un groupe de stratégies.

Déplacez les LIF pour améliorer les performances dans Active IQ Unified Manager

Déplacer les interfaces logiques (LIF) vers un port moins occupé peut contribuer à améliorer l'équilibrage de charge, faciliter les opérations de maintenance et l'optimisation des performances, et réduire l'accès indirect.

L'accès indirect peut réduire l'efficacité du système. Ce phénomène se produit lorsqu'un workload de volume utilise différents nœuds pour le traitement réseau et le traitement des données. Pour réduire l'accès indirect, vous pouvez réorganiser les LIF, ce qui implique de déplacer les LIF afin qu'elles utilisent le même nœud pour le traitement réseau et le traitement des données. Vous pouvez configurer l'équilibrage de charge pour qu'ONTAP déplace automatiquement les LIF occupées vers un autre port, ou vous pouvez déplacer une LIF manuellement.

Avantages	Considérations
• Améliorer la répartition de charge. • Réduisez l'accès indirect.	Lors du déplacement d'une interface logique (LIF) connectée à des partages CIFS, les clients accédant aux partages CIFS sont déconnectés. Toute requête de lecture ou d'écriture sur les partages CIFS est interrompue.

Vous utilisez les commandes ONTAP pour configurer l'équilibrage de charge. Pour plus d'informations, consultez la documentation réseau ONTAP.

Vous utilisez ONTAP System Manager et les commandes ONTAP CLI pour déplacer manuellement les LIF.

Effectuez les opérations d'efficacité du stockage aux heures creuses

Planifiez les opérations d'efficacité du stockage pendant les périodes de moindre activité dans Active IQ Unified Manager

Vous pouvez modifier la stratégie ou la planification qui gère les opérations d'efficacité du stockage afin qu'elles s'exécutent lorsque les workloads des volumes concernés sont moins sollicités.

Les opérations d'efficacité du stockage peuvent consommer une quantité importante de ressources CPU du cluster et impacter négativement les volumes sur lesquels elles sont exécutées. Si ces volumes sont fortement

sollicités simultanément à ces opérations, leur latence peut augmenter et déclencher un événement.

Sur la page Détails de l'événement, la section Diagnostic système affiche les workloads du groupe de règles QoS en fonction du pic d'écart d'activité afin d'identifier les workloads perturbateurs. Si « `storage efficiency` » s'affiche en haut du tableau, ces opérations perturbent les workloads victimes. En modifiant la règle d'efficacité ou la planification afin qu'elles s'exécutent lorsque ces workloads sont moins occupés, vous pouvez empêcher les opérations d'efficacité du stockage de provoquer une contention sur un cluster.

Vous pouvez utiliser ONTAP System Manager pour gérer les règles d'efficacité. Vous pouvez utiliser les commandes ONTAP pour gérer les règles d'efficacité et les planifications.

Comprendre l'efficacité du stockage dans Active IQ Unified Manager

L'efficacité du stockage vous permet de stocker un maximum de données au moindre coût et de prendre en charge une croissance rapide du volume des données tout en consommant moins d'espace. NetApp strategy for storage efficiency repose sur les fondements intégrés de la virtualisation du stockage et du stockage unifié fournis par son système d'exploitation ONTAP principal et le système de fichiers Write Anywhere File Layout (WAFL).

L'efficacité du stockage inclut l'utilisation de technologies telles que le provisionnement fin, la copie Snapshot, la déduplication, la compression des données, FlexClone, la réplication fine avec SnapVault et volume SnapMirror, RAID-DP, Flash Cache, l'agrégat Flash Pool et les agrégats compatibles FabricPool, qui contribuent à augmenter l'utilisation du stockage et à diminuer les coûts de stockage.

L'architecture de stockage unifiée vous permet de consolider efficacement un réseau de stockage (SAN), un stockage en réseau (NAS) et un stockage secondaire sur une seule plateforme.

Les disques durs haute densité, tels que les disques SATA (Serial Advanced Technology Attachment) configurés au sein d'un agrégat Flash Pool ou avec la technologie Flash Cache et RAID-DP, augmentent l'efficacité sans affecter les performances et la résilience.

Un agrégat compatible FabricPool comprend un agrégat entièrement SSD ou un agrégat HDD (à partir de ONTAP 9.8) comme niveau de performance local et un stockage objet que vous spécifiez comme niveau cloud. La configuration de FabricPool vous permet de gérer le niveau de stockage (niveau local ou niveau cloud) sur lequel les données doivent être stockées en fonction de leur fréquence d'accès.

Des technologies telles que le provisionnement fin, la copie Snapshot, la déduplication, la compression des données, la réplication fine avec SnapVault et SnapMirror de volume, ainsi que FlexClone®, offrent de meilleures économies. Vous pouvez utiliser ces technologies individuellement ou ensemble pour atteindre une efficacité de stockage maximale.

Comprendre comment l'ajout de disques affecte la réallocation des données dans Active IQ Unified Manager

Vous pouvez ajouter des disques à un agrégat pour augmenter sa capacité de stockage et ses performances. Après l'ajout des disques, l'amélioration des performances en lecture ne sera visible qu'après la réallocation des données entre les disques ajoutés.

Vous pouvez utiliser ces instructions lorsque Unified Manager a reçu des événements d'agrégat déclenchés par des seuils dynamiques ou par des seuils de performance définis par le système :

- Lorsque vous recevez un événement de seuil dynamique, sur la page de détails de l'événement, l'icône du composant de cluster qui représente l'agrégat en conflit est mise en évidence en rouge.

  Sous l'icône, entre parenthèses, figure 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 indique le nom de l'agrégat qui rencontre le problème.

  Vous pouvez ajouter des disques et réallouer des données sur cet agrégat.

Les disques que vous ajoutez à l'agrégat doivent déjà être présents dans le cluster. Si le cluster ne dispose pas de disques supplémentaires, vous devrez peut-être contacter votre administrateur ou acheter davantage de disques. Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour ajouter des disques à un agrégat.

Vous devez réallouer les données uniquement lorsque vous utilisez des agrégats HDD et Flash Pool. Ne réallouez pas les données sur des agrégats SSD ou FabricPool.

Améliorez les performances des charges de travail en activant Flash Cache sur un nœud dans Active IQ Unified Manager

Vous pouvez améliorer les performances du workload en activant la mise en cache intelligente des données Flash Cache™ sur chaque nœud du cluster.

Un module Flash Cache, ou module de mémoire PCIe Performance Acceleration Module, optimise les performances des workloads à forte intensité de lectures aléatoires en fonctionnant comme un cache de lecture externe intelligent. Ce matériel fonctionne de concert avec le composant logiciel WAFL External Cache d'ONTAP.

Dans Unified Manager, sur la page Détails de l'événement, l'icône du composant de cluster représentant l'agrégat en conflit est surlignée en rouge. Sous l'icône, entre parenthèses, figure le nom de l'agrégat, qui permet de l'identifier. Vous pouvez activer Flash Cache sur le nœud hébergeant l'agrégat.

Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour vérifier si Flash Cache est installé ou activé, et pour l'activer si ce n'est pas déjà le cas. La commande suivante indique si Flash Cache est activé sur un nœud spécifique `cluster::> run local options flexscale.enable` :

Pour plus d'informations sur Flash Cache et les exigences relatives à son utilisation, veuillez consulter le rapport technique suivant :

"Rapport technique 3832 : guide des bonnes pratiques de Flash Cache"

Améliorez les performances des charges de travail en activant Flash Pool sur un agrégat de stockage dans Active IQ Unified Manager

Vous pouvez améliorer les performances du workload en activant la fonctionnalité Flash Pool sur un agrégat. Un Flash Pool est un agrégat qui intègre à la fois des HDD et des SSD. Les HDD servent au stockage principal, tandis que les SSD fournissent un cache de lecture et d'écriture haute performance afin d'améliorer les performances de l'agrégat.

Dans Unified Manager, la page Détails de l'événement affiche le nom de l'agrégat en conflit. Vous pouvez

utiliser ONTAP System Manager ou les commandes ONTAP pour voir si Flash Pool est activé pour un agrégat. Si vous avez des SSD installés, vous pouvez l'activer à l'aide de l'interface de ligne de commande. Si vous avez des SSD installés, vous pouvez exécuter la commande suivante sur l'agrégat pour voir si Flash Pool est activé : **`cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`**

Dans cette commande, *`aggr_name`* correspond au nom de l'agrégat, tel que l'agrégat en contention.

Pour plus d'informations sur Flash Pool et les exigences relatives à son utilisation, consultez le *Clustered Data ONTAP Physical Storage Management Guide*.

Vérifiez l'état de la configuration MetroCluster dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour examiner l'état des clusters dans une configuration MetroCluster sur IP ou FC. L'état et les événements associés vous aident à déterminer si des problèmes matériels ou logiciels peuvent affecter les performances de vos workloads.

Si vous configurez Unified Manager pour envoyer des alertes par e-mail, vous pouvez consulter votre messagerie pour détecter tout problème d'intégrité sur le cluster local ou distant susceptible d'avoir contribué à un incident de performance. Dans l'interface graphique d'Unified Manager, vous pouvez sélectionner **Gestion des événements** pour afficher la liste des événements en cours, puis utiliser les filtres pour n'afficher que les événements de configuration MetroCluster.

Pour plus d'informations, voir "Vérification de l'état des clusters dans une configuration MetroCluster"

Vérifiez les configurations MetroCluster dans Active IQ Unified Manager

Vous pouvez éviter les problèmes de performance des workloads mis en miroir dans une configuration MetroCluster sur FC et IP en vous assurant que la configuration MetroCluster est correctement configurée. Vous pouvez également améliorer les performances des workloads en modifiant la configuration ou en mettant à niveau les composants logiciels ou matériels.

Consultez "Documentation MetroCluster" pour obtenir des instructions sur la configuration des clusters dans la configuration MetroCluster, y compris les commutateurs Fibre Channel (FC), les câbles et les liaisons inter-commutateurs (ISL). Cela vous aide également à configurer le logiciel MetroCluster afin que les clusters locaux et distants puissent communiquer avec les données de volume miroir. Pour obtenir des informations spécifiques à votre configuration MetroCluster over IP, consultez "Installer une configuration IP MetroCluster".

Vous pouvez comparer votre configuration MetroCluster aux exigences dans "Documentation MetroCluster" afin de déterminer si la modification ou la mise à niveau de composants de votre configuration MetroCluster pourrait améliorer les performances du workload. Cette comparaison peut vous aider à répondre aux questions suivantes :

- Ces contrôleurs sont-ils adaptés à vos workloads ?
- Avez-vous besoin de mettre à niveau vos bundles ISL vers une bande passante plus élevée pour gérer un débit plus important ?
- Pouvez-vous ajuster les crédits de tampon à tampon (BBC) sur vos commutateurs pour augmenter la bande passante?
- Si vos workloads présentent un débit d'écriture élevé vers un stockage SSD, devez-vous mettre à niveau vos ponts FC-SAS pour prendre en charge ce débit ?

Informations connexes

- Pour plus d'informations sur le remplacement ou la mise à niveau des composants MetroCluster, consultez le "Documentation MetroCluster".
- Pour plus d'informations sur la mise à niveau des contrôleurs, consultez "Mise à niveau des contrôleurs dans une configuration FC MetroCluster à l'aide du basculement et du rétablissement" et "Mise à niveau des contrôleurs dans une configuration IP MetroCluster à l'aide du basculement et du rétablissement"

Déplacez les charges de travail vers un autre agrégat dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour identifier un agrégat moins sollicité que l'agrégat où résident actuellement vos workloads, puis déplacer les volumes ou LUN sélectionnés vers cet agrégat. Le déplacement de workloads hautes performances vers un agrégat moins sollicité, ou vers un agrégat avec stockage Flash activé, permet au workload de fonctionner plus efficacement.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous devez avoir noté le nom de l'agrégat qui rencontre actuellement un problème de performance.
- Vous devez avoir enregistré la date et l'heure auxquelles l'agrégat a reçu l'événement.
- Unified Manager doit avoir collecté et analysé au moins un mois de données de performance.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les charges de travail les plus performantes vers un agrégat moins utilisé :

- Les agrégats du même cluster qui sont moins utilisés
- Les volumes les plus performants sur l'agrégat actuel

Étapes

1. Identifiez l'agrégat du cluster qui est le moins utilisé :
   a. Sur la page de détails de l'**événement**, cliquez sur le nom du cluster sur lequel se trouve l'agrégat.

      Les détails du cluster sont affichés sur la page de destination Performance/Cluster.

   b. Sur la page **Résumé**, cliquez sur **Aggregates** dans le volet **Managed Objects**.

      La liste des agrégats de ce cluster est affichée.

   c. Cliquez sur la colonne **Utilisation** pour trier les agrégats du moins utilisé au plus utilisé.

      Vous pouvez également identifier les agrégats présentant la plus grande **capacité libre**. Ceci fournit une liste d'agrégats potentiels vers lesquels vous pourriez déplacer des workloads.

   d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les workloads.
2. Identifiez les volumes les plus performants parmi l'agrégat ayant reçu l'événement :
   a. Cliquez sur l'agrégat qui présente le problème de performance.

      Les détails de l'agrégat sont affichés sur la page Performance/Explorateur d'agrégats.

b. Dans le sélecteur **Plage de temps**, sélectionnez **30 derniers jours**, puis cliquez sur **Appliquer la plage**.

   Cela vous permet de consulter un historique des performances sur une période plus longue que les 72 heures par défaut. Vous souhaitez déplacer un volume qui utilise beaucoup de ressources de manière constante, et pas seulement au cours des 72 dernières heures.

c. Dans **Afficher et comparer**, sélectionnez **Volumes sur cet agrégat**.

   Une liste des volumes FlexVol et des volumes constitutifs FlexGroup de cet agrégat est affichée.

d. Triez les volumes par débit en Mo/s le plus élevé, puis par nombre d'IOPS le plus élevé, afin de visualiser les volumes les plus performants.

e. Notez les noms des volumes que vous souhaitez déplacer vers un autre agrégat.

3. Déplacez les volumes les plus performants vers l'agrégat que vous avez identifié comme ayant une faible utilisation.

   Vous pouvez effectuer l'opération de déplacement à l'aide de ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacez les charges de travail vers un autre nœud dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour identifier un agrégat sur un autre nœud moins sollicité que le nœud sur lequel vos workloads s'exécutent actuellement, puis déplacer les volumes sélectionnés vers cet agrégat. Le déplacement des workloads les plus performants vers un agrégat sur un nœud moins sollicité permet aux workloads sur les deux nœuds de s'exécuter plus efficacement.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous avez dû noter le nom du nœud qui rencontre actuellement un problème de performance.
- Vous devez avoir enregistré la date et l'heure auxquelles le nœud a reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé des données de performance pendant un mois ou plus.

Cette procédure vous aide à identifier les ressources suivantes afin que vous puissiez déplacer les workloads à hautes performances vers un nœud moins utilisé :

- Les nœuds du même cluster qui disposent de la plus grande capacité de performance disponible
- Les agrégats du nouveau nœud qui disposent de la plus grande capacité de performances disponible
- Les volumes les plus performants sur le nœud actuel

Étapes

1. Identifiez un nœud du cluster qui dispose de la plus grande capacité de performances disponible :

   a. Sur la page **Détails de l'événement**, cliquez sur le nom du cluster sur lequel se trouve le nœud.

      Les détails du cluster sont affichés sur la page de destination Performance/Cluster.

b. Dans l'onglet **Résumé**, cliquez sur **Nœuds** dans le volet **Objets gérés**.

   La liste des nœuds de ce cluster est affichée.

c. Cliquez sur la colonne **Capacité de performance utilisée** pour trier les nœuds par pourcentage d'utilisation le plus faible.

   Ceci fournit une liste de nœuds potentiels vers lesquels vous pourriez déplacer des workloads.

d. Notez le nom du nœud vers lequel vous souhaitez déplacer les workloads.

2. Identifiez sur le nouveau nœud l'agrégat le moins utilisé :

   a. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats** et sélectionnez **Performances** > **Tous les agrégats** dans le menu Affichage.

      La vue « Performances : Tous les agrégats » s'affiche.

   b. Cliquez sur **Filtrage**, sélectionnez **Nœud** dans le menu déroulant de gauche, saisissez le nom du nœud dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

      La vue « Performances : Tous les agrégats » s'affiche à nouveau avec la liste des agrégats disponibles sur ce nœud.

   c. Cliquez sur la colonne **Capacité de performance utilisée** pour trier les agrégats du moins utilisé au plus utilisé.

      Cela fournit une liste des agrégats potentiels vers lesquels vous pourriez déplacer des workloads.

   d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les workloads.

3. Identifiez les workloads les plus performants du nœud qui a reçu l'événement :

   a. Revenez à la page **Détails de l'événement** pour cet événement.

   b. Dans le champ **Volumes concernés**, cliquez sur le lien correspondant au nombre de volumes.

      La vue « Performances : Tous les volumes » affiche une liste filtrée des volumes présents sur ce nœud.

   c. Cliquez sur la colonne **Capacité totale** pour trier les volumes selon l'espace alloué le plus important.

      Ceci fournit une liste des volumes potentiels que vous souhaiterez peut-être déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que les noms des agrégats actuels sur lesquels ils se trouvent.

4. Déplacez les volumes vers les agrégats que vous avez identifiés comme disposant de la plus grande capacité de performances disponible sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement à l'aide de ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vous pourrez vérifier si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacez les charges de travail vers un agrégat sur un autre nœud dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour identifier un agrégat sur un autre nœud moins sollicité que le nœud sur lequel vos workloads s'exécutent actuellement, puis déplacer les volumes sélectionnés vers cet agrégat. Le déplacement de workloads hautement performants vers un agrégat sur un nœud moins sollicité permet aux workloads sur les deux nœuds de fonctionner plus efficacement.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous avez dû noter le nom du nœud qui rencontre actuellement un problème de performance.
- Vous devez avoir enregistré la date et l'heure auxquelles le nœud a reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé au moins un mois de données de performance.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les workloads les plus performants vers un nœud moins utilisé :

- Les nœuds du même cluster qui sont moins utilisés
- Les agrégats sur le nouveau nœud qui sont les moins utilisés
- Les volumes les plus performants sur le nœud actuel

Étapes

1. Identifiez le nœud du cluster qui est le moins utilisé :
   a. Sur la page de détails de l'**événement**, cliquez sur le nom du cluster sur lequel se trouve le nœud.

      Les détails du cluster sont affichés sur la page de destination Performance/Cluster.

   b. Sur la page **Résumé**, cliquez sur **Nœuds** dans le volet **Objets gérés**.

      La liste des nœuds de ce cluster est affichée.

   c. Cliquez sur la colonne **Utilisation** pour trier les nœuds du moins utilisé au plus utilisé.

      Vous pouvez également identifier les nœuds disposant de la plus grande **capacité libre**. Cela vous fournit une liste de nœuds potentiels vers lesquels vous pourriez déplacer des workloads.

   d. Notez le nom du nœud vers lequel vous souhaitez déplacer les workloads.
2. Identifiez sur le nouveau nœud l'agrégat le moins utilisé :
   a. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats** et sélectionnez **Performances** > **Tous les agrégats** dans le menu Affichage.

      La vue « Performances : Tous les agrégats » s'affiche.

   b. Cliquez sur **Filtrage**, sélectionnez **Nœud** dans le menu déroulant de gauche, saisissez le nom du nœud dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

      La vue « Performances : Tous les agrégats » s'affiche à nouveau avec la liste des agrégats disponibles sur ce nœud.

c. Cliquez sur la colonne **Utilisation** pour trier les agrégats du moins utilisé au plus utilisé.

   Vous pouvez également identifier les agrégats présentant la plus grande **capacité libre**. Ceci fournit une liste d'agrégats potentiels vers lesquels vous pourriez déplacer des workloads.

d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les workloads.

3. Identifiez les workloads les plus performants du nœud qui a reçu l'événement :
   a. Retournez à la page des détails de l'**Event** pour l'événement.
   b. Dans le champ **Volumes concernés**, cliquez sur le lien correspondant au nombre de volumes.

      La vue « Performances : Tous les volumes » affiche une liste filtrée des volumes présents sur ce nœud.

   c. Cliquez sur la colonne **Capacité totale** pour trier les volumes selon l'espace alloué le plus important.

      Ceci fournit une liste des volumes potentiels que vous souhaiterez peut-être déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que les noms des agrégats actuels sur lesquels ils se trouvent.
4. Déplacez les volumes vers les agrégats que vous avez identifiés comme ayant une faible utilisation sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement à l'aide de ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacez les charges de travail vers un nœud d'une autre paire haute disponibilité dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour identifier un agrégat sur un nœud d'une autre paire haute disponibilité (HA) disposant de plus de capacité de performance disponible que la paire haute disponibilité sur laquelle vos workloads s'exécutent actuellement. Vous pouvez ensuite déplacer les volumes sélectionnés vers des agrégats de la nouvelle paire haute disponibilité.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Votre cluster doit comporter au minimum deux paires haute disponibilité

  Vous ne pouvez pas utiliser cette procédure de correction si votre cluster ne comporte qu'une seule paire haute disponibilité.

- Vous devez avoir noté 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 auxquelles les nœuds ont reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé des données de performance pendant un mois ou plus.

Le déplacement de workloads à hautes performances vers un agrégat sur un nœud disposant d'une plus grande capacité de performance disponible permet aux workloads des deux nœuds de fonctionner plus

efficacement. Cette procédure vous aide à identifier les ressources suivantes afin que vous puissiez déplacer des workloads à hautes performances vers un nœud disposant d'une plus grande capacité de performance disponible sur une autre paire haute disponibilité :

- Les nœuds d'une autre paire haute disponibilité sur le même cluster qui disposent de la plus grande capacité de performance disponible
- Les agrégats sur les nouveaux nœuds qui ont la plus grande capacité de performances disponible
- Les volumes les plus performants sur les nœuds actuels

Étapes

1. Identifiez les nœuds qui font partie d'une paire haute disponibilité différente 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 sont affichés sur la page de destination Performance/Cluster.

   b. Sur la page **Résumé**, cliquez sur **Nœuds** dans le volet **Objets gérés**.

      La liste des nœuds de ce cluster est affichée dans la vue Performances : Tous les nœuds.

   c. Notez les noms des nœuds qui appartiennent à des paires haute disponibilité différentes de la paire haute disponibilité qui rencontre actuellement un problème de performance.
2. Identifiez, dans la nouvelle paire haute disponibilité, le nœud qui dispose de la plus grande capacité de performances disponible :
   a. Dans la vue **Performances : Tous les nœuds**, cliquez sur la colonne **Capacité de performance utilisée** pour trier les nœuds par pourcentage d'utilisation le plus faible.

      Ceci fournit une liste de nœuds potentiels vers lesquels vous pourriez déplacer des workloads.

   b. Notez le nom du nœud sur une autre paire haute disponibilité vers lequel vous souhaitez déplacer les workloads.
3. Identifiez un agrégat sur le nouveau nœud qui dispose de la plus grande capacité de performances disponible :
   a. Dans la vue **Performances : Tous les nœuds**, cliquez sur le nœud.

      Les détails du nœud sont affichés dans la page Performance/Node Explorer.

   b. Dans le menu **Affichage et comparaison**, sélectionnez **Agrégats sur ce nœud**.

      Les agrégats de ce nœud sont affichés dans la grille.

   c. Cliquez sur la colonne **Capacité de performance utilisée** pour trier les agrégats du moins utilisé au plus utilisé.

      Cela fournit une liste des agrégats potentiels vers lesquels vous pourriez déplacer des workloads.

   d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les workloads.
4. Identifiez les workloads les plus performants parmi les nœuds ayant reçu l'événement :
   a. Retournez à la page des détails de l'**Event** pour l'événement.
   b. Dans le champ **Volumes affectés**, cliquez sur le lien correspondant au nombre de volumes pour le premier nœud.

La vue « Performances : Tous les volumes » affiche une liste filtrée des volumes présents sur ce nœud.

c. Cliquez sur la colonne **Capacité totale** pour trier les volumes selon l'espace alloué le plus important.

Cela fournit une liste des volumes potentiels que vous souhaiterez peut-être déplacer.

d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que les noms des agrégats actuels sur lesquels ils se trouvent.

e. Effectuez les étapes 4c et 4d pour le deuxième nœud qui faisait partie de cet événement afin d'identifier les volumes possibles que vous souhaitez également déplacer à partir de ce nœud.

5. Déplacez les volumes vers les agrégats que vous avez identifiés comme disposant de la plus grande capacité de performances disponible sur le nouveau nœud.

Vous pouvez effectuer l'opération de déplacement à l'aide de ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vous pourrez vérifier si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Déplacez les charges de travail vers un autre nœud d'une paire haute disponibilité dans Active IQ Unified Manager

Vous pouvez utiliser Unified Manager pour identifier un agrégat sur un nœud d'une autre paire haute disponibilité moins sollicité que la paire haute disponibilité sur laquelle vos workloads s'exécutent actuellement. Vous pouvez ensuite déplacer les volumes sélectionnés vers des agrégats de cette nouvelle paire haute disponibilité. Le déplacement de workloads très performants vers un agrégat sur un nœud moins sollicité permet aux workloads sur les deux nœuds de fonctionner plus efficacement.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Votre cluster doit comporter au minimum deux paires haute disponibilité ; vous ne pouvez pas utiliser cette procédure de correction si votre cluster ne comporte qu'une seule paire haute disponibilité.
- Vous devez avoir noté les noms des deux nœuds de la paire haute disponibilité qui rencontrent actuellement le problème de performance.
- Vous devez avoir enregistré la date et l'heure auxquelles les nœuds ont reçu l'événement de performance.
- Unified Manager doit avoir collecté et analysé au moins un mois de données de performance.

Ces étapes vous aident à identifier les ressources suivantes afin que vous puissiez déplacer les workloads hautes performances vers un nœud moins utilisé sur une autre paire haute disponibilité :

- Les nœuds d'une autre paire haute disponibilité sur le même cluster qui sont moins utilisés
- Les agrégats des nouveaux nœuds qui sont les moins utilisés
- Les volumes les plus performants sur les nœuds actuels

Étapes

1. Identifiez les nœuds qui font partie d'une paire haute disponibilité différente sur le même cluster :

a. Dans le volet de navigation de gauche, cliquez sur **Storage** > **Clusters** et sélectionnez **Performance** > **All Clusters** dans le menu **View**.

   La vue « Performances : Tous les clusters » s'affiche.

b. Cliquez sur le nombre dans le champ **Nombre de nœuds** pour le cluster actuel.

   La vue « Performances : Tous les nœuds » s'affiche.

c. Notez les noms des nœuds qui appartiennent à des paires haute disponibilité différentes de la paire haute disponibilité qui présente actuellement le problème de performance.

2. Identifiez un nœud de la nouvelle paire haute disponibilité qui est le moins utilisé :

   a. Cliquez sur la colonne **Utilisation** pour trier les nœuds du moins utilisé au plus utilisé.

      Vous pouvez également identifier les nœuds disposant de la plus grande **capacité libre**. Cela vous fournit une liste de nœuds potentiels vers lesquels vous pourriez déplacer des workloads.

   b. Notez le nom du nœud vers lequel vous souhaitez déplacer les workloads.

3. Identifiez sur le nouveau nœud l'agrégat le moins utilisé :

   a. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats** et sélectionnez **Performances** > **Tous les agrégats** dans le menu Affichage.

      La vue « Performances : Tous les agrégats » s'affiche.

   b. Cliquez sur **Filtrage**, sélectionnez **Nœud** dans le menu déroulant de gauche, saisissez le nom du nœud dans le champ de texte, puis cliquez sur **Appliquer le filtre**.

      La vue « Performances : Tous les agrégats » s'affiche à nouveau avec la liste des agrégats disponibles sur ce nœud.

   c. Cliquez sur la colonne **Utilisation** pour trier les agrégats du moins utilisé au plus utilisé.

      Vous pouvez également identifier les agrégats présentant la plus grande **capacité libre**. Ceci fournit une liste d'agrégats potentiels vers lesquels vous pourriez déplacer des workloads.

   d. Notez le nom de l'agrégat vers lequel vous souhaitez déplacer les workloads.

4. Identifiez les workloads les plus performants parmi les nœuds ayant reçu l'événement :

   a. Retournez à la page des détails de l'**Event** pour l'événement.

   b. Dans le champ **Volumes affectés**, cliquez sur le lien correspondant au nombre de volumes pour le premier nœud.

      La vue « Performances : Tous les volumes » affiche une liste filtrée des volumes présents sur ce nœud.

   c. Cliquez sur la colonne **Capacité totale** pour trier les volumes selon l'espace alloué le plus important.

      Cela fournit une liste des volumes potentiels que vous souhaiterez peut-être déplacer.

   d. Notez les noms des volumes que vous souhaitez déplacer, ainsi que les noms des agrégats actuels sur lesquels ils se trouvent.

   e. Effectuez les étapes 4c et 4d pour le deuxième nœud qui faisait partie de cet événement afin d'identifier les volumes possibles que vous souhaitez également déplacer à partir de ce nœud.

5. Déplacez les volumes vers les agrégats que vous avez identifiés comme ayant une faible utilisation sur le nouveau nœud.

   Vous pouvez effectuer l'opération de déplacement à l'aide de ONTAP System Manager, OnCommand Workflow Automation, des commandes ONTAP ou d'une combinaison de ces outils.

Après quelques jours, vérifiez si vous recevez le même type d'événements de ce nœud ou de cet agrégat.

Utilisez les paramètres de stratégie QoS pour prioriser les charges de travail des nœuds dans Active IQ Unified Manager

Vous pouvez définir une limite pour un groupe de stratégie QoS afin de contrôler la limite de débit des workloads en E/S par seconde (IOPS) ou en Mo/s qu'il contient. Si les workloads se trouvent dans un groupe de stratégie sans limite définie, comme le groupe de stratégie par défaut, ou si la limite définie ne répond pas à vos besoins, vous pouvez l'augmenter ou déplacer les workloads vers un groupe de stratégie nouveau ou existant disposant de la limite souhaitée.

Si un événement de performance sur un nœud est dû à des workloads qui surutilisent 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/s afin de voir quels workloads présentent l'utilisation la plus élevée et ont pu contribuer à l'événement.

En attribuant les volumes qui utilisent excessivement les ressources du nœud à un paramètre de groupe de stratégies plus restrictif, le groupe de stratégies limite les workloads afin de restreindre leur activité, ce qui peut réduire l'utilisation des ressources sur ce nœud.

Vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour gérer les groupes de stratégies, notamment les tâches suivantes :

- Création d'un groupe de règles
- Ajout ou suppression de workloads dans un groupe de stratégies
- Déplacer un workload entre des groupes de stratégie
- Modification de la limite de débit d'un groupe de stratégies

Supprimez les volumes et les LUN inactifs dans Active IQ Unified Manager

Si l'espace libre de l'agrégat a été identifié comme un problème, vous pouvez rechercher les volumes et les LUN inutilisés et les supprimer de l'agrégat. Cela peut contribuer à atténuer le problème d'espace disque insuffisant.

Si un événement de performance sur un agrégat est dû à un espace disque insuffisant, il existe plusieurs façons de déterminer quels volumes et LUN ne sont plus utilisés.

Pour identifier les volumes inutilisés :

- Sur la page de 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. À partir de là, vous pouvez trier les volumes concernés par **IOPS** pour voir quels volumes n'ont pas été actifs.

Pour identifier les LUN inutilisés :

1. Sur la page des 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** > **All LUNs** dans le menu **View**.
3. Cliquez sur **Filtrage**, sélectionnez **Agrégat** dans le menu déroulant de gauche, saisissez le nom de l'agrégat dans le champ de texte, puis cliquez sur **Appliquer le filtre**.
4. Triez la liste obtenue des LUN concernées par **IOPS** pour afficher les LUN qui ne sont pas actives.

Une fois que vous avez identifié les volumes et les LUN inutilisés, vous pouvez utiliser ONTAP System Manager ou les commandes ONTAP pour supprimer ces objets.

Comprendre comment l'ajout de disques affecte la disposition des agrégats dans Active IQ Unified Manager

Vous pouvez ajouter des disques à un agrégat pour augmenter sa capacité de stockage et ses performances. Après l'ajout des disques, l'amélioration des performances ne sera visible qu'après la reconstruction de l'agrégat.

Lorsque vous recevez un événement de seuil défini par le système sur la page Détails de l'événement, le texte de description de l'événement indique le nom de l'agrégat qui présente le problème. Vous pouvez ajouter des disques et reconstruire les données sur cet agrégat.

Les disques que vous ajoutez à l'agrégat doivent déjà être présents dans le cluster. Si le cluster ne dispose pas de disques supplémentaires, vous devrez peut-être contacter votre administrateur ou acheter davantage 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"

Établissez une connexion entre un serveur Unified Manager et un fournisseur de données externe

Établissez une connexion entre Active IQ Unified Manager et un fournisseur de données externe

Une connexion entre un serveur Unified Manager et un fournisseur de données externe vous permet d'envoyer des données de performances du cluster à un serveur externe afin que les administrateurs du stockage puissent représenter graphiquement les indicateurs 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 « `External Data Provider` » dans la console de maintenance.

Envoyez les données de performance d'Active IQ Unified Manager à un serveur externe

Unified Manager collecte diverses données de performance provenant de tous les clusters qu'il surveille. Vous pouvez envoyer des groupes de données spécifiques vers

un serveur externe.

Selon les données de performance que vous souhaitez représenter graphiquement, vous pouvez choisir d'envoyer l'un des groupes de statistiques suivants :

Groupe de statistiques	Données incluses	Détails
Moniteur de performances	Statistiques de performance de haut niveau pour les objets suivants : • LUN • Volumes	Ce groupe fournit le nombre total d'IOPS ou la latence pour tous les LUN et volumes de l'ensemble des clusters surveillés. Ce groupe fournit le plus petit nombre de statistiques.
Utilisation des ressources	Statistiques d'utilisation des ressources pour les objets suivants : • Nœuds • Agrégats	Ce groupe fournit des statistiques d'utilisation pour le nœud et les ressources physiques de l'agrégat dans tous les clusters surveillés. Il fournit également les statistiques collectées dans le groupe Performance Monitor.
Explorer en détail	Statistiques de lecture/écriture de bas niveau et par protocole pour tous les objets suivis : • Nœuds • Agrégats • LUN • Volumes • Disques • LIF • Ports/cartes réseau	Ce groupe fournit des analyses détaillées des opérations de lecture/écriture et par protocole pour les sept types d'objets suivis dans tous les clusters surveillés. Il fournit également les statistiques collectées dans le groupe Moniteur de performances et dans le groupe Utilisation des ressources. Ce groupe fournit le plus grand nombre de statistiques.

Si le nom d'un cluster ou d'un objet de cluster est modifié sur le système de stockage, l'ancien objet et le nouvel objet contiendront tous deux des données de performance sur le serveur externe (appelé "metric_path"). Les deux objets ne sont pas corrélés comme étant le même objet. Par exemple, si vous changez le nom d'un volume de "volume1_acct" en "acct_vol1", vous verrez les anciennes données de performance pour l'ancien volume et les nouvelles données de performance pour le nouveau volume.

Consultez l'article 30096 de la base de connaissances pour obtenir la liste de tous les compteurs de performance pouvant être envoyés à un fournisseur de données externe.

"Compteurs de performance d'Unified Manager pouvant être exportés vers un fournisseur de données externe"

Configurez Graphite pour recevoir les données de performance de Active IQ Unified Manager

Graphite est un logiciel libre permettant de collecter et de représenter graphiquement les données de performance des systèmes informatiques. Votre serveur et votre logiciel Graphite doivent être correctement configurés pour recevoir les données statistiques d'Unified Manager.

NetApp ne teste ni ne vérifie les versions spécifiques de Graphite ou d'autres outils tiers.

Le serveur Graphite ne reçoit pas de données de performance pour les volumes provenant d'Unified Manager.

Après avoir installé Graphite conformément aux instructions d'installation, vous devez apporter les modifications suivantes pour prendre en charge le transfert de données statistiques depuis Unified Manager :

- Dans le `/opt/graphite/conf/carbon.conf` fichier, le nombre 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, des milliers de nouveaux fichiers peuvent devoir être créés initialement. À raison de 200 fichiers par minute, la création initiale de tous les fichiers de métriques peut prendre 15 minutes, voire plus. Une fois tous les fichiers de métriques uniques créés, ce paramètre n'est plus pertinent.

- Si vous exécutez Graphite sur un serveur déployé avec une adresse IPv6, la valeur de LINE_RECEIVER_INTERFACE dans le `/opt/graphite/conf/carbon.conf` fichier doit être modifiée de "0.0.0.0" à "::" (**`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 rétention sur le nombre de jours adapté à votre environnement.

  La durée de conservation peut être aussi longue que votre environnement le permet, mais la fréquence doit être définie sur 5 minutes pour au moins une configuration de conservation. Dans l'exemple suivant, une section est définie pour Unified Manager à l'aide du `pattern` paramètre, et les valeurs définissent la fréquence initiale à 5 minutes et la durée de conservation à 100 jours: **`[OPM]`**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  Si l'étiquette de fournisseur par défaut est modifiée et passe de « `netapp-performance` » à une autre, cette modification doit également être reflétée dans le `pattern` paramètre.

Si le serveur Graphite est indisponible lorsque le serveur Unified Manager tente d'envoyer des données de performance, les données ne sont pas transmises et il y aura un manque dans les données collectées.

Configurez une connexion entre Active IQ Unified Manager et un fournisseur de données externe

Unified Manager peut envoyer des données de performance du cluster à un serveur externe. Vous pouvez spécifier le type de données statistiques envoyées, ainsi que l'intervalle d'envoi.

Avant de commencer

- Vous devez disposer d'un identifiant utilisateur autorisé à vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez disposer des informations suivantes concernant le fournisseur de données externe :
  - Nom du serveur ou adresse IP (IPv4 ou IPv6)
  - Port par défaut du serveur (si vous n'utilisez pas le port par défaut 2003)
- Vous devez avoir configuré le serveur distant et le logiciel tiers afin qu'ils puissent recevoir des données statistiques du serveur Unified Manager.
- Vous devez savoir quel groupe de statistiques vous souhaitez envoyer :
  - INDICATEUR DE PERFORMANCE: statistiques du moniteur de performances
  - RESOURCE_UTILIZATION: Statistiques du moniteur d'utilisation des ressources et des performances
  - DRILL_DOWN: Toutes les statistiques
- Vous devez connaître l'intervalle de temps auquel vous souhaitez transmettre les statistiques : 5, 10 ou 15 minutes

  Par défaut, Unified Manager collecte les statistiques toutes les 5 minutes. Si vous définissez l'intervalle de transmission sur 10 (ou 15) minutes, la quantité de données envoyées à chaque transmission est deux (ou trois) fois supérieure à celle obtenue avec l'intervalle par défaut de 5 minutes.

  Si vous modifiez l'intervalle de collecte des performances d'Unified Manager à 10 ou 15 minutes, vous devez modifier l'intervalle de transmission afin qu'il soit égal ou supérieur à l'intervalle de collecte d'Unified Manager.

Vous pouvez configurer une connexion entre un serveur Unified Manager et un serveur externe de fournisseur de données.

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 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 une connexion serveur**.

   Les informations de connexion au serveur actuel sont affichées.

4. Lorsque vous y êtes invité, saisissez `y` pour continuer.

5. Lorsque vous y êtes invité, saisissez l'adresse IP ou le nom du serveur de destination et les informations relatives au port du serveur (si différent du port par défaut 2003).
6. Lorsque vous y êtes invité, saisissez **`y`** pour vérifier que les informations que vous avez saisies sont correctes.
7. Appuyez sur n'importe quelle touche pour revenir au menu Connexion au serveur externe.
8. Saisissez le numéro de l'option de menu **Modifier la configuration du serveur**.

   Les informations de configuration actuelles du serveur s'affichent.

9. Lorsque vous y êtes invité, saisissez **`y`** pour continuer.
10. Lorsque vous y êtes invité, saisissez le type de statistiques à envoyer, l'intervalle de temps auquel elles sont envoyées et si vous souhaitez activer immédiatement la transmission des statistiques :

Pour..	**Entrez…**
ID du groupe de statistiques	**`0`** - INDICATEUR_DE_PERFORMANCE (par défaut) **`1`** - UTILISATION DES RESSOURCES **`2`** - FORAGE_EN BAS
Étiquette du fournisseur	Nom descriptif du dossier où les statistiques seront stockées sur le serveur externe. « `netapp-performance` » est le nom par défaut, mais vous pouvez en saisir un autre. En utilisant la notation pointée, vous pouvez définir une structure de dossiers hiérarchique. Par exemple, en saisissant **`stats.performance.netapp`**, les statistiques seront stockées 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, saisissez **`y`** pour vérifier que les informations que vous avez saisies sont correctes.
12. Appuyez sur n'importe quelle touche pour revenir au menu Connexion au serveur externe.
13. Tapez **`x`** pour quitter la console de maintenance.

Une fois la connexion configurée, les données de performance sélectionnées sont envoyées au serveur de destination à l'intervalle de temps spécifié. Quelques minutes peuvent s'écouler avant que les métriques commencent à apparaître dans l'outil externe. Il est possible que vous deviez actualiser votre navigateur pour voir les nouvelles métriques dans la hiérarchie des métriques.

Surveiller et gérer l’état du cluster

Introduction à la surveillance de l’état de santé d’Active IQ Unified Manager

Découvrez la surveillance de l’état de santé avec Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) vous permet de superviser un grand nombre de systèmes exécutant le logiciel ONTAP via une interface utilisateur centralisée. L’infrastructure serveur d’Unified Manager offre une évolutivité, une facilité de maintenance et des fonctionnalités avancées de surveillance et de notification.

Les principales fonctionnalités d’Unified Manager incluent la surveillance, l’émission d’alertes, la gestion de la disponibilité et de la capacité des clusters, la gestion des fonctionnalités de protection, ainsi que le regroupement des données de diagnostic et leur envoi à l’assistance technique.

Vous pouvez utiliser Unified Manager pour surveiller vos clusters. Lorsque des problèmes surviennent dans le cluster, Unified Manager vous informe des détails de ces problèmes par le biais d’événements. Certains événements vous proposent également une action corrective que vous pouvez entreprendre pour résoudre les problèmes. Vous pouvez configurer des alertes pour les événements afin que, lorsque des problèmes surviennent, vous soyez averti par e-mail et par traps SNMP.

Vous pouvez utiliser Unified Manager pour gérer les objets de stockage de votre environnement en les associant à des annotations. Vous pouvez créer des annotations personnalisées et associer dynamiquement des clusters, des machines virtuelles de stockage (SVM), et des volumes à ces annotations via des règles.

Vous pouvez également planifier les besoins de stockage de vos objets de cluster à l’aide des informations fournies dans les graphiques de capacité et de santé pour l’objet de cluster correspondant.

Capacité physique et logique

Unified Manager utilise les concepts d’espace physique et d’espace logique pour les objets de stockage ONTAP.

- Capacité physique : l’espace physique désigne les blocs de stockage physiques utilisés dans le volume. La « capacité physique utilisée » est généralement inférieure à la capacité logique utilisée en raison de la réduction des données due aux mécanismes d’optimisation du stockage (tels que la déduplication et la compression).
- Capacité logique : l’espace logique désigne l’espace utilisable (les blocs logiques) dans un volume. L’espace logique indique comment l’espace théorique peut être utilisé, sans tenir compte des résultats de la déduplication ou de la compression. « Espace logique utilisé » correspond à l’espace physique utilisé plus les économies réalisées grâce aux fonctionnalités d’efficacité du stockage (telles que la déduplication et la compression) qui ont été configurées. Cette mesure apparaît souvent plus élevée que la capacité physique utilisée, car elle ne reflète pas la compression des données ni les autres réductions de l’espace physique. Ainsi, la capacité logique totale peut être supérieure à l’espace provisionné.

Unités de mesure de capacité

Unified Manager calcule la capacité de stockage sur la base d’unités binaires de 1024 (2^{10}) octets. Dans ONTAP 9.10.0 et les versions antérieures, ces unités étaient affichées sous la forme KB, MB, GB, TB et PB. À

partir de ONTAP 9.10.1, elles sont affichées dans Unified Manager sous la forme KiB, MiB, GiB, TiB et PiB.

Les unités utilisées pour le débit restent les kilooctets par seconde (Kbps), les mégaoctets par seconde (Mbps), les gigaoctets par seconde (Gbps) ou les téraoctets par seconde (Tbps), etc., pour toutes les versions de 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

Comprendre les fonctionnalités de surveillance de l'état de santé d'Active IQ Unified Manager

Unified Manager repose sur une infrastructure serveur offrant évolutivité, facilité de maintenance et fonctionnalités avancées de surveillance et de notification. Unified Manager prend en charge la surveillance des systèmes exécutant le logiciel ONTAP.

Unified Manager inclut les fonctionnalités suivantes :

- Découverte, surveillance et notifications pour les systèmes installés avec le logiciel ONTAP :
  - Objets physiques : nœuds, disques, baies de disques, paires SFO, ports et Flash Cache
  - Objets logiques : clusters, machines virtuelles de stockage (SVM), agrégats, volumes, LUN, espaces de noms, qtrees, LIF, copies Snapshot, chemins de jonction, partages NFS, partages SMB, quotas d'utilisateurs et de groupes, groupes de stratégies QoS et groupes d'initiateurs
  - Protocoles : CIFS, NFS, FC, iSCSI, NVMe et FCoE
  - Efficacité du stockage : agrégats SSD, agrégats Flash Pool, agrégats FabricPool, déduplication et compression
  - Protection : relations SnapMirror (synchrones et asynchrones) et relations SnapVault
- Affichage de l'état de découverte et de surveillance du cluster
- MetroCluster sur les configurations FC et IP : visualisation et surveillance de la configuration, des problèmes et de l'état de connectivité des composants du cluster. Commutateurs et ponts MetroCluster pour les configurations MetroCluster sur FC
- Infrastructure améliorée d'alertes, d'événements et de seuils
- Authentification LDAP, LDAPS, SAML et prise en charge des utilisateurs locaux
- RBAC (pour un ensemble prédéfini de rôles)
- AutoSupport et pack de support
- Tableau de bord amélioré affichant la capacité, la disponibilité, la protection et l'état de santé des performances de l'environnement

- Interopérabilité des mouvements de volume, historique des mouvements de volume et historique des modifications de chemin de jonction
- Zone d'impact qui affiche graphiquement les ressources affectées par des événements tels que « Certains disques défaillants », « Dégradation de la mise en miroir de l'agrégat MetroCluster » et « Disques de rechange MetroCluster laissés de côté »
- Zone d'effet possible affichant l'effet des événements MetroCluster
- Zone Actions correctives suggérées qui affiche les actions pouvant être effectuées pour traiter des événements tels que Certains disques défaillants, MetroCluster Mise en miroir des agrégats dégradée et MetroCluster Disques de spare laissés derrière
- La section « Ressources potentiellement impactées » affiche les ressources susceptibles d'être affectées par des événements tels que « Volume hors ligne », « Volume restreint » et « Espace de volume à provisionnement fin à risque »
- Prise en charge des SVM avec des volumes FlexVol® ou FlexGroup
- Prise en charge de la surveillance des volumes racine des nœuds
- Surveillance améliorée des copies Snapshot, incluant le calcul de l'espace récupérable et la suppression des copies Snapshot
- Annotations pour les objets de stockage
- Création et gestion de rapports sur les informations relatives aux objets de stockage, telles que la capacité physique et logique, l'utilisation, les économies d'espace, les performances et les événements associés
- Intégration avec OnCommand Workflow Automation pour exécuter des flux de travail

  "Téléchargement WFA"

Utilisez les interfaces d'Active IQ Unified Manager pour gérer l'état du système de stockage

Ces sections contiennent des informations sur les deux interfaces utilisateur qu'Active IQ Unified Manager fournit pour résoudre les problèmes de capacité, de disponibilité et de protection du stockage des données. Les deux interfaces utilisateur sont l'interface utilisateur web Unified Manager et la console de maintenance.

Si vous souhaitez utiliser les fonctionnalités de protection d'Unified Manager, vous devez également installer et configurer OnCommand Workflow Automation (WFA).

interface utilisateur Web de Unified Manager

L'interface utilisateur Web de Unified Manager permet à un administrateur de surveiller et de résoudre les problèmes de cluster liés à la capacité, à la disponibilité et à la protection du stockage des données.

Ces sections décrivent certains workflows 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 de Unified Manager.

Console de maintenance

La console de maintenance Unified Manager permet à un administrateur de surveiller, de diagnostiquer et de résoudre les problèmes liés au système d'exploitation, aux mises à niveau de version, aux accès utilisateurs et au réseau du serveur Unified Manager lui-même. Si l'interface utilisateur web de Unified Manager est indisponible, la console de maintenance est le seul moyen d'accéder 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.

Gérer et surveiller les clusters et l'état des objets de cluster

Comprendre la surveillance des clusters

Comprendre la surveillance des clusters dans Active IQ Unified Manager

Vous pouvez ajouter des clusters à la base de données Unified Manager pour surveiller leur disponibilité, leur capacité et d'autres détails, tels que l'utilisation du processeur, les statistiques d'interface, l'espace disque libre, l'utilisation des qtree et l'environnement du châssis.

Des événements sont générés en cas d'anomalie ou lorsqu'un seuil prédéfini est dépassé. Si cette option est configurée, Unified Manager envoie une notification à un destinataire spécifié lorsqu'un événement déclenche une alerte.

Comprendre les volumes racine des nœuds dans Active IQ Unified Manager

Vous pouvez surveiller le volume racine du nœud à l'aide d'Unified Manager. La bonne pratique consiste à ce que le volume racine du nœud dispose d'une capacité suffisante pour éviter toute panne du nœud.

Lorsque la capacité utilisée du volume racine du nœud dépasse 80 % de la capacité totale du volume racine du nœud, l'événement « Espace du volume racine du nœud presque plein » est généré. Vous pouvez configurer une alerte pour recevoir une notification. Vous pouvez prendre les mesures appropriées pour éviter que le nœud ne tombe en panne à l'aide de ONTAP System Manager ou de ONTAP CLI.

> La fonctionnalité de surveillance des volumes racine des nœuds n'est pas disponible si les clusters exécutent ONTAP version 9.14.1 ou ultérieure.

Comprendre les événements et les seuils des agrégats racine de nœud dans Active IQ Unified Manager

Vous pouvez surveiller l'agrégat racine du nœud à l'aide d'Unified Manager. La bonne pratique consiste à provisionner de manière 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. De plus, les valeurs de seuil utilisées par Unified Manager ne s'appliquent pas aux agrégats racine des nœuds. Seul un représentant du support technique peut modifier les paramètres afin que ces événements soient générés. Lorsque le représentant du support technique modifie les paramètres, les valeurs de seuil de capacité sont appliquées à l'agrégat racine du nœud.

Vous pouvez prendre les mesures appropriées pour empêcher le nœud de s'arrêter en utilisant soit ONTAP System Manager, soit l'ONTAP CLI.

> La fonctionnalité de surveillance des agrégats racine des nœuds n'est pas disponible si les clusters exécutent ONTAP version 9.14.1 ou ultérieure.

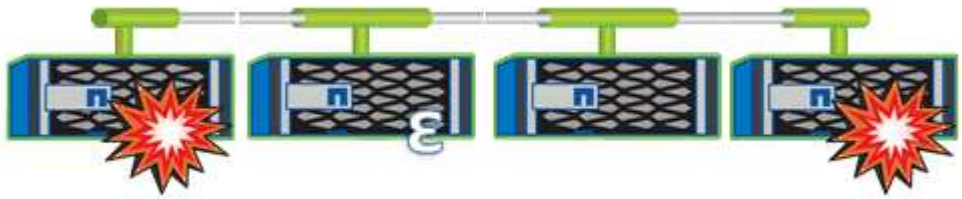
Comprendre le quorum et l'epsilon dans les clusters ONTAP dans Active IQ Unified Manager

Le quorum et l'epsilon sont des mesures importantes de la santé et du fonctionnement des clusters qui, ensemble, indiquent comment les clusters relèvent les défis potentiels en matière de communication et de connectivité.

Le *quorum* est une condition préalable au bon fonctionnement d'un cluster. Lorsqu'un cluster est en quorum, une majorité simple de nœuds sont sains et peuvent communiquer entre eux. Lorsque le quorum est perdu, le cluster perd la capacité d'effectuer les opérations normales du cluster. Une seule collection de nœuds peut être en quorum à un moment donné, 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 divergente, il n'est plus possible de réconcilier les données en une vue unique des données.

Chaque nœud du cluster participe à un protocole de vote qui élit un nœud maître ; chacun des nœuds restants est un nœud secondaire. Le nœud maître est chargé de synchroniser les informations dans l'ensemble du cluster. Une fois le quorum formé, il est maintenu par un vote continu. Si le nœud maître passe hors ligne et que le cluster conserve le quorum, un nouveau maître est élu par les nœuds qui restent en ligne.

Comme il existe une possibilité d'égalité dans un cluster comportant un nombre pair de nœuds, l'un des nœuds possède un poids de vote fractionnaire supplémentaire appelé epsilon. Si la connectivité entre deux portions égales d'un grand cluster est interrompue, le groupe de nœuds contenant epsilon maintient le quorum, à condition que tous les nœuds soient opérationnels. Par exemple, l'illustration suivante montre un cluster à quatre nœuds dans lequel deux des nœuds sont défaillants. Cependant, comme l'un des nœuds restants détient epsilon, le cluster reste en quorum même s'il n'y a pas de majorité simple de nœuds opérationnels.



Epsilon est automatiquement attribué au premier nœud lors de la création du cluster. Si le nœud détenant epsilon devient défaillant, prend le relais de son partenaire haute disponibilité ou est repris par son partenaire haute disponibilité, epsilon est automatiquement réattribué à un nœud sain appartenant à une autre paire haute disponibilité.

La mise hors ligne d'un nœud peut affecter la capacité du cluster à conserver le quorum. Par conséquent, ONTAP émet un message d'avertissement si vous tentez une opération qui fera soit sortir le cluster du quorum, soit le rendra vulnérable à une perte de quorum en cas d'une panne supplémentaire. Vous pouvez désactiver les messages d'avertissement relatifs au quorum à l'aide de la commande cluster quorum-service options modify au niveau de privilège avancé.

En général, en supposant une connectivité fiable entre les nœuds du cluster, un cluster plus grand est plus stable qu'un cluster plus petit. Le quorum requis (majorité simple de la moitié des nœuds plus epsilon) est plus facile à maintenir dans un cluster de 24 nœuds que dans un cluster de deux nœuds.

Un cluster à deux nœuds présente des défis uniques pour le maintien du quorum. Les clusters à deux nœuds utilisent la HA de cluster, dans laquelle aucun nœud ne détient l'epsilon ; les deux nœuds sont interrogés en continu afin de garantir que, si l'un des nœuds tombe en panne, l'autre dispose d'un accès complet en lecture-écriture aux données, ainsi que d'un accès aux interfaces logiques et aux fonctions de gestion.

Consultez la liste et les détails des clusters dans Active IQ Unified Manager

La vue « État : Tous les clusters » vous permet de consulter l'inventaire de vos clusters. La vue « Capacité : Tous les clusters » vous permet de consulter un résumé des informations relatives à la capacité et à l'utilisation du stockage dans tous les clusters.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez également consulter les détails de clusters individuels, tels que l'état du cluster, la capacité, la configuration, les LIF, les nœuds et les disques de ce cluster, à l'aide de la page de détails Cluster / Health.

Les informations affichées dans la vue « État : Tous les clusters », la vue « Capacité : Tous les clusters » et la page « Détails du cluster/État » vous aident à planifier votre stockage. Par exemple, avant de provisionner un nouvel agrégat, vous pouvez sélectionner un cluster spécifique dans la vue « État : Tous les clusters » et consulter les détails de sa capacité afin de déterminer s'il dispose de l'espace requis.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.
2. Dans le menu View, sélectionnez la vue **Health: All Clusters** pour afficher les informations d'état de santé, ou la vue **Capacity: All Clusters** pour afficher les détails sur la capacité de stockage et l'utilisation dans tous les clusters.
3. Cliquez sur le nom d'un cluster pour afficher tous les détails de ce cluster sur la page de détails **Cluster / Health**.

Informations connexes

- "Page de détails Cluster / Santé"
- "Performances: Vue de tous les clusters"
- "Surveillance des MetroCluster configurations"
- "Affichage de l'état de sécurité des clusters et des machines virtuelles de stockage"
- "Quels critères de sécurité sont évalués"

Vérifiez l'état des clusters dans une configuration MetroCluster dans Active IQ Unified Manager

Vous pouvez utiliser Active IQ Unified Manager (Unified Manager) pour vérifier l'état opérationnel des clusters et de leurs composants dans des configurations MetroCluster sur FC et MetroCluster sur IP. Si les clusters ont été impliqués dans un incident de performance détecté par Unified Manager, leur état de fonctionnement peut vous aider à déterminer si un problème matériel ou logiciel a contribué à l'incident.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- 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.

Déterminer l'état du cluster dans une configuration MetroCluster sur FC

Suivez ces étapes pour déterminer l'état du cluster dans une configuration MetroCluster over FC.

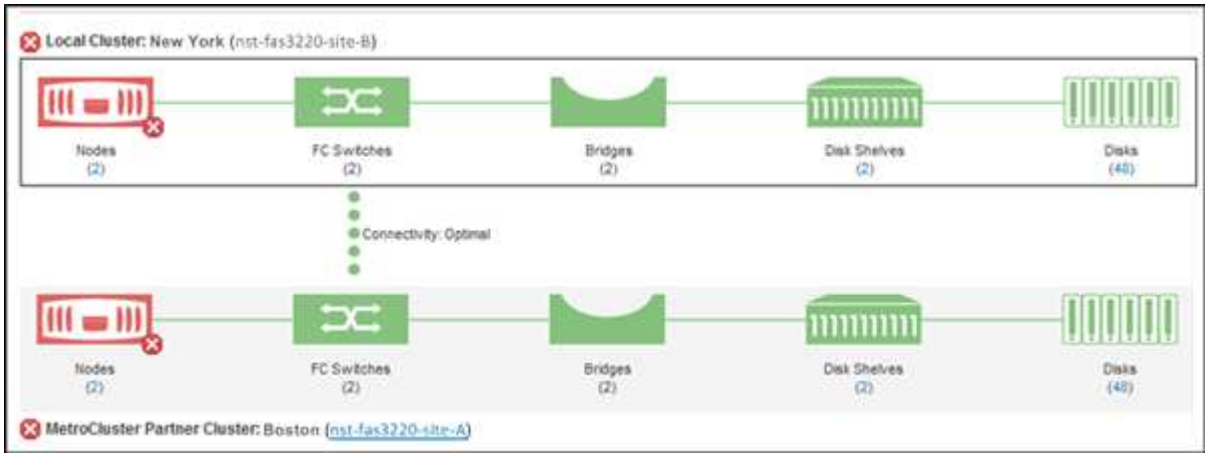
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements** pour afficher la liste des événements.
2. Dans le panneau de filtres, sélectionnez tous les filtres MetroCluster de la catégorie **Type de source**. Vous voyez tous les événements générés dans votre environnement pour toutes les configurations MetroCluster.
3. À côté d'un événement MetroCluster, cliquez sur le nom du cluster.

   Si aucun événement MetroCluster n'est affiché, vous pouvez utiliser la barre de recherche pour rechercher le nom du cluster impliqué dans l'événement lié à votre configuration MetroCluster sur FC.

   La vue « Santé : Tous les clusters » affiche des informations détaillées sur l'événement.

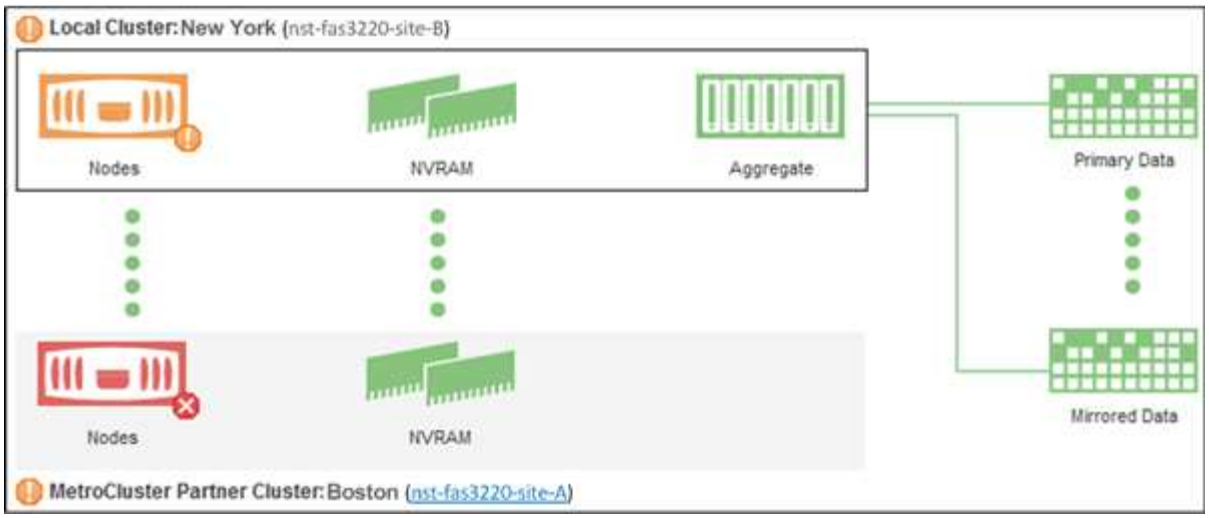
4. Sélectionnez l'onglet **MetroCluster Connectivity** pour afficher l'état de la connexion entre le cluster sélectionné et son cluster partenaire.



   Dans cet exemple, les noms et les composants du cluster local et de son cluster partenaire sont affichés. Une icône jaune ou rouge indique un événement d'intégrité pour le composant mis en évidence. L'icône de connectivité représente la liaison entre les clusters. Vous pouvez placer le pointeur de votre souris sur une icône pour afficher des informations sur l'événement, ou cliquer sur l'icône pour afficher les événements. Un problème d'intégrité sur l'un ou l'autre cluster peut avoir contribué à l'événement de performances.

   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 d'intégrité de la liaison peut être à l'origine de l'incident de performance.

5. Sélectionnez l'onglet **MetroCluster Replication**.



Dans cet exemple, si l'icône NVRAM sur le cluster local ou partenaire est jaune ou rouge, un problème d'intégrité de la NVRAM peut avoir causé l'incident de performance. S'il n'y a aucune icône rouge ou jaune sur la page, un problème de performance sur le cluster partenaire peut avoir causé l'incident de performance.

Déterminer l'état du cluster dans une configuration MetroCluster sur IP

Suivez ces étapes pour déterminer l'état de santé du cluster dans une configuration MetroCluster over IP.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements** pour afficher la liste des événements.
2. Dans le panneau de filtres, sous la catégorie **Type de source**, sélectionnez le `MetroCluster Relationship` filtre. Vous voyez tous les événements déclenchés dans votre environnement pour toutes les configurations MetroCluster.

> Si vous ne pouvez pas voir les événements signalés de MetroCluster, vous pouvez utiliser la barre de recherche pour effectuer une recherche par nom du cluster impliqué dans l'événement lié à votre configuration MetroCluster over IP.

3. À côté de l'événement MetroCluster concerné, cliquez sur le nom du cluster. La page Clusters s'affiche avec les détails de ce cluster. Pour plus d'informations sur l'identification des problèmes de santé, consultez "Surveiller les problèmes de connectivité dans la configuration MetroCluster sur IP".

Consultez l'état de santé et la capacité de tous les clusters All SAN Array dans Active IQ Unified Manager

Vous pouvez utiliser les pages d'inventaire du cluster pour afficher l'état de santé et la capacité de vos clusters All SAN Array.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez consulter des informations générales sur les clusters All SAN Array dans les vues « État : Tous les clusters » et « Capacité : Tous les clusters ». Vous pouvez également consulter les détails sur la page « Détails du cluster / État ».

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.
2. Assurez-vous que la colonne « `Personality` » est affichée dans la vue **Health: All Clusters**, ou ajoutez-la à l'aide de la commande **Show / Hide**.

   Cette colonne affiche « `All SAN Array` » pour vos clusters All SAN Array.

3. Examinez les informations.
4. Pour afficher des informations sur la capacité de stockage de ces clusters, sélectionnez la vue Capacité : Tous les clusters.
5. Pour afficher des informations détaillées sur l'état et la capacité de stockage de ces clusters, cliquez sur le nom d'un cluster All SAN Array.

   Consultez les détails dans les onglets Health, Capacity et Nodes de la page de détails Cluster / Health

Consultez la liste des nœuds et les détails dans Active IQ Unified Manager

La vue « État : Tous les nœuds » permet d'afficher la liste des nœuds de vos clusters. La page « Détails du cluster/État » fournit des informations détaillées sur les nœuds du cluster surveillé.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez consulter des informations détaillées telles que l'état du nœud, le cluster auquel il appartient, les détails de capacité agrégée (utilisée et totale) et les détails de capacité brute (utilisable, disponible et totale). Vous pouvez également obtenir des informations sur les paires haute disponibilité, les baies de disques et les ports.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Nœuds**.
2. Dans la vue **Santé : Tous les nœuds**, cliquez sur le nœud dont vous souhaitez afficher les détails.

   Les informations détaillées du nœud sélectionné s'affichent dans la page des détails Cluster / Health. Le volet de gauche affiche la liste des paires haute disponibilité. Par défaut, le volet Détails HA est ouvert et affiche les détails de l'état HA ainsi que les événements liés à la paire haute disponibilité sélectionnée.

3. Pour afficher d'autres détails concernant le nœud, effectuez l'action appropriée :

Pour consulter…	**Cliquez…**
Détails sur les tiroirs disques	**Baies de disques**.
Informations relatives au port	**Ports**.

Pour plus d'informations, consultez :

- "Performances: vue de tous les nœuds"
- "Affichage des valeurs IOPS disponibles au niveau du nœud et de l'agrégat"
- "Affichage des valeurs de capacité de performance utilisées des nœuds et des agrégats"

Générez un rapport d'inventaire matériel pour le renouvellement du contrat dans Active IQ Unified Manager

Vous pouvez générer un rapport contenant une liste complète des informations sur le cluster et les nœuds, telles que les numéros de modèle et les numéros de série du matériel, les types et le nombre de disques, les licences installées, et bien plus encore. Ce rapport est utile pour le renouvellement des contrats au sein de sites sécurisés (« `dark` ») qui ne sont pas connectés à la plateforme NetAppActive IQ.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Nœuds**.
2. Accédez à la vue **Santé : Tous les nœuds** ou à la vue **Performances : Tous les nœuds**.
3. Sélectionnez **Rapports** > ***** > Rapport d'inventaire du matériel*.

   Le rapport d'inventaire du matériel est téléchargé sous la forme d'un fichier .csv contenant toutes les informations à la date du jour.

4. Veuillez transmettre ces informations à votre contact du support NetApp pour le renouvellement de votre contrat.

Consultez la liste et les détails des machines virtuelles de stockage dans Active IQ Unified Manager

Dans la vue « État : toutes les machines virtuelles de stockage », vous pouvez surveiller votre inventaire de machines virtuelles de stockage (SVM). Vous pouvez utiliser la page « Détails de l'état de la machine virtuelle de stockage » pour afficher des informations détaillées sur les SVM surveillées.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez consulter les détails d'une SVM, tels que sa capacité, son efficacité et sa configuration. Vous pouvez également consulter des informations sur les périphériques associés et les alertes liées à cette SVM.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Machines virtuelles de stockage**.
2. Choisissez l'une des méthodes suivantes pour afficher les détails du SVM :
   - Pour afficher des informations sur l'état de santé de toutes les SVM dans tous les clusters, dans le menu Affichage, sélectionnez la vue État : toutes les machines virtuelles de stockage.
   - Pour afficher tous les détails, cliquez sur le nom de la machine virtuelle de stockage.

     Vous pouvez également afficher tous les détails en cliquant sur **Afficher les détails** dans la boîte de dialogue des détails minimaux.

3. Pour afficher les objets liés au SVM, cliquez sur **Afficher les éléments associés** dans la boîte de dialogue de détails minimaux.

Informations connexes

- "Page de détails sur l'état de la machine virtuelle de stockage"
- "Performances : vue de toutes les machines virtuelles de stockage"
- "Sécurité: Vue anti-ransomware"
- "Affichage de l'état de sécurité des clusters et des machines virtuelles de stockage"
- "Relation : vue Toutes les relations"

Affichez la liste des agrégats et les détails dans Active IQ Unified Manager

La vue « Santé : Tous les agrégats » vous permet de suivre votre inventaire d'agrégats. La vue « Capacité : Tous les agrégats » vous permet de consulter les informations relatives à la capacité et à l'utilisation des agrégats dans tous les clusters.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

La page « Détails de l'agrégat/de l'état » vous permet de consulter des informations telles que la capacité et la configuration de l'agrégat, ainsi que les informations sur les disques. Vous pouvez utiliser ces informations avant de configurer les paramètres de seuil, si nécessaire.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Choisissez l'une des méthodes suivantes pour afficher les détails de l'agrégat :
   - Pour afficher des informations sur l'état de santé de tous les agrégats dans tous les clusters, dans le menu Affichage, sélectionnez la vue Santé : Tous les agrégats.
   - Pour afficher des informations sur la capacité et l'utilisation de tous les agrégats dans tous les clusters, dans le menu Affichage, sélectionnez la vue Capacité : tous les agrégats.
   - Pour afficher tous les détails, cliquez sur le nom de l'agrégat.

     Vous pouvez également afficher tous les détails en cliquant sur **Afficher les détails** dans la boîte de dialogue des détails minimaux.
3. Pour afficher les objets liés à l'agrégat, cliquez sur **Afficher les éléments associés** dans la boîte de dialogue des détails minimaux.

Informations connexes

- "Page de détails de l'agrégat / état de santé"
- "Performances: Vue de tous les agrégats"
- "Créez un rapport pour visualiser les agrégats atteignant leur pleine capacité dans Active IQ Unified Manager"

Consultez les informations de capacité de FabricPool dans Active IQ Unified Manager

Vous pouvez consulter les informations de capacité FabricPool des clusters, des agrégats et des volumes sur les pages d'inventaire et de détails Capacité et

performances de ces objets. Ces pages affichent également les informations de miroir FabricPool lorsqu'un niveau miroir a été configuré.

Ces pages affichent des informations telles que la capacité disponible sur le niveau de performance local et sur le niveau cloud, la quantité de capacité utilisée dans les deux niveaux, les agrégats rattachés à un niveau cloud et les volumes qui mettent en œuvre les fonctionnalités FabricPool en déplaçant certaines informations vers le niveau cloud.

Lorsqu'un niveau cloud est dupliqué vers un autre fournisseur de cloud (le « niveau miroir »), les deux niveaux cloud sont affichés dans la page de détails Aggregate / Health.

Étapes

1. Effectuez l'une des actions suivantes :

Pour consulter les informations de capacité pour…	**Faites ceci…**
Groupes	a. Dans la vue Capacité : Tous les clusters, cliquez sur un cluster. b. Sur la page des détails Cluster / Health, cliquez sur l'onglet **Configuration**. L'affichage indique les noms de tous les niveaux de cloud auxquels ce cluster est connecté.
Agrégats	a. Dans la vue Capacité : Tous les agrégats, cliquez sur un agrégat dont le champ Type indique « `SSD (FabricPool)` » ou « `HDD (FabricPool)` ». b. Sur la page des détails de l'agrégat et de l'état, cliquez sur l'onglet **Capacité**. L'affichage indique la capacité totale utilisée dans le niveau cloud. c. Cliquez sur l'onglet **Informations sur le disque**. L'écran affiche le nom du niveau de cloud et la capacité utilisée. d. Cliquez sur l'onglet **Configuration**. L'écran affiche le nom du niveau de cloud et d'autres informations détaillées le concernant.

Pour consulter les informations de capacité pour…	Faites ceci…
Volumes	a. Dans la vue Capacité : Tous les volumes, cliquez sur un volume où un nom de stratégie apparaît dans le champ « `Stratégie de hiérarchisation` ». b. Sur la page Détails du volume/de l'état, cliquez sur l'onglet **Configuration**. L'écran affiche le nom de la stratégie de hiérarchisation FabricPool attribuée au volume.

2. Sur la page **Workload Analysis**, vous pouvez sélectionner “Cloud Tier View” dans la zone **Capacity Trend** pour voir la capacité utilisée dans le niveau de performances local et dans le Cloud Tier au cours du mois précédent.

Pour plus d'informations sur les agrégats FabricPool, voir "Aperçu des disques et des agrégats".

Consultez les détails du pool de stockage dans Active IQ Unified Manager

Vous pouvez consulter les détails du pool de stockage pour surveiller son état, le cache total et disponible, ainsi que les allocations utilisées et disponibles.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Cliquez sur le nom d'un agrégat.

   Les détails de l'agrégat sélectionné sont affichés.

3. Cliquez sur l'onglet **Informations sur le disque**.

   Des informations détaillées sur le disque s'affichent.

   Le tableau Cache s'affiche uniquement lorsque l'agrégat sélectionné utilise un pool de stockage.

4. Dans le tableau Cache, déplacez le pointeur sur le nom du pool de stockage requis.

   Les détails du pool de stockage s'affichent.

Consultez la liste des volumes et les détails dans Active IQ Unified Manager

La vue « Santé : Tous les volumes » vous permet de surveiller votre inventaire de volumes. La vue « Capacité : Tous les volumes » vous permet de consulter les informations relatives à la capacité et à l'utilisation des volumes d'un cluster.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez également utiliser la page Détails du volume/de l'état pour afficher des informations détaillées sur les volumes surveillés, notamment leur capacité, leur efficacité, leur configuration et leur protection. Vous pouvez également afficher des informations sur les périphériques associés et les alertes associées à un volume spécifique.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Choisissez l'une des méthodes suivantes pour afficher les détails du volume :
   - Pour afficher des informations détaillées sur l'état des volumes d'un cluster, dans le menu Affichage, sélectionnez la vue État : tous les volumes.
   - Pour afficher des informations détaillées sur la capacité et l'utilisation des volumes dans un cluster, dans le menu Affichage, sélectionnez la vue Capacité : Tous les volumes.
   - Pour afficher tous les détails, cliquez sur le nom du volume.

     Vous pouvez également afficher tous les détails en cliquant sur **Afficher les détails** dans la boîte de dialogue des détails minimaux.
3. **Facultatif:** Consultez les objets liés au volume en cliquant sur **Afficher les éléments associés** dans la boîte de dialogue des détails minimaux.

Informations connexes

- "Volume: page de détails sur l'état"
- "Performance : vue de tous les volumes"
- "Sécurité: Vue anti-ransomware"
- "Affichage des relations de protection du volume"
- "Création d'un rapport pour afficher les graphiques de capacité disponible des volumes"

Consultez les détails relatifs aux partages NFS dans Active IQ Unified Manager

Vous pouvez afficher des détails sur tous les partages NFS, tels que leur état, le chemin associé au volume (volumes FlexGroup ou volumes FlexVol®), les niveaux d'accès des clients aux partages NFS et les règles d'export définies pour les volumes exportés. Utilisez la vue Santé : tous les partages NFS pour afficher tous les partages NFS sur l'ensemble des clusters surveillés, et utilisez la page Détails de la VM de stockage / Santé pour afficher tous les partages NFS sur une machine virtuelle de stockage (SVM) spécifique.

Avant de commencer

- La licence NFS doit être activée sur le cluster.
- Les interfaces réseau desservant les partages NFS doivent être configurées.
- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étape

1. Dans le volet de navigation de gauche, suivez les étapes ci-dessous selon que vous souhaitez afficher tous les partages NFS ou uniquement les partages NFS d'une SVM particulière.

À…	Suivez ces étapes…
Afficher tous les partages NFS	Cliquez sur **Stockage** > **Partages NFS**
Afficher les partages NFS pour une seule SVM	a. Cliquez sur **Stockage** > **Machines virtuelles de stockage** b. Cliquez sur le SVM pour lequel vous souhaitez afficher les détails des partages NFS. c. Dans la page Détails de la machine virtuelle de stockage / État, 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".

Affichez les détails concernant les partages SMB/CIFS dans Active IQ Unified Manager

Vous pouvez consulter les détails de tous les partages SMB/CIFS, tels que le nom du partage, le chemin de jonction, les objets contenus, les paramètres de sécurité et les règles d'export définies pour le partage. Utilisez la vue « État : Tous les partages SMB » pour afficher tous les partages SMB sur tous les clusters surveillés, et la page « Détails de l'état de la machine virtuelle de stockage » pour afficher tous les partages SMB sur une machine virtuelle de stockage (SVM) spécifique.

Avant de commencer

- La licence CIFS doit être activée sur le cluster.
- Les interfaces réseau desservant les partages SMB/CIFS doivent être configurées.
- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Les partages dans les dossiers ne sont pas affichés.

Étape

1. Dans le volet de navigation de gauche, suivez les étapes ci-dessous selon que vous souhaitez afficher tous les partages SMB/CIFS ou uniquement les partages d'une SVM particulière.

À…	Suivez ces étapes…
Afficher tous les partages SMB/CIFS	Cliquez sur **Stockage** > **Partages SMB**
Afficher les partages SMB/CIFS pour une seule SVM	a. Cliquez sur **Stockage** > **Machines virtuelles de stockage** b. Cliquez sur le SVM pour lequel vous souhaitez afficher les détails du partage CIFS. c. Dans la page de détails de la machine virtuelle de stockage / État, cliquez sur l'onglet **Partages SMB**.

Pour plus d'informations, consultez "Provisionnement des partages de fichiers CIFS et NFS à l'aide d'API".

Consultez la liste des copies Snapshot dans Active IQ Unified Manager

Vous pouvez consulter la liste des copies Snapshot d'un volume sélectionné. Cette liste vous permet de calculer l'espace disque récupérable en supprimant une ou plusieurs copies Snapshot, et de les supprimer si nécessaire.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Le volume contenant les copies Snapshot doit être en ligne.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans la vue **Santé : Tous les volumes**, sélectionnez le volume contenant les copies Snapshot que vous souhaitez consulter.
3. Sur la page de détails **Volume / Santé**, cliquez sur l'onglet **Capacité**.
4. Dans le volet **Détails** de l'onglet **Capacité**, dans la section Autres détails, cliquez sur le lien en regard de **Copies instantanées**.

   Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

Informations connexes

"Page Santé/Volumes"

Supprimer les copies d'instantané dans Active IQ Unified Manager

Vous pouvez supprimer une copie Snapshot pour économiser de l'espace ou pour libérer de l'espace disque, ou vous pouvez supprimer la copie Snapshot si elle n'est plus nécessaire.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Le volume doit être en ligne.

Pour supprimer une copie Snapshot occupée ou verrouillée, vous devez avoir libéré la copie Snapshot de l'application qui l'utilisait.

- Vous ne pouvez pas supprimer la copie Snapshot de base dans un volume parent si un volume FlexClone utilise cette copie Snapshot.

  La copie Snapshot de base est la copie Snapshot utilisée pour créer le volume FlexClone et affiche l'état `Busy` et la dépendance de l'application en tant que `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 est requise pour la prochaine mise à jour.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.

2. Dans la vue **Santé : Tous les volumes**, sélectionnez le volume contenant les copies Snapshot que vous souhaitez consulter.

   La liste des copies Snapshot s'affiche.

3. Sur la page de détails **Volume / Santé**, cliquez sur l'onglet **Capacité**.
4. Dans le volet **Détails** de l'onglet **Capacité**, dans la section Autres détails, cliquez sur le lien en regard de **Copies instantanées**.

   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 que vous souhaitez supprimer, puis cliquez sur **Supprimer la sélection**.

Calculer l'espace récupérable pour les copies Snapshot dans Active IQ Unified Manager

Vous pouvez calculer la quantité d'espace disque qui peut être récupérée si une ou plusieurs copies Snapshot sont supprimées.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- 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 **Stockage** > **Volumes**.
2. Dans la vue **Santé : Tous les volumes**, sélectionnez le volume contenant les copies Snapshot que vous souhaitez consulter.

   La liste des copies Snapshot s'affiche.

3. Sur la page de détails **Volume / Santé**, cliquez sur l'onglet **Capacité**.
4. Dans le volet **Détails** de l'onglet **Capacité**, dans la section Autres détails, cliquez sur le lien en regard de **Copies instantanées**.

   Le nombre de copies Snapshot est un lien qui affiche la liste des copies Snapshot.

5. Dans la vue **Snapshot Copies**, sélectionnez les copies Snapshot pour lesquelles vous souhaitez calculer l'espace récupérable.
6. Cliquez sur **Calculate**.

   L'espace récupérable (en pourcentage, et en Ko, Mo, Go, etc.) sur le volume est affiché.

7. Pour recalculer l'espace récupérable, sélectionnez les copies Snapshot requises et cliquez sur **Recalculer**.

Comprendre les fenêtres et boîtes de dialogue des objets de cluster dans Active IQ Unified Manager

Vous pouvez consulter tous vos clusters et objets de cluster depuis la page de l'objet de stockage correspondant. Vous pouvez également consulter les détails depuis la page de détails de l'objet de stockage correspondant. Vous pouvez désormais lancer l'interface utilisateur de System Manager depuis les sections STOCKAGE et PROTECTION de l'INVENTAIRE.

- Pages Inventaire du cluster, Santé du cluster et Performances du cluster
- Pages Inventaire des agrégats, État des agrégats et Performances des agrégats
- Pages d'inventaire, d'état de santé et de performances des volumes
- Pages d'inventaire des nœuds et de performance des nœuds
- Pages d'inventaire, d'état et de performances de StorageVM
- Pages de relation de protection

Flux de travail et tâches courants de surveillance de l'état dans Unified Manager

Comprendre les flux de travail et les tâches de santé courants d'Active IQ Unified Manager

Les flux de travail et les tâches administratives courants associés à Unified Manager comprennent la sélection des clusters de stockage à surveiller, 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, ainsi que le regroupement et l'envoi des données de diagnostic au support technique (le cas échéant).

Unified Manager permet aux administrateurs du stockage de consulter 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 en vue de leur résolution tout problème spécifique susceptible de survenir.

Les problèmes les plus importants liés à un cluster, à une machine virtuelle de stockage (SVM), à un volume ou à un volume FlexGroup, et qui affectent la capacité de stockage ou la disponibilité des données de vos objets de stockage gérés, sont affichés dans les graphiques et les événements d'état du système sur la page Tableau de bord. Lorsque des problèmes critiques sont identifiés, cette page fournit des liens vers les procédures de dépannage appropriées.

Unified Manager peut également être inclus dans des flux de travail qui incluent des outils de gestion associés, tels que OnCommand Workflow Automation (WFA), pour prendre en charge la configuration directe des ressources de stockage.

Les flux de travail courants liés aux tâches administratives suivantes sont décrits dans ce document :

- Diagnostic et gestion des problèmes de disponibilité

Si une défaillance matérielle ou des problèmes de configuration des ressources de stockage entraînent l'affichage d'événements de disponibilité des données sur la page Tableau de bord, les administrateurs du stockage peuvent suivre les liens intégrés pour consulter les informations de connectivité concernant la ressource de stockage concernée, consulter des conseils de dépannage et attribuer la résolution du problème à d'autres administrateurs.

- Configuration et surveillance des incidents de performance

  L'administrateur peut surveiller et gérer les performances des ressources du système de stockage surveillées. Consultez "Introduction à la surveillance des performances d'Active IQ Unified Manager" pour plus d'informations.

- Diagnostic et gestion des problèmes de capacité des volumes

  Si des problèmes de capacité de stockage des volumes sont affichés sur la page Dashboard, les administrateurs du stockage peuvent suivre les liens intégrés pour consulter les tendances actuelles et historiques relatives à la capacité de stockage du volume concerné, consulter des conseils de dépannage et attribuer la résolution du problème à d'autres administrateurs.

- Configuration, surveillance et diagnostic des problèmes liés aux relations de protection

  Après avoir créé et configuré les relations de protection, les administrateurs du stockage peuvent consulter les problèmes potentiels liés aux relations de protection, l'état actuel des relations de protection, les informations actuelles et historiques sur la réussite des tâches de protection concernant les relations affectées, ainsi que des conseils de dépannage. Consultez la documentation "Découvrez comment gérer et surveiller les relations de protection" pour plus d'informations.

- Création de fichiers de sauvegarde et restauration des données à partir de fichiers de sauvegarde.
- Associer des objets de stockage à des annotations

  En associant des objets de stockage à des annotations, les administrateurs du stockage peuvent filtrer et afficher les événements liés à ces objets, ce qui leur permet de hiérarchiser par ordre de priorité et de résoudre les problèmes associés à ces événements.

- Utilisez les API REST pour aider à gérer vos clusters en consultant les informations relatives à leur état, leur capacité et leurs performances, collectées par Unified Manager. Voir "Premiers pas avec les API REST d'Active IQ Unified Manager" pour plus d'informations.
- Envoi d'un dossier de support à l'assistance technique

  Les administrateurs du stockage peuvent récupérer et envoyer un dossier de support au support technique à l'aide de la console de maintenance. Les dossiers de support doivent être envoyés au support technique lorsque le problème nécessite un diagnostic et un dépannage plus détaillés que ce qu'un message AutoSupport fournit.

Surveiller et résoudre les problèmes de disponibilité des données

Surveillez et dépannez la disponibilité des données dans Active IQ Unified Manager

Unified Manager surveille la fiabilité avec laquelle les utilisateurs autorisés peuvent accéder à vos données stockées, vous alerte en cas de conditions bloquant ou entravant cet accès, et vous permet de diagnostiquer ces conditions, d'attribuer et de suivre leur résolution.

Les rubriques du workflow de disponibilité de cette section décrivent des exemples de la manière dont un administrateur du stockage peut utiliser l'interface utilisateur Web de Unified Manager pour découvrir, diagnostiquer et attribuer en vue de leur résolution des problèmes matériels et logiciels qui affectent négativement la disponibilité des données.

Rechercher et résoudre les problèmes de liaison d'interconnexion de basculement du stockage en panne

Recherchez et résolvez les conditions de liaison d'interconnexion de basculement de stockage hors service dans Active IQ Unified Manager

Ce flux de travail fournit un exemple de la manière dont vous pouvez rechercher, évaluer et résoudre les défaillances des liaisons d'interconnexion de basculement du stockage. Dans ce scénario, vous êtes un administrateur qui utilise Unified Manager pour analyser les risques de basculement du stockage avant de lancer une mise à niveau de version ONTAP sur vos nœuds.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Si les interconnexions de basculement du stockage entre les nœuds d'une paire haute disponibilité échouent lors d'une tentative de mise à niveau sans interruption de service, la mise à niveau échoue. Par conséquent, il est courant que l'administrateur surveille et confirme la fiabilité du basculement du stockage sur les nœuds de cluster ciblés pour la mise à niveau avant de la lancer.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans la page d'inventaire **Gestion des événements**, sélectionnez **événements de disponibilité active**.
3. En haut de la page d'inventaire **Gestion des événements**, dans la colonne **Nom**, cliquez sur et entrez `*failover` dans la zone de texte pour limiter l'affichage de l'événement aux événements liés au basculement du stockage.

   Tous les événements passés liés 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 du stockage s'affichent sur la page d'inventaire **Gestion des événements**, procédez comme suit :

   a. Cliquez sur le lien du titre de l'événement pour afficher les détails de cet événement.

      Dans cet exemple, vous cliquez sur le titre de l'événement “Storage Failover Interconnect One or More Links Down”.

   La page des détails de cet événement s'affiche.

   a. Sur la page de détails de l'événement, vous pouvez effectuer une ou plusieurs des tâches suivantes :
      - Examinez le message d'erreur dans le champ Cause et évaluez le problème.
      - Attribuez l'événement à un administrateur.
      - Acquittez l'événement.

Informations connexes

"Page de détails de l'événement"

"Rôles et fonctionnalités des utilisateurs d'Unified Manager"

Effectuez une action corrective en cas de défaillance d'une liaison d'interconnexion de basculement de stockage dans Active IQ Unified Manager

Lorsque vous affichez la page de détails de l'événement relatif à un 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 une solution possible à celui-ci.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Dans cet exemple, le résumé de l'événement fourni sur la page Détails de l'événement contient les informations suivantes concernant l'état de la liaison d'interconnexion de basculement de stockage :

```
Event: Storage Failover Interconnect One or More Links Down

Summary

Severity: Warning
State: New
Impact Level: Risk
Impact Area: Availability
Source: aardvark
Source Type: Node
Acknowledged By:
Resolved By:
Assigned To:
Cause: At least one storage failover interconnected link
       between the nodes aardvark and bonobo is down.
       RDMA interconnect is up (Link0 up, Link1 down)
```

L'exemple d'information d'événement indique qu'une liaison d'interconnexion de basculement de stockage, Link1, entre les nœuds de la paire haute disponibilité aardvark et bonobo est hors service, tandis que Link0 entre Apple et Boy est active. Comme une liaison est active, l'accès direct à la mémoire à distance (RDMA) fonctionne toujours et une opération de basculement de stockage peut encore réussir.

Toutefois, pour éviter que les deux liaisons ne tombent en panne et que la protection de basculement du stockage ne soit totalement désactivée, vous décidez de diagnostiquer plus en détail la raison de l'arrêt de Link1.

Étapes

1. Depuis la page de détails de l'**événement**, vous pouvez cliquer sur le lien vers l'événement spécifié dans le champ Source pour obtenir plus de détails sur d'autres événements susceptibles d'être liés à l'état

d'indisponibilité de la liaison d'interconnexion de basculement du stockage.

Dans cet exemple, la source de l'événement est le nœud nommé aardvark. Cliquer sur ce nom de nœud affiche les HA Details de la paire haute disponibilité concernée, aardvark et bonobo, dans l'onglet Nodes de la page Cluster / Health details, et affiche d'autres événements survenus récemment sur la paire haute disponibilité concernée.

2. Consultez **HA Details** pour plus d'informations concernant l'événement.

   Dans cet exemple, les informations pertinentes se trouvent dans le tableau Events. Le tableau affiche l'événement "Storage Failover Connection One or More Link Down", l'heure à laquelle l'événement a été généré et, là encore, le nœud d'où cet événement provient.

À l'aide des informations d'emplacement des nœuds dans HA Details, demandez ou effectuez vous-même une inspection physique et la réparation du problème de basculement du stockage sur les nœuds de la paire haute disponibilité concernée.

Informations connexes

"Page de détails de l'événement"

"Rôles et fonctionnalités des utilisateurs d'Unified Manager"

Résoudre les problèmes de volume hors ligne

Résoudre les problèmes de volume hors ligne dans Active IQ Unified Manager

Ce flux de travail illustre comment évaluer et résoudre un incident de mise hors ligne d'un volume, tel qu'il peut apparaître dans la page d'inventaire de gestion des événements d'Unified Manager. Dans ce scénario, vous êtes un administrateur utilisant Unified Manager pour résoudre un ou plusieurs incidents de mise hors ligne d'un volume.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Les volumes peuvent être signalés comme hors ligne pour plusieurs raisons :

- L'administrateur SVM a délibérément mis le volume hors ligne.
- Le nœud de cluster hébergeant le volume est hors service et le basculement du stockage vers son partenaire de la paire haute disponibilité a également échoué.
- La machine virtuelle de stockage (SVM) hébergeant le volume est arrêtée car le nœud hébergeant le volume racine de cette SVM est hors service.
- L'agrégat hébergeant le volume est hors service en raison de la défaillance simultanée de deux disques RAID.

Vous pouvez utiliser la page d'inventaire Event Management et les pages de détails Cluster/Health, Storage VM/Health et Volume/Health pour confirmer ou éliminer une ou plusieurs de ces possibilités.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.
2. Dans la page d'inventaire **Gestion des événements**, sélectionnez **événements de disponibilité active**.

3. Cliquez sur le lien hypertexte affiché pour l'événement Volume Offline.

   La page de détails de l'événement relatif à l'incident de disponibilité s'affiche.

4. Sur cette page, consultez les notes pour vérifier si l'administrateur SVM a mis le volume en question hors ligne.
5. Sur la page de détails de l'**événement**, vous pouvez consulter les informations relatives à une ou plusieurs des tâches suivantes :
   - Consultez les informations affichées dans le champ Cause pour obtenir d'éventuelles indications de diagnostic.

     Dans cet exemple, l'information du champ Cause vous indique seulement que le volume est hors ligne.

   - Consultez la section Notes et mises à jour pour vérifier si l'administrateur SVM a délibérément mis hors ligne le volume en question.
   - Cliquez sur la source de l'événement, en l'occurrence le volume signalé comme 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.

Effectuez des actions de diagnostic pour les conditions de mise hors ligne des volumes dans Active IQ Unified Manager

Après avoir accédé à la page de détails Volume / Health d'un volume signalé comme hors ligne, vous pouvez rechercher des informations supplémentaires utiles pour diagnostiquer l'état hors ligne du volume.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Si le volume signalé comme hors ligne n'a pas été mis hors ligne délibérément, il peut être hors ligne pour plusieurs raisons.

À partir de la page Détails du volume / de l'état du volume hors ligne, vous pouvez accéder à d'autres pages et volets pour confirmer ou éliminer les causes possibles :

- Cliquez sur les liens de la page de détails **Volume / Health** pour déterminer si le volume est hors ligne parce que son nœud hôte est hors service et que le basculement du stockage vers sa paire haute disponibilité a également échoué.

  Voir "Déterminer si l'état hors ligne d'un volume est causé par un nœud en panne".

- Cliquez sur les liens de la page de détails **Volume / Health** pour déterminer si le volume est hors ligne et si sa machine virtuelle de stockage hôte (SVM) est arrêtée parce que le nœud hébergeant le volume racine de cette SVM est hors service.

  Voir "Déterminer si un volume est hors ligne et si la SVM est arrêtée parce qu'un nœud est hors service".

- Cliquez sur les liens de la page de détails **Volume / Santé** pour déterminer si le volume est hors ligne en raison de disques défectueux dans son agrégat hôte.

  Voir "Déterminer si un volume est hors ligne en raison de disques défectueux dans un agrégat".

Informations connexes

"Rôles et fonctionnalités des utilisateurs d'Unified Manager"

Déterminez si un volume est hors ligne parce que son nœud hôte est hors service dans Active IQ Unified Manager

Vous pouvez utiliser l'interface utilisateur Web de Unified Manager pour confirmer ou exclure la possibilité qu'un volume soit hors ligne parce que son nœud hôte est hors service et que le basculement du stockage vers son partenaire de la paire haute disponibilité a échoué.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Pour déterminer si l'indisponibilité du volume est due à une défaillance du nœud hôte et à un basculement de stockage infructueux, effectuez les actions suivantes :

Étapes

1. Repérez et cliquez sur le lien hypertexte affiché sous SVM dans le volet **Périphériques associés** de la page de détails **Volume / État** du volume hors ligne.

   La page des détails de la VM de stockage / état affiche des informations sur la machine virtuelle de stockage (SVM) qui héberge le volume hors ligne.

2. Dans le volet **Related Devices** de la page de détails **Storage VM / Health**, repérez 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 la colonne État de la vue **Santé : Tous les volumes**, cliquez sur le symbole de filtre, puis sélectionnez l'option **Hors ligne**.

   Seuls les volumes SVM à l'état hors ligne sont répertoriés.

4. Dans la vue Santé : Tous les volumes, cliquez sur le symbole de la grille, puis sélectionnez l'option **Nœuds du cluster**.

   Vous devrez peut-être faire défiler la zone de sélection de la grille pour trouver l'option **Cluster Nodes**.

   La colonne « Nœuds du 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**, repérez l'entrée du volume hors ligne et, dans sa colonne Nœud de cluster, cliquez sur le nom de son nœud hôte.

   L'onglet Nœuds de la page Détails du cluster/de l'état affiche l'état de la paire haute disponibilité à laquelle appartient le nœud hôte. L'état du nœud hôte et la réussite de toute opération de basculement du cluster sont indiqués dans l'affichage.

Après avoir confirmé que le volume est hors ligne parce que son nœud hôte est hors service 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 hors service et résoudre le problème de basculement du stockage.

Déterminez si un volume est hors ligne parce que son SVM est arrêté dans Active IQ Unified Manager

Vous pouvez utiliser l'interface utilisateur web Unified Manager pour confirmer ou écarter la possibilité qu'un volume soit hors ligne parce que sa machine virtuelle de stockage hôte (SVM) est arrêtée en raison de la panne du nœud qui héberge le volume racine de cette SVM.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Pour déterminer si l'état hors ligne du volume est dû à l'arrêt de la SVM hôte parce que le nœud hébergeant le volume racine de cette SVM est hors service, effectuez les actions suivantes :

Étapes

1. Repérez et cliquez sur le lien hypertexte affiché sous le SVM dans le volet **Périphériques associés** de la page de détails **Volume / État** du volume hors ligne.

   La page de détails Storage VM / Health affiche le statut "running" ou "stopped" du SVM hôte. Si le statut du SVM est `running`, l'état hors ligne du volume n'est pas causé par une panne du nœud hébergeant le volume racine de ce SVM.

2. Si l'état du SVM est à l'arrêt, cliquez sur **Afficher les SVM** pour identifier plus précisément la cause de l'arrêt du SVM hôte.
3. Dans l'en-tête de colonne SVM de la vue **Santé : Toutes les machines virtuelles de stockage**, cliquez sur le symbole de filtre puis saisissez le nom de la SVM arrêtée.

   Les informations relatives à cette 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 racine est ajoutée à l'inventaire des SVM et affiche le nom du volume racine du SVM arrêté.

5. Dans la colonne Volume racine, cliquez sur le nom du volume racine pour afficher la page de détails **VM de stockage / État** de ce volume.

   Si l'état du volume racine de la SVM est (Online), l'état hors ligne du volume d'origine n'est pas dû à une panne du nœud qui héberge le volume racine de cette SVM.

6. Si l'état du volume racine de la SVM est (Hors ligne), recherchez et cliquez sur le lien hypertexte affiché sous Agrégat dans le volet Appareils associés de la page Détails Volume / Santé du volume racine de la SVM.
7. Repérez et cliquez sur le lien hypertexte affiché sous Nœud dans le volet **Appareils associés** de la page de détails **Agrégat / Santé** de l'agrégat.

   L'onglet Nœuds de la page Détails du cluster/de l'état affiche l'état de la paire haute disponibilité de nœuds à laquelle appartient le nœud hébergeant le volume racine de la SVM. L'état du nœud est indiqué à l'écran.

Après avoir confirmé que l'état hors ligne du volume est dû à l'état hors ligne du SVM hôte de ce volume, lui-même causé par la panne du nœud hébergeant le volume racine de ce SVM, contactez l'administrateur ou l'opérateur compétent pour redémarrer manuellement le nœud en panne.

Déterminez si un volume est hors ligne en raison de disques défectueux dans Active IQ Unified Manager

Vous pouvez utiliser l'interface utilisateur web de Unified Manager pour confirmer ou infirmer la possibilité qu'un volume soit hors ligne en raison de problèmes de disque RAID ayant mis hors service son agrégat hôte.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Pour déterminer si l'indisponibilité du volume est due à des problèmes de disque RAID qui mettent l'agrégat hôte hors ligne, effectuez les actions suivantes :

Étapes

1. Repérez et cliquez sur le lien hypertexte affiché sous **Agrégat** dans le volet **Périphériques associés** de la page de détails **Volume / Santé**.

   La page « Détails de l'agrégat/de l'état » affiche l'état en ligne ou hors ligne de l'agrégat hébergeant. Si l'agrégat est en ligne, les problèmes de disque RAID ne sont pas à l'origine de l'indisponibilité du volume.

2. Si l'état de l'agrégat est hors ligne, cliquez sur **Informations disque** et recherchez les événements de disque défectueux dans la liste **Événements** de l'onglet **Informations disque**.
3. Pour identifier plus précisément les disques défectueux, cliquez sur le lien hypertexte affiché sous Node dans le volet **Related Devices**.

   La page de détails du cluster/de l'état de santé s'affiche.

4. Cliquez sur **Disques**, puis sélectionnez **Défectueux** dans le volet **Filtres** pour afficher tous les disques en état de panne.

   Si les disques défectueux ont entraîné la mise hors ligne de l'agrégat hôte, le nom de l'agrégat est affiché dans la colonne Agrégat impacté.

Après avoir confirmé que l'état hors ligne du volume est dû à des disques RAID défectueux et à l'agrégat hôte hors ligne qui en résulte, contactez l'administrateur ou l'opérateur approprié pour remplacer manuellement les disques défectueux et remettre l'agrégat en ligne.

Résoudre les problèmes de capacité

Résoudre les problèmes de capacité dans Active IQ Unified Manager

Ce processus illustre comment vous pouvez résoudre un problème de capacité. Dans ce scénario, vous êtes un administrateur ou un opérateur et vous accédez à la page Unified ManagerDashboard pour vérifier si l'un des objets de stockage surveillés présente des problèmes de capacité. Vous souhaitez déterminer la cause possible du problème et sa résolution.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Sur la page Tableau de bord, recherchez un événement d'erreur "Volume Space Full" dans le panneau Capacité, sous la liste déroulante des événements.

Étapes

1. Dans le panneau **Capacity** de la page **Dashboard**, cliquez sur le nom de l'événement d'erreur « Volume Space Full ».

   La page de détails de l'événement relatif à l'erreur s'affiche.

2. Depuis la page de détails de l'**événement**, vous pouvez effectuer une ou plusieurs des tâches suivantes :
   - Examinez le message d'erreur dans le champ Cause et cliquez sur les suggestions sous Actions correctives suggérées pour consulter les descriptions des solutions possibles.
   - Cliquez sur le nom de l'objet, dans ce cas un volume, dans le champ Source pour obtenir des détails sur l'objet.
   - Recherchez les notes qui auraient pu être ajoutées concernant cet événement.
   - Ajouter une note à l'événement.
   - Attribuer l'événement à un autre utilisateur.
   - Acquittez l'événement.
   - Marquez l'événement comme résolu.

Informations connexes

"Page de détails de l'événement"

Effectuez les actions correctives suggérées pour un volume complet dans Active IQ Unified Manager

Après avoir reçu un événement d'erreur « `Volume Space Full` », vous consultez les actions correctives suggérées sur la page de détails de l'événement et décidez d'effectuer l'une des actions suggérées.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Un utilisateur, quel que soit son rôle, peut effectuer toutes les tâches de ce flux de travail qui utilisent Unified Manager.

Dans cet exemple, vous avez vu un événement d'erreur « Volume Space Full » sur la page d'inventaire de gestion Unified ManagerEvent et vous avez cliqué sur le nom de l'événement.

Voici quelques actions correctives que vous pourriez entreprendre pour un volume plein :

- Activation de l'extension automatique, de la déduplication ou de la compression du volume
- Redimensionner ou déplacer le volume
- Suppression ou déplacement de données du volume

Bien que toutes ces actions doivent être effectuées à partir de ONTAP System Manager ou de l'interface de ligne de commande ONTAP, vous pouvez utiliser Unified Manager pour trouver les informations dont vous pourriez avoir besoin pour déterminer les actions à entreprendre.

Étapes

1. Depuis la page de détails de l'**événement**, cliquez sur le nom du volume dans le champ Source pour afficher les détails concernant le volume concerné.

2. Sur la page de détails **Volume / Health**, cliquez sur **Configuration** et constatez que la déduplication et la compression sont déjà activées sur le volume.

   Vous décidez de redimensionner le volume.

3. Dans le volet **Related Devices**, cliquez sur le nom de l'agrégat hébergeur pour voir si l'agrégat peut accueillir un volume plus grand.
4. Sur la page de détails **Aggregate / Health**, vous constatez que l'agrégat hébergeant le volume plein dispose d'une capacité non allouée suffisante, vous utilisez donc ONTAP System Manager pour redimensionner le volume et lui attribuer une capacité supplémentaire.

Informations connexes

"Page de détails de l'événement"

Gérer les seuils de santé

Découvrez les seuils de santé de la capacité de stockage dans Active IQ Unified Manager

Un seuil d'intégrité de la capacité de stockage est le point auquel le serveur Unified Manager génère des événements pour signaler tout problème de capacité des objets de stockage. Vous pouvez configurer des alertes pour envoyer une notification chaque fois que de tels événements se produisent.

Les seuils de santé de la capacité de stockage pour tous les agrégats, volumes et qtrees sont définis sur leurs valeurs par défaut. Vous pouvez modifier ces paramètres selon les besoins d'un objet ou d'un groupe d'objets.

Configurer les paramètres globaux de seuil de santé

Configurez les paramètres de seuil de santé global dans Active IQ Unified Manager

Vous pouvez configurer des conditions de seuil d'état de santé globales pour la capacité, la croissance, la réserve Snapshot, les quotas et les inodes afin de surveiller efficacement la taille de votre agrégat, de votre volume et de votre qtree. Vous pouvez également modifier les paramètres de génération d'événements en cas de dépassement des seuils de décalage.

Les paramètres de seuil de santé globale s'appliquent à tous les objets auxquels ils sont associés, tels que les agrégats, les volumes, etc. Lorsqu'un seuil est franchi, 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 des valeurs recommandées, mais vous pouvez les modifier pour générer des événements à des intervalles adaptés à vos besoins spécifiques. Lorsque les seuils sont modifiés, des événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Les paramètres globaux de seuil de santé sont accessibles depuis la section « Seuils d'événements » du menu de navigation de gauche. Vous pouvez également modifier les paramètres de seuil pour chaque objet, depuis sa page d'inventaire ou sa page de détails.

- Pour plus d'informations, consultez "Configuration des valeurs de seuil globales de santé 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 de suivre tout dépassement de seuil.

- Pour plus d'informations, consultez "Configuration des valeurs de seuil globales de l'état de santé des volumes".

  Vous pouvez modifier les paramètres de seuil d'état pour la capacité, les copies Snapshot, les quotas qtree, la croissance du volume, l'espace de réserve d'écrasement et les inodes pour tous les volumes afin de suivre tout dépassement de seuil.

- Pour plus d'informations, consultez "Configuration des valeurs globales de seuil d'état des qtree".

  Vous pouvez modifier les paramètres de seuil de santé de la capacité pour tous les qtrees afin de détecter tout dépassement de seuil.

- Pour plus d'informations, consultez "Modification des paramètres de seuil d'intégrité du retard pour les relations de protection non gérées".

  Vous pouvez augmenter ou diminuer le pourcentage de délai d'avertissement ou d'erreur afin de générer des événements à des intervalles plus adaptés à vos besoins.

Configurez les valeurs seuils globales de santé agrégée dans Active IQ Unified Manager

Vous pouvez configurer des valeurs globales de seuils de santé pour tous les agrégats afin de suivre tout dépassement de seuil. Des événements appropriés sont générés en cas de dépassement de seuil, et vous pouvez prendre des mesures préventives en fonction de ces événements. Vous pouvez configurer ces valeurs globales en fonction des paramètres de bonne pratique pour les seuils qui s'appliquent à tous les agrégats surveillés.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous configurez les options globalement, les valeurs par défaut des objets sont modifiées. Cependant, si les valeurs par défaut ont été modifiées au niveau de l'objet, les valeurs globales restent inchangées.

Les options de seuil possèdent des valeurs par défaut pour une meilleure surveillance, toutefois, vous pouvez modifier ces valeurs en fonction des exigences de votre environnement.

Lorsque Autogrow est activé sur les volumes qui se trouvent sur l'agrégat, les seuils de capacité de l'agrégat sont considérés comme dépassés en fonction de la taille maximale du volume définie par autogrow, et non en fonction de la taille du volume d'origine.

Les valeurs de seuil d'état de santé ne s'appliquent pas à l'agrégat racine du nœud.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Seuils d'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"

Configurez les valeurs seuils de santé des volumes globaux dans Active IQ Unified Manager

Vous pouvez configurer les valeurs globales de seuil d'intégrité pour tous les volumes afin de suivre tout dépassement de seuil. Des événements appropriés sont générés en cas de dépassement des seuils d'intégrité, et vous pouvez prendre des mesures préventives en fonction de ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de bonne pratique pour les seuils qui s'appliquent à tous les volumes surveillés.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

La plupart des options de seuil possèdent des valeurs par défaut pour une meilleure surveillance. Vous pouvez toutefois les modifier en fonction des besoins de votre environnement.

Notez que lorsque Autogrow est activé sur un volume, les seuils de capacité sont considérés comme dépassés en fonction de la taille maximale du volume définie par Autogrow, et non en fonction de la taille du volume d'origine.

> La valeur par défaut de 1 000 copies Snapshot s'applique uniquement aux volumes FlexVol lorsque la version d'ONTAP est 9.4 ou ultérieure, et aux volumes FlexGroup lorsque la version d'ONTAP est 9.8 ou ultérieure. Pour les clusters installés avec des versions plus anciennes du logiciel ONTAP, le nombre maximal est de 250 copies Snapshot par volume. Pour ces versions plus anciennes, Unified Manager interprète ce nombre de 1 000 (et tout nombre compris entre 1 000 et 250) comme 250 ; cela signifie que vous continuerez à recevoir des événements lorsque le nombre de copies Snapshot atteindra 250. Si vous souhaitez définir ce seuil à une valeur inférieure à 250 pour ces versions plus anciennes, vous devez définir le seuil sur 250 ou moins ici, dans la vue Health: All Volumes, ou dans la page de détails Volume / Health.

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"

Configurez les valeurs de seuil de santé globales de qtree dans Active IQ Unified Manager

Vous pouvez configurer les valeurs de seuil d'intégrité globales pour tous les qtrees afin de suivre tout dépassement de seuil. Des événements appropriés sont générés en cas de dépassement des seuils d'intégrité, et vous pouvez prendre des mesures préventives en fonction de ces événements. Vous pouvez configurer les valeurs globales en fonction des paramètres de bonne pratique pour les seuils qui s'appliquent à tous les qtrees surveillés.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Les options de seuil possèdent des valeurs par défaut pour une meilleure surveillance, toutefois, vous pouvez modifier ces valeurs en fonction des exigences de votre environnement.

Des événements sont générés pour un qtree uniquement lorsqu'un quota Qtree ou un quota par défaut a été défini sur ce 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**.

Configurez les seuils de latence pour les relations de protection non gérées dans Active IQ Unified Manager

Vous pouvez modifier les paramètres globaux par défaut d'avertissement de retard et de seuil d'erreur d'intégrité pour les relations de protection non gérées afin que les événements soient générés à des intervalles adaptés à vos besoins.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Le délai de latence ne doit pas dépasser l'intervalle défini de la planification du transfert. Par exemple, si la planification du transfert est horaire, le délai de latence ne doit pas dépasser une heure. Le seuil de latence spécifie un pourcentage que le délai de latence ne doit pas dépasser. En reprenant l'exemple d'une heure, si le seuil de latence est défini à 150 %, vous recevrez un événement lorsque le délai de latence dépassera 1,5 heure.

Les paramètres décrits dans cette tâche s'appliquent globalement à toutes les relations de protection non gérées. Ils ne peuvent pas être spécifiés et appliqués exclusivement à une seule relation de protection non gérée.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Seuils d'événements** > **Relation**.
2. Augmentez ou diminuez, selon les besoins, le pourcentage global par défaut du délai des avertissements ou des erreurs.
3. Pour empêcher le déclenchement d'un avertissement ou d'une erreur, quel que soit le seuil de décalage, décochez la case en regard de **Enabled**.
4. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Modifiez les paramètres de seuil de santé des agrégats individuels dans Active IQ Unified Manager

Vous pouvez modifier les paramètres de seuil d'intégrité pour la capacité, la croissance et les copies Snapshot d'un ou de plusieurs agrégats. Lorsqu'un seuil est franchi, des alertes sont générées et vous recevez des notifications. Ces notifications vous aident à prendre des mesures préventives en fonction de l'événement généré.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

En fonction des modifications apportées aux valeurs de seuil, des événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Lorsque Autogrow est activé sur les volumes qui se trouvent sur l'agrégat, les seuils de capacité de l'agrégat sont considérés comme dépassés en fonction de la taille maximale du volume définie par autogrow, et non en fonction de la taille du volume d'origine.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Dans la vue **Santé: Tous les agrégats**, sélectionnez un ou plusieurs agrégats, puis cliquez sur **Modifier les seuils**.
3. Dans la boîte de dialogue **Modifier les seuils d'agrégat**, modifiez les paramètres de seuil de l'un des éléments suivants : la capacité, la croissance ou les copies Snapshot, en sélectionnant la case à cocher appropriée puis en modifiant les paramètres.
4. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Modifiez les paramètres de seuil de santé du volume individuel dans Active IQ Unified Manager

Vous pouvez modifier les paramètres de seuil d'état de santé relatifs à la capacité, à la croissance, au quota et à 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 permettent de prendre des mesures préventives en fonction de l'événement généré.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

En fonction des modifications apportées aux valeurs de seuil, des événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Notez que lorsque Autogrow est activé sur un volume, les seuils de capacité sont considérés comme dépassés en fonction de la taille maximale du volume définie par Autogrow, et non en fonction de la taille du volume d'origine.

> La valeur par défaut de 1 000 copies Snapshot s'applique uniquement aux volumes FlexVol lorsque la version d'ONTAP est 9.4 ou ultérieure, et aux volumes FlexGroup lorsque la version d'ONTAP est 9.8 ou ultérieure. Pour les clusters installés avec des versions plus anciennes du logiciel ONTAP, le nombre maximal est de 250 copies Snapshot par volume. Pour ces versions plus anciennes, Unified Manager interprète ce nombre de 1 000 (et tout nombre compris entre 1 000 et 250) comme 250 ; cela signifie que vous continuerez à recevoir des événements lorsque le nombre de copies Snapshot atteindra 250. Si vous souhaitez définir ce seuil à une valeur inférieure à 250 pour ces versions plus anciennes, vous devez définir le seuil sur 250 ou moins ici, dans la vue Health: All Volumes, ou dans la page de détails Volume / Health.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans la vue **Santé: Tous les volumes**, sélectionnez un ou plusieurs volumes puis cliquez sur **Modifier les seuils**.
3. Dans la boîte de dialogue **Modifier les seuils de volume**, modifiez les paramètres de seuil de l'un des éléments suivants : capacité, copies Snapshot, quota qtree, croissance ou inodes, en sélectionnant la case à cocher appropriée, puis en modifiant les paramètres.
4. Cliquez sur **Enregistrer**.

Informations connexes

"Ajout d'utilisateurs"

Modifiez les paramètres de seuil de santé individuels des qtrees dans Active IQ Unified Manager

Vous pouvez modifier les paramètres de seuil de santé pour la capacité d'un ou de plusieurs qtrees. Lorsqu'un seuil est franchi, des alertes sont générées et vous recevez des notifications. Ces notifications vous aident à prendre des mesures préventives en fonction de l'événement généré.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

En fonction des modifications apportées aux valeurs de seuil, des événements sont générés ou rendus obsolètes lors du prochain cycle de surveillance.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Qtrees**.
2. Dans la vue **Capacité : Tous les Qtrees**, sélectionnez un ou plusieurs qtrees, puis cliquez sur **Modifier les seuils**.
3. Dans la boîte de dialogue **Modifier les seuils Qtree**, modifiez les seuils de capacité pour le ou les qtrees sélectionnés et cliquez sur **Enregistrer**.

Vous pouvez également définir des seuils qtree individuels à partir de l'onglet Qtrees de la page de détails Storage VM / Health.

Gérer les objectifs de sécurité du cluster

Gérer les objectifs de sécurité du cluster dans Active IQ Unified Manager

Unified Manager fournit un tableau de bord qui identifie le niveau de sécurité de vos clusters ONTAP, de vos machines virtuelles de stockage (SVM) et de vos volumes, en fonction des recommandations définies dans le *NetApp Security Hardening Guide for ONTAP 9*.

Le tableau de bord de sécurité a pour objectif de montrer les domaines dans lesquels vos clusters ONTAP ne sont pas conformes aux recommandations de NetApp, afin que vous puissiez corriger ces problèmes potentiels. Dans la plupart des cas, vous corrigerez les problèmes à l'aide de ONTAP System Manager ou de ONTAP CLI. Votre organisation ne suit peut-être pas toutes les recommandations, donc, dans certains cas, vous n'aurez pas besoin d'apporter de modifications.

Voir le "NetApp Guide de renforcement de la sécurité pour ONTAP 9" (TR-4569) pour des recommandations et des résolutions détaillées.

Outre le signalement de 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 Event Management, et configurer des alertes afin que votre administrateur du stockage soit notifié lorsque de nouveaux événements de sécurité se produisent.

Pour plus d'informations, consultez "Quels critères de sécurité sont évalués".

Quels critères de sécurité sont évalués

Comprendre comment Active IQ Unified Manager évalue les critères de sécurité

En général, les critères de sécurité de vos clusters ONTAP, de vos machines virtuelles de stockage (SVM) et de vos volumes sont évalués en fonction des recommandations définies dans le *NetApp Security Hardening Guide for ONTAP 9*.

Voici quelques exemples de contrôles de sécurité :

- si un cluster utilise une méthode d'authentification sécurisée, telle que SAML
- si les communications entre les clusters appariés sont chiffrées
- vérifier si une VM de stockage a son journal des audits activé
- si le chiffrement logiciel ou matériel est activé sur vos volumes

Consultez les rubriques relatives aux catégories de conformité et le "NetApp Guide de renforcement de la sécurité pour ONTAP 9" pour obtenir des informations détaillées.

> Les événements de mise à niveau signalés par la plateforme Active IQ sont également considérés comme des événements de sécurité. Ces événements identifient des problèmes dont la résolution vous oblige à mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les avis de sécurité). Ces événements ne s'affichent pas dans le panneau Security, mais ils sont disponibles depuis la page d'inventaire Event Management.

Pour plus d'informations, consultez "Gestion des objectifs de sécurité du cluster".

Comprendre les catégories de conformité des clusters dans Active IQ Unified Manager

Ce tableau décrit les paramètres de conformité de sécurité du cluster évalués par Unified Manager, la recommandation de NetApp et indique si le paramètre influe sur la détermination globale de la conformité ou non-conformité du cluster.

La présence de SVM non conformes au sein d'un cluster affectera le niveau de conformité de ce dernier. Il peut donc être nécessaire, dans certains cas, de corriger une faille de sécurité liée à une SVM avant que la sécurité du cluster ne soit considérée comme conforme.

Notez que tous les paramètres répertoriés ci-dessous n'apparaissent pas pour toutes les installations. Par exemple, si vous n'avez aucun cluster apparié, ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments « Appairage de clusters » ou « Transport HTTPS de AutoSupport » dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Affecte 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 TLSv1.1 et TLSv1.2 sont autorisés.	Activé	Oui
Telnet	Indique si l'accès Telnet au système est activé ou désactivé. NetApp recommande Secure Shell (SSH) pour un accès distant sécurisé.	Désactivées	Oui
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Non	Oui
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs accédant au système.	Activé	Oui
Interconnexion de clusters	Indique si la communication entre les clusters appariés est chiffrée ou non chiffrée. Le chiffrement doit être configuré sur les clusters source et de destination pour que ce paramètre soit considéré comme conforme.	Chiffré	Oui
Protocole de temps réseau	Indique si le cluster possède un ou plusieurs serveurs NTP configurés. Pour une redondance et un service optimaux, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	configuré	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
OCSP	À partir de la version 9.14.1, Active IQ Unified Manager fournit des informations d'état OCSP (Online Certificate Status Protocol) au niveau de la machine virtuelle de stockage (SVM, anciennement appelée Vserver). Cela signifie que la validation OCSP est appliquée à toutes les connexions SSL/TLS établies avec la SVM et garantit l'intégrité et la validité des certificats utilisés dans ces connexions.	Activé	Non
Journalisation des audits à distance	Indique si le transfert des journaux (Syslog) est chiffré ou non chiffré.	Chiffré	Oui
Transport HTTPS AutoSupport	Indique si HTTPS est utilisé comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.	Activé	Oui
Utilisateur administrateur par défaut	Indique si l'utilisateur administrateur par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tout compte intégré inutile.	Désactivées	Oui
Utilisateurs SAML	Indique si SAML est configuré. SAML vous permet de configurer l'authentification multifacteur (MFA) comme méthode de connexion pour l'authentification unique.	Non	Non

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Utilisateurs Active Directory	Indique si Active Directory est configuré. Active Directory et LDAP sont les mécanismes d'authentification privilégiés pour les utilisateurs accédant aux clusters.	Non	Non
Utilisateurs LDAP	Indique si LDAP est configuré. Active Directory et LDAP sont les mécanismes d'authentification privilégiés pour les utilisateurs gérant des clusters par rapport aux utilisateurs locaux.	Non	Non
Utilisateurs de certificats	Indique si un utilisateur disposant d'un certificat est configuré pour se connecter au cluster.	Non	Non
Utilisateurs locaux	Indique si les utilisateurs locaux sont configurés pour se connecter au cluster.	Non	Non
Shell à distance	Indique si le protocole RSH est activé. Pour des raisons de sécurité, il est recommandé de désactiver RSH. L'utilisation de Secure Shell (SSH) est préférable pour un accès distant sécurisé.	Désactivées	Oui
MD5 en cours d'utilisation	Indique si les comptes utilisateurs ONTAP utilisent la fonction de hachage MD5 moins sécurisée. Il est recommandé de migrer les comptes utilisateurs utilisant le hachage MD5 vers une fonction de hachage cryptographique plus sécurisée, telle que SHA-512.	Non	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Type d'émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé par CA	Non

Comprendre les catégories de conformité des machines virtuelles de stockage dans Active IQ Unified Manager

Ce tableau décrit les critères de conformité de sécurité des machines virtuelles de stockage (SVM) qu'Unified Manager évalue, la recommandation de NetApp, et indique si le paramètre affecte la détermination globale de la conformité ou non de la SVM.

Paramètre	Description	Recommandation	Affecte la conformité de la 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 accédant aux SVMs sur le système.	Activé	Oui
Chiffrement 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
Signature de la charge utile LDAP	Indique si LDAP Payload Signing est activé ou désactivé.	Activé	Non
Paramètres CHAP	Indique si CHAP est activé ou désactivé.	Activé	Non
Kerberos V5	Indique si l'authentification Kerberos V5 est activée ou désactivée.	Activé	Non
Authentification NIS	Indique si l'utilisation de l'authentification NIS est configurée.	Désactivées	Non
Statut FPolicy actif	Indique si FPolicy est créé ou non.	Oui	Non

Paramètre	Description	Recommandation	Affecte la conformité de la SVM
Chiffrement SMB activé	Indique si SMB -Signing & Sealing n'est pas activé.	Oui	Non
Signature SMB activée	Indique si SMB -Signing n'est pas activé.	Oui	Non

Comprendre les catégories de conformité des volumes dans Active IQ Unified Manager

Ce tableau décrit les paramètres de chiffrement des volumes que Unified Manager évalue pour déterminer si les données de vos volumes sont suffisamment protégées contre l'accès par des utilisateurs non autorisés.

Notez que les paramètres de chiffrement du volume n'ont aucune incidence sur la conformité du cluster ou de la machine virtuelle de stockage.

Paramètre	Description
Chiffré par logiciel	Affiche le nombre de volumes protégés à l'aide des solutions de chiffrement logiciel 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).
Logiciels et matériels chiffrés	Affiche le nombre de volumes protégés à la fois par le chiffrement logiciel et matériel.
Non chiffré	Affiche le nombre de volumes non chiffrés.

Découvrez l'état de conformité des clusters et des SVM dans Active IQ Unified Manager

Les clusters et les machines virtuelles de stockage (SVM) sont considérés comme non conformes lorsqu'un des critères de sécurité évalués par rapport aux recommandations définies dans le *NetApp Security Hardening Guide for ONTAP 9* n'est pas respecté. De plus, un cluster est considéré comme non conforme lorsqu'une SVM est signalée comme non conforme.

Les icônes d'état figurant sur les cartes de sécurité ont les significations suivantes en matière de conformité :

- - Le paramètre est configuré comme recommandé.
- - Ce 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 n'a aucune incidence sur le fait que le cluster ou la SVM soient considérés comme conformes.

Consultez l'état de sécurité des clusters et des Storage VMs dans Active IQ Unified Manager

Active IQ Unified Manager vous permet de visualiser l'état de sécurité des objets de stockage de votre environnement depuis différents points de l'interface. Vous pouvez collecter et analyser des informations et des rapports en fonction de paramètres définis, et détecter les comportements suspects ou les modifications système non autorisées sur les clusters et les machines virtuelles de stockage surveillés.

Pour les recommandations de sécurité, consultez le "NetApp Guide de renforcement de la sécurité pour ONTAP 9"

Consultez l'état de sécurité au niveau de l'objet sur la page Sécurité

En tant qu'administrateur système, vous pouvez utiliser la page **Sécurité** pour obtenir une visibilité sur le niveau de sécurité de vos clusters ONTAP et de vos machines virtuelles de stockage aux niveaux du centre de données et du site. Les objets pris en charge sont les clusters, les machines virtuelles de stockage et les volumes. Procédez comme suit :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. Selon que vous souhaitiez 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 vers la droite dans le panneau **Sécurité**. La page Sécurité s'affiche.

Lorsque vous cliquez sur les graphiques à barres, les décomptes et les `View Reports` liens, vous êtes redirigé vers la page Volumes, Clusters ou Storage VMs afin de consulter les détails correspondants ou de générer des rapports, selon vos besoins.

La page Sécurité affiche les panneaux suivants :

- **Conformité des clusters** : état de sécurité (nombre de clusters conformes ou non conformes) de tous les clusters d'un centre de données
- **Conformité des machines virtuelles de stockage** : état de sécurité (nombre de machines virtuelles de stockage conformes ou non conformes) de toutes les machines virtuelles de stockage de votre centre de données
- **Chiffrement des volumes** : état du chiffrement des volumes (nombre de volumes chiffrés ou non chiffrés) de tous les volumes de votre environnement
- **État de la protection anti-ransomware des volumes** : état de sécurité (nombre de volumes avec protection anti-ransomware activée ou désactivée) de tous les volumes de votre environnement
- **Authentification et certificats des clusters** : le nombre de clusters utilisant chaque type de méthode d'authentification, comme SAML, Active Directory, ou via des certificats et l'authentification locale. Le panneau affiche également le nombre de clusters dont les certificats ont expiré ou vont expirer dans 60 jours.

Consultez les détails de sécurité de tous les clusters sur la page Clusters

La page de détails **Clusters / Sécurité** vous permet de consulter l'état de conformité en matière 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**.

Les paramètres de sécurité par défaut, tels que Global FIPS, Telnet, les paramètres SSH non sécurisés, la bannière de connexion, le protocole NTP, AutoSupport HTTPS Transport et l'état d'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 **Security** de Unified Manager ou dans System Manager. Vous devez disposer d'identifiants valides pour consulter ces détails dans System Manager.

ⓘ Si le certificat d'un cluster a expiré, vous pouvez cliquer `expired` sous **Validité du certificat du cluster** et le renouveler depuis System Manager (9.10.1 et versions ultérieures). Vous ne pouvez pas cliquer `expired` si l'instance de System Manager exécute une version antérieure à 9.10.1.

Consultez les détails de sécurité de tous les clusters depuis la page des machines virtuelles de stockage

La page de détails **VM de stockage / Sécurité** vous permet de consulter l'état de conformité de sécurité au niveau d'une VM de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.
2. Sélectionnez **Affichage > Sécurité > Toutes les VM de stockage**. Une liste des clusters avec les paramètres de sécurité s'affiche.

Vous pouvez obtenir une vue par défaut de la conformité de sécurité des machines virtuelles de stockage en vérifiant les paramètres de sécurité, tels que les machines virtuelles de stockage, le cluster, la bannière de connexion, le journal des audits 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 **Security** de Unified Manager ou dans System Manager. Vous devez disposer d'identifiants valides pour consulter ces détails dans System Manager.

Pour plus de détails sur la sécurité anti-ransomware des volumes et des machines virtuelles de stockage, voir "Affichage de l'état de protection anti-ransomware de tous les volumes et machines virtuelles de stockage".

Consultez les événements de sécurité susceptibles de nécessiter des mises à jour logicielles ou micrologicielles dans Active IQ Unified Manager

Certains événements de sécurité ont une zone d'impact de "Upgrade". Ces événements sont signalés par la plateforme Active IQ et identifient des problèmes dont la résolution nécessite que vous mettiez à niveau le logiciel ONTAP, le microprogramme du nœud ou le logiciel du système d'exploitation (pour les avis de sécurité).

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez prendre immédiatement des mesures correctives pour certains de ces problèmes, tandis que d'autres peuvent attendre votre prochaine maintenance planifiée. Vous pouvez consulter tous ces événements et les attribuer à des utilisateurs capables de résoudre les problèmes. De plus, s'il existe certains événements de mise à niveau de sécurité pour lesquels vous ne souhaitez pas recevoir de notification, cette liste peut vous

aider à identifier ces événements afin que vous puissiez les désactiver.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

   Par défaut, tous les événements actifs (nouveaux et acquittés) s'affichent sur la page d'inventaire de gestion des événements.

2. Dans le menu Affichage, sélectionnez **Événements de mise à niveau**.

   Cette page affiche tous les événements de sécurité de mise à niveau actifs.

Découvrez comment les clusters gèrent l'authentification des utilisateurs sur tous les clusters dans Active IQ Unified Manager

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 en utilisant chaque type. Cela vous permet de vérifier que l'authentification des utilisateurs est effectuée de manière sécurisée, conformément aux exigences de votre organisation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. En haut du tableau de bord, sélectionnez **Tous les clusters** dans le menu déroulant.
3. Cliquez sur la flèche vers la droite dans le panneau **Sécurité** pour afficher la page **Sécurité**.
4. Consultez la carte **Authentification du cluster** pour voir le nombre d'utilisateurs qui accèdent au système avec chaque type d'authentification.
5. Consultez la carte **Cluster Security** pour voir les mécanismes d'authentification utilisés pour authentifier les utilisateurs sur chaque cluster.

Si certains utilisateurs accèdent au système à l'aide d'une méthode non sécurisée ou d'une méthode non recommandée par NetApp, vous pouvez désactiver cette méthode.

Affichez l'état de chiffrement de tous les volumes dans Active IQ Unified Manager

Vous pouvez consulter la liste de tous les volumes et leur état de chiffrement actuel afin de déterminer si les données de vos volumes sont suffisamment protégées contre l'accès par des utilisateurs non autorisés.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Les types de chiffrement pouvant être appliqués à un volume sont :

- Logiciel - Volumes protégés à l'aide des solutions de chiffrement logiciel NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
- Matériel - Volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
- Logiciel et matériel - Volumes protégés par un chiffrement à la fois logiciel et matériel.
- Aucun - Volumes non chiffrés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **Chiffrement des volumes**
3. Dans la vue **Santé : Chiffrement des volumes**, triez sur le champ **Type de chiffrement** ou utilisez le filtre pour afficher les volumes qui ont un type de chiffrement spécifique ou qui ne sont pas chiffrés (Type de chiffrement « `None` »).

Consultez l'état de protection anti-ransomware de tous les volumes et machines virtuelles de stockage dans Active IQ Unified Manager

Vous pouvez consulter la liste de tous les volumes et machines virtuelles de stockage (SVM), ainsi que leur état actuel de protection anti-ransomware, afin de déterminer si les données de vos volumes et SVM sont correctement protégées contre les attaques de ransomware.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Pour plus d'informations sur les différents statuts anti-ransomware, voir "ONTAP: Activer la protection anti-ransomware".

Consultez les détails de sécurité de tous les volumes dotés d'une détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **Sécurité** > **Anti-ransomware**
3. Dans la vue **Sécurité : Anti-ransomware**, vous pouvez trier selon différents champs ou utiliser le filtre.

> La protection anti-ransomware n'est pas prise en charge pour les volumes hors ligne, les volumes restreints, les volumes SnapLock, les volumes FlexGroup, les volumes FlexCache, les volumes SAN uniquement, les volumes des machines virtuelles de stockage arrêtées, les volumes racine des machines virtuelles de stockage ou les volumes de protection des données.

Consultez les détails de sécurité de toutes les machines virtuelles de stockage dotées d'une détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.
2. Sélectionnez **Affichage > Sécurité > Anti-ransomware**. Une liste des SVM avec leur statut anti-ransomware s'affiche.

> La surveillance anti-ransomware n'est pas prise en charge sur les machines virtuelles de stockage dont le protocole NAS n'est pas activé.

Consultez tous les événements de sécurité actifs dans Active IQ Unified Manager

Vous pouvez consulter tous les événements de sécurité actifs et attribuer chacun d'eux à un utilisateur capable de résoudre le problème. De plus, s'il existe certains événements de sécurité que vous ne souhaitez pas recevoir, cette liste peut vous aider à identifier les

événements que vous souhaitez désactiver.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

   Par défaut, les événements New et Acknowledged sont affichés sur la page d'inventaire Event Management.

2. Dans le menu Affichage, sélectionnez **Événements de sécurité actifs**.

   Cette page affiche tous les événements de sécurité nouveaux et reconnus générés au cours des 7 derniers jours.

Ajoutez des alertes pour les événements de sécurité dans Active IQ Unified Manager

Vous pouvez configurer des alertes pour des événements de sécurité individuels, comme pour tout autre événement reçu par Unified Manager. De plus, si vous souhaitez traiter tous les événements de sécurité de la même manière et envoyer un e-mail à la même personne, vous pouvez créer une alerte unique qui vous notifiera lorsque des événements de sécurité sont déclenchés.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

L'exemple ci-dessous montre comment créer une alerte pour l'événement de sécurité « `Telnet Protocol Enabled` ». Cela enverra une alerte si l'accès Telnet est configuré pour l'administration à distance du cluster. Vous pouvez utiliser cette même méthode pour créer des alertes pour tous les événements de sécurité.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et sélectionnez le ou les clusters sur lesquels vous souhaitez activer cette alerte.
5. Cliquez sur **Événements** et effectuez les actions suivantes :
   a. Dans la liste Gravité de l'événement, sélectionnez **Avertissement**.
   b. Dans la liste des événements correspondants, sélectionnez **Protocole Telnet activé**.
6. Cliquez sur **Actions**, puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
7. Configurez les autres options sur cette page concernant la fréquence des notifications, l'émission de traps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Désactiver certains événements de sécurité dans Active IQ Unified Manager

Tous les événements sont activés par défaut. Vous pouvez désactiver certains événements pour éviter la génération de notifications concernant ceux qui ne sont pas importants dans votre environnement. Vous pouvez réactiver les événements désactivés si vous souhaitez à nouveau recevoir des notifications les concernant.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous désactivez des événements, ceux précédemment générés dans le système sont marqués comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications pour ces événements sont générées à partir du prochain cycle de surveillance.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration de l'événement**.
2. Dans la page de configuration **Event**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Si vous voulez…	Ensuite, faites ceci…
Désactiver les événements	a. Cliquez sur **Disable**. b. Dans la boîte de dialogue Désactiver les événements, sélectionnez le niveau de gravité **Avertissement**. Il s'agit de la catégorie de tous les événements de sécurité. c. Dans la colonne Événements correspondants, sélectionnez les événements de sécurité que vous souhaitez désactiver, puis cliquez sur la flèche vers la droite pour déplacer ces événements vers la colonne Désactiver les événements. d. Cliquez sur **Enregistrer et fermer**. e. Vérifiez que les événements que vous avez désactivés apparaissent dans la vue de liste de la page Configuration des événements.
Activer les événements	a. Dans la liste des événements désactivés, cochez la case à cocher correspondant à l'événement ou aux événements que vous souhaitez réactiver. b. Cliquez sur **Enable**.

Consultez les événements de sécurité dans Active IQ Unified Manager

Les événements de sécurité vous fournissent des informations sur l'état de sécurité des clusters ONTAP, des machines virtuelles de stockage (SVM) et des volumes, en fonction des paramètres définis dans le *Guide de renforcement de la sécurité NetApp pour*

ONTAP 9. Ces événements vous signalent les problèmes potentiels afin que vous puissiez en évaluer la gravité et les corriger si nécessaire.

Les événements de sécurité sont regroupés par type de source et comprennent le nom de l'événement et du trap, le niveau d'impact et la gravité. Ces événements apparaissent dans les catégories d'événements du cluster et des VM de stockage.

Gérer les opérations de sauvegarde et de restauration

Gérez les opérations de sauvegarde et de restauration dans Active IQ Unified Manager

Vous pouvez créer des sauvegardes d'Active IQ Unified Manager et utiliser la fonctionnalité de restauration pour restaurer la sauvegarde sur le même système (local) ou sur un nouveau système (distant) en cas de panne du système ou de perte de données.

Il existe trois méthodes de sauvegarde et de restauration selon le système d'exploitation sur lequel Unified Manager est installé et le nombre de clusters et de nœuds gérés :

Système d'exploitation	Taille du déploiement	Méthode de sauvegarde recommandée
VMware vSphere	N'importe lequel	Instantané VMware de l'appliance virtuelle Unified Manager
Red Hat Enterprise Linux	Petit	Sauvegarde de la base de données MySQL de Unified Manager
	Grand	NetApp Instantané de la base de données Unified Manager
Microsoft Windows	Petit	Sauvegarde de la base de données MySQL de Unified Manager
	Grand	NetApp Instantané de la base de données Unified Manager avec le protocole iSCSI

Ces différentes méthodes sont décrites dans les sections suivantes.

Sauvegarde et restauration d'Active IQ Unified Manager sur une appliance virtuelle

Le modèle de sauvegarde et de restauration d'Unified Manager, lorsqu'il est installé sur une appliance virtuelle, consiste à capturer et à restaurer une image de l'application virtuelle complète.

Les tâches suivantes vous permettent d'effectuer une sauvegarde de l'appliance virtuelle :

1. Mettez la machine virtuelle hors tension et prenez un instantané VMware de l'appliance virtuelle Unified Manager.
2. Créez une NetApp copie Snapshot sur la banque de données pour capturer l'instantané VMware.

   Si la banque de données n'est pas hébergée sur un système exécutant le logiciel ONTAP, suivez les instructions du fournisseur de stockage pour créer une sauvegarde de l'instantané VMware.

3. Répliquez la copie Snapshot NetApp, ou son équivalent, sur un support de stockage alternatif.
4. Supprimez l'instantané VMware.

Vous devez mettre en place un plan de sauvegarde à l'aide de ces tâches afin de garantir la protection de l'appliance virtuelle Unified Manager en cas de problème.

Pour restaurer la machine virtuelle, vous pouvez utiliser l'instantané VMware que vous avez créé pour la restaurer à l'état correspondant au point de sauvegarde.

Sauvegarde et restauration à l'aide d'une sauvegarde de base de données MySQL

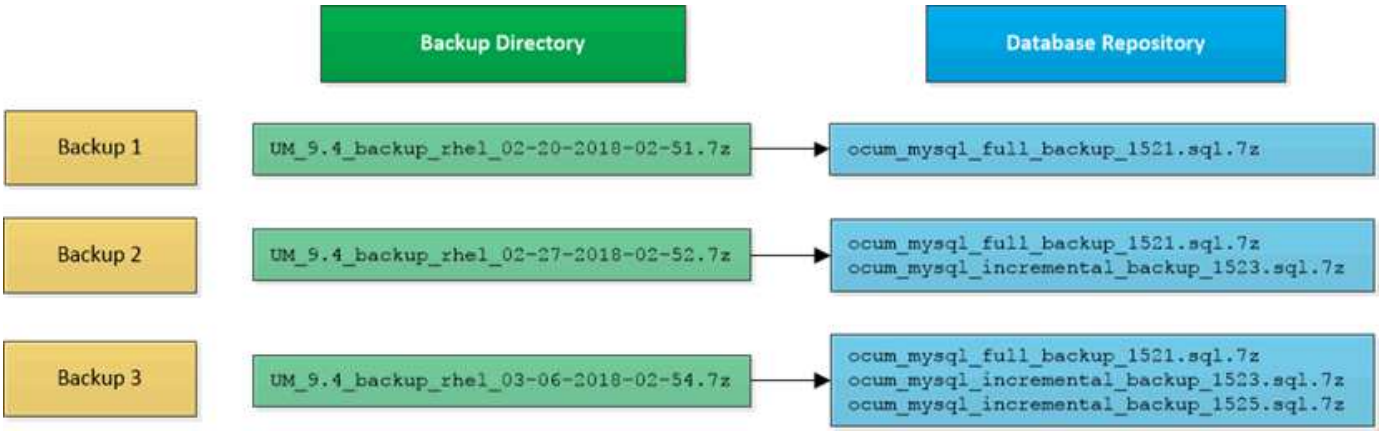
Sauvegarde et restauration à l'aide d'un dump de base de données MySQL dans Active IQ Unified Manager

Une sauvegarde par export de la base de données MySQL est une copie de la base de données et des fichiers de configuration d'Active IQ Unified Manager que vous pouvez utiliser en cas de panne du système ou de perte de données. Vous pouvez planifier l'écriture d'une sauvegarde vers un emplacement local ou distant. Il est fortement recommandé de définir un emplacement distant externe au système hôte Active IQ Unified Manager.

La sauvegarde de la base de données MySQL est le mécanisme de sauvegarde par défaut lorsque Unified Manager est installé sur un serveur Linux ou Windows. Toutefois, si Unified Manager gère un grand nombre de clusters et de nœuds, ou si vos sauvegardes MySQL prennent plusieurs heures, vous pouvez effectuer la sauvegarde à l'aide de copies Snapshot. Cette fonctionnalité est disponible sur Red Hat Enterprise Linux et Windows.

Une sauvegarde de vidage de base de données se compose d'un seul fichier dans le répertoire de sauvegarde et d'un ou plusieurs fichiers dans le répertoire du référentiel de base de données. Le fichier dans le répertoire de sauvegarde est très petit, car il 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 fichier unique est créé dans le répertoire de sauvegarde et un fichier de sauvegarde complète est créé dans le répertoire du référentiel de base de données. La fois suivante que vous générez une sauvegarde, un fichier unique est créé dans le répertoire de sauvegarde et un fichier de sauvegarde incrémentielle est créé dans le répertoire du référentiel de base de données, contenant les différences par rapport au fichier de sauvegarde complète. Ce processus se poursuit à mesure que vous créez des sauvegardes supplémentaires, jusqu'au paramètre de rétention maximal, comme illustré dans la figure suivante.



Ne renommez ni ne supprimez aucun des fichiers de sauvegarde dans ces deux répertoires, sinon toute opération de restauration ultérieure échouera.

Si vous enregistrez vos fichiers de sauvegarde sur le système local, vous devriez lancer un processus de copie de ces fichiers vers un emplacement distant afin qu'ils soient disponibles en cas de problème système nécessitant une restauration complète.

Avant de lancer une opération de sauvegarde, Active IQ Unified Manager effectue un contrôle d'intégrité pour vérifier que tous les fichiers et répertoires de sauvegarde requis existent et sont accessibles en écriture. Il vérifie également que l'espace disponible sur le système est suffisant pour créer le fichier de sauvegarde.

Configurez les paramètres de sauvegarde de la base de données dans Active IQ Unified Manager

Vous pouvez configurer les paramètres de sauvegarde du vidage de la base de données Unified Manager afin de définir le chemin de sauvegarde de la base de données, le nombre de rétentions et la planification des sauvegardes. Vous pouvez activer des sauvegardes planifiées quotidiennes ou hebdomadaires. Par défaut, les sauvegardes planifiées sont désactivées, mais vous devez définir une planification des sauvegardes.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous devez disposer d'un minimum de 150 Go d'espace disponible à l'emplacement que vous définissez comme chemin de sauvegarde.

  Il est recommandé d'utiliser un emplacement distant externe au système hôte Unified Manager.

- Lorsque Unified Manager est installé sur un système Linux et utilise une sauvegarde MySQL, assurez-vous que les autorisations et les propriétaires suivants sont définis sur le répertoire de sauvegarde.

  Autorisations : 0750, Propriétaire : jboss:maintenance

- Lorsqu'Unified Manager est installé sur un système Windows et utilise une sauvegarde MySQL, assurez-vous que seul l'administrateur a accès au répertoire de sauvegarde.

La première sauvegarde prend plus de temps que les suivantes, car il s'agit d'une sauvegarde complète. Une sauvegarde complète peut dépasser 1 Go et durer de trois à quatre heures. Les sauvegardes suivantes sont incrémentales et requièrent moins de temps.

- Si le nombre de fichiers de sauvegarde incrémentielle est trop important par rapport à l'espace alloué aux sauvegardes, vous pouvez effectuer une sauvegarde complète régulièrement pour remplacer l'ancienne sauvegarde et ses fichiers incrémentiels. Vous pouvez également effectuer une sauvegarde à l'aide de copies Snapshot.
- Les sauvegardes effectuées pendant les 15 premiers jours suivant l'ajout d'un nouveau cluster peuvent ne pas être suffisamment précises pour obtenir les données de performance historiques.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Sauvegarde de la base de données**.
2. Sur la page **Sauvegarde de la base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Configurez les valeurs appropriées pour un chemin de sauvegarde, un nombre de sauvegardes à

conserver et une planification.

La valeur par défaut du nombre de sauvegardes à conserver est de 10 ; vous pouvez utiliser 0 pour créer un nombre illimité de sauvegardes.

4. Sélectionnez le bouton **Planifié quotidiennement** ou **Planifié hebdomadairement**, puis spécifiez les détails de la planification.
5. Cliquez sur **Appliquer**.

Les fichiers de sauvegarde de la base de données sont créés selon la planification. Vous pouvez consulter les fichiers de sauvegarde disponibles sur la page Sauvegarde de la base de données.

Découvrez la restauration de base de données dans Active IQ Unified Manager

La restauration d'une base de données MySQL consiste à restaurer un fichier de sauvegarde Unified Manager existant sur le même serveur Unified Manager ou sur un autre serveur Unified Manager. Vous effectuez l'opération de restauration depuis la console de maintenance de Unified Manager.

Si vous effectuez une opération de restauration sur le même système (local) et que tous les fichiers de sauvegarde sont stockés localement, vous pouvez exécuter l'option de restauration en utilisant l'emplacement par défaut. Si vous effectuez une opération de restauration sur un autre système Unified Manager (un système distant), vous devez copier le ou les fichiers de sauvegarde depuis le stockage secondaire vers le disque local avant d'utiliser l'option de restauration.

Pendant le processus de restauration, vous êtes déconnecté d'Unified Manager. Vous pouvez vous connecter au système une fois le processus de restauration terminé.

Si vous restaurez l'image de sauvegarde sur un nouveau serveur, vous devrez générer un nouveau certificat de sécurité HTTPS et redémarrer le serveur Unified Manager une fois la restauration terminée. Vous devrez également reconfigurer les paramètres d'authentification SAML, le cas échéant, 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. Afin de libérer de l'espace, tous les anciens fichiers de sauvegarde, à l'exception du plus récent, sont automatiquement supprimés lors de la mise à niveau d'Unified Manager.

Informations connexes

"Génération d'un certificat de sécurité HTTPS"

"Activation de l'authentification SAML"

"Authentification via Active Directory ou OpenLDAP"

Restaurez une sauvegarde de base de données MySQL sur un système Linux dans Active IQ Unified Manager

En cas de perte de données ou de corruption des données, vous pouvez restaurer Unified Manager à son état stable précédent avec une perte de données minimale. Vous pouvez restaurer la base de données Unified Manager sur un système Red Hat Enterprise Linux local ou distant à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez disposer des identifiants de l'utilisateur root pour l'hôte Linux sur lequel Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez 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 effectuerez 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 sous-répertoire `/database-dumps-repo` du répertoire `/ocum-backup`.

- Les fichiers de sauvegarde doivent être de `.7z` type.

La fonction de restauration est spécifique à la plateforme et à la version. Vous ne pouvez restaurer une sauvegarde Unified Manager 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.



Si le nom du dossier de sauvegarde contient un espace, vous devez inclure le chemin absolu ou relatif entre guillemets doubles.

Étapes

1. Si vous effectuez une restauration sur un nouveau serveur, après l'installation d'Unified Manager, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification lorsque l'installation est terminée. Le fichier de sauvegarde renseignera ces informations lors de la restauration.
2. Utilisez Secure Shell pour vous connecter à l'adresse IP ou au nom de domaine complet du système Unified Manager.
3. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de l'utilisateur de maintenance (umadmin).
4. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
5. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarde et restauration**.
6. Saisissez le numéro de **Restore MySQL Backup**.
7. Lorsque vous y êtes invité, saisissez le chemin d'accès 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 pourrez vous connecter à Unified Manager.

Après avoir restauré la sauvegarde, si le serveur OnCommand Workflow Automation ne fonctionne pas, procédez comme suit :

1. Sur le serveur Workflow Automation, modifiez l'adresse IP du serveur Unified Manager pour qu'elle pointe vers la machine la plus récente.

2. Sur le serveur Unified Manager, réinitialisez le mot de passe de la base de données si l'acquisition échoue à l'étape 1.

Restaurez une sauvegarde de base de données MySQL sous Windows dans Active IQ Unified Manager

En cas de perte de données ou de corruption des données, vous pouvez utiliser la fonction de restauration pour rétablir Unified Manager dans son état stable précédent avec une perte minimale. Vous pouvez restaurer la base de données MySQL de Unified Manager sur un système Windows local ou un système Windows distant à l'aide de la console de maintenance de Unified Manager.

Avant de commencer

- 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 effectuerez l'opération de restauration.

  Il est recommandé de copier le fichier de sauvegarde dans le répertoire par défaut `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. Les fichiers du référentiel de base de données doivent être copiés dans le `\database_dumps_repo`sous-répertoire du répertoire `\backup`.

- Les fichiers de sauvegarde doivent être de `.7z` type.

La fonction de restauration est spécifique à la plateforme et à la version. Vous ne pouvez restaurer une sauvegarde MySQL d'Unified Manager que sur la même version d'Unified Manager, et une sauvegarde Windows ne peut être restaurée que sur une plateforme Windows.



Si les noms de dossiers contiennent un espace, vous devez inclure le chemin absolu ou relatif du fichier de sauvegarde entre guillemets doubles.

Étapes

1. Si vous effectuez une restauration sur un nouveau serveur, après l'installation d'Unified Manager, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification lorsque l'installation est terminée. Le fichier de sauvegarde renseignera ces informations lors de la restauration.
2. Connectez-vous au système Unified Manager avec les identifiants d'administrateur.
3. Lancez PowerShell ou une invite de commandes en tant qu'administrateur Windows.
4. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
5. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarde et restauration**.
6. Saisissez le numéro de **Restore MySQL Backup**.
7. Lorsque vous y êtes invité, saisissez le chemin d'accès 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 pourrez vous connecter à Unified Manager.

Après avoir restauré la sauvegarde, si le serveur OnCommand Workflow Automation ne fonctionne pas, procédez comme suit :

1. Sur le serveur Workflow Automation, modifiez l'adresse IP du serveur Unified Manager pour qu'elle pointe vers la machine la plus récente.
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 NetApp Snapshots

Sauvegarde et restauration à l'aide des snapshots NetApp dans Active IQ Unified Manager

Une copie Snapshot NetApp crée une image à un instant précis de la base de données Unified Manager et des fichiers de configuration, que vous pouvez utiliser pour restaurer en cas de défaillance du système ou de perte de données. Vous planifiez l'écriture périodique d'une copie Snapshot sur un volume de l'un de vos clusters ONTAP afin de toujours disposer d'une copie à jour.

Cette fonctionnalité n'est pas disponible pour Active IQ Unified Manager installé sur une appliance virtuelle.

Configurer la sauvegarde sous Linux dans Active IQ Unified Manager

Si votre Active IQ Unified Manager est installé sur une machine Linux, vous pouvez alors configurer votre sauvegarde et votre restauration à l'aide de NetApp Snapshots.

Les copies Snapshot prennent très peu de temps, généralement quelques minutes seulement, et la base de données Unified Manager est verrouillée pendant une très courte durée, ce qui entraîne très peu de perturbations pour votre installation. L'image consomme un espace de stockage minimal et n'entraîne qu'une surcharge de performances négligeable, car elle n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot. Comme la Snapshot est créée sur un cluster ONTAP, vous pouvez tirer parti d'autres fonctionnalités NetApp, telles que SnapMirror, pour créer une protection secondaire, si nécessaire.

Avant de lancer une opération de sauvegarde, Unified Manager effectue un contrôle d'intégrité pour vérifier que le système de destination est disponible.

- Vous pouvez restaurer une copie Snapshot uniquement sur la même version d'Active IQ Unified Manager.

  Par exemple, si vous avez créé une sauvegarde sur Unified Manager 9.18, vous ne pouvez restaurer la sauvegarde que sur des systèmes Unified Manager 9.18.

- Toute modification de la configuration de Snapshot peut rendre ce dernier invalide.

Configurer l'emplacement de la copie Snapshot dans Active IQ Unified Manager

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 ONTAP CLI.

Avant de commencer

Le cluster, la machine virtuelle de stockage et le volume doivent répondre aux exigences suivantes :

- Exigences du cluster :
  - ONTAP 9.3 ou version ultérieure doit être installé
  - Il doit être géographiquement proche du serveur Unified Manager
  - Il peut être surveillé par Unified Manager, mais ce n'est pas obligatoire
- Configuration requise pour les machines virtuelles de stockage :
  - Le commutateur de noms et le mappage de noms doivent être configurés pour utiliser « `files` »
  - Utilisateurs locaux créés pour correspondre aux utilisateurs côté client
  - Assurez-vous que l'accès en lecture/écriture total est sélectionné
  - Assurez-vous que l'accès superutilisateur est défini sur "any" dans les règles d'export
  - NFS pour NetApp Snapshot pour Linux
  - NFSv4 doit être activé sur le serveur NFS et le domaine d'identification NFSv4 doit être spécifié sur le client et la machine virtuelle de stockage
  - Le volume doit être au moins le double de la taille du répertoire Unified Manager/opt/netapp/data

    Utilisez la commande du -sh /opt/netapp/data/ pour vérifier la taille actuelle.
- Exigences en matière de volume :
  - Le volume doit être au moins deux fois plus grand que le répertoire /opt/netapp/data d'Unified Manager
  - Le style de sécurité doit être défini sur UNIX
  - La stratégie de snapshot locale doit être désactivée
  - Le dimensionnement automatique du volume doit être activé
  - Le niveau de service de performance doit être défini sur une politique avec un nombre élevé d'IOPS et une faible latence, telle que "Extreme"

Pour connaître les étapes détaillées de création du volume NFS, consultez "Comment configurer NFSv4 dans ONTAP 9" et "Guide de configuration rapide de NFS pour ONTAP 9".

Spécifiez l'emplacement de destination des copies Snapshot dans Active IQ Unified Manager

Vous devez configurer l'emplacement de destination des copies Snapshot de 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 cet emplacement.

- Vous devez disposer des identifiants de l'utilisateur root pour l'hôte Linux sur lequel Active IQ Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez disposer de l'adresse IP de gestion du cluster, du nom de la machine virtuelle de stockage, du nom du volume, ainsi que du nom d'utilisateur et du mot de passe du système de stockage.
- Vous devez avoir monté le volume sur l'hôte Active IQ Unified Manager, et vous devez disposer du chemin de montage.

Étapes

1. Utilisez Secure Shell pour vous connecter à l'adresse IP ou au domaine complet (FQDN) du système Active IQ Unified Manager.
2. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de l'utilisateur de maintenance (umadmin).
3. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
4. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarde et restauration**.
5. Saisissez le numéro pour **Configurer la sauvegarde Snapshot NetApp**.
6. Saisissez le numéro pour configurer NFS.
7. Examinez les informations que vous devrez fournir, puis entrez le numéro correspondant à **Enter Backup Configuration Details**.
8. Pour identifier le volume sur lequel le Snapshot sera écrit, saisissez l'adresse IP de l'interface de gestion du cluster, le nom de la VM de stockage, le nom du volume, le nom du LUN, le nom d'utilisateur et le mot de passe du système de stockage, ainsi que le chemin de montage.
9. Vérifiez ces informations et saisissez `y`.

   Le système effectue les tâches suivantes :

   - Établit la connexion au cluster
   - Arrête tous les services
   - Crée un nouveau répertoire dans le volume et y copie les fichiers de configuration de la base de données Active IQ Unified Manager
   - Supprime les fichiers d'Active IQ Unified Manager et crée un lien symbolique vers le nouveau répertoire de la base de données
   - Redémarrer tous les services
10. Quittez la console de maintenance et lancez l'interface Active IQ Unified Manager pour créer une planification pour la copie Snapshot si vous ne l'avez pas déjà fait.

Configurer la sauvegarde sous Windows dans Active IQ Unified Manager

Active IQ Unified Manager prend en charge la sauvegarde et la restauration à l'aide de NetApp Snapshots sur le système d'exploitation Windows à l'aide d'un LUN utilisant le protocole iSCSI.

La sauvegarde basée sur Snapshot peut être effectuée pendant que tous les services Unified Manager sont en cours d'exécution. Un état cohérent de la base de données est capturé dans le cadre du Snapshot, car la sauvegarde applique un verrouillage global en lecture sur l'ensemble de la base de données, ce qui empêche toute écriture simultanée. Pour que votre système Unified Manager installé sur Windows OS puisse effectuer la sauvegarde et la restauration à l'aide des Snapshots NetApp, vous devez d'abord configurer la sauvegarde Unified Manager en mode 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.

- Configurer le cluster ONTAP
- Configurer la machine hôte Windows

Configurez un emplacement de sauvegarde pour Active IQ Unified Manager sur Windows

Vous devez configurer le volume pour stocker les copies Snapshot après avoir sauvegardé Unified Manager sous Windows.

Avant de commencer

Le cluster, la machine virtuelle de stockage et le volume doivent répondre aux exigences suivantes :

- Exigences du cluster :
  - ONTAP 9.3 ou version ultérieure doit être installé
  - Il doit être 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'un LUN dédiés à la configuration de sauvegarde. Le volume sélectionné ne doit contenir qu'un seul LUN et rien d'autre.
  - La taille du LUN doit être au moins deux fois supérieure à la taille des données qui devraient être traitées dans Active IQ Unified Manager 9.9.

    Cela impose également la même exigence de taille sur le volume.
  - Assurez-vous que l'accès en lecture/écriture total est sélectionné
  - Assurez-vous que l'accès superutilisateur est défini sur "any" dans les règles d'export
- Exigences en matière de volume et de LUN :
  - Le volume doit être au moins le double de la taille du répertoire de données MySQL d'Unified Manager.
  - Le style de sécurité doit être défini sur Windows
  - La stratégie de snapshot locale doit être désactivée
  - Le dimensionnement automatique du volume doit être activé
  - Le niveau de service de performance doit être défini sur une politique avec un nombre élevé d'IOPS et une faible latence, telle que "Extreme"

Configurez un cluster ONTAP pour la sauvegarde et la restauration dans Active IQ Unified Manager

Vous devez effectuer quelques étapes de préconfiguration sur les clusters ONTAP avant de pouvoir sauvegarder et restaurer Active IQ Unified Manager à l'aide d'une copie Snapshot sur les systèmes Windows.

Vous pouvez configurer un cluster ONTAP à l'aide de l'invite de commandes ou de l'interface utilisateur de System Manager. La configuration d'un cluster ONTAP implique de configurer des LIF de données afin qu'elles puissent être attribuées en tant que LIF iSCSI à la machine virtuelle de stockage. L'étape suivante consiste à configurer une machine virtuelle de stockage avec iSCSI activé à l'aide de l'interface utilisateur de System Manager. Vous devrez configurer une route réseau statique pour cette machine virtuelle 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'un LUN pour la configuration de sauvegarde. Le volume sélectionné ne doit contenir qu'un seul LUN. La taille du LUN doit être au moins deux fois supérieure à la taille des données qu'Active IQ Unified Manager est censé 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 ayant la même configuration.
2. Configurez une route réseau pour la machine virtuelle de stockage configurée.
3. Configurez un volume de capacité appropriée et un seul LUN à l'intérieur, en veillant à ce que le volume soit dédié uniquement à ce LUN.

> Dans un scénario où la LUN est créée sur System Manager, la suppression du mappage de la LUN peut supprimer l'igroup, et la restauration peut échouer. Pour éviter ce scénario, assurez-vous que, lors de la création d'une LUN, elle est créée explicitement et n'est pas supprimée lorsque le mappage de la LUN est supprimé.

4. Configurez un groupe d'initiateurs dans la machine virtuelle de stockage.
5. Configurer un ensemble de ports.
6. Intégrez l'igroup au portset.
7. Associez le LUN à l'igroup.

Configurer une machine hôte Windows dans Active IQ Unified Manager

Vous devez configurer votre machine hôte Windows avant de pouvoir utiliser NetApp Snapshot pour sauvegarder et restaurer Active IQ Unified Manager. Pour démarrer l'initiateur iSCSI Microsoft sur une machine hôte Windows, saisissez « `iscsi` » dans la barre de recherche et cliquez sur **iSCSI Initiator**.

Avant de commencer

Vous devez supprimer toute configuration précédente sur la machine hôte.

Si vous essayez de démarrer l'initiateur iSCSI sur une nouvelle installation de Windows, une demande de confirmation s'affiche et, après 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 en cours de connexion. Vous devrez donc vous assurer que toutes les configurations précédentes sur l'hôte Windows sont supprimées.

Étapes

1. Supprimez toutes les configurations précédentes sur la machine hôte.
2. Découvrez le portail cible.
3. Connectez-vous au portail cible.
4. Connectez-vous au portail cible en utilisant le multipath.
5. Découvrez les deux LIFs.
6. Découvrez le LUN configuré sur la machine Windows en tant que périphérique.
7. Configurez le LUN détecté comme nouveau lecteur de volume dans Windows.

Spécifiez l'emplacement de destination des copies Snapshot sous Windows dans Active IQ Unified Manager

Vous devez configurer l'emplacement de destination des copies Snapshot de 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 cet emplacement.

- Vous devez disposer des privilèges d'administrateur sur l'hôte Windows sur lequel Active IQ Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.
- Vous devez disposer de l'adresse IP de gestion du cluster, du nom de la machine virtuelle de stockage, du nom du volume, du nom du LUN, ainsi que du nom d'utilisateur et du mot de passe du système de stockage.
- Vous devez avoir monté le volume en tant que lecteur réseau sur l'hôte Active IQ Unified Manager, et vous devez disposer du lecteur monté.

Étapes

1. À l'aide de Power Shell, connectez-vous à l'adresse IP ou au domaine complet du système Active IQ Unified Manager.
2. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de l'utilisateur de maintenance (umadmin).
3. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
4. Dans la console de maintenance **Menu principal**, saisissez le numéro de l'option **Sauvegarde et restauration**.
5. Saisissez le numéro pour **Configurer la sauvegarde Snapshot NetApp**.
6. Saisissez le numéro pour configurer iSCSI.
7. Examinez les informations que vous devrez fournir, puis entrez le numéro correspondant à **Enter Backup Configuration Details**.
8. Pour identifier le volume sur lequel le Snapshot sera écrit, saisissez l'adresse IP de l'interface de gestion du cluster, le nom de la machine virtuelle de stockage, le nom du volume, le nom du LUN, le nom d'utilisateur et le mot de passe du système de stockage, ainsi que le lecteur monté.
9. Vérifiez ces informations et saisissez `y`.

   Le système effectue les tâches suivantes :

   - La machine virtuelle de stockage est validée
   - Le volume est validé
   - Le lecteur est monté et son état est vérifié.
   - Existence et état du LUN
   - Existence du lecteur réseau
   - La présence d'un espace recommandé (supérieur à deux fois la taille du répertoire de données mysql) sur le volume monté est vérifiée
   - Chemin de LUN correspondant à la LUN dédiée dans le volume
   - nom de l'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 pour les copies Snapshot.

Configurez une sauvegarde par instantané depuis la console de maintenance dans Active IQ Unified Manager

Pour effectuer une sauvegarde d'Active IQ Unified Manager à l'aide d'une copie Snapshot, vous devez suivre quelques étapes de configuration à partir de la console de maintenance.

Avant de commencer

Vous devriez disposer des informations suivantes concernant votre système :

- Adresse IP du cluster
- Nom de la machine virtuelle de stockage
- Nom du volume
- Nom LUN
- Chemin de montage
- Identifiants du système de stockage

Étapes

1. Accédez à la console de maintenance d'Unified Manager.
2. Saisissez 4 pour sélectionner **Sauvegarde et restauration**.
3. Saisissez 2 pour sélectionner **Sauvegarde et restauration à l'aide de NetApp Snapshot**.

   Si vous souhaitez modifier la configuration de sauvegarde, saisissez 3 pour sélectionner **Mettre à jour NetApp Snapshot Backup Configuration**. Vous pouvez uniquement mettre à jour le mot de passe.

4. Dans le menu, saisissez 1 pour sélectionner **Configurer la sauvegarde Snapshot NetApp**.
5. Saisissez 1 pour fournir les informations requises.
6. Veuillez fournir le nom d'utilisateur et le mot de passe de la console de maintenance, puis confirmer que LUN est monté sur l'hôte.

   Le processus vérifie ensuite que le répertoire de données, le chemin de la LUN, la machine virtuelle de stockage, les volumes, l'espace disponible, le disque, etc. que vous avez fournis sont corrects. Les opérations qui s'exécutent en arrière-plan sont les suivantes :

   - Les services sont arrêtés
   - Le répertoire de la base de données a été déplacé vers un stockage monté
   - Le répertoire de la base de données est supprimé et des liens symboliques sont créés
   - Les services redémarrent une fois la configuration terminée dans l'interface Active IQ Unified Manager, et le type de sauvegarde est remplacé par NetApp Snapshot et apparaît dans l'interface utilisateur comme Database backup (Snapshot based).

Avant de lancer une opération de sauvegarde, vous devez vérifier s'il y a eu une modification de la configuration Snapshot, car cela pourrait rendre le Snapshot non valide. Supposons que vous ayez configuré la sauvegarde sur le lecteur G et qu'un Snapshot ait été créé. Vous avez ensuite reconfiguré la sauvegarde sur le lecteur E et les données sont enregistrées sur le lecteur E conformément à la nouvelle configuration. Si vous essayez de restaurer le Snapshot créé lorsqu'il était sur le lecteur G, l'opération échoue avec une erreur indiquant que le lecteur G n'existe pas.

Vous pouvez, à l'aide de l'interface utilisateur de Unified Manager, configurer la planification de création des copies Snapshot d'Unified Manager.

Avant de commencer

- Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
- Vous devez avoir configuré les paramètres de création de copies Snapshot à partir de la console de maintenance pour identifier la destination où les copies Snapshot seront créées.

Les copies Snapshot sont créées en quelques minutes seulement et la base de données de Unified Manager n'est verrouillée que pendant quelques secondes.

Les sauvegardes effectuées pendant les 15 premiers jours suivant l'ajout d'un nouveau cluster peuvent ne pas être suffisamment précises pour obtenir les données de performance historiques.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Sauvegarde de la base de données**.
2. Sur la page **Sauvegarde de la base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Saisissez le nombre maximal de copies Snapshot que vous souhaitez conserver dans le champ **Nombre de copies à conserver**.

   La valeur par défaut du nombre de copies Snapshot est de 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 utiliser la valeur maximale, quelle que soit la version de ONTAP.

4. Sélectionnez le bouton **Planifié quotidiennement** ou **Planifié hebdomadairement**, puis spécifiez les détails de la planification.
5. Cliquez sur **Appliquer**.

Des copies Snapshot sont créées selon la planification. Vous pouvez voir les fichiers de sauvegarde disponibles dans la page Database Backup.

Compte tenu de l'importance de ce volume et des copies Snapshot, vous souhaiterez peut-être créer une ou deux alertes pour ce volume afin d'être averti lorsque :

- L'espace du volume est rempli à 90 %. Utilisez l'événement **Volume Space Full** pour configurer l'alerte.

  Vous pouvez augmenter la capacité du volume à l'aide de ONTAP System Manager ou de ONTAP CLI afin que la base de données Unified Manager ne manque pas d'espace.

- Le nombre de copies Snapshot est sur le point d'atteindre le nombre maximal. Utilisez l'événement **Too Many Snapshot Copies** pour configurer l'alerte.

  Vous pouvez supprimer les anciens snapshots à l'aide de ONTAP System Manager ou de ONTAP CLI afin qu'il y ait toujours de la place pour de nouvelles copies Snapshot.

Vous configurez les alertes sur la page Configuration des alertes.

Restaurez Active IQ Unified Manager à l'aide de copies Snapshot

En cas de perte de données ou de corruption des données, vous pouvez restaurer Unified Manager à son précédent état stable avec une perte de données minimale. Vous pouvez restaurer la base de données Snapshot de Unified Manager sur un système d'exploitation local ou distant à l'aide de la console de maintenance de Unified Manager.

Avant de commencer

- Vous devez disposer des identifiants de l'utilisateur root pour l'hôte Linux et des privilèges d'administrateur pour la machine hôte Windows sur laquelle Unified Manager est installé.
- Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

La fonction de restauration est spécifique à la plateforme et à la version. Vous ne pouvez restaurer une sauvegarde d'Unified Manager que sur la même version d'Unified Manager.

Étapes

1. Connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager.
   - Linux : Secure Shell
   - Windows : Power Shell
2. Connectez-vous au système avec les identifiants de l'utilisateur root.
3. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
4. Dans la console de maintenance **Main Menu**, saisissez 4 pour l'option **Backup Restore**.
5. Saisissez 2 pour sélectionner **Sauvegarde et restauration à l'aide de l'instantané NetApp Snapshot**.

   Si vous effectuez une restauration sur un nouveau serveur, après l'installation de Unified Manager, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification une fois l'installation terminée. Saisissez 1 pour sélectionner **Configurer la sauvegarde Snapshot NetApp** et configurez les paramètres des copies Snapshot comme sur le système d'origine.
6. Saisissez 3 pour sélectionner **Restaurer à l'aide d'un instantané NetApp**.
7. Sélectionnez la copie Snapshot à partir de laquelle vous souhaitez restaurer Unified Manager. Appuyez sur **Enter**.
8. Une fois le processus de restauration terminé, connectez-vous à l'interface utilisateur d'Unified Manager.

Après avoir restauré la sauvegarde, si le serveur Workflow Automation ne fonctionne pas, procédez comme suit :

1. Sur le serveur Workflow Automation, modifiez l'adresse IP du serveur Unified Manager pour qu'elle pointe vers la machine la plus récente.
2. Sur le serveur Unified Manager, réinitialisez le mot de passe de la base de données si l'acquisition échoue à l'étape 1.

Modifiez le type de sauvegarde dans Active IQ Unified Manager

Si vous souhaitez modifier le type de sauvegarde de votre système Active IQ Unified Manager, vous pouvez utiliser les options de la console de maintenance. L'option **Unconfigure NetApp Snapshot Backup** vous permet de revenir à la sauvegarde basée

sur MySQL.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

Étapes

1. Accédez à la console de maintenance.
2. Sélectionnez 4 dans le **Main Menu** pour la sauvegarde et la restauration.
3. Sélectionnez 2 dans le **menu Sauvegarde et restauration**.
4. Sélectionnez 4 pour **Déconfigurer NetApp Snapshot Backup**.

   Les actions effectuées sont affichées : arrêter les services, rompre le lien symbolique, déplacer les données du stockage vers le répertoire, puis redémarrer les services.

   Une fois la méthode de sauvegarde modifiée, le mécanisme de sauvegarde passe de Snapshot copy à la sauvegarde MySQL par défaut. Ce changement apparaît dans la section « Sauvegarde de la base de données » des paramètres généraux.

Comprendre la sauvegarde à la demande pour Active IQ Unified Manager

Vous pouvez utiliser l'interface utilisateur Active IQ Unified Manager pour générer une sauvegarde à la demande chaque fois que nécessaire. La sauvegarde à la demande vous permet de créer instantanément une sauvegarde à l'aide de la méthode de sauvegarde existante. La sauvegarde à la demande ne fait pas de distinction entre une sauvegarde MySQL et une sauvegarde basée sur Snapshot NetApp.

Vous pouvez effectuer une sauvegarde à la demande à l'aide du bouton **Backup Now** sur la page Sauvegarde de la base de données. Cette sauvegarde à la demande est indépendante des planifications que vous avez configurées pour Active IQ Unified Manager.

Migrez une appliance virtuelle Active IQ Unified Manager vers un système Linux

Vous pouvez restaurer une sauvegarde par vidage de la base de données MySQL d'Unified Manager depuis une appliance virtuelle vers un système Red Hat Enterprise Linux si vous souhaitez modifier le système d'exploitation hôte sur lequel Unified Manager s'exécute.

Avant de commencer

- Sur l'appliance virtuelle :
  - Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.
  - Vous devez connaître le nom de l'utilisateur de maintenance d'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 figurant dans "Installation de Unified Manager sur les 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.

- Après l'installation, ne lancez pas l'interface utilisateur et ne configurez aucun cluster, utilisateur ou paramètre d'authentification sur le système Linux. Le fichier de sauvegarde renseignera ces informations lors de la restauration.
- Vous devez disposer des identifiants de l'utilisateur root pour l'hôte Linux.

Ces étapes décrivent comment créer un fichier de sauvegarde sur l'appliance virtuelle, copier les fichiers de sauvegarde vers Red Hat Enterprise Linux, puis restaurer la sauvegarde de la base de données sur le nouveau système.

Étapes

1. Sur l'appliance virtuelle, cliquez sur **Gestion** > **Sauvegarde de la base de données**.
2. Sur la page **Sauvegarde de la base de données**, cliquez sur **Paramètres de sauvegarde**.
3. Modifiez le chemin de sauvegarde en /jail/support.
4. Dans la section Planification, sélectionnez **Planifié quotidiennement**, puis saisissez une heure quelques minutes après l'heure actuelle pour créer la sauvegarde dans quelques instants.
5. Cliquez sur **Appliquer**.
6. Veuillez patienter quelques heures le temps que la sauvegarde soit générée.

   Une sauvegarde complète peut dépasser 1 Go et prendre entre trois et quatre heures pour se terminer.

7. Connectez-vous en tant qu'utilisateur root à l'hôte Linux sur lequel Unified Manager est installé et copiez les fichiers de sauvegarde depuis /support sur l'appliance virtuelle à l'aide de SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   ```
   root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
   ```

   Assurez-vous d'avoir copié le fichier de sauvegarde .7z et tous les fichiers du dépôt .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.
- Modifiez le chemin de sauvegarde pour utiliser le paramètre par défaut de votre système Linux (/data/ocum-backup), ou un nouveau chemin de votre choix, car il n'existe pas de chemin /jail/support sur le système Linux.
- Reconfigurez les deux côtés de votre connexion Workflow Automation si vous utilisez WFA.
- Reconfigurez les paramètres d'authentification SAML, si vous utilisez SAML.

Une fois que vous avez vérifié que tout fonctionne comme prévu sur votre système Linux, vous pouvez arrêter et supprimer l'appliance virtuelle Unified Manager.

Gérer les scripts

Gérer les scripts dans Active IQ Unified Manager

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 importer des scripts personnalisés et tester leur exécution lorsqu'une alerte est générée.

La possibilité de charger des scripts dans Unified Manager et de les exécuter est activée par défaut. Si votre organisation ne souhaite pas autoriser cette fonctionnalité pour des raisons de sécurité, vous pouvez la désactiver dans **Gestion du stockage** > **Paramètres des fonctionnalités**.

Comprendre le fonctionnement des scripts avec les alertes dans Active IQ Unified Manager

Vous pouvez associer une alerte à votre script afin que celui-ci s'exécute lorsqu'une alerte est déclenchée par 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 à l'origine des 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 alte à un script, ce dernier est exécuté. Vous trouverez dans l'e-mail d'alerte le détail des arguments transmis au script.

> Si vous avez créé un script personnalisé et l'avez associé à une alerte pour un type d'événement spécifique, les actions sont effectuées en fonction de votre script personnalisé pour ce type d'événement, et les actions **Corriger** ne sont pas disponibles par défaut sur la page Actions de gestion ou sur le tableau de bord Unified Manager.

Le script utilise les arguments suivants pour son exécution :

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Vous pouvez utiliser les arguments dans vos scripts et recueillir des informations sur les événements associés ou modifier les objets de stockage.

Exemple d'obtention d'arguments à partir de scripts

```
print "$ARGV[0] : $ARGV[1]\n"
```

```
print "$ARGV[7] : $ARGV[8]\n"
```

Lorsqu'une alerte est générée, le système exécute ce script et affiche le résultat suivant :

```
-eventID : 290
-eventSourceID : 4138
```

Ajouter des scripts dans Active IQ Unified Manager

Vous pouvez ajouter des scripts dans Unified Manager et associer les scripts à des alertes. Ces scripts s'exécutent automatiquement lorsqu'une alerte est générée et vous permettent d'obtenir des informations sur les objets de stockage pour lesquels l'événement est généré.

Avant de commencer

- Vous devez avoir créé et enregistré les scripts que vous souhaitez ajouter au serveur Unified Manager.
- Les formats de fichiers pris en charge pour les scripts sont Perl, Shell, PowerShell, Python et `.bat` fichiers.

Plateforme sur laquelle Unified Manager est installé	Langues prises en charge
VMware	Scripts Perl et Shell
Linux	Scripts Perl, Python et Shell
Windows	PowerShell, Perl, Python et scripts .bat

  - Pour les scripts Perl, Perl doit être installé sur le serveur Unified Manager. Sur les installations VMware, Perl 5 est installé par défaut et les scripts ne prendront en charge que les fonctionnalités de Perl 5. 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 ces fichiers journaux ne sont créés nulle part dans le dossier d'installation d'Unified Manager.

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez télécharger des scripts personnalisés et recueillir des détails sur l'événement lié à l'alerte.

> Si cette fonctionnalité n'apparaît pas dans l'interface utilisateur, c'est parce qu'elle a été désactivée par votre administrateur. Si nécessaire, vous pouvez activer cette fonctionnalité dans **Gestion du stockage** > **Paramètres des fonctionnalités**.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Scripts**.
2. Sur 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 **Add**.

Supprimer les scripts dans Active IQ Unified Manager

Vous pouvez supprimer un script de Unified Manager lorsque celui-ci n'est plus nécessaire ou n'est plus valide.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Le script ne doit pas être associé à une alerte.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Scripts**.
2. Sur 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 dans Active IQ Unified Manager

Vous pouvez vérifier que votre script s'exécute correctement lorsqu'une alerte est générée pour un objet de stockage.

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir téléchargé un script dans le format de fichier pris en charge vers Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Scripts**.
2. Sur la page Scripts, ajoutez votre script de test.
3. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
4. Sur la page **Configuration des alertes**, effectuez l'une des actions suivantes :

À…	Faites ceci…
Ajouter une alerte	a. Cliquez sur **Add**. 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. Sur la page **Configuration des alertes**, sélectionnez l'alerte que vous avez ajoutée ou modifiée, puis cliquez sur **Tester**.

   Le script est exécuté avec l'argument « `-test` », et une alerte de notification est envoyée aux adresses

électroniques qui ont été spécifiées lors de la création de l'alerte.

Gérer et surveiller les groupes

Comprendre les groupes

Découvrez les groupes dans Active IQ Unified Manager

Un groupe est un ensemble dynamique d'objets de stockage hétérogène (clusters, SVM ou volumes). Vous pouvez créer des groupes dans Unified Manager pour gérer facilement un ensemble d'objets de stockage. Les membres d'un groupe peuvent changer en fonction des objets de stockage surveillés par Unified Manager à un instant donné.

- Chaque groupe possède un nom unique.
- Vous devez configurer au minimum une règle de groupe pour chaque groupe.
- Vous pouvez associer un groupe à plusieurs règles de groupe.
- Chaque groupe peut inclure plusieurs types d'objets de stockage tels que des clusters, des SVM ou des volumes.
- Les objets de stockage sont ajoutés dynamiquement à un groupe en fonction du moment où une règle de groupe est créée ou lorsque Unified Manager termine un cycle de surveillance.
- Vous pouvez appliquer simultanément des actions à tous les objets de stockage d'un groupe, par exemple définir des seuils pour les volumes.

Comprendre le fonctionnement des règles de groupe dans Active IQ Unified Manager

Une règle de groupe est un critère que vous définissez pour permettre d'inclure des objets de stockage (volumes, clusters ou SVM) dans un groupe spécifique. Vous pouvez utiliser des groupes de conditions ou des conditions pour définir une règle de groupe pour un groupe.

- Vous devez associer une règle de groupe à un groupe.
- Vous devez associer un type d'objet à une règle de groupe ; un seul type d'objet peut être 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 comporter un ou plusieurs groupes de conditions, et chaque groupe de conditions peut comporter une ou plusieurs conditions.
- Les objets de stockage peuvent appartenir à plusieurs groupes en fonction des règles de groupe que vous créez.

Conditions

Vous pouvez créer plusieurs groupes de conditions, et chaque groupe de conditions peut comporter une ou plusieurs conditions. Vous pouvez appliquer tous les groupes de conditions définis dans une règle de groupe pour les 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 l'opérateur 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 pour appliquer, sélectionner et regrouper uniquement les objets de stockage qui satisfont 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 inclure dans un groupe.

Vous pouvez créer des conditions avec des objets de stockage en utilisant les opérandes et l'opérateur suivants, et en spécifiant la valeur requise.

Type d'objet de stockage	Opérandes applicables
Volume	• Nom de l'objet • Nom du cluster propriétaire • Nom de la SVM propriétaire • Annotations
SVM	• Nom de l'objet • Nom du cluster propriétaire • Annotations
Cluster	• Nom de l'objet • Annotations

Lorsque vous sélectionnez une annotation comme opérande pour n'importe quel objet de stockage, l'opérateur "Is" est disponible. Pour tous les autres opérandes, vous pouvez sélectionner "Is" ou "Contains" comme opérateur.

- Opérande

  La liste des opérandes dans Unified Manager varie selon le type d'objet sélectionné. Elle comprend le nom de l'objet, le nom du cluster propriétaire, le nom du SVM propriétaire et les annotations définies dans Unified Manager.

- Opérateur

  La liste des opérateurs varie selon l'opérande sélectionné pour une condition. Les opérateurs pris en charge par Unified Manager sont « Is » et « Contains ».

  Lorsque vous sélectionnez l'opérateur « `Is` », la condition est évaluée afin de vérifier une correspondance exacte entre la valeur de l'opérande et la valeur fournie pour l'opérande sélectionné.

  Lorsque vous sélectionnez l'opérateur « `Contains` », la condition est évaluée afin de déterminer si elle répond à l'un des critères suivants :

  ◦ La valeur de l'opérande correspond exactement à la valeur fournie pour l'opérande sélectionné

  ◦ La valeur de l'opérande contient la valeur fournie pour l'opérande sélectionné

- Valeur

  La valeur du champ change en fonction de l'opérande sélectionné.

Exemple de règle de groupe avec conditions

Considérons un groupe de conditions pour un volume avec les deux conditions suivantes :

- Le nom contient « `vol` »
- Le nom de la SVM est « `data_svm` »

Ce groupe de conditions sélectionne tous les volumes qui incluent « `vol` » dans leur nom et qui sont hébergés sur des SVM portant le nom « `data_svm` ».

Groupes de conditions

Les groupes de conditions sont exécutés à l'aide de l'opérateur logique OU, puis appliqués aux objets de stockage. Les objets de stockage doivent satisfaire à l'un des groupes de conditions pour être inclus dans un groupe. Les objets de stockage de tous les groupes de conditions sont combinés. Vous pouvez utiliser les groupes de conditions pour élargir la portée des objets de stockage à inclure dans un groupe.

Exemple de règle de groupe avec groupes de conditions

Considérez deux groupes de conditions pour un volume, chaque groupe contenant les deux conditions suivantes :

- Groupe de conditions 1
  - Le nom contient « `vol` »
  - Le nom de la SVM est « `data_svm` » Le groupe de conditions 1 sélectionne tous les volumes qui incluent « `vol` » dans leur nom et qui sont hébergés sur des SVM portant le nom « `data_svm` ».
- Groupe de conditions 2
  - Le nom contient « `vol` »
  - La valeur d'annotation de data-priority est « `critical` » Le groupe de conditions 2 sélectionne tous les volumes qui incluent « `vol` » dans leur nom et qui comportent la valeur d'annotation data-priority « `critical` ».

Lorsqu'une règle de groupe contenant ces deux groupes de conditions est appliquée à des objets de stockage, les objets de stockage suivants sont ajoutés au groupe sélectionné :

- Tous les volumes qui incluent « `vol` » dans leur nom et qui sont hébergés sur la SVM nommée « `data_svm` ».
- Tous les volumes qui incluent « `vol` » dans leur nom et qui sont annotés avec la valeur d'annotation de priorité des données « `critical` ».

Comprendre le fonctionnement des actions de groupe sur les objets de stockage dans Active IQ Unified Manager

Une action de groupe est une opération effectuée sur tous les objets de stockage d'un groupe. Par exemple, vous pouvez configurer une action de groupe pour les seuils de volume afin de modifier simultanément les valeurs de seuil de volume de tous les volumes d'un groupe.

Les groupes prennent en charge des types d'actions de groupe uniques. Un groupe ne peut comporter qu'une seule action de type « seuil d'intégrité des volumes ». Toutefois, vous pouvez configurer un autre type d'action

de groupe, s'il est disponible, pour ce même groupe. Le rang d'une action de groupe détermine l'ordre dans lequel elle est appliquée aux objets de stockage. La page de détails d'un objet de stockage indique l'action de groupe qui lui est appliquée.

Exemple d'actions de groupe uniques

Considérez un volume A qui appartient aux groupes G1 et G2, et pour lequel les actions de groupe de seuil de santé du volume suivantes sont configurées :

- `Change_capacity_threshold`action de groupe avec le rang 1, pour configurer la capacité du volume
- `Change_snapshot_copies`Action de groupe de rang 2 pour configurer les copies Snapshot du volume

L' `Change_capacity_threshold`action de groupe est toujours prioritaire sur l' `Change_snapshot_copies`action de groupe et s'applique au volume A. Lorsque Unified Manager termine un cycle de surveillance, les événements liés au seuil d'intégrité du volume A sont réévalués conformément à l' `Change_capacity_threshold`action de groupe. Vous ne pouvez pas configurer un autre type d'action de groupe pour le seuil de volume, ni pour le groupe G1 ni pour le groupe G2.

Ajouter des groupes dans Active IQ Unified Manager

Vous pouvez créer des groupes pour combiner des clusters, des volumes et des machines virtuelles de stockage (SVMs) afin de faciliter la gestion.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez définir des règles de groupe pour ajouter ou supprimer des membres du groupe et pour modifier les actions du groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Groupes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un groupe**, saisissez un nom et une description pour le groupe.
4. Cliquez sur **Add**.

Modifier les groupes dans Active IQ Unified Manager

Vous pouvez modifier le nom et la description d'un groupe que vous avez créé dans Unified Manager.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous modifiez un groupe pour en mettre à jour le nom, vous devez spécifier un nom unique ; vous ne pouvez pas utiliser un nom de groupe existant.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Groupes**, sélectionnez le groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le groupe**, modifiez le nom du groupe, sa description ou les deux.

4. Cliquez sur **Enregistrer**.

Supprimer des groupes dans Active IQ Unified Manager

Vous pouvez supprimer un groupe dans Unified Manager lorsque celui-ci n'est plus nécessaire.

Avant de commencer

- Aucun des objets de stockage (clusters, SVM ou volumes) ne doit être associé à une règle de groupe associée au groupe que vous souhaitez supprimer.
- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Groupes**, sélectionnez le groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

   La suppression d'un groupe n'entraîne pas la suppression des actions de groupe qui lui sont associées. Cependant, ces actions de groupe ne seront plus associées après la suppression du groupe.

Ajouter des règles de groupe dans Active IQ Unified Manager

Vous pouvez créer des règles de groupe pour ajouter dynamiquement des objets de stockage, tels que des volumes, des clusters ou des machines virtuelles de stockage (SVM), à un groupe. Pour créer une règle de groupe, vous devez configurer au moins un groupe de conditions avec au moins une condition.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Les objets de stockage actuellement surveillés sont ajoutés dès la création de la règle de groupe. Les nouveaux objets ne sont ajoutés qu'une fois le cycle de surveillance terminé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Règles du groupe**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle de groupe**, spécifiez un nom pour la règle de groupe.
4. Dans le champ **Type d'objet cible**, sélectionnez le type d'objet de stockage que vous souhaitez regrouper.
5. Dans le champ **Groupe**, sélectionnez le groupe requis pour lequel vous souhaitez créer des règles de groupe.
6. Dans la section **Conditions**, procédez comme suit pour créer une condition, un groupe de conditions ou les deux :

Créer….	Faites ceci…
Une condition	a. Sélectionnez un opérande dans la liste des opérandes. b. Sélectionnez **Contient** ou **Est** comme opérateur. c. Saisissez une valeur, ou sélectionnez-en une dans la liste disponible.
Un groupe de conditions	a. Cliquez sur **Ajouter un groupe de conditions** b. Sélectionnez un opérande dans la liste des opérandes. c. Sélectionnez **Contient** ou **Est** comme opérateur. d. Saisissez une valeur, ou sélectionnez-en une dans la liste disponible. e. Cliquez sur **Ajouter une condition** pour créer d'autres conditions si nécessaire, et répétez les étapes a à d pour chaque condition.

7. Cliquez sur **Add**.

Exemple de création d'une règle de groupe

Pour créer une règle de groupe, procédez comme suit dans la boîte de dialogue Ajouter une règle de groupe : configurez une condition et ajoutez 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. Saisissez la valeur sous la forme de `svm_data`.
7. Cliquez sur **Ajouter un groupe de conditions**.
8. Sélectionnez **Nom de l'objet** comme opérande.
9. Sélectionnez **Contient** comme opérateur.
10. Saisissez la valeur sous la forme `vol`.
11. Cliquez sur **Ajouter une condition**.
12. Répétez les étapes 8 à 10 en sélectionnant **data-priority** comme opérande à l'étape 8, **Is** comme opérateur à l'étape 9 et **critical** comme valeur à l'étape 10.
13. Cliquez sur **Ajouter** pour créer la condition de la règle de groupe.

Modifier les règles de groupe dans Active IQ Unified Manager

Vous pouvez modifier les règles de groupe pour changer les groupes de conditions et les

conditions au sein d'un groupe de conditions afin d'ajouter des objets de stockage à un groupe spécifique ou d'en supprimer.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Règles de groupe**, sélectionnez la règle de groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier la règle de groupe**, modifiez le nom de la règle de groupe, le nom du groupe associé, les groupes de conditions et les conditions selon vos besoins.

   Vous ne pouvez pas modifier le type d'objet cible d'une règle de groupe.

4. Cliquez sur **Enregistrer**.

Supprimer les règles de groupe dans Active IQ Unified Manager

Vous pouvez supprimer une règle de groupe dans Active IQ Unified Manager lorsque cette règle n'est plus nécessaire.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsqu'une règle de groupe est supprimée, les objets de stockage associés seront retirés du groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Règles de groupe**, sélectionnez la règle de groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Ajouter des actions de groupe dans Active IQ Unified Manager

Vous pouvez configurer des actions de groupe à appliquer aux objets de stockage d'un groupe. Configurer ces actions pour un groupe vous permet de gagner du temps, car vous n'avez pas besoin de les ajouter individuellement à chaque objet.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Actions de groupe**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une action de groupe**, saisissez un nom et une description pour l'action.
4. Dans le menu **Groupe**, sélectionnez le groupe pour lequel vous souhaitez configurer l'action.

5. Dans le menu **Type d'action**, sélectionnez un type d'action.

   La boîte de dialogue s'agrandit, vous permettant de configurer le type d'action sélectionné avec les paramètres requis.

6. Saisissez les valeurs appropriées pour les paramètres requis afin de configurer une action de groupe.
7. Cliquez sur **Add**.

Modifier les actions de groupe dans Active IQ Unified Manager

Vous pouvez modifier les paramètres d'action de groupe que vous avez configurés dans Unified Manager, tels que le nom de l'action de groupe, sa description, le nom du groupe associé et les paramètres du type d'action.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Actions de groupe**, sélectionnez l'action de groupe que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier l'action de groupe**, modifiez, si nécessaire, le nom de l'action de groupe, sa description, le nom du groupe associé et les paramètres du type d'action.
4. Cliquez sur **Enregistrer**.

Configurez les seuils de santé des volumes pour les groupes dans Active IQ Unified Manager

Vous pouvez configurer des seuils d'état de santé des volumes au niveau du groupe pour la capacité, les copies Snapshot, les quotas qtree, la croissance et les inodes.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

L'action de groupe de type seuil de santé de volume s'applique uniquement aux volumes d'un groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Actions de groupe**, cliquez sur **Ajouter**.
3. Saisissez un nom et une description pour l'action de groupe.
4. Dans la liste déroulante **Groupe**, sélectionnez un groupe pour lequel vous souhaitez configurer une action de groupe.
5. Sélectionnez **Type d'action** comme seuil d'état de santé du volume.
6. Sélectionnez la catégorie pour laquelle vous souhaitez définir le seuil.
7. Saisissez les valeurs requises pour le seuil de santé.
8. Cliquez sur **Add**.

Supprimer les actions de groupe dans Active IQ Unified Manager

Vous pouvez supprimer une action de groupe depuis Unified Manager lorsque cette action de groupe n'est plus nécessaire.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous supprimez l'action de groupe associée au seuil d'intégrité du volume, les seuils globaux sont appliqués aux objets de stockage de ce groupe. Les seuils d'intégrité définis au niveau de l'objet de stockage ne sont pas affectés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Actions de groupe**, sélectionnez l'action de groupe que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, confirmez la suppression en cliquant sur **Oui**.

Réorganiser les actions de groupe dans Active IQ Unified Manager

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 manière séquentielle en fonction de leur rang. Le rang le plus bas est attribué à l'action de groupe que vous avez configurée en dernier. Vous pouvez modifier le rang de l'action de groupe en fonction de vos besoins.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez sélectionner une seule ligne ou plusieurs lignes, puis effectuer plusieurs opérations de glisser-déposer pour modifier l'ordre de priorité des actions de groupe. Toutefois, vous devez enregistrer les modifications pour que la nouvelle priorisation soit prise en compte dans la grille des actions de groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Groupes**.
2. Dans l'onglet **Actions de groupe**, cliquez sur **Réorganiser**.
3. Dans la boîte de dialogue **Réorganiser les actions de groupe**, faites glisser-déposer les lignes pour réorganiser la séquence des actions de groupe selon vos besoins.
4. Cliquez sur **Enregistrer**.

Prioriser les événements des objets de stockage à l'aide d'annotations

En savoir plus sur les annotations

Découvrez les annotations dans Active IQ Unified Manager

Une annotation est une chaîne de texte (le nom) attribuée à une autre chaîne de texte (la valeur). Chaque paire nom-valeur d'annotation peut être associée dynamiquement à des objets de stockage à l'aide de règles d'annotation. Lorsque vous associez des objets de

stockage à des annotations prédéfinies, vous pouvez filtrer et afficher les événements qui leur sont associés. Vous pouvez appliquer des annotations aux clusters, aux volumes et aux machines virtuelles de stockage (SVM).

Chaque nom d'annotation peut avoir plusieurs valeurs ; chaque paire nom-valeur peut être associée à un objet de stockage via des règles.

Par exemple, vous pouvez créer une annotation nommée "data-center" avec les valeurs "Boston" et "Canada". Vous pouvez ensuite appliquer l'annotation "data-center" avec la valeur "Boston" au volume v1. Lorsqu'une alerte est générée pour un événement sur le volume v1 annoté avec "data-center", l'e-mail généré indique l'emplacement du volume, "Boston", ce qui vous permet de hiérarchiser et de résoudre le problème.

Comprendre le fonctionnement des règles d'annotation dans Active IQ Unified Manager

Une règle d'annotation est un critère que vous définissez pour annoter les objets de stockage (volumes, clusters ou machines virtuelles de stockage (SVM)). Vous pouvez utiliser des groupes de conditions ou des conditions pour définir des règles d'annotation.

- Vous devez associer une règle d'annotation à une annotation.
- Vous devez associer un type d'objet 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 aux objets de stockage après chaque cycle de surveillance ou lorsqu'une règle est créée, modifiée, supprimée ou réorganisée.
- Une règle d'annotation peut comporter un ou plusieurs groupes de conditions, et chaque groupe de conditions peut comporter une ou plusieurs conditions.
- Les objets de stockage peuvent comporter plusieurs annotations. Une règle d'annotation pour une annotation particulière peut également utiliser différentes annotations dans les conditions de la règle afin d'ajouter une autre annotation à des objets déjà annotés.

Conditions

Vous pouvez créer plusieurs groupes de conditions, chacun pouvant contenir une ou plusieurs conditions. Vous pouvez appliquer tous les groupes de conditions définis dans une règle d'annotation d'une annotation afin d'annoter des objets de stockage.

Les conditions d'un groupe de conditions sont exécutées à l'aide d'un ET logique. Toutes les conditions du groupe 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. Vous pouvez utiliser plusieurs conditions au sein d'un groupe de conditions lorsque vous souhaitez limiter la portée des objets de stockage à annoter.

Vous pouvez créer des conditions avec des objets de stockage en utilisant les opérandes et l'opérateur suivants, et en spécifiant la valeur requise.

Type d'objet de stockage	Opérandes applicables
Volume	• Nom de l'objet • Nom du cluster propriétaire • Nom de la SVM propriétaire • Annotations

Type d’objet de stockage	Opérandes applicables
SVM	• Nom de l’objet • Nom du cluster propriétaire • Annotations
Cluster	• Nom de l’objet • Annotations

Lorsque vous sélectionnez une annotation comme opérande pour un objet de stockage, l’opérateur « Est » est disponible. Pour tous les autres opérandes, vous pouvez sélectionner « Est » ou « Contient » comme opérateur. Lorsque vous sélectionnez l’opérateur « Est », la condition est évaluée afin de vérifier 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 afin de vérifier qu’au moins un des critères suivants est rempli :

- La valeur de l’opérande correspond exactement à la valeur de l’opérande sélectionné.
- La valeur de l’opérande contient la valeur fournie pour l’opérande sélectionné.

Exemple de règle d’annotation avec conditions

Considérez une règle d’annotation avec un groupe de conditions pour un volume présentant les deux conditions suivantes :

- Le nom contient « `vol` »
- Le nom de la SVM est « `data_svm` »

Cette règle d’annotation annote tous les volumes qui incluent « `vol` » dans leur nom et qui sont hébergés sur des SVM portant le nom « `data_svm` » avec l’annotation sélectionnée et le type d’annotation.

Groupes de conditions

Les groupes de conditions sont exécutés à l’aide d’un OU logique, puis appliqués aux objets de stockage. Pour être annotés, les objets de stockage doivent satisfaire aux exigences d’au moins un groupe de conditions. Les objets de stockage qui satisfont aux conditions de tous les groupes de conditions sont annotés. Vous pouvez utiliser des groupes de conditions pour étendre la portée des objets de stockage à annoter.

Exemple de règle d’annotation avec groupes de conditions

Considérez une règle d’annotation comportant deux groupes de conditions pour un volume ; chaque groupe contient les deux conditions suivantes :

- Groupe de conditions 1
  - Le nom contient « `vol` »
  - Le nom de la SVM est « `data_svm` » Ce groupe de conditions annote tous les volumes qui incluent « `vol` » dans leur nom et qui sont hébergés sur des SVM portant le nom « `data_svm` ».
- Groupe de conditions 2
  - Le nom contient « `vol` »
  - La valeur d’annotation de data-priority est « `critical` » Ce groupe de conditions annote tous les

volumes qui incluent « `vol` » dans leur nom et qui sont annotés avec la valeur d'annotation data-priority comme « `critical` ».

Lorsqu'une règle d'annotation contenant ces deux groupes de conditions est appliquée à des objets de stockage, les objets de stockage suivants sont annotés :

- Tous les volumes qui incluent « `vol` » dans leur nom et qui sont hébergés sur une SVM nommée « `data_svm` ».
- Tous les volumes qui incluent « `vol` » dans leur nom et qui sont annotés avec la valeur d'annotation de priorité des données « `critical` ».

Comprendre les valeurs d'annotation prédéfinies dans Active IQ Unified Manager

Data-priority est une annotation prédéfinie qui a pour valeurs Mission critical, High et Low. 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:Mission critique**

  Cette annotation s'applique aux objets de stockage qui contiennent des données stratégiques. Par exemple, les objets qui contiennent des applications de production peuvent être considérés comme stratégiques.

- **Priorité des données:Élevée**

  Cette annotation s'applique aux objets de stockage contenant des données hautement prioritaires. Par exemple, les objets hébergeant des applications métier peuvent être considérés comme hautement prioritaires.

- **Priorité des données:Faible**

  Cette annotation s'applique aux objets de stockage contenant des données de faible priorité. Par exemple, les objets situés sur un stockage secondaire, comme les destinations de sauvegarde et de mise en miroir, peuvent être de faible priorité.

Ajoutez des annotations de manière dynamique dans Active IQ Unified Manager

Lorsque vous créez des annotations personnalisées, Unified Manager associe dynamiquement les clusters, les machines virtuelles de stockage (SVM) et les volumes à ces annotations à l'aide de règles. Ces règles attribuent automatiquement les annotations aux objets de stockage.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Sur la page **Annotations**, cliquez sur **Ajouter une annotation**.
3. Dans la boîte de dialogue **Ajouter une annotation**, saisissez un nom et une description pour l'annotation.

4. Facultatif : dans la section **Valeurs d'annotation**, cliquez sur **Ajouter** pour ajouter des valeurs à l'annotation.
5. Cliquez sur **Enregistrer**.

Ajouter des valeurs aux annotations dans Active IQ Unified Manager

Vous pouvez ajouter des valeurs aux annotations, puis associer des objets de stockage à une paire nom-valeur d'annotation particulière. L'ajout de valeurs aux annotations vous permet de gérer plus efficacement les objets de stockage.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous ne pouvez pas ajouter de valeurs aux annotations prédéfinies.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Sur 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 **Add**.

Supprimer les annotations dans Active IQ Unified Manager

Vous pouvez supprimer les annotations personnalisées et leurs valeurs lorsqu'elles ne sont plus nécessaires.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Les valeurs d'annotation ne doivent pas être utilisées dans d'autres annotations ou règles de groupe.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Annotations**, sélectionnez l'annotation que vous souhaitez supprimer.

   Les détails de l'annotation sélectionnée 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.

Consultez la liste des annotations et les détails dans Active IQ Unified Manager

Vous pouvez consulter la liste des annotations associées dynamiquement aux clusters, aux volumes et aux machines virtuelles de stockage (SVM). Vous pouvez également consulter des détails tels que la description, créé par, la date de création, les valeurs, les règles et les objets associés à l'annotation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Annotations**, cliquez sur le nom de l'annotation pour afficher les détails associés.

Supprimer les valeurs des annotations dans Active IQ Unified Manager

Vous pouvez supprimer les valeurs associées aux annotations personnalisées lorsque cette valeur ne s'applique plus à l'annotation.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- La valeur d'annotation ne doit pas être associée à une règle d'annotation ni à une règle de groupe.

Vous ne pouvez pas supprimer les valeurs des annotations prédéfinies.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans la liste des annotations de l'onglet **Annotations**, sélectionnez l'annotation dont vous souhaitez supprimer une valeur.
3. Dans la section **Valeurs** de l'onglet **Annotations**, sélectionnez la valeur que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
4. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui**.

   La valeur est supprimée et n'apparaît plus dans la liste des valeurs de l'annotation sélectionnée.

Créez des règles d'annotation dans Active IQ Unified Manager

Vous pouvez créer des règles d'annotation que Unified Manager utilise pour annoter dynamiquement les objets de stockage tels que les volumes, les clusters ou les machines virtuelles de stockage (SVMs).

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

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 **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Règles d'annotation**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle d'annotation**, spécifiez un nom pour la règle d'annotation.
4. Dans le champ **Type d'objet cible**, sélectionnez le type d'objet de stockage que vous souhaitez annoter.
5. Dans les champs **Appliquer l'annotation**, sélectionnez l'annotation et la valeur d'annotation que vous souhaitez utiliser.
6. Dans la section Conditions, effectuez l'action appropriée pour créer une condition, un groupe de conditions ou les deux :

Pour créer…	Faites ceci…
Une condition	a. Sélectionnez un opérande dans la liste des opérandes. b. Sélectionnez **Contient** ou **Est** comme opérateur. c. Saisissez une valeur, ou sélectionnez-en une dans la liste disponible.
Un groupe de conditions	a. Cliquez sur **Ajouter un groupe de conditions**. b. Sélectionnez un opérande dans la liste des opérandes. c. Sélectionnez **Contient** ou **Est** comme opérateur. d. Saisissez une valeur, ou sélectionnez-en une dans la liste disponible. e. Cliquez sur **Ajouter une condition** pour créer d'autres conditions si nécessaire, et répétez les étapes a à d pour chaque condition.

7. Cliquez sur **Add**.

Exemple de création d'une règle d'annotation

Pour créer une règle d'annotation, procédez comme suit dans la boîte de dialogue Ajouter une règle d'annotation : configurez une condition et ajoutez 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. Saisissez la valeur sous la forme de `svm_data`.
7. Cliquez sur **Ajouter un groupe de conditions**.
8. Sélectionnez **Nom de l'objet** comme opérande.
9. Sélectionnez **Contient** comme opérateur.
10. Saisissez la valeur sous la forme `vol`.
11. Cliquez sur **Ajouter une condition**.
12. Répétez les étapes 8 à 10 en sélectionnant **data-priority** comme opérande à l'étape 8, **Is** comme opérateur à l'étape 9 et **mission-critical** comme valeur à l'étape 10.
13. Cliquez sur **Add**.

Ajoutez manuellement des annotations aux objets de stockage individuels dans Active IQ Unified Manager

Vous pouvez annoter manuellement les volumes, clusters et SVM sélectionnés sans utiliser de règles d'annotation. Vous pouvez annoter un ou plusieurs objets de stockage et spécifier la combinaison nom-valeur requise pour l'annotation.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Accédez aux objets de stockage que vous souhaitez annoter :

Pour ajouter une annotation à…	Faites ceci…
Groupes	a. Cliquez sur **Stockage** > **Clusters**. b. Sélectionnez un ou plusieurs clusters.
Volumes	a. Cliquez sur **Stockage** > **Volumes**. b. Sélectionnez un ou plusieurs volumes.
SVM	a. Cliquez sur **Storage** > **SVMs**. b. Sélectionnez une ou plusieurs SVMs.

2. Cliquez sur **Annotate** et sélectionnez une paire nom-valeur.
3. Cliquez sur **Appliquer**.

Modifier les règles d'annotation dans Active IQ Unified Manager

Vous pouvez modifier les règles d'annotation afin de modifier les groupes de conditions et les conditions au sein du groupe de conditions pour ajouter ou supprimer des annotations sur les objets de stockage.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Les annotations sont dissociées des objets de stockage lorsque vous modifiez les règles d'annotation associées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Règles d'annotation**, sélectionnez la règle d'annotation que vous souhaitez modifier, puis cliquez sur **Actions** > **Modifier**.
3. Dans la boîte de dialogue **Modifier la règle d'annotation**, modifiez le nom de la règle, le nom et la valeur de l'annotation, les groupes de conditions et les conditions selon vos besoins.

   Vous ne pouvez pas modifier le type d'objet cible d'une règle d'annotation.

4. Cliquez sur **Enregistrer**.

Configurez les conditions des règles d'annotation dans Active IQ Unified Manager

Vous pouvez configurer une ou plusieurs conditions pour créer des règles d'annotation que Unified Manager applique aux objets de stockage. Les objets de stockage qui satisfont à la règle d'annotation sont annotés avec la valeur spécifiée dans la règle.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Règles d'annotation**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une règle d'annotation**, saisissez un nom pour la règle.
4. Sélectionnez un type d'objet dans la liste Type d'objet cible, puis sélectionnez un nom et une valeur d'annotation dans la liste.
5. Dans la section **Conditions** de la boîte de dialogue, sélectionnez un opérande et un opérateur dans la liste et saisissez une valeur de condition, ou cliquez sur **Ajouter une condition** pour créer une nouvelle condition.
6. Cliquez sur **Enregistrer et ajouter**.

Exemple de configuration d'une condition pour une règle d'annotation

Considérez une condition pour le type d'objet SVM, où le nom de l'objet contient « `svm_data` ».

Dans la boîte de dialogue Ajouter une règle d'annotation, procédez comme suit pour configurer la condition :

Étapes

1. Saisissez un nom pour la règle d'annotation.
2. Sélectionnez SVM comme type d'objet cible.
3. Sélectionnez une annotation dans la liste des annotations et une valeur.
4. Dans le champ **Conditions**, sélectionnez **Nom de l'objet** comme opérande.
5. Sélectionnez **Contient** comme opérateur.
6. Saisissez la valeur sous la forme de `svm_data`.
7. Cliquez sur **Add**.

Supprimer les règles d'annotation dans Active IQ Unified Manager

Vous pouvez supprimer les règles d'annotation de Active IQ Unified Manager lorsque ces règles ne sont plus nécessaires.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous supprimez une règle d'annotation, l'annotation est dissociée et supprimée des objets de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Règles d'annotation**, sélectionnez la règle d'annotation que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Avertissement**, cliquez sur **Oui** pour confirmer la suppression.

Réorganiser les règles d'annotation dans Active IQ Unified Manager

Vous pouvez modifier l'ordre dans lequel Unified Manager applique les règles d'annotation aux objets de stockage. Les règles d'annotation sont appliquées aux objets de stockage de manière séquentielle en fonction de leur priorité. Lorsque vous configurez une règle d'annotation, sa priorité est la plus basse. Mais vous pouvez modifier la priorité de la règle d'annotation selon vos besoins.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez sélectionner une seule ligne ou plusieurs lignes et effectuer de nombreuses opérations de glisser-déposer pour modifier l'ordre des règles d'annotation. Toutefois, vous devez enregistrer les modifications pour que le nouvel ordre de priorité s'affiche dans l'onglet « Règles d'annotation ».

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Annotations**.
2. Dans l'onglet **Règles d'annotation**, cliquez sur **Réorganiser**.
3. Dans la boîte de dialogue **Réorganiser les règles d'annotation**, faites glisser-déposer une ou plusieurs lignes pour réorganiser l'ordre des règles d'annotation.
4. Cliquez sur **Enregistrer**.

   Vous devez enregistrer les modifications pour que le nouvel ordre s'affiche.

Envoyer un bundle de support via l'interface utilisateur web et la console de maintenance

Envoyez un dossier de support via l'interface web et la console de maintenance dans Active IQ Unified Manager

Vous devez envoyer un dossier de support lorsque le problème que vous rencontrez nécessite un diagnostic et un dépannage plus détaillés que ce qu'un message AutoSupport fournit. Vous pouvez envoyer un dossier de support au support technique à l'aide de l'interface Web Ui de Unified Manager et de la console de maintenance.

Unified Manager stocke au maximum deux ensembles de support complets et trois ensembles de support allégés à la fois.

Informations connexes

"Rôles et fonctionnalités des utilisateurs d'Unified Manager"

Envoyez des messages AutoSupport au support technique dans Active IQ Unified Manager

La page AutoSupport vous permet d'envoyer des messages AutoSupport prédéfinis et à la demande à votre équipe de support technique afin de garantir le bon fonctionnement de votre environnement et de vous aider à en préserver l'intégrité. AutoSupport est activé par défaut et ne doit pas être désactivé afin que vous puissiez bénéficier des avantages de NetAppActive IQ.

Vous pouvez envoyer des informations de diagnostic système et des données détaillées sur le serveur Unified Manager dans un message au besoin, programmer l'envoi périodique d'un message, ou même générer et envoyer des ensembles de support à l'équipe de support technique.

> Un utilisateur disposant du rôle d'administrateur du stockage peut générer et envoyer des messages AutoSupport à la demande ainsi que des kits de support au support technique. Cependant, seul un administrateur ou un utilisateur de maintenance peut activer ou désactiver AutoSupport périodique et configurer les paramètres HTTP, comme décrit dans la section « Configuration du serveur proxy HTTP ». Dans un environnement nécessitant l'utilisation d'un serveur proxy HTTP, la configuration doit être terminée avant qu'un administrateur du stockage puisse envoyer des messages AutoSupport à la demande ainsi que des kits de support au support technique.

Envoyer des messages AutoSupport à la demande

Vous pouvez générer et envoyer un message à la demande au support technique, à un destinataire d'e-mail spécifique ou aux deux.

Étapes

1. Accédez à **Général** > **AutoSupport**, et effectuez l'une ou les deux actions suivantes :
2. Si vous souhaitez envoyer le message AutoSupport au support technique, cochez la case à cocher **Send to Technical Support**.
3. Si vous souhaitez envoyer le message AutoSupport à un destinataire de courrier électronique spécifique, cochez la case à cocher **Send to Email Recipient**, puis saisissez l'adresse électronique du destinataire.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **Générer et envoyer AutoSupport**.

Activer AutoSupport périodique

Vous pouvez envoyer périodiquement des messages prédéfinis au support technique pour le diagnostic et la résolution des problèmes. Cette fonctionnalité est activée par défaut. Si elle est désactivée, un administrateur ou un utilisateur de maintenance peut activer ces paramètres.

Étapes

1. Accédez à **Général** > **AutoSupport**.
2. Dans la section AutoSupport périodique, sélectionnez la case à cocher **Activer l'envoi périodique des données AutoSupport à Active IQ**.
3. Si nécessaire, définissez le nom, le port et les informations d'authentification du serveur proxy HTTP comme décrit dans la section « Configuration du serveur proxy HTTP ».
4. Cliquez sur **Enregistrer**.

Télécharger le bundle de support à la demande

Vous pouvez générer et envoyer un dossier de support au support technique selon les besoins du dépannage. Unified Manager ne conserve que les deux dossiers de support les plus récemment générés. Les dossiers de support plus anciens sont supprimés du système.

Étant donné que certains types de données de support peuvent consommer beaucoup de ressources du cluster ou nécessiter un temps de traitement important, lorsque vous sélectionnez le pack de support complet, vous pouvez inclure ou exclure certains types de données afin d'en réduire la taille. Vous pouvez également créer un pack de support allégé contenant uniquement les journaux des 30 derniers jours et les enregistrements de la base de données de configuration ; ce pack exclut les données de performance, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

Étapes

1. Accédez à **Général** > **AutoSupport**.
2. Dans la section « Pack d'assistance à la demande », cliquez sur **Générer et envoyer le pack d'assistance**.
3. Pour envoyer un ensemble de support léger au support technique, dans la fenêtre contextuelle Générer et envoyer un ensemble de support, cochez la case à cocher **Générer un ensemble de support léger**.
4. Vous pouvez également, pour envoyer un dossier de support complet, cocher la case à cocher **Generate full support bundle**. Sélectionnez les types de données spécifiques à inclure dans le dossier de support ou à en exclure.

   Même si vous ne sélectionnez aucun type de données, le bundle de support est tout de même généré avec d'autres données Unified Manager.

5. Cochez la case à cocher **Send the bundle to technical support** pour générer et envoyer le bundle au support technique. Si vous ne cochez pas cette case à cocher, le bundle est généré et stocké localement sur le serveur Unified Manager. Le bundle de support généré est disponible pour une utilisation ultérieure dans le répertoire /support sur les systèmes VMware, dans `/opt/netapp/data/support/` sur les systèmes Linux, et dans `ProgramData\NetApp\OnCommandAppData\ocum\support` sur les systèmes Windows.
6. Cliquez sur **Envoyer**.

Configurer un serveur proxy HTTP

Vous pouvez désigner un proxy pour fournir l'accès à Internet afin d'envoyer le contenu AutoSupport au support si votre environnement ne permet pas d'accès direct depuis le serveur Unified Manager. Cette section est réservée aux administrateurs et aux utilisateurs de maintenance.

- **Utilisez un proxy HTTP**

  Cochez cette case pour identifier le serveur utilisé comme proxy HTTP.

  Saisissez le nom de l'hôte ou l'adresse IP du serveur proxy, ainsi que le numéro de port utilisé pour se connecter au serveur.

- **Utilisez l'authentification**

  Cochez cette case si vous devez fournir des informations d'authentification pour accéder au serveur utilisé comme proxy HTTP.

  Saisissez le nom d'utilisateur et le mot de passe requis pour vous authentifier auprès du proxy HTTP.

Les serveurs proxy HTTP qui fournissent uniquement Basic Authentication ne sont pas pris en charge.

Accédez à la console de maintenance dans Active IQ Unified Manager

Si l'interface utilisateur d'Unified Manager n'est pas opérationnelle, ou si vous devez exécuter des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour gérer votre système Unified Manager.

Avant de commencer

Vous devez avoir installé et configuré Unified Manager.

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

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. Suivez ces étapes pour accéder à la console de maintenance :

Sur ce système d'exploitation…	Suivez ces étapes…
VMware	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. b. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe de maintenance.
Linux	a. Utilisez Secure Shell pour vous connecter à l'adresse IP ou au nom de domaine complet du système Unified Manager. b. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de l'utilisateur de maintenance (umadmin). c. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
Windows	a. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Saisissez la commande `maintenance_console` et appuyez sur Entrée.

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

Générez et téléversez un bundle de support depuis Active IQ Unified Manager

Vous pouvez générer un dossier de support contenant des informations de diagnostic afin de l'envoyer au support technique pour obtenir de l'aide au dépannage.

À partir de Unified Manager 9.8, si votre serveur Unified Manager est connecté à Internet, vous pouvez également envoyer le bundle de support à NetApp depuis la console de maintenance.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu'utilisateur de maintenance.

Étant donné que certains types de données de support peuvent consommer beaucoup de ressources du cluster ou nécessiter un temps de traitement important, lorsque vous sélectionnez le pack de support complet, vous pouvez spécifier les types de données à inclure ou à exclure afin de réduire sa taille. Vous pouvez également créer un pack de support allégé contenant uniquement les journaux des 30 derniers jours et les enregistrements de la base de données de configuration — il exclut les données de performance, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

Unified Manager ne conserve que les deux derniers bundles de support générés. Les bundles de support plus anciens sont supprimés du système.

Étapes

1. Dans la console **Menu principal**, sélectionnez **Support/Diagnostics**.
2. Sélectionnez **Générer un pack de support léger** ou **Générer un pack de support** selon le niveau de détail que vous souhaitez inclure dans le pack de support.
3. Si vous choisissez le pack de support complet, sélectionnez ou désélectionnez les types de données suivants à inclure ou à exclure du pack de support :

   - **dump de base de données**

     Une sauvegarde de la base de données MySQL Server.

   - **vidage du tas**

     Aperçu de l'état des principaux processus du serveur Unified Manager. Cette option est désactivée par défaut et ne doit être sélectionnée que sur demande du support client.

   - **enregistrements d'acquisition**

     Enregistrement de toutes les communications entre Unified Manager et les clusters surveillés.

   Si vous désélectionnez tous les types de données, le bundle de support est tout de même généré avec d'autres données Unified Manager.

4. Tapez `g`, puis appuyez sur Entrée pour générer le bundle de support.

   Comme la génération d'un bundle de support est une opération gourmande en mémoire, il vous est demandé de confirmer que vous voulez vraiment générer le bundle de support maintenant.

5. Tapez `y`, puis appuyez sur Entrée pour générer le bundle de support.

   Si vous ne souhaitez pas générer le package de support pour le moment, saisissez `n`, puis appuyez sur Entrée.

6. Si vous avez inclus des fichiers de vidage de la base de données dans le pack de support complet, vous serez invité à préciser la période pour laquelle vous souhaitez inclure les statistiques de performance. L'inclusion des statistiques de performance peut prendre beaucoup de temps et d'espace. Vous pouvez donc également vider la base de données sans inclure les statistiques de performance :

   a. Saisissez la date de début au format AAAAMMJJ.

      Par exemple, saisissez `20210101` pour le 1er janvier 2021. Saisissez `n` si vous ne souhaitez pas inclure les statistiques de performance.

   b. Saisissez le nombre de jours de statistiques à inclure, à compter de 0 h à la date de début spécifiée.

      Vous pouvez saisir un nombre de 1 à 10.

   Si vous incluez des statistiques de performance, le système affiche la période pendant laquelle ces statistiques seront collectées.

7. Une fois le package de support créé, il vous sera demandé si vous souhaitez le télécharger vers NetApp. Tapez `y`, puis appuyez sur Entrée.

   Saisissez votre numéro de dossier de support.

8. Si vous disposez déjà d'un numéro de dossier, saisissez-le et appuyez sur Entrée. Sinon, appuyez simplement sur Entrée.

   Le bundle de support est téléchargé sur NetApp.

Si votre serveur Unified Manager n'est pas connecté à Internet ou si vous ne pouvez pas téléverser le support bundle pour une autre raison, vous pouvez le récupérer et l'envoyer manuellement. Vous pouvez le récupérer à l'aide d'un client SFTP ou de commandes CLI UNIX ou Linux. Sur les installations Windows, vous pouvez utiliser Remote Desktop (RDP) pour récupérer le support bundle.

Le package de support généré se trouve dans le répertoire /support sur les systèmes VMware, dans /opt/netapp/data/support/ sur les systèmes Linux et dans ProgramData\NetApp\OnCommandAppData\ocum\support sur les systèmes Windows.

Informations connexes

"Rôles et fonctionnalités des utilisateurs d'Unified Manager"

Récupérez le bundle de support à l'aide d'un client Windows dans Active IQ Unified Manager

Si vous utilisez Windows, vous pouvez télécharger et installer un outil permettant de récupérer le bundle de support depuis votre serveur Unified Manager. Vous pouvez ensuite envoyer ce bundle au support technique pour un diagnostic plus approfondi du problème. Filezilla ou WinSCP sont des exemples d'outils que vous pouvez utiliser.

Avant de commencer

Vous devez être l'utilisateur de maintenance pour effectuer cette tâche.

Vous devez utiliser un outil prenant en charge SCP ou SFTP.

Étapes

1. Téléchargez et installez l'outil permettant de récupérer le pack de support.

2. Ouvrez l'outil.
3. Connectez-vous à votre serveur de gestion Unified Manager via SFTP.

   Cet outil affiche le contenu du répertoire /support et vous permet de visualiser tous les bundles de support existants.

4. Sélectionnez le répertoire de destination du support bundle 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.

Récupérez le bundle de support à l'aide d'un client UNIX ou Linux dans Active IQ Unified Manager

Si vous êtes un utilisateur UNIX ou Linux, vous pouvez récupérer le package de support à partir de votre vApp en utilisant l'interface de ligne de commande (CLI) sur votre serveur client Linux. Vous pouvez utiliser SCP ou SFTP pour récupérer le package de support.

Avant de commencer

Vous devez être l'utilisateur de maintenance pour effectuer cette tâche.

Vous devez avoir généré un bundle de support à l'aide de la console de maintenance et disposer du nom de ce bundle.

Étapes

1. Accédez à l'interface de ligne de commande (CLI) via Telnet ou la console à partir de votre serveur client Linux.
2. Accédez au /`support` répertoire.
3. Récupérez le package de support et copiez-le dans le répertoire local à l'aide de la commande suivante :

Si vous utilisez…	Utilisez ensuite 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 bundle de support vous est fourni lorsque vous le générez à l'aide de la console de maintenance.

4. Saisissez le mot de passe de l'utilisateur de maintenance.

Exemples

L'exemple suivant utilise SCP pour récupérer le paquet 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 package 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
```

Envoyez un bundle de support au support technique depuis Active IQ Unified Manager

Lorsqu'un problème nécessite des informations de diagnostic et de dépannage plus détaillées que celles fournies par un message AutoSupport, vous pouvez envoyer un dossier de support au support technique.

Avant de commencer

Vous devez avoir accès au support bundle pour l'envoyer au support technique.

Vous devez disposer d'un numéro de dossier généré par le site web d'assistance technique.

Étapes

1. Connectez-vous au site d'assistance NetApp.
2. Téléversez le fichier.

   "Comment téléverser un fichier sur NetApp"

Tâches et informations relatives à plusieurs flux de travail

Comprendre la contention des composants du cluster dans Active IQ Unified Manager

Vous pouvez identifier les problèmes de performance du cluster lorsqu'un composant du cluster est en contention. Les performances des workloads qui utilisent ce composant ralentissent et leur temps de réponse (latence) aux requêtes client augmente, ce qui déclenche un événement dans Unified Manager.

Un composant en situation de contention ne peut pas fonctionner à un niveau optimal. Ses performances ont diminué, et les performances des autres composants du cluster et des workloads, appelés « victimes », peuvent présenter une latence accrue. Pour sortir un composant de la contention, vous devez réduire son workload ou augmenter sa capacité à traiter davantage de travail, afin que les performances puissent revenir à des niveaux normaux. Comme Unified Manager collecte et analyse les performances des workloads à intervalles de cinq minutes, il détecte uniquement lorsqu'un composant du cluster est constamment surutilisé. Les pics transitoires de surutilisation qui ne durent qu'une courte période pendant l'intervalle de cinq minutes ne sont pas détectés.

Par exemple, un agrégat de stockage peut être en situation de contention parce qu'une ou plusieurs workloads qu'il contient se disputent le traitement de leurs requêtes d'E/S. D'autres workloads sur l'agrégat peuvent être affectés, ce qui entraîne une baisse de leurs performances. Pour réduire le niveau d'activité sur l'agrégat, vous pouvez prendre différentes mesures, par exemple déplacer une ou plusieurs workloads vers un agrégat ou un nœud moins sollicité, afin de réduire la demande globale de workload sur l'agrégat actuel. Pour un groupe de stratégies QoS, vous pouvez ajuster la limite de débit ou déplacer des workloads vers un autre groupe de stratégies, afin que les workloads ne soient plus limités.

Unified Manager surveille les composants de cluster suivants pour vous alerter lorsqu'ils sont en contention :

- **Réseau**

  Représente le temps d'attente des requêtes d'E/S par les protocoles réseau externes du cluster. Ce temps d'attente correspond au temps nécessaire pour que les transactions « transfer ready » soient terminées avant que le cluster puisse répondre à une requête d'E/S. Si le composant réseau est en contention, cela signifie qu'un temps d'attente élevé au niveau du protocole impacte la latence d'une ou plusieurs charges de travail.

- **Traitement réseau**

  Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre la couche protocolaire et le cluster. Le nœud gérant le traitement réseau a peut-être changé depuis la détection de l'événement. Si le composant de traitement réseau est en contention, cela signifie qu'une utilisation élevée du nœud de traitement réseau impacte la latence d'un ou de plusieurs workloads.

  Lors de l'utilisation d'un cluster All SAN Array en configuration active-active, la valeur de latence de traitement réseau est affichée pour les deux nœuds afin que vous puissiez vérifier que la charge est répartie équitablement entre eux.

- **Limite QoS maximale**

  Représente le paramètre de débit maximal (de pointe) du groupe de règles de qualité de service (QoS) du stockage attribué au workload. Si le composant du groupe de règles est en conflit, cela signifie que tous les workloads du groupe de règles sont limités par la limite de débit définie, ce qui affecte la latence d'un ou de plusieurs de ces workloads.

- **Limite minimale de QoS**

  Représente la latence d'un workload causée par le paramètre minimal de débit QoS (attendu) attribué à d'autres workloads. Si le minimum QoS défini sur certains workloads utilise la majeure partie de la bande passante pour garantir le débit promis, les autres workloads seront limités et présenteront une latence plus élevée.

- **Interconnexion de cluster**

  Représente les câbles et adaptateurs auxquels les nœuds du cluster sont physiquement connectés. Si le composant d'interconnexion de cluster est saturé, cela signifie qu'un temps d'attente élevé pour les requêtes d'E/S au niveau de l'interconnexion de cluster affecte la latence d'un ou de plusieurs workloads.

- **Data Processing**

  Représente le composant logiciel du cluster impliqué dans le traitement des E/S entre le cluster et l'agrégat de stockage qui contient le workload. Le nœud gérant le traitement des données a peut-être changé depuis la détection de l'événement. Si le composant de traitement des données est en contention, cela signifie qu'une utilisation élevée au niveau du nœud de traitement des données affecte la latence d'un ou

de plusieurs workloads.

- **Activation du volume**

  Représente le processus qui suit l'utilisation de tous les volumes actifs. Dans les environnements de grande taille où plus de 1 000 volumes sont actifs, ce processus suit le nombre de volumes critiques qui doivent accéder simultanément aux ressources via le nœud. Lorsque le nombre de volumes actifs simultanés dépasse le seuil maximal recommandé, certains volumes non critiques présentent une latence, comme indiqué ici.

- **MetroCluster Ressources**

  Représente les ressources MetroCluster, notamment NVRAM et les liaisons inter-commutateurs (ISL), utilisées pour mettre en miroir les données entre les clusters dans une configuration MetroCluster. Si le composant MetroCluster est en conflit, cela signifie qu'un débit d'écriture élevé provenant des workloads sur le cluster local ou un problème d'état de la liaison affecte la latence d'un ou de plusieurs workloads sur le cluster local. Si le cluster n'est pas dans une configuration MetroCluster, cette icône n'est pas affichée.

- **Opérations sur des agrégats ou des agrégats SSD**

  Représente l'agrégat de stockage sur lequel les workloads s'exécutent. Si le composant d'agrégat est en contention, cela signifie qu'une utilisation élevée de l'agrégat affecte la latence d'un ou de plusieurs workloads. Un agrégat se compose uniquement de HDD, ou d'un mélange de HDD et de SSD (un agrégat Flash Pool), ou d'un mélange de HDD et d'un niveau cloud (un agrégat FabricPool). Un « `SSD Aggregate` » se compose uniquement de SSD (un agrégat 100 % Flash), ou d'un mélange de SSD et d'un niveau cloud (un agrégat FabricPool).

- **Latence du cloud**

  Ce composant logiciel du cluster gère les entrées/sorties entre le cluster et le niveau cloud où sont stockées les données utilisateur. Si le composant de latence cloud est saturé, cela signifie qu'un grand nombre de lectures sur des volumes hébergés sur le niveau cloud impactent la latence d'un ou plusieurs workloads.

- **Synchronisation SnapMirror**

  Représente le composant logiciel du cluster impliqué dans la réplication des données utilisateur du volume principal vers le volume secondaire dans une relation synchrone SnapMirror. Si le composant de synchronisation SnapMirror est en contention, cela signifie que l'activité des opérations synchrones SnapMirror affecte la latence d'un ou de plusieurs workloads.

Consultez la page Détails du volume/de la santé dans Active IQ Unified Manager

La page Détails du volume/de l'état vous permet de consulter des informations détaillées sur un volume sélectionné, telles que sa capacité, son efficacité de stockage, sa configuration, sa protection, ses annotations et les événements générés. Vous pouvez également y consulter des informations sur les objets associés et les alertes relatives à ce volume.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour le volume sélectionné :

- **Passer à la vue Performance**

  Permet d'accéder à la page de détails du volume/des performances.

- **Actions**
  - Ajouter une alerte

    Permet d'ajouter une alerte au volume sélectionné.

  - Modifier les seuils

    Permet de modifier les paramètres de seuil pour le volume sélectionné.

  - Annoter

    Permet d'annoter le volume sélectionné.

  - Protéger

    Permet de créer des relations SnapMirror ou SnapVault pour le volume sélectionné.

  - Relation

    Permet d'exécuter les opérations suivantes relatives aux relations de protection :

    - Modifier

      Ouvre la boîte de dialogue Modifier la relation, qui vous permet de modifier les politiques SnapMirror, les planifications et les taux de transfert maximum pour une relation de protection existante.

    - Abandonner

      Interrompt les transferts en cours pour une relation sélectionnée. Permet également de supprimer le point de contrôle de redémarrage pour les transferts autres que le transfert de base. Il est impossible de supprimer le point de contrôle d'un transfert de base.

    - Suspendre

      Désactive temporairement les mises à jour planifiées pour une relation sélectionnée. Les transferts déjà en cours doivent se terminer avant que la relation ne soit mise en attente.

    - Rompre

      Rompt la relation entre les volumes source et de destination et transforme le volume de destination en un volume de lecture-écriture.

    - Retirer

      Supprime définitivement la relation entre la source et la destination sélectionnées. Les volumes ne sont pas détruits et les copies Snapshot présentes sur ces volumes ne sont pas supprimées. Cette opération est irréversible.

    - Résumé

Active les transferts planifiés pour une relation mise en pause. Au prochain intervalle de transfert planifié, un point de contrôle de redémarrage est utilisé, s'il en existe un.

- Resynchroniser

  Permet de resynchroniser une relation précédemment rompue.

- Initialiser/Mettre à jour

  Permet d'effectuer un premier transfert de base sur une nouvelle relation de protection, ou d'effectuer une mise à jour manuelle si la relation est déjà initialisée.

- Resynchronisation inversée

  Permet de rétablir une relation de protection précédemment interrompue, en inversant la fonction de la source et de la destination en faisant de la source une copie de la destination d'origine. Le contenu de la source est écrasé par celui de la destination, et toutes les données plus récentes que celles de la copie Snapshot commune sont supprimées.

◦ Restaurer

Permet de restaurer des données d'un volume vers un autre volume. Pour plus d'informations, consultez "Restauration des données à l'aide de la page Détails du volume / de l'état".

> Le bouton Restaurer et les boutons d'opération de la relation ne sont pas disponibles pour les volumes qui se trouvent dans des relations de protection synchrone.

- **Afficher les volumes**

  Permet d'accéder à la vue Santé : Tous les volumes.

Onglet Capacité

L'onglet Capacité affiche des détails sur le volume sélectionné, tels que sa capacité physique, sa capacité logique, ses paramètres de seuil, sa capacité de quota et des informations sur toute opération de déplacement de volume:

- **Capacité physique**

  Indique la capacité physique du volume :

  ◦ Débordement de l'instantané

  Affiche l'espace de données consommé par les copies Snapshot.

  ◦ Utilisé

  Affiche l'espace utilisé par les données dans le volume.

  ◦ Avertissement

  Indique que l'espace dans le volume est presque plein. Si ce seuil est dépassé, l'événement « Espace presque plein » est généré.

  ◦ Erreur

Indique que l'espace dans le volume est plein. Si ce seuil est dépassé, l'événement Space Full est généré.

- Inutilisable

  Indique qu'un événement « Espace à risque pour un volume à provisionnement fin » a été généré et que l'espace du volume à provisionnement fin est menacé en raison de problèmes de capacité de l'agrégat. La capacité inutilisable est affichée uniquement pour les volumes à provisionnement fin.

- Graphique de données

  Affiche la capacité totale de données et la capacité de données utilisée du volume.

  Si l'extension automatique est activée, le graphique de données affiche également l'espace disponible dans l'agrégat. Ce graphique affiche l'espace de stockage effectif utilisable par les données du volume, qui peut prendre l'une des valeurs suivantes :

  - Capacité de données réelle du volume pour les conditions suivantes :
    - La croissance automatique est désactivée.
    - Le volume en mode de croissance automatique a atteint sa taille maximale.
    - Le volume à provisionnement épais avec croissance automatique activée ne peut plus croître.
  - Capacité de données du volume après prise en compte de la taille maximale du volume (pour les volumes à provisionnement fin et pour les volumes à provisionnement épais lorsque l'agrégat dispose d'espace pour que le volume atteigne sa taille maximale)
  - Capacité de données du volume après prise en compte de la prochaine taille d'extension automatique possible (pour les volumes à provisionnement dense ayant un seuil de pourcentage d'extension automatique)

- Graphique des 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 de dépassement de la réserve Snapshot par la capacité Snapshot si la capacité Snapshot utilisée dépasse la réserve Snapshot.

- **Capacité logique**

  Affiche les caractéristiques de l'espace logique du volume. L'espace logique indique la taille réelle des données stockées sur le disque sans appliquer les économies permises par l'utilisation des technologies d'efficacité du stockage ONTAP.

  - Rapports sur l'espace logique

    Indique si le volume est configuré pour le rapport d'espace logique. La valeur peut être Activée, Désactivée ou Non applicable. « Non applicable » s'affiche pour les volumes sur des versions antérieures de ONTAP ou pour les volumes qui ne prennent pas en charge le rapport d'espace logique.

  - Utilisé

    Affiche la quantité d'espace logique utilisé par les données dans le volume, ainsi que le pourcentage d'espace logique utilisé par rapport à 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. Lorsqu’elle est activée, la taille logique utilisée du volume ne peut pas être supérieure à la taille physique du volume actuellement définie.

- **Croissance automatique**

  Indique si le volume augmente automatiquement lorsqu’il manque d’espace.

- **Garantie d’espace**

  Affiche le contrôle du paramètre du volume FlexVol lorsqu’un volume supprime des blocs libres d’un agrégat. Ces blocs sont alors garantis comme disponibles pour l’écriture dans les fichiers du volume. La garantie d’espace peut être définie sur l’une des valeurs suivantes :

  - Aucune

    Aucune garantie d’espace n’est configurée pour le volume.

  - Fichier

    La taille totale des fichiers écrits de manière éparse (par exemple, les LUN) est garantie.

  - Volume

    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 sur 100 Mo par défaut. 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 par la suite, la garantie d’espace minimale n’est pas incrémentée.

  La garantie d’espace est partielle lorsque le volume est de type Data-Cache.

- **Détails (physiques)**

  Affiche les caractéristiques physiques du volume.

- **Capacité totale**

  Affiche la capacité physique totale dans le volume.

- **Capacité des données**

  Affiche l’espace physique occupé par le volume (capacité utilisée) et l’espace physique restant disponible (capacité libre) dans le volume. Ces valeurs sont également affichées en pourcentage de la capacité physique totale.

  Lorsque l’événement « Espace à risque pour les volumes à provisionnement fin » est généré pour des volumes à provisionnement fin, la quantité d’espace utilisée par le volume (capacité utilisée) et la quantité d’espace disponible dans le volume, mais inutilisable (capacité inutilisable) en raison de problèmes de

capacité de l’agrégat, s’affichent.

- **Réserve de snapshots**

  Affiche l’espace utilisé par les copies Snapshot (capacité utilisée) et l’espace disponible pour les copies Snapshot (capacité libre) dans le volume. Ces valeurs sont également affichées en pourcentage de la réserve Snapshot totale.

  Lorsque l’événement « Espace à risque pour les volumes à provisionnement fin » est généré pour les volumes à provisionnement fin, la quantité d’espace utilisée par les copies Snapshot (capacité utilisée) et la quantité d’espace disponible dans le volume, mais qui ne peut pas être utilisée pour créer des copies Snapshot (capacité inutilisable) en raison de problèmes de capacité de l’agrégat, sont affichées.

- **Seuils de volume**

  Affiche les seuils de capacité de volume suivants :

  - Seuil de remplissage presque complet

    Indique le pourcentage auquel un volume est presque plein.

  - Seuil plein

    Indique le pourcentage de remplissage d’un volume.

- **Autres détails**

  - Taille maximale de croissance automatique

    Affiche la taille maximale que le volume peut atteindre automatiquement. La valeur par défaut est de 120 % de la taille du volume à sa création. Ce champ s’affiche uniquement lorsque l’extension automatique est activée pour le volume.

  - Capacité engagée du quota Qtree

    Affiche l’espace réservé dans les quotas.

  - Capacité de surallocation du quota Qtree

    Affiche la quantité d’espace utilisable avant que le système ne génère l’événement « Volume Qtree Quota Overcommitted ».

  - Réserve fractionnaire

    Contrôle la taille de la réserve pour écrasement. Par défaut, la réserve fractionnaire est définie sur 100 %, ce qui indique que 100 % de l’espace réservé requis est réservé afin que les objets soient entièrement protégés contre les écrasements. Si la réserve fractionnaire est inférieure à 100 %, l’espace réservé pour tous les fichiers à espace réservé de ce volume est réduit au pourcentage de la réserve fractionnaire.

  - Taux de croissance quotidien de Snapshot

    Affiche la modification (en pourcentage, ou en Ko, Mo, Go, etc.) qui survient toutes les 24 heures dans les copies Snapshot du volume sélectionné.

  - Jours avant saturation de Snapshot

Affiche le nombre estimé de jours restants avant que l'espace réservé aux copies Snapshot dans le volume n'atteigne le seuil spécifié.

Le champ « Jours avant remplissage de Snapshot » affiche la valeur « Non applicable » lorsque le taux de croissance des copies Snapshot dans le volume est nul ou négatif, ou lorsqu'il n'y a pas suffisamment de données pour calculer le taux de croissance.

◦ Suppression automatique des copies Snapshot

Indique si les copies Snapshot sont automatiquement supprimées pour libérer de l'espace 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 dans le volume.

Le nombre de copies Snapshot dans le volume est affiché sous forme de lien. Lorsque vous cliquez sur ce lien, la boîte de dialogue « Copies Snapshot d'un volume » s'ouvre et affiche les détails des copies Snapshot.

Le nombre de copies Snapshot est mis à jour environ toutes les heures ; cependant, la liste des copies Snapshot est mise à jour au moment où vous cliquez sur l'icône. Il peut donc y avoir une différence entre le nombre de copies Snapshot affiché 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 effectuée sur le volume, ainsi que d'autres détails, tels que la phase actuelle de l'opération de déplacement de volume en cours, l'agrégat source, l'agrégat de destination, l'heure de début, l'heure de fin et l'heure de fin estimée.

Affiche également le nombre d'opérations de déplacement de volume effectuées sur le volume sélectionné. Pour plus d'informations sur ces opérations, cliquez sur le lien **Historique des déplacements de volume**.

Onglet Configuration

L'onglet Configuration affiche des détails sur le volume sélectionné, tels que les règles d'export, le type RAID, la capacité et les fonctionnalités liées à l'efficacité du stockage du volume :

- **Aperçu**

◦ Nom complet

Affiche le nom complet du volume.

◦ Agrégats

Affiche le nom de l'agrégat sur lequel réside le volume, ou le nombre d'agrégats sur lesquels réside le volume FlexGroup.

◦ Politique de hiérarchisation

Affiche la stratégie de hiérarchisation définie pour le volume, si celui-ci est déployé sur un agrégat compatible avec FabricPool. La stratégie peut être Aucune, Instantané uniquement, Sauvegarde,

Automatique ou Toutes.

- VM de stockage

  Affiche le nom de la SVM qui contient le volume.

- Chemin de jonction

  Affiche l'état du chemin, qui peut être actif ou inactif. Le chemin dans la SVM sur lequel le volume est monté s'affiche également. Vous pouvez cliquer sur le lien **Historique** pour afficher les cinq modifications les plus récentes apportées au chemin de jonction.

- Règles d'export

  Affiche le nom de la règles d'export créée pour le volume. Vous pouvez cliquer sur le lien pour afficher des détails sur les règles d'export, les protocoles d'authentification et l'accès activé sur les volumes appartenant à la SVM.

- Style

  Affiche le style de volume. Le style de volume peut être FlexVol ou FlexGroup.

- Type

  Affiche le type du volume sélectionné. Le type de volume peut être : Lecture-écriture, Partage de charge, Protection des données, Cache de données ou Temporaire.

- Type RAID

  Affiche le type RAID du volume sélectionné. Le type RAID peut être RAID0, RAID4, RAID-DP ou RAID-TEC.

  Plusieurs types RAID peuvent s'afficher pour les volumes FlexGroup, car les volumes constitutifs des FlexGroups peuvent se trouver sur des agrégats de types différents.

- Type de SnapLock

  Affiche le type SnapLock de l'agrégat qui contient le volume.

- SnapLock Expiration

  Affiche la date d'expiration du volume SnapLock.

- **Capacité**
  - Provisionnement fin

    Indique si le provisionnement est configuré pour le volume.

  - Dimensionnement automatique

    Indique si le volume flexible augmente automatiquement dans un agrégat.

  - Suppression automatique des copies Snapshot

    Indique si les copies Snapshot sont automatiquement supprimées pour libérer de l'espace 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

    Indique si l'opération de déduplication activée sur un volume est manuelle, planifiée ou basée sur une stratégie. Si le mode est défini sur Planifiée, la planification de l'opération est affichée, et si le mode est défini sur une stratégie, le nom de la stratégie est affiché.

  - Type de déduplication

    Spécifie le type d'opération de déduplication exécutée sur le volume. Si le volume est dans une relation SnapVault, le type affiché est SnapVault. Pour tout autre volume, le type affiché est Régulier.

  - Politique d'efficacité du stockage

    Indique le nom des règles d'efficacité attribuées à ce volume via Unified Manager. Ces règles peuvent contrôler les paramètres de compression et de déduplication.

- **Protection**
  - Copies Snapshot

    Indique si les copies Snapshot automatiques sont activées ou désactivées.

Onglet Protection

L'onglet Protection affiche des détails de protection sur le volume sélectionné, tels que les informations sur le retard, le type de relation et la topologie de la relation.

- **Résumé**

  Affiche les propriétés des relations de protection (SnapMirror, SnapVault ou Storage VM DR) pour un volume sélectionné. Pour tout autre type de relation, seule la propriété Type de relation est affichée. Si un volume principal est sélectionné, seules les stratégies de copie Snapshot gérée et locale sont affichées. Les propriétés affichées pour les relations SnapMirror et SnapVault incluent les suivantes :

  - Volume source

    Affiche le nom de la source du volume sélectionné si celui-ci est une destination.

  - État du retard

    Affiche l'état du délai de mise à jour ou de transfert d'une relation de protection. L'état peut être Erreur,

Avertissement ou Critique.

L'état du décalage ne s'applique pas aux relations synchrones.

- Durée du décalage

  Affiche le délai de décalage temporel entre les données du miroir et celles de 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 un service de stockage et est géré par celui-ci.

- Version de la réplication flexible

  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 option de sauvegarde » indique la mise en œuvre de la protection SnapMirror avec la possibilité de conserver plusieurs versions des copies de sauvegarde sur la destination. « Aucun » indique que la réplication flexible de version n'est pas activée.

- Capacité de la 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 tout type de relation, y compris Miroir asynchrone, coffre-fort asynchrone, MirrorVault asynchrone, StrictSync et Sync.

- État de la relation

  Affiche l'état de la relation SnapMirror ou SnapVault. L'état peut être Uninitialized, SnapMirrored ou Broken-Off. Si un volume source est sélectionné, l'état de la relation n'est pas applicable et n'est pas affiché.

- État du transfert

  Affiche l'état du transfert pour la relation de protection. L'état du transfert peut être l'un des suivants :

  - Annulation en cours

    Les transferts SnapMirror sont activés ; cependant, une opération d'annulation de transfert pouvant inclure la suppression du point de contrôle est en cours.

- Vérification

  Le volume de destination subit une vérification diagnostique 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 incrémentiels SnapVault.

- Inactif

  Les transferts sont activés et aucun transfert n'est en cours.

- Synchronisé

  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

  SnapMirror est activé pour les transferts. Le volume est actuellement dans la phase de pré-transfert pour les transferts incrémentiels SnapVault.

- En file d'attente

  SnapMirror les transferts sont activés. Aucun transfert n'est en cours.

- Suspendu

  Les transferts SnapMirror sont désactivés. Aucun transfert n'est en cours.

- Suspension

  Un transfert SnapMirror est en cours. Les transferts supplémentaires sont désactivés.

- Transfert

  SnapMirror est activé et un transfert est en cours.

- Transition

  Le transfert asynchrone des données du volume source vers le volume de destination est terminé et la transition vers un fonctionnement synchrone a commencé.

- En attente

  Un transfert SnapMirror a été lancé, mais certaines tâches associées sont en attente de mise en file d'attente.

◦ Taux de transfert maximal

Affiche le débit de transfert maximal pour la relation. Le débit de transfert maximal peut être une valeur numérique en kilo-octets par seconde (Kbps), mégaoctets par seconde (Mbps), gigaoctets par seconde

(Gbps) ou téraoctets par seconde (Tbps). Si la mention « Aucune limite » apparaît, le transfert de base entre les relations est illimité.

- SnapMirror stratégie

  Affiche la stratégie de protection du volume. DPDefault indique la stratégie de protection par défaut « Miroir asynchrone », XDPDefault indique la stratégie par défaut « Vault asynchrone » et DPSyncDefault indique la stratégie par défaut MirrorVault asynchrone. StrictSync indique la stratégie de protection stricte synchrone par défaut, et Sync indique la stratégie synchrone par défaut. Vous pouvez cliquer sur le nom de la stratégie pour afficher les détails associés à cette stratégie, y compris les informations suivantes :

  - priorité de transfert
  - Ignorer le paramètre de temps d'accès
  - Limite de tentatives
  - Commentaires
  - SnapMirror étiquettes
  - Paramètres de rétention
  - Copies Snapshot réelles
  - Conserver les copies Snapshot
  - Seuil d'alerte de rétention
  - Copies Snapshot sans paramètres de rétention Dans une relation SnapVault en cascade où la source est un volume de protection des données (DP), seule la règle « `sm_created` » s'applique.

- Calendrier de mise à jour

  Affiche la planification SnapMirror associée à la relation. Placez votre curseur sur l'icône d'information pour afficher les détails de la planification.

- Stratégie Snapshot locale

  Affiche la stratégie de copie Snapshot pour le volume. La stratégie est Default, None ou tout nom donné à une stratégie personnalisée.

- Protégé par

  Affiche le type de protection utilisé pour le volume sélectionné. Par exemple, si un volume est protégé par des relations de volume Consistency Group et SnapMirror, ce champ affiche à la fois SnapMirror et Consistency Group. Ce champ fournit également un lien qui vous redirige vers la page Relationships pour afficher l'état unifié des relations. Le lien s'applique uniquement aux relations de constituants.

- 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. Cette topologie comprend des représentations graphiques de tous les volumes liés au volume sélectionné. Le volume sélectionné est indiqué par une bordure gris foncé, et les lignes entre les volumes indiquent le type de relation de protection. Le sens des

relations dans la topologie est affiché de gauche à droite, la source de chaque relation étant à gauche et la destination à droite.

Les doubles traits gras indiquent une relation Mirror asynchrone, un seul trait gras indique une relation Vault asynchrone, les doubles traits simples indiquent une relation MirrorVault asynchrone, et un trait gras et un trait non gras indiquent une relation synchrone. Le tableau ci-dessous indique si la relation synchrone est de type StrictSync ou Sync.

Un clic droit sur un volume affiche un menu qui vous permet de choisir de protéger le volume ou d'y restaurer des données. Un clic droit sur une relation affiche un menu qui vous permet de choisir de modifier, d'interrompre, de mettre en pause, de rompre, de supprimer ou de reprendre une relation.

Les menus ne s'afficheront pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action, par exemple si vous ne disposez que de privilèges d'opérateur
- Si le volume fait partie d'une relation de protection synchrone
- Lorsque l'ID du volume est inconnu, par exemple lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert, le fait de cliquer sur un autre volume dans la topologie sélectionne ce volume et affiche les informations le concernant. 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 de capacité sont manquantes. Le fait de placer votre curseur sur le point d'interrogation affiche des informations supplémentaires, y compris des suggestions d'actions correctives.

La topologie affiche des informations sur la capacité du volume, le retard, les copies Snapshot et le dernier transfert de données réussi si elle correspond à l'un de plusieurs modèles de topologie courants. Si une topologie ne correspond à aucun de ces modèles, les informations sur le retard du volume et le dernier transfert de données réussi s'affichent dans un tableau des relations sous la topologie. Dans ce cas, la ligne mise en surbrillance dans le tableau indique le volume sélectionné et, dans la vue de topologie, des lignes en gras avec un point bleu indiquent la relation entre le volume sélectionné et son volume source.

Les vues topologiques comprennent les informations suivantes :

- Capacité

  Affiche la capacité totale utilisée par le volume. Lorsque vous placez le curseur sur un volume dans la topologie, les paramètres de seuil d'avertissement et 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 **Edit Thresholds** dans la boîte de dialogue « Paramètres de seuil actuels ». Si vous décochez la case à cocher **Capacity**, toutes les informations de capacité de tous les volumes de la topologie sont masquées.

- Décalage

  Affiche la durée du décalage et l'état du décalage des relations de protection entrantes. Le fait de décocher la case à cocher **Lag** masque toutes les informations de décalage pour tous les volumes de la topologie. Lorsque la case à cocher **Lag** est grisée, les informations de décalage du volume sélectionné s'affichent dans le tableau des relations situé sous la topologie, ainsi que les informations de décalage de tous les volumes associés.

- Instantané

  Affiche le nombre de copies Snapshot disponibles pour un volume. Décocher la case à cocher **Snapshot** masque toutes les informations relatives aux copies Snapshot pour tous les volumes de la topologie.

Cliquer sur l'icône de copie Snapshot () affiche la liste des copies Snapshot d'un volume. Le nombre de copies Snapshot affiché à côté de l'icône est mis à jour environ toutes les heures ; cependant, la liste des copies Snapshot est mise à jour lorsque vous cliquez sur l'icône. Cela peut entraîner une différence entre le nombre de copies Snapshot affiché 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 à cocher **Last Successful Transfer** est grisée, les informations relatives au dernier transfert de données réussi du volume sélectionné s'affichent dans le tableau des relations situé sous la topologie, ainsi que les informations relatives au dernier transfert de données réussi de tous les volumes associés.

  - **Histoire**

    Affiche sous forme de graphique l'historique des relations de protection entrantes SnapMirror et SnapVault pour le volume sélectionné. Trois graphiques d'historique sont disponibles : durée du décalage des relations entrantes, durée du transfert des relations entrantes et taille du transfert des relations entrantes. Les informations d'historique ne sont affichées que lorsque vous sélectionnez un volume de destination. Si vous sélectionnez un volume principal, les graphiques sont vides et le message No data found s'affiche. Si les volumes sont protégés par des relations de groupe de cohérence et SnapMirror synchrones, les informations sur la durée du transfert des relations et la taille du transfert des relations ne sont pas affichées.

  Vous pouvez sélectionner un type de graphique dans la liste déroulante située en haut du volet Historique. Vous pouvez également consulter les détails d'une période spécifique en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques d'historique peuvent vous aider à identifier des tendances : par exemple, si d'importantes quantités de données sont transférées à la même heure de la journée ou le même jour de la semaine, ou si le seuil d'avertissement de retard ou le seuil d'erreur de retard est régulièrement dépassé, vous pouvez prendre les mesures appropriées. De plus, vous pouvez cliquer sur le bouton **Export** pour créer un rapport au format CSV pour le graphique que vous consultez.

Les graphiques d'historique de protection affichent les informations suivantes :

- **Durée du décalage de la relation**

  Affiche les secondes, les minutes ou les heures sur l'axe vertical (y), et les jours, les mois ou les années sur l'axe horizontal (x), selon la période de durée sélectionnée. La valeur supérieure sur l'axe y indique la durée de retard maximale atteinte pendant la période de durée affichée sur l'axe x. La ligne orange horizontale du graphique représente le seuil d'erreur de retard, et la ligne jaune horizontale représente le seuil d'avertissement de retard. Lorsque vous placez votre curseur sur ces lignes, le paramètre de seuil s'affiche. La ligne bleue horizontale représente la durée de retard. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur une zone d'intérêt.

- **Durée du transfert de relation**

  L'axe vertical (y) affiche les secondes, les minutes ou les heures, et l'axe horizontal (x) les jours, les mois ou les années, selon la période sélectionnée. La valeur supérieure sur l'axe des y indique la durée de transfert maximale atteinte pendant la période affichée sur l'axe des x. Vous pouvez afficher les détails de points précis du graphique en plaçant votre curseur sur la zone souhaitée.

  > Ce graphique n'est pas disponible pour les volumes faisant l'objet de relations de protection synchrones.

- **Taille transférée de la relation**

L'axe vertical (y) affiche les octets, kilo-octets, méga-octets, etc., en fonction de la taille du transfert, et l'axe horizontal (x) affiche les jours, mois ou années en fonction de la période sélectionnée. La valeur maximale sur l'axe y correspond à la taille maximale du transfert atteinte pendant la période indiquée sur l'axe x. Vous pouvez afficher les détails de points précis du graphique en plaçant votre curseur sur la zone souhaitée.

Ce graphique n'est pas disponible pour les volumes faisant l'objet de relations de protection synchrones.

Zone historique

La section Historique affiche des graphiques fournissant des informations sur la capacité et les réservations d'espace du volume sélectionné. Vous pouvez également cliquer sur le bouton **Exporter** pour générer un rapport au format CSV à partir du graphique affiché.

Les graphiques peuvent être vides et le message No data found peut s'afficher 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 consulter les détails d'une période spécifique en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques d'historique peuvent vous aider à identifier les tendances ; par exemple, si l'utilisation du volume dépasse régulièrement le seuil « Presque plein », vous pouvez prendre les mesures appropriées.

Les graphiques historiques affichent les informations suivantes :

- **Capacité utilisée du volume**

  Affiche la capacité utilisée dans le volume ainsi que la tendance d'utilisation de la capacité du volume, en fonction de l'historique d'utilisation, sous forme de graphiques linéaires en octets, kilo-octets, méga-octets, etc., sur l'axe vertical (y). La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques sur le graphique en plaçant votre curseur sur une zone donnée. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende « Capacité utilisée du volume », la courbe du graphique Capacité utilisée du volume est masquée.

- **Capacité du volume utilisée par rapport à la capacité totale**

  Affiche l'évolution de l'utilisation de la capacité du volume en fonction de l'historique d'utilisation, ainsi que la capacité utilisée, la capacité totale et les détails des économies d'espace grâce à la déduplication et à la compression, sous forme de graphiques linéaires, en octets, kilo-octets, mégaoctets, etc., sur l'axe vertical (y). La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'un an. Vous pouvez afficher les détails de points spécifiques sur le graphique en plaçant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Trend Capacity Used, la ligne du graphique Trend Capacity Used est masquée.

- **Capacité du volume utilisée (%)**

  Affiche la capacité utilisée dans le volume et la tendance de l'utilisation de la capacité du volume en fonction de l'historique d'utilisation, sous forme de courbes, en pourcentage, sur l'axe vertical (y). La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'une année. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher une courbe en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Volume Used Capacity, la courbe Volume Used Capacity est masquée.

- **Capacité de snapshot utilisée (%)**

  Affiche la réserve Snapshot et le seuil d'avertissement Snapshot sous forme de courbes, ainsi que la capacité utilisée par les copies Snapshot sous forme de graphique en aires, en pourcentage, sur l'axe vertical (y). Le dépassement Snapshot est représenté par différentes couleurs. La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'un an. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher une courbe en cliquant sur la légende correspondante. Par exemple, lorsque vous cliquez sur la légende Snapshot Reserve, la courbe Snapshot Reserve est masquée.

Liste des événements

La liste des événements affiche des détails sur les événements nouveaux et acquittés :

- **Gravité**

  Indique la gravité de l'événement.

- **Événement**

  Affiche le nom de l'événement.

- **Heure de déclenchement**

  Affiche le temps écoulé depuis la génération de l'événement. Si ce temps dépasse une semaine, l'horodatage de la génération de l'événement s'affiche.

Volet des annotations associées

Le volet Annotations associées vous permet d'afficher les détails des annotations associées au volume sélectionné. Ces détails comprennent le nom de l'annotation et les valeurs d'annotation appliquées au volume. Vous pouvez également supprimer manuellement des annotations depuis le volet Annotations associées.

Volet Appareils associés

Le volet Périphériques associés vous permet d'afficher les SVM, les agrégats, les qtrees, les LUN et les copies Snapshot liés au volume, et d'y accéder :

- **Machine virtuelle de stockage**

  Affiche la capacité et l'état de santé de la 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 qui composent 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, selon le niveau de gravité le plus élevé. Par exemple, si un agrégat contient dix volumes, dont cinq affichent l'état « Avertissement » et les cinq autres l'état « Critique », l'état affiché est « Critique ». Ce composant n'apparaît pas pour les volumes FlexGroup.

- **Qtrees**

  Affiche le nombre de qtrees que contient le volume sélectionné ainsi que la capacité des qtrees avec quota que contient le volume sélectionné. La capacité des qtrees avec quota est affichée par rapport à la capacité de données du volume. L'état de santé des qtrees est également affiché, en fonction du niveau de gravité le plus élevé. Par exemple, si un volume comporte dix qtrees, cinq avec l'état Avertissement et les cinq autres avec 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 tous les LUN du volume sélectionné. L'état de santé des LUN est également affiché, selon le niveau de gravité le plus élevé.

- **Quotas par utilisateur et par groupe**

  Affiche le nombre et l'état des quotas d'utilisateurs et de groupes d'utilisateurs associés au volume et à ses qtrees.

- **Volumes FlexClone®**

  Affiche le nombre et la capacité de tous les volumes clonés du volume sélectionné. Le nombre et la capacité ne sont affichés que si le volume sélectionné contient des volumes clonés.

- **Volume parent**

  Affiche le nom et la capacité du volume parent d'un volume FlexClone sélectionné. Le volume parent n'est affiché que si le volume sélectionné est un volume FlexClone.

volet Groupes associés

Le volet Groupes associés vous permet d'afficher la liste des groupes associés au volume sélectionné.

Volet Alertes associées

Le volet « Alertes associées » vous permet de consulter la liste des alertes créées pour le volume sélectionné. Vous pouvez également ajouter une alerte en cliquant sur le lien « Ajouter une alerte » ou modifier une alerte existante en cliquant sur son nom.

Consultez la page de détails sur l'état de santé de la Storage VM dans Active IQ Unified Manager

La page « Détails de la machine virtuelle de stockage / État » vous permet de consulter des informations détaillées sur la machine virtuelle de stockage sélectionnée, telles que son état, sa capacité, sa configuration, ses stratégies de données, ses interfaces logiques (LIF), ses LUN, ses qtrees, ses quotas d'utilisateurs et de groupes d'utilisateurs, ainsi que les détails de sa protection. Vous pouvez également consulter des informations sur les objets associés et les alertes associées à la machine virtuelle de stockage.

Vous pouvez surveiller uniquement la machine virtuelle de stockage des données.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour la machine virtuelle de stockage sélectionnée :

- **Passer à la vue Performance**

  Permet d'accéder à la page des détails des performances de la Storage VM.

- **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 d'accéder à la vue « État : Toutes les machines virtuelles de stockage ».

Onglet Santé

L'onglet Santé affiche des informations détaillées sur la disponibilité des données, la capacité des données et les problèmes de protection de divers objets tels que les volumes, les agrégats, les LIF NAS, les LIF SAN, les LUNs, les protocoles, les services, les partages NFS et les partages CIFS.

Vous pouvez cliquer sur le graphique d'un objet pour afficher la liste filtrée des objets. Par exemple, vous pouvez cliquer sur le graphique de capacité du volume qui affiche des avertissements pour voir la liste des volumes présentant des problèmes de capacité avec un niveau de gravité « avertissement ».

- **Problèmes de disponibilité**

  Affiche, sous forme de graphique, le nombre total d'objets, y compris ceux présentant des problèmes de disponibilité et ceux qui n'en présentent aucun. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations situées sous le graphique détaillent les problèmes de disponibilité susceptibles d'affecter, ou ayant déjà affecté, la disponibilité des données dans la VM de stockage. Par exemple, des informations concernant les LIF NAS et SAN en panne ainsi que les volumes hors ligne sont affichées.

  Vous pouvez également consulter des informations sur les protocoles et services associés actuellement en cours d'exécution, ainsi que sur 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 ceux présentant des problèmes de capacité et ceux n'en présentant aucun. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations situées sous le graphique détaillent les problèmes de capacité susceptibles d'affecter, ou ayant déjà affecté, la capacité des données dans la machine virtuelle de stockage. Par exemple, des informations sont affichées concernant les agrégats susceptibles de dépasser les seuils définis.

- **Problèmes de protection**

  Offre un aperçu rapide de l'état de santé lié à la protection des machines virtuelles de stockage en affichant, sous forme de boîte de dialogue de champ, le nombre total de relations, y compris celles présentant des problèmes de protection et celles ne présentant aucun problème lié à la protection. Vous pouvez également consulter l'état de la relation DR de la machine virtuelle de stockage sélectionnée. Les événements des relations DR des machines virtuelles de stockage sont affichés ici, et le fait de cliquer sur les événements vous redirige vers la page de détails de l'événement. Lorsqu'il existe des volumes non protégés, le fait de cliquer sur le lien vous redirige vers la vue Santé : Tous les volumes, où vous pouvez consulter une liste filtrée des volumes non protégés sur la machine virtuelle de stockage. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Le fait de cliquer sur un graphique vous redirige vers la vue Relation : Toutes les relations, où vous pouvez consulter une liste filtrée des détails des relations de protection. Les informations sous le graphique fournissent des détails sur les problèmes de protection qui peuvent affecter ou ont déjà affecté la protection des données dans la machine virtuelle de stockage. Par exemple, des informations sont affichées sur les volumes dont la réserve de Snapshot copy est presque pleine ou sur les problèmes de retard des relations SnapMirror.

Onglet Capacité

L'onglet Capacité affiche des informations détaillées sur la capacité de données de la SVM sélectionnée.

Les informations suivantes s'affichent pour une machine virtuelle de stockage avec un volume FlexVol ou un volume FlexGroup :

- **Capacité**

  La zone Capacité affiche des détails sur la capacité utilisée et disponible allouée 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 Storage VM.

  - Disponibilité garantie

    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 présentant des problèmes de capacité**

  La liste des volumes présentant des problèmes de capacité affiche, sous forme de tableau, des détails sur les volumes qui rencontrent des problèmes de capacité :

  - Statut

    Indique que le volume présente un problème de capacité de la gravité indiquée.

    Vous pouvez déplacer le pointeur sur l'état pour afficher plus d'informations sur l'événement ou les

événements liés à la capacité générés pour le volume.

Si l'état du volume est déterminé par un seul événement, vous pouvez consulter des informations telles que le nom de l'événement, la date et l'heure de son déclenchement, le nom de l'administrateur auquel l'événement est attribué et la cause de l'événement. Vous pouvez utiliser le bouton **Afficher les détails** pour afficher plus d'informations sur l'événement.

Si l'état du volume est déterminé par plusieurs événements de même gravité, les trois principaux événements sont affichés avec des informations telles que le nom de l'événement, la date et l'heure de son déclenchement, ainsi que le nom de l'administrateur auquel l'événement est assigné. 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 **View All Events** pour afficher la liste des événements générés.

> Un volume peut contenir plusieurs événements de même gravité ou de gravités différentes. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un volume contient deux événements de gravité « Erreur » et « Avertissement », seule la gravité « Erreur » est affichée.

- Volume

  Affiche le nom du volume.

- Capacité de données utilisée

  Affiche, sous forme de graphique, des informations sur le taux d'utilisation de la capacité du volume (en pourcentage).

- Jours avant saturation

  Affiche le nombre estimé de jours restants avant que le volume n'atteigne sa capacité maximale.

- Provisionnement fin

  Indique si une garantie d'espace est activée pour le volume sélectionné. Les valeurs possibles sont Oui et Non.

- Agrégats

  Pour les volumes FlexVol, affiche le nom de l'agrégat qui contient le volume. Pour les volumes FlexGroup, affiche le nombre d'agrégats utilisés dans le FlexGroup.

Onglet Configuration

L'onglet Configuration affiche les détails de configuration de la machine virtuelle de stockage sélectionnée, tels que son cluster, son volume racine, le type de volumes qu'elle contient (volumes FlexVol), les stratégies et la protection créée sur la machine virtuelle de stockage :

- **Aperçu**
  - Cluster

    Affiche le nom du cluster auquel appartient la machine virtuelle de stockage.

  - Type de volume autorisé

    Affiche le type de volumes pouvant être créés dans la machine virtuelle de stockage. Le type peut être FlexVol ou FlexVol/FlexGroup.

- Volume racine

  Affiche le nom du volume racine de la machine virtuelle de stockage.

- Protocoles autorisés

  Affiche le type de protocoles qui peuvent être configurés sur la VM de stockage. Indique également si un protocole est actif (), inactif () ou non 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 actives () ou inactives ().

  - SAN

    Affiche le nombre d'interfaces SAN associées à la VM de stockage. Indique également si les interfaces sont actives () ou inactives ().

  - FC-NVMe

    Affiche le nombre d'interfaces FC-NVMe associées à la machine virtuelle de stockage. Indique également si les interfaces sont actives () ou inactives ().

- **Interfaces réseau de gestion**
  - Disponibilité

    Affiche le nombre d'interfaces de gestion associées à la Storage VM. Indique également si les interfaces de gestion sont actives () ou inactives ().

- **Politiques**
  - Snapshots

    Affiche le nom de la stratégie Snapshot créée sur la Storage VM.

  - Règles d'export

    Affiche soit le nom des règles d'export si une seule règle est créée, soit le nombre de règles d'export si plusieurs règles sont créées.

- **Protection**
  - DR de VM de stockage

    Indique si la VM de stockage sélectionnée est protégée, de destination ou non protégée, ainsi que le nom de la destination sur laquelle la VM de stockage est protégée. Si la VM de stockage sélectionnée est de destination, les détails de la VM de stockage source s'affichent. En cas de fan-out, ce champ indique le nombre total de VM de stockage de destination sur lesquelles la VM de stockage est protégée. Le lien de nombre vous mène à la grille des relations des VM de stockage filtrée sur la VM de stockage source.

  - Volumes protégés

    Affiche le nombre de volumes protégés sur la machine virtuelle de stockage sélectionnée, par rapport

au nombre total de volumes. Si vous consultez une machine virtuelle de stockage de destination, le lien numérique correspond 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 VM de stockage. Il peut s'agir d'un système de noms de domaine (DNS) ou d'un service d'informations réseau (NIS).

  - État

    Affiche l'état du service, qui peut être En service (), En panne () ou Non configuré ().

  - Nom de domaine

    Affiche les noms de domaine complets (FQDN) du serveur DNS pour les services DNS ou du serveur NIS pour les services NIS. Lorsque le serveur NIS est activé, le FQDN actif du serveur NIS est affiché. Lorsque le serveur NIS est désactivé, la liste de tous les FQDN est affichée.

  - Adresse IP

    Affiche les adresses IP du serveur DNS ou NIS. Lorsque le serveur NIS est activé, son adresse IP active est affichée. Lorsque le serveur NIS est désactivé, la liste de toutes les adresses IP est affichée.

Onglet Interfaces réseau

L'onglet Interfaces réseau affiche des détails sur les interfaces réseau de données (LIF) créées sur la machine virtuelle de stockage sélectionnée :

- **Interface réseau**

  Affiche le nom de l'interface créée sur la machine virtuelle de stockage sélectionnée.

- **État opérationnel**

  Affiche l'état opérationnel de l'interface, qui peut être Up (), Down () ou Unknown (). L'état opérationnel d'une interface est déterminé par l'état de ses ports physiques.

- **Statut administratif**

  Affiche l'état administratif de l'interface, qui peut être actif (), inactif () ou inconnu (). L'état administratif d'une interface est contrôlé par l'administrateur de stockage pour apporter des modifications à la configuration ou à des fins de maintenance. L'état administratif peut être différent de l'état opérationnel. Toutefois, si l'état administratif d'une interface est inactif, l'état opérationnel est inactif par défaut.

- **Adresse IP / WWPN**

  Affiche l'adresse IP des interfaces Ethernet et le World Wide Port Name (WWPN) 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 de type Données ou Gestion.

- **port d'attache**

  Affiche le port physique auquel l'interface était initialement associée.

- **Port actuel**

  Affiche le port physique auquel l'interface est actuellement associée. Si l'interface a été migrée, le port actuel peut être différent du port d'attache.

- **Ensemble de ports**

  Affiche le jeu de ports auquel l'interface est associée.

- **Politique de basculement**

  Affiche la stratégie de basculement configurée pour l'interface. Pour les interfaces NFS, CIFS et FlexCache, la stratégie de basculement par défaut est « Prochaine interface disponible ». La stratégie de basculement ne s'applique pas aux interfaces FC et iSCSI.

- **Groupes de routage**

  Affiche le nom du groupe de routage. Cliquez sur le nom du groupe de routage pour afficher plus d'informations sur les routes et la passerelle de destination.

  Les groupes de routage ne sont pas pris en charge pour ONTAP 8.3 ou version ultérieure et, par conséquent, une colonne vide s'affiche pour ces clusters.

- **Groupe de basculement**

  Affiche le nom du groupe de basculement.

Onglet Qtrees

L'onglet Qtrees affiche des détails sur les qtrees et leurs quotas. Vous pouvez cliquer sur le bouton **Modifier les seuils** si vous souhaitez modifier les paramètres de seuil de santé pour la capacité d'un ou de 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 sur les qtrees pour la VM de stockage actuelle, pour toutes les VM de stockage du cluster actuel, ou pour toutes les VM de stockage de tous les clusters de votre centre de données. Des champs qtrees supplémentaires apparaissent dans le fichier CSV exporté.

- **Statut**

  Affiche l'état actuel du qtree. L'état peut être Critique (), Erreur (), Avertissement () ou Normal ().

  Vous pouvez placer le pointeur sur l'icône d'état pour afficher davantage d'informations sur l'événement ou

les événements générés pour le qtree.

Si l'état du qtree est déterminé par un seul événement, vous pouvez consulter des informations telles que le nom de l'événement, la date et l'heure de son déclenchement, le nom de l'administrateur auquel il est attribué et sa cause. Vous pouvez utiliser **Afficher les détails** pour obtenir davantage d'informations sur l'événement.

Si l'état du qtree est déterminé par plusieurs événements de même gravité, les trois premiers événements sont affichés avec des informations telles que le nom de l'événement, la date et l'heure de déclenchement des événements, ainsi que le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également utiliser **Afficher tous les événements** pour consulter la liste des événements générés.



Un qtree peut contenir plusieurs événements de même gravité ou de gravités différentes. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un qtree contient deux événements de gravité « Erreur » et « Avertissement », seule la gravité « Erreur » est affichée.

- **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 contenant le qtree.

  Vous pouvez déplacer le pointeur sur le nom du volume pour afficher plus d'informations à son sujet.

- **Quota défini**

  Indique si un quota est activé ou désactivé sur le qtree.

- **Type de quota**

  Indique si le quota concerne 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.

- **% d'espace disque utilisé**

  Affiche le pourcentage d'espace disque utilisé. Si une limitation stricte de disque est définie, cette valeur

est basée sur la limitation stricte de disque. Si le quota est défini sans limitation stricte de disque, la valeur est basée sur l'espace de données du volume. Si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree, alors « `Not applicable` » s'affiche sur la page de la grille et le champ est vide dans les données d'exportation CSV.

- **Limitation stricte du disque**

  Affiche la quantité maximale d'espace disque allouée au qtree. Unified Manager génère un événement critique lorsque cette limite est atteinte et qu'aucune écriture supplémentaire sur disque n'est autorisée. La valeur s'affiche sous la forme « `Unlimited` » dans les cas suivants : si le quota est défini sans limitation stricte d'espace disque, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree.

- **Limite logicielle du disque**

  Affiche la quantité d'espace disque allouée au qtree avant la génération d'un événement d'avertissement. La valeur s'affiche comme "Unlimited" dans les conditions suivantes : si le quota est défini sans limitation logicielle de disque, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

- **Seuil de disque**

  Affiche la valeur de seuil définie sur l'espace disque. La valeur s'affiche sous la forme « `Unlimited` » dans les cas suivants : si le quota est défini sans limite de seuil de disque, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

- **Fichiers utilisés %**

  Affiche le pourcentage de fichiers utilisés dans le qtree. Si la limitation stricte des fichiers est définie, cette valeur est basée sur la limitation stricte des fichiers. Aucune valeur n'est affichée si le quota est défini sans limitation stricte des fichiers. Si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree, « `Not applicable` » s'affiche dans la page de grille et le champ est vide dans les données d'exportation CSV.

- **Limitation stricte des fichiers**

  Affiche la limitation stricte du nombre de fichiers autorisés sur les qtrees. La valeur s'affiche sous la forme "Unlimited" dans les conditions suivantes : si le quota est défini sans limitation stricte de fichiers, si le quota n'est pas défini, ou si les quotas sont désactivés sur le volume auquel appartient le qtree.

- **Limite souple de fichiers**

  Affiche la limite souple du nombre de fichiers autorisés sur les qtrees. La valeur s'affiche sous la forme « `Unlimited` » dans les cas suivants : si le quota est défini sans limite souple de fichiers, si le quota n'est pas défini ou si les quotas sont désactivés sur le volume auquel appartient le qtree. Par défaut, cette colonne est masquée.

Onglet Quotas d'utilisateurs et de groupes

Affiche des détails sur les quotas utilisateur et de quota au groupe pour la VM de stockage sélectionnée. Vous pouvez consulter des informations telles que l'état du quota, le nom de l'utilisateur ou du groupe d'utilisateurs, les limites souples et les limitations strictes définies sur les disques et les fichiers, la quantité d'espace disque et le nombre de fichiers utilisés, ainsi que la valeur du seuil de disque. Vous pouvez également modifier l'adresse e-mail associée à un utilisateur ou à un groupe d'utilisateurs.

- **Bouton de commande Modifier l'adresse e-mail**

  Ouvre la boîte de dialogue Modifier l'adresse e-mail, qui affiche l'adresse e-mail actuelle de l'utilisateur ou du groupe d'utilisateurs sélectionné. Vous pouvez modifier cette adresse. 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, leurs noms s'affichent séparés par des virgules. De plus, 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**

  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 VM de stockage. Le système envoie une notification à l'adresse e-mail spécifiée en cas de dépassement de quota.

- **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 consulter des informations telles que le nom de l'événement, la date et l'heure de son déclenchement, le nom de l'administrateur auquel l'événement est attribué et la cause de l'événement. Vous pouvez utiliser **View Details** pour afficher davantage d'informations sur l'événement.

  Si le statut 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, la date et l'heure de son déclenchement, ainsi que le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également utiliser **Afficher tous les événements** pour afficher la liste des événements générés.

  > Un quota peut comporter plusieurs événements de même gravité ou de gravités différentes. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un quota comporte deux événements de gravité « Erreur » et « Avertissement », seule la gravité « Erreur » est affichée.

- **Utilisateur ou groupe**

  Affiche le nom de l'utilisateur ou du groupe d'utilisateurs. Si plusieurs utilisateurs ont le même quota, leurs noms sont affichés séparés par des virgules.

  La valeur s'affiche comme « `Unknown` » lorsque ONTAP ne fournit pas de nom d'utilisateur valide en raison d'erreurs SecD.

- **Type**

  Indique si le quota concerne un utilisateur ou un groupe d'utilisateurs.

- **Volume ou Qtree**

  Affiche le nom du volume ou du qtree sur lequel le quota utilisateur ou le quota au groupe est spécifié.

Vous pouvez déplacer le pointeur sur le nom du volume ou du qtree pour afficher plus d'informations sur le volume ou le qtree.

- **% d'espace disque utilisé**

  Affiche le pourcentage d'espace disque utilisé. La valeur s'affiche comme « `Non applicable` » si le quota est défini sans limitation stricte.

- **Limitation stricte du disque**

  Affiche la quantité maximale d'espace disque allouée au quota. Unified Manager génère un événement critique lorsque cette limite est atteinte et qu'aucune écriture supplémentaire sur le disque n'est autorisée. La valeur s'affiche sous la forme « `Unlimited` » si le quota est défini sans limitation stricte de disque.

- **Limite logicielle du disque**

  Affiche la quantité d'espace disque allouée au quota avant qu'un avertissement ne soit généré. La valeur s'affiche sous la forme « `Unlimited` » si le quota est défini sans limitation souple d'espace disque. Par défaut, cette colonne est masquée.

- **Seuil de disque**

  Affiche la valeur seuil définie sur l'espace disque. La valeur s'affiche sous la forme « `Unlimited` » 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 s'affiche comme « `Non applicable` » si le quota est défini sans limitation stricte.

- **Limitation stricte des fichiers**

  Affiche la limitation stricte du nombre de fichiers autorisés sur le quota. La valeur s'affiche comme "Unlimited" si le quota est défini sans limitation stricte du nombre de fichiers.

- **Limite souple de fichiers**

  Affiche la limite souple du nombre de fichiers autorisés sur le quota. La valeur est affichée comme « `Unlimited` » si le quota est défini sans limite souple de fichiers. Par défaut, cette colonne est masquée.

- **Adresse e-mail**

  Affiche l'adresse électronique de l'utilisateur ou du groupe d'utilisateurs auquel les notifications sont envoyées en cas de dépassement des quotas.

Onglet Partages NFS

L'onglet Partages NFS affiche des informations sur les partages NFS, telles que leur statut, le chemin associé au volume (FlexGroup volumes ou FlexVol volumes), les niveaux d'accès des clients aux partages NFS et les règles d'export définies 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 aux règles d'export du 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 sur lequel le volume est monté. Si des règles d'export NFS explicites sont appliquées à un qtree, la colonne affiche le chemin du volume par lequel le qtree est accessible.

- **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 du qtree auquel les règles d'export sont appliquées. Si des règles d'export sont appliquées à un qtree du volume, la colonne affiche à la fois le nom du volume et celui du qtree.

  Vous pouvez cliquer sur le lien pour afficher les détails de l'objet sur la page de détails correspondante. S'il s'agit d'un qtree, des liens vers le qtree et le volume s'affichent.

- **État du volume**

  Affiche l'état du volume en cours d'exportation. Cet état peut être Hors ligne, En ligne, Restreint ou Mixte.

  - Hors ligne

    L'accès en lecture ou en écriture au volume n'est pas autorisé.

  - En ligne

    L'accès en lecture et en écriture au volume est autorisé.

  - Restreint

    Des opérations limitées, telles que la reconstruction de la parité, sont autorisées, mais l'accès aux données n'est pas autorisé.

  - Mixte

    Les constituants d'un volume FlexGroup ne sont pas tous dans le même état.

- **Style de sécurité**

  Affiche l'autorisation d'accès pour les volumes exportés. Le style de sécurité peut être UNIX, Unified, NTFS ou Mixed.

  - UNIX (clients NFS)

    Les fichiers et répertoires du volume disposent d'autorisations UNIX.

  - Unifié

    Les fichiers et répertoires du volume ont un style de sécurité unifié.

  - NTFS (clients CIFS)

    Les fichiers et répertoires du volume possèdent des autorisations Windows NTFS.

- Mixte

  Les fichiers et les répertoires du volume peuvent avoir des autorisations UNIX ou des autorisations NTFS Windows.

- **Autorisation UNIX**

  Affiche les bits de permission UNIX sous forme de chaîne octale, définis pour les volumes exportés. Ce format est similaire à celui des bits de permission UNIX.

- **Règles d'export**

  Affiche les règles qui définissent l'autorisation d'accès aux volumes exportés. Vous pouvez cliquer sur le lien pour consulter les détails des règles associées aux règles d'export, comme les protocoles d'authentification et l'autorisation d'accès.

Onglet Partages SMB

Affiche des informations sur les partages SMB de la machine virtuelle de stockage sélectionnée. Vous pouvez consulter des informations telles que l'état du partage SMB, son nom, le chemin d'accès associé à la machine virtuelle de stockage, l'état du chemin de jonction du partage, l'objet conteneur, l'état du volume conteneur, les données de sécurité du partage et les règles d'export définies pour le partage. Vous pouvez également déterminer s'il existe un chemin NFS équivalent pour le partage SMB.

Les partages contenus dans les dossiers ne sont pas affichés dans l'onglet Partages SMB.

- **Bouton de commande Afficher le mappage utilisateur**

  Ouvre la boîte de dialogue de mappage des utilisateurs.

  Vous pouvez consulter les détails du mappage des utilisateurs pour la VM de stockage.

- **Afficher le bouton de commande ACL**

  Ouvre la boîte de dialogue Contrôle d'accès pour le partage.

  Vous pouvez consulter les détails de l'utilisateur et des autorisations pour le partage sélectionné.

- **Statut**

  Affiche l'état actuel du partage. L'état peut être Normal ( ) ou Error ( ).

- **Nom du 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 conteneur**

Affiche le nom de l'objet conteneur auquel appartient le partage. Cet objet conteneur peut être un volume ou un qtree.

En cliquant sur le lien, vous pouvez consulter les détails de l'objet conteneur sur la page de détails correspondante. Si l'objet conteneur est un qtree, des liens s'affichent pour le qtree et le volume.

- **État du volume**

  Affiche l'état du volume en cours d'exportation. Cet état peut être Hors ligne, En ligne, Restreint ou Mixte.

  - Hors ligne

    L'accès en lecture ou en écriture au volume n'est pas autorisé.

  - En ligne

    L'accès en lecture et en écriture au volume est autorisé.

  - Restreint

    Des opérations limitées, telles que la reconstruction de la parité, sont autorisées, mais l'accès aux données n'est pas autorisé.

  - Mixte

    Les constituants d'un volume FlexGroup ne sont pas tous dans le même état.

- **Sécurité**

  Affiche l'autorisation d'accès pour les volumes exportés. Le style de sécurité peut être UNIX, Unified, NTFS ou Mixed.

  - UNIX (clients NFS)

    Les fichiers et répertoires du volume disposent d'autorisations UNIX.

  - Unifié

    Les fichiers et répertoires du volume ont un style de sécurité unifié.

  - NTFS (clients CIFS)

    Les fichiers et répertoires du volume possèdent des autorisations Windows NTFS.

  - Mixte

    Les fichiers et les répertoires du volume peuvent avoir des autorisations UNIX ou des autorisations NTFS Windows.

- **Règles d'export**

  Affiche le nom des règles d'export applicables au partage. Si les règles d'export ne sont pas spécifiées pour la machine virtuelle de stockage, la valeur affichée est « Non activé ».

  Vous pouvez cliquer sur le lien pour consulter les détails des règles associées aux règles d'export, telles que les protocoles d'accès et les autorisations. Le lien est désactivé si les règles d'export sont désactivées

pour la machine virtuelle de stockage sélectionnée.

- **Équivalent NFS**

  Indique s'il existe un équivalent NFS pour le partage.

Onglet SAN

Affiche les détails des LUN, des groupes d'initiateurs et des initiateurs pour la VM de stockage sélectionnée. Par défaut, la vue des LUN s'affiche. Vous pouvez consulter les détails des groupes d'initiateurs dans l'onglet « Groupes d'initiateurs » et ceux des initiateurs dans l'onglet « Initiateurs ».

- **Onglet LUNs**

  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, l'état de la LUN (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 des données et le numéro de série de la LUN. La colonne Performances de la LUN fournit un lien vers la page de détails LUN/Performance.

  Vous pouvez également consulter des informations indiquant si le provisionnement fin est activé sur le LUN et si celui-ci est associé à un groupe d'initiateurs. Si ce LUN est associé à un initiateur, vous pouvez afficher les groupes d'initiateurs et les initiateurs associés au LUN sélectionné.

- **Onglet Groupes d'initiateurs**

  Affiche les détails des groupes d'initiateurs. Vous pouvez consulter des informations telles que le nom du groupe d'initiateurs, l'état d'accès, le type de système d'exploitation hôte utilisé par tous les initiateurs du groupe et le protocole pris en charge. Lorsque vous cliquez sur le lien dans la colonne d'état d'accès, vous pouvez afficher l'état d'accès actuel du groupe d'initiateurs.

  - **Normal**

    Le groupe initiateur est connecté à plusieurs chemins d'accès.

  - **Chemin unique**

    Le groupe initiateur est connecté à un seul chemin d'accès.

  - **Aucun chemin**

    Aucun chemin d'accès n'est connecté au groupe d'initiateurs.

    Vous pouvez voir si les groupes d'initiateurs sont associés à toutes les interfaces ou à des interfaces spécifiques via un ensemble de ports. Lorsque vous cliquez sur le lien du nombre dans la colonne Interfaces associées, toutes les interfaces ou les interfaces spécifiques d'un ensemble de ports s'affichent. Les interfaces associées via le portail cible ne sont pas affichées. Le nombre total d'initiateurs et de LUN associés à un groupe d'initiateurs s'affiche.

  Vous pouvez également visualiser les LUN et les initiateurs associés au groupe d'initiateurs sélectionné.

- **Onglet Initiateurs**

  Affiche le nom et le type de l'initiateur ainsi que le nombre total de groupes d'initiateurs associés à cet initiateur pour la machine virtuelle de stockage sélectionnée.

```
initiator groups that are mapped to the selected initiator group.
```

Volet des annotations associées

Le volet Annotations associées vous permet d'afficher les détails des annotations associées à la VM de stockage sélectionnée. Ces détails incluent le nom de l'annotation et les valeurs d'annotation appliquées à la VM de stockage. Vous pouvez également supprimer des annotations manuelles depuis le volet Annotations associées.

Volet Appareils associés

Le volet « Périphériques associés » vous permet d'afficher le cluster, les agrégats et les volumes liés à la machine virtuelle de stockage :

- **Cluster**

  Affiche l'état de santé du cluster auquel appartient la machine virtuelle de stockage.

- **Agrégats**

  Affiche le nombre d'agrégats appartenant à la machine virtuelle de stockage sélectionnée. L'état de santé des agrégats est également affiché, selon le niveau de gravité le plus élevé. Par exemple, si une machine virtuelle de stockage contient dix agrégats, dont cinq affichent l'état « Avertissement » et les cinq autres l'état « Critique », l'état affiché est « Critique ».

- **Agrégats attribués**

  Affiche le nombre d'agrégats affectés à une machine virtuelle de stockage. L'état de santé des agrégats est également affiché, selon le 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, selon le niveau de gravité le plus élevé. Lorsqu'il existe des volumes FlexGroup dans la machine virtuelle de stockage, le nombre inclut également les FlexGroups ; il n'inclut pas les constituants FlexGroup.

volet Groupes associés

Le volet Groupes associés vous permet d'afficher la liste des groupes associés à la machine virtuelle de stockage sélectionnée.

Volet Alertes associées

Le volet « Alertes associées » vous permet de consulter la liste des alertes créées pour la machine virtuelle de stockage sélectionnée. Vous pouvez également ajouter une alerte en cliquant sur le lien « Ajouter une alerte » ou modifier une alerte existante en cliquant sur le nom de l'alerte.

Consultez la page Détails du cluster/de l'état dans Active IQ Unified Manager

La page « Détails du cluster/de l'état » fournit des informations détaillées sur un cluster sélectionné, telles que son état, sa capacité et sa configuration. Vous pouvez également consulter des informations sur les interfaces réseau (LIF), les nœuds, les disques, les

périphériques associés et les alertes relatives au cluster.

L'état affiché à côté du nom du cluster, par exemple (Good), représente l'état de la communication, à savoir si Unified Manager peut communiquer avec le cluster. Il ne représente pas l'état de basculement ni l'état général du cluster.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour le cluster sélectionné :

- **Passer à la vue Performance**

  Permet d'accéder à la page de détails Cluster / Performance.

- **Actions**

  - Ajouter une alerte : ouvre la boîte de dialogue Ajouter une alerte, qui vous permet d'ajouter une alerte au cluster sélectionné.
  - Redécouverte : Lance une actualisation manuelle du cluster, permettant à Unified Manager de détecter les modifications récentes apportées au cluster.

    Si Unified Manager est associé à OnCommand Workflow Automation, l'opération de redécouverte récupère également les données mises en cache de WFA, le cas échéant.

  Une fois l'opération de redécouverte lancée, un lien vers les détails de la tâche associée s'affiche pour permettre le suivi de son état d'avancement.

  - Annoter : vous permet d'annoter le cluster sélectionné.

- **Afficher les clusters**

  Permet d'accéder à la vue Santé : Tous les clusters.

Onglet Santé

Affiche des informations détaillées sur les problèmes de disponibilité des données et de capacité des données de différents objets du cluster, tels que les nœuds, les SVM et les agrégats. Les problèmes de disponibilité sont liés à la capacité des objets du cluster à fournir les données. Les problèmes de capacité sont liés à la capacité des objets du cluster à stocker les données.

Vous pouvez cliquer sur le graphique d'un objet pour afficher une liste filtrée des objets. Par exemple, vous pouvez cliquer sur le graphique de capacité des SVM affichant des avertissements pour afficher une liste filtrée des SVM. Cette liste contient les SVM dont les volumes ou les qtrees présentent des problèmes de capacité de niveau « Avertissement ». Vous pouvez également cliquer sur le graphique de disponibilité des SVM affichant des avertissements pour afficher la liste des SVM présentant des problèmes de disponibilité de niveau « Avertissement ».

Problèmes de disponibilité

Affiche graphiquement le nombre total d'objets, y compris les objets qui présentent des problèmes de disponibilité et ceux qui ne présentent aucun problème lié à la disponibilité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations sous le graphique fournissent des détails sur les problèmes de disponibilité qui peuvent affecter ou ont déjà affecté la disponibilité des données dans le cluster. Par exemple, des informations sont affichées sur les baies de disques hors service et les agrégats hors ligne.

Les données affichées pour le graphique à barres SFO sont basées sur l'état HA des nœuds. Les données affichées pour tous les autres graphiques à barres sont calculées en fonction des événements générés.

Problèmes de capacité

Affiche graphiquement le nombre total d'objets, y compris les objets présentant des problèmes de capacité et les objets ne présentant aucun problème lié à la capacité. Les couleurs du graphique représentent les différents niveaux de gravité des problèmes. Les informations situées sous le graphique fournissent des détails sur les problèmes de capacité susceptibles d'affecter ou ayant déjà affecté la capacité des données dans le cluster. Par exemple, des informations sont affichées sur les agrégats susceptibles de dépasser 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 concernant la capacité utilisée et la capacité disponible de tous les agrégats alloués:

- Espace logique utilisé

  La taille réelle des données stockées sur l'ensemble des agrégats de ce cluster sans appliquer les économies liées à l'utilisation des technologies d'efficacité du stockage ONTAP. Cela n'inclut pas les copies Snapshot.

- Réduction des données

  Affiche le ratio sans les copies Snapshot et avec deux chiffres significatifs, par exemple 1,8 à 1. Ce ratio est basé sur les paramètres d'efficacité du stockage ONTAP configurés.

- Utilisé

  La capacité physique utilisée par les données sur l'ensemble des agrégats. Cela n'inclut pas la capacité utilisée pour la parité, le redimensionnement et la réservation.

- disponible

  Affiche la capacité disponible pour les données.

- Pièces détachées

  Affiche la capacité pouvant être utilisée pour le stockage sur tous les disques de rechange.

- Provisionné

  Affiche la capacité allouée à 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. Celle-ci n'inclut pas la capacité allouée à la parité.

- Utilisé

  Affiche la capacité utilisée par les données. Cela n'inclut pas la capacité utilisée pour la parité, le redimensionnement et la réservation.

- disponible

  Affiche la capacité disponible pour les données.

- Provisionné

  Affiche la capacité allouée à tous les volumes sous-jacents.

- Pièces détachées

  Affiche la capacité pouvant être utilisée pour le stockage sur tous les disques de rechange.

Niveau cloud

Affiche la capacité totale du niveau cloud utilisée, ainsi que la capacité utilisée pour chaque niveau cloud connecté pour les agrégats compatibles avec FabricPool sur le cluster. Un FabricPool peut être sous licence ou non.

Capacité physique ventilée par type de disque

La section « Répartition de la capacité physique par type de disque » affiche des informations détaillées sur la capacité des différents types de disques du cluster. En cliquant sur un type de disque, vous accédez à des informations supplémentaires dans l'onglet « Disques ».

- Capacité utile totale

  Affiche la capacité disponible et la capacité de réserve des disques de données.

- disque dur

  Représente graphiquement la capacité utilisée et la capacité disponible de tous les disques de données HDD du cluster. La ligne pointillée représente la capacité de réserve des disques de données du HDD.

- Flash
  - SSD Data

    Affiche graphiquement la capacité utilisée et la capacité disponible des disques de données SSD du cluster.

  - Cache SSD

    Affiche graphiquement la capacité de stockage des disques de cache SSD du cluster.

  - SSD de rechange

    Affiche graphiquement la capacité disponible des disques SSD, de données et de cache du cluster.

- Disques non attribués

  Affiche le nombre de disques non attribués dans le cluster.

Liste des agrégats présentant des problèmes de capacité

Affiche sous forme de tableau des informations détaillées sur la capacité utilisée et la capacité disponible des agrégats présentant des problèmes de risque de capacité.

- Statut

  Indique que l'agrégat présente un problème de capacité d'une certaine gravité.

  Vous pouvez déplacer le pointeur sur l'état pour afficher plus d'informations sur l'événement ou les événements générés pour l'agrégat.

  Si l'état de l'agrégat est déterminé par un seul événement, vous pouvez consulter des informations telles que le nom de l'événement, la date et l'heure de son déclenchement, le nom de l'administrateur responsable et sa cause. Vous pouvez cliquer sur le bouton **Afficher les détails** pour obtenir plus d'informations.

  Si l'état de l'agrégat est déterminé par plusieurs événements de même gravité, les trois premiers événements sont affichés avec des informations telles que le nom de l'événement, l'heure et la date de déclenchement des événements, ainsi que le nom de l'administrateur auquel l'événement est attribué. Vous pouvez afficher plus de détails sur chacun de ces événements en cliquant sur le nom de l'événement. Vous pouvez également cliquer sur le lien **View All Events** pour afficher la liste des événements générés.

  > Un agrégat peut comporter plusieurs événements liés à la capacité, de même gravité ou de gravités différentes. Toutefois, seule la gravité la plus élevée est affichée. Par exemple, si un agrégat comporte deux événements de gravité « Error » et « Critical », seule la gravité « Critical » est affichée.

- Agrégat

  Affiche le nom de l'agrégat.

- Capacité de données utilisée

  Affiche graphiquement des informations sur l'utilisation de la capacité de l'agrégat (en pourcentage).

- Jours avant saturation

  Affiche le nombre estimé de jours restants avant que l'agrégat n'atteigne sa pleine capacité.

Onglet Configuration

Affiche les détails relatifs au cluster sélectionné, tels que l'adresse IP, les coordonnées et l'emplacement :

Aperçu du cluster

- Interface de gestion

  Affiche la LIF de gestion du cluster utilisée par Unified Manager pour se connecter au cluster. L'état 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 gestion du cluster utilisée par Unified Manager pour se connecter au cluster.

- FQDN

  Affiche le nom de domaine complet (FQDN) du cluster.

- Version du système d’exploitation

  Affiche la version d’ONTAP exécutée par le cluster. Si les nœuds du cluster exécutent des versions différentes d’ONTAP, la version d’ONTAP la plus ancienne est affichée.

- Contact

  Affiche les informations relatives à l’administrateur à contacter en cas de problème avec le cluster.

- Pays

  Affiche l’emplacement du cluster.

- Personnalité

  Indique s’il s’agit d’un cluster configuré en tant qu’All SAN Array.

Aperçu du cluster distant

Fournit des détails sur le cluster distant dans une configuration MetroCluster. Ces informations ne sont affichées que pour les configurations MetroCluster.

- Cluster

  Affiche le nom du cluster distant. Vous pouvez cliquer sur le nom du cluster pour accéder à la page de détails du cluster.

- Nom d’hôte ou adresse IP

  Affiche le FQDN, le nom court ou l’adresse IP du cluster distant.

- Pays

  Affiche l’emplacement du cluster distant.

MetroCluster Aperçu

Fournit des détails sur le cluster local dans les configurations MetroCluster over FC ou MetroCluster over IP. Ces informations sont affichées uniquement pour les configurations MetroCluster over FC ou IP.

- Type

  Indique si le type MetroCluster comporte deux ou quatre nœuds. Pour MetroCluster sur IP, seul le type à quatre nœuds est pris en charge.

- Configuration

Affiche la configuration MetroCluster sur FC et IP, qui peut prendre les valeurs suivantes :

Pour FC

- Configuration étendue avec câbles SAS
- Configuration étendue avec pont FC-SAS
- Configuration de la fabric avec des commutateurs FC



Pour un 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 automatique non planifié (AUSO)

    Indique si le basculement automatique non planifié est activé pour le cluster local. Par défaut, AUSO est activé pour tous les clusters dans une configuration à deux nœuds MetroCluster dans Unified Manager. Vous pouvez utiliser l'interface de ligne de commande pour modifier le paramètre AUSO. Cette fonctionnalité est prise en charge uniquement pour MetroCluster over FC.

  - Mode de basculement

    Affiche le mode de basculement pour la configuration MetroCluster sur IP. Les valeurs disponibles sont les suivantes : `Active`, `Negotiated Switchover` et `Automatic Unplanned Switchover`.

Nœuds

- Disponibilité

  Affiche le nombre de nœuds qui sont en marche (🟢) ou en panne (🟠) dans le cluster.

- Versions du système d'exploitation

  Affiche les versions de ONTAP exécutées par les nœuds, 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.

Machines virtuelles de stockage

- Disponibilité

  Affiche le nombre de SVM qui sont en fonctionnement (🟢) ou en panne (🟠) dans le cluster.

Interfaces réseau

- Disponibilité

  Affiche le nombre de LIF non dédiées aux données qui sont actives (🟢) ou hors service (🟠) dans le cluster.

- Interfaces de gestion de cluster

Affiche le nombre de LIF de gestion du cluster.

- Interfaces de gestion des nœuds

  Affiche le nombre de LIF de gestion de nœud.

- Interfaces de cluster

  Affiche le nombre de LIF du cluster.

- Interfaces inter-clusters

  Affiche le nombre de LIFs intercluster.

Protocoles

- Protocoles de données

  Affiche la liste des protocoles de données sous licence activés pour le cluster. Ces protocoles incluent iSCSI, CIFS, NFS, NVMe et FC/FCoE.

Protection

- Médiateurs

  Indique si le cluster prend en charge les médiateurs et l'état de connectivité du médiateur. Précise si le médiateur est configuré et, le cas échéant, affiche l'état des médiateurs.

  - Non applicable

    S'affiche lorsque le cluster ne prend pas en charge les médiateurs.

  - Non configuré

    S'affiche lorsque le cluster prend en charge les médiateurs, mais que le médiateur n'est pas configuré.

  - Adresse IP

    S'affiche lorsque le cluster prend en charge les médiateurs et que le médiateur est configuré. L'état du médiateur est indiqué par une couleur. La couleur verte indique que l'état du médiateur est joignable. La couleur rouge indique que l'état du médiateur est injoignable.

Niveaux de cloud

Cette liste répertorie les noms des niveaux de cloud auxquels ce cluster est connecté. Elle indique également leur type (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage ou StorageGRID) et leur état (disponible ou indisponible).

MetroCluster Onglet Connectivité

Affiche les problèmes et l'état de connectivité des composants du cluster dans la configuration MetroCluster sur FC. Un cluster est affiché dans un cadre rouge lorsque le partenaire de reprise après sinistre du cluster rencontre des problèmes.

L'onglet Connectivité MetroCluster s'affiche uniquement pour les clusters dans une configuration

MetroCluster sur FC.

Vous pouvez accéder à la page de détails d'un cluster distant en cliquant sur le nom du cluster distant. Vous pouvez également afficher les détails des composants en cliquant sur le lien de nombre d'un composant. Par exemple, cliquer sur le lien de nombre du nœud dans le cluster affiche l'onglet Nœud dans la page de détails du cluster. Cliquer sur le lien de nombre des disques dans le cluster distant affiche l'onglet Disque dans la page de détails du cluster distant.

Lors de la gestion d'une configuration MetroCluster à huit nœuds, cliquer sur le lien de nombre du composant Tiroirs de disques n'affiche que les tiroirs locaux de la paire haute disponibilité par défaut. De plus, il n'existe aucun moyen d'afficher les tiroirs locaux de 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 consulter plus d'informations sur le ou les événements générés par ce problème.

Si l'état du problème de connectivité entre les composants est déterminé par un événement unique, vous pouvez consulter des informations telles que le nom de l'événement, la date et l'heure de son déclenchement, le nom de l'administrateur responsable et sa cause. Le bouton « Afficher les détails » fournit des informations supplémentaires sur l'événement.

Si l'état du problème de connectivité entre les composants est déterminé par plusieurs événements de même gravité, les trois événements les plus importants sont affichés avec des informations telles que leur nom, la date et l'heure de leur déclenchement, ainsi que le nom de l'administrateur responsable. Vous pouvez consulter plus de détails sur chacun de ces événements en cliquant sur son nom. Vous pouvez également cliquer sur le lien « Afficher tous les événements » pour consulter la liste des événements générés.

MetroCluster onglet Réplication

Affiche l'état des données répliquées dans une configuration MetroCluster over FC. Vous pouvez utiliser l'onglet Réplication de MetroCluster pour garantir la protection des données en les mettant en miroir de manière synchrone avec les clusters déjà appariés. Un cluster s'affiche dans un cadre rouge lorsque le partenaire de reprise après sinistre du cluster rencontre des problèmes.

L'onglet Réplication MetroCluster s'affiche uniquement pour les clusters qui sont dans une configuration MetroCluster over FC.

Dans un environnement MetroCluster, vous pouvez utiliser cet onglet pour vérifier les connexions logiques et l'appairage du cluster local avec le cluster distant. Vous pouvez visualiser la représentation objective des composants du cluster avec leurs connexions logiques. Cela permet d'identifier les problèmes qui pourraient survenir lors de la mise en miroir des métadonnées et des données.

Dans l'onglet Réplication de MetroCluster, le cluster local fournit une représentation graphique détaillée du cluster sélectionné et le partenaire MetroCluster fait référence au cluster distant.

Onglet Interfaces réseau

Affiche les détails de toutes les LIF non liées aux données qui sont créées sur le cluster sélectionné.

Interface réseau

Affiche le nom de la LIF créée sur le cluster sélectionné.

État opérationnel

Affiche l'état opérationnel de l'interface, qui peut être actif (), inactif () ou inconnu (). L'état opérationnel d'une interface réseau est déterminé par l'état de ses ports physiques.

Statut administratif

Affiche l'état administratif de l'interface, qui peut être Up (), Down () ou Unknown (). Vous pouvez contrôler l'état administratif d'une interface lorsque vous apportez des modifications à la configuration ou pendant la maintenance. L'état administratif peut être différent de l'état opérationnel. Toutefois, si l'état administratif d'une LIF est Down, l'état opérationnel est Down par défaut.

Adresse IP

Affiche l'adresse IP de l'interface.

Rôle

Affiche le rôle de l'interface. Les rôles possibles sont : LIF de gestion de cluster, LIF de gestion de nœud, LIF de cluster et LIF inter-cluster.

Port d'attache

Affiche le port physique auquel l'interface était initialement associée.

Port actuel

Affiche le port physique auquel l'interface est actuellement associée. Après une migration de LIF, le port actuel peut être différent du port d'attache.

Politique de basculement

Affiche la stratégie de basculement configurée pour l'interface.

Groupes de routage

Affiche le nom du groupe de routage. Cliquez sur le nom du groupe de routage pour afficher plus d'informations sur les routes et la passerelle de destination.

Les groupes de routage ne sont pas pris en charge pour ONTAP 8.3 ou version ultérieure et, par conséquent, une colonne vide s'affiche pour ces clusters.

Groupe de basculement

Affiche le nom du groupe de basculement.

Onglet Nœuds

Affiche des informations sur les nœuds du cluster sélectionné. Vous pouvez consulter des informations détaillées sur les paires haute disponibilité, les baies de disques et les ports :

Détails HA

Fournit une représentation graphique de l'état HA et de l'état de santé des nœuds de la paire 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 contrôle du nœud partenaire ou le nœud rencontre des problèmes environnementaux.

- **Rouge**

  Le nœud est hors service.

Vous pouvez consulter les informations relatives à la disponibilité de la paire haute disponibilité et prendre les mesures nécessaires pour prévenir tout risque. Par exemple, en cas d'opération de basculement possible, le message suivant s'affiche : Storage failover possible.

Vous pouvez consulter la liste des événements liés à la paire haute disponibilité et à son environnement, tels que les ventilateurs, les alimentations, la batterie NVRAM, les cartes mémoire flash, le processeur de service et la connectivité des tiroirs disque. Vous pouvez également consulter l'heure à laquelle les événements ont été déclenchés.

Vous pouvez consulter d'autres informations relatives au nœud, telles que le numéro de modèle.

S'il existe des clusters à nœud unique, vous pouvez également consulter les détails relatifs aux nœuds.

Tiroirs disque

Affiche des informations sur les tiroirs disque de la paire haute disponibilité.

Vous pouvez également consulter les événements générés pour les tiroirs disque et les composants environnementaux, ainsi que l'heure à laquelle ces événements ont été déclenchés.

- **ID du tiroir**

  Affiche l'identifiant du tiroir disque où se trouve le disque.

- **État du composant**

  Affiche les détails environnementaux des tiroirs disque, tels que les alimentations, les ventilateurs, les capteurs de température, les capteurs de courant, la connectivité des disques et les capteurs de tension. Les détails environnementaux sont affichés sous forme d'icônes dans les couleurs suivantes :

  - **Vert**

    Les composants environnementaux fonctionnent correctement.

  - **Gris**

    Aucune donnée n'est disponible pour les composants environnementaux.

  - **Rouge**

    Certains composants environnementaux sont hors service.

- **État**

Affiche l'état du tiroir disque. Les états possibles sont : Hors ligne, En ligne, Aucun statut, Initialisation requise, Manquant et Inconnu.

- **Modèle**

  Affiche le numéro de modèle du tiroir disque.

- **Tiroir disque local**

  Indique si le tiroir disque se trouve sur le cluster local ou sur le cluster distant. Cette colonne n'est affichée que pour les clusters dans une configuration MetroCluster.

- **Identifiant unique**

  Affiche l'identifiant unique du tiroir disque.

- **Version du firmware**

  Affiche la version du firmware du tiroir disque.

Ports

Affiche des informations sur les ports FC, FCoE et Ethernet associés. Vous pouvez consulter les détails des ports et des interfaces logiques (LIF) associées en cliquant sur les icônes des ports.

Vous pouvez également consulter les événements générés pour les ports.

Vous pouvez consulter les détails suivants concernant le port :

- ID du port

  Affiche le nom du port. Par exemple, les noms de port peuvent être e0M, e0a et e0b.

- Rôle

  Affiche le rôle du port. Les rôles possibles sont Cluster, 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 nom mondial du port (WWPN).

- Révision du firmware

  Affiche la version du firmware du port FC/FCoE.

- Statut

  Affiche l'état actuel du port. Les états possibles sont Actif, Désactivé, Liaison non connectée ou Inconnu ().

Vous pouvez consulter les événements liés au port dans la liste des événements. Vous pouvez également consulter les détails de la LIF associée, tels que le nom de la LIF, son état opérationnel, son adresse IP ou WWPN, les protocoles, le nom de la SVM associée à la LIF, le port actuel, la stratégie de basculement et le groupe de basculement.

Onglet Disques

Affiche les détails des disques du cluster sélectionné. Vous pouvez consulter des informations telles que le nombre de disques utilisés, de disques de rechange, de disques défectueux et de disques non attribués. Vous pouvez également consulter d'autres détails comme le nom du disque, son type et le nœud propriétaire du disque.

Résumé du pool de disques

Affiche le nombre de disques, classés par type effectif (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN et VMDISK), ainsi que l'état des disques. Vous pouvez également afficher d'autres détails, tels que le nombre d'agrégats, de disques partagés, de disques de secours, de disques en panne, de disques non attribués et de disques non pris en charge. Si vous cliquez sur le lien du nombre du type de disque effectif, les disques de l'état sélectionné et du type effectif sélectionné s'affichent. Par exemple, si vous cliquez sur le lien du nombre pour l'état de disque Broken et le type effectif SAS, tous les disques dont l'état de disque est Broken et dont le type effectif est SAS s'affichent.

Disque

Affiche le nom du disque.

Groupes RAID

Affiche le nom du groupe RAID.

Nœud propriétaire

Affiche le nom du nœud auquel appartient le disque. Si le disque n'est pas attribué, aucune valeur n'est affichée dans cette colonne.

État

Affiche l'état du disque : Agrégé, Partagé, De rechange, Défaillant, Non attribué, Non pris en charge ou Inconnu. Par défaut, cette colonne est triée pour afficher les états dans l'ordre suivant : Défaillant, Non attribué, Non pris en charge, De rechange, Agrégé et Partagé.

Disque local

Affiche Oui ou Non pour indiquer si le disque se trouve sur le cluster local ou le cluster distant. Cette colonne n'est affichée que 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 affectés

Affiche le nombre d'agrégats impactés en raison de la défaillance de disque. Vous pouvez déplacer le pointeur

sur le lien de nombre pour afficher les agrégats impactés, puis cliquer sur le nom de l'agrégat pour en afficher les détails. Vous pouvez également cliquer sur le nombre d'agrégats pour afficher la liste des agrégats impactés dans la vue « Health: All Aggregates ».

Aucune valeur n'est affichée dans cette colonne pour les cas suivants :

- Pour les disques défectueux lorsqu'un cluster contenant de tels disques est ajouté à Unified Manager
- Lorsqu'il n'y a pas de disques défaillants

Pool de stockage

Affiche le nom du pool de stockage auquel appartient le SSD. Vous pouvez survoler le nom du pool de stockage avec le pointeur pour afficher les détails du pool de stockage.

Capacité stockable

Affiche la capacité de disque disponible à l'utilisation.

Capacité brute

Affiche la capacité du disque brut, non formaté, avant le redimensionnement et la configuration RAID. Cette colonne est masquée par défaut.

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 pour la création et l'ajout à des agrégats, ainsi que pour la gestion des disques de rechange. ONTAP attribue un type de disque effectif à chaque type de disque.

Pourcentage de blocs de rechange consommés

Affiche en pourcentage les blocs de réserve consommés sur le disque SSD. Cette colonne est vide pour les disques autres que les disques SSD.

Durée de vie nominale utilisée %

Affiche en pourcentage une estimation de la durée de vie du SSD utilisée, basée sur l'utilisation réelle du SSD et sur la prévision du fabricant concernant la durée de vie du SSD. Une valeur supérieure à 99 indique que l'endurance estimée a été consommée, mais peut ne pas indiquer une défaillance du SSD. Si la valeur est inconnue, le disque est omis.

Micrologiciel

Affiche la version du firmware du disque.

RPM

Affiche la vitesse de rotation du disque (tours par minute, tr/min). Cette colonne est masquée par défaut.

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'identifiant du tiroir disque où se trouve le disque.

Compartiment

Affiche l'identifiant de la baie où se trouve le disque.

Volet des annotations associées

Permet de consulter les détails des annotations associées au cluster sélectionné. Ces détails comprennent le nom de l'annotation et les valeurs d'annotation appliquées au cluster. Vous pouvez également supprimer manuellement des annotations depuis le volet « Annotations associées ».

Volet Appareils associés

Permet de consulter 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 fonctionnement. Vous pouvez cliquer sur le lien correspondant au nombre pour obtenir une analyse plus approfondie de ce périphérique.

Vous pouvez utiliser le volet Partenaire MetroCluster pour obtenir le nombre ainsi que des détails sur le partenaire MetroCluster distant, ainsi que sur les composants de cluster associés, tels que les nœuds, les agrégats et les SVM. Le volet Partenaire MetroCluster s'affiche uniquement pour les clusters dans une configuration MetroCluster.

Le volet « Périphériques associés » vous permet d'afficher et de naviguer parmi les nœuds, les SVM et les agrégats liés au cluster :

MetroCluster Partenaire

Affiche l'état de santé du partenaire MetroCluster. En utilisant le lien « Nombre », vous pouvez aller plus loin dans la navigation et obtenir des informations sur l'état de santé et la capacité des composants du cluster.

Nœuds

Affiche le nombre, la capacité et l'état de santé des nœuds appartenant au cluster sélectionné. La capacité indique la capacité utilisable totale par rapport à la capacité disponible.

Machines virtuelles de stockage

Affiche le nombre de SVM appartenant au cluster sélectionné.

Agrégats

Affiche le nombre, la capacité et l'état de santé des agrégats appartenant au cluster sélectionné.

volet Groupes associés

Permet de visualiser la liste des groupes qui incluent le cluster sélectionné.

Volet Alertes associées

Le volet « Alertes associées » vous permet de consulter la liste des alertes du cluster sélectionné. Vous pouvez également ajouter une alerte en cliquant sur le lien « Ajouter une alerte » ou modifier une alerte existante en cliquant sur son nom.

Informations connexes

"Page des volumes" "Affichage de la liste et des détails des clusters"

Affichez la page Détails de l'agrégat / Santé dans Active IQ Unified Manager

La page Détails de l'agrégat/de l'état vous permet de consulter des informations détaillées sur l'agrégat sélectionné, telles que sa capacité, les informations sur les disques, les détails de configuration et les événements générés. Vous pouvez également consulter des informations sur les objets associés et les alertes liées à cet agrégat.

Boutons de commande

> Lors de la surveillance d'un agrégat avec FabricPool activé, les valeurs de capacité allouée et surallouée affichées sur cette page concernent uniquement la capacité locale, ou celle du niveau de performance. L'espace disponible dans le niveau cloud n'est pas pris en compte dans les valeurs de surallocation. De même, les valeurs de seuil de l'agrégat concernent uniquement le niveau de performance local.

Les boutons de commande vous permettent d'effectuer les tâches suivantes pour l'agrégat sélectionné :

- **Passer à la vue Performance**

  Permet d'accéder à la page de détails Aggregate / Performance.

- **Actions**
  - Ajouter une alerte

    Permet d'ajouter une alerte à l'agrégat sélectionné.

  - Modifier les seuils

    Permet de modifier les paramètres de seuil pour l'agrégat sélectionné.

- **Afficher les agrégats**

Permet d'accéder à la vue Santé : Tous les agrégats.

Onglet Capacité

L'onglet Capacité affiche des informations détaillées sur l'agrégat sélectionné, telles que sa capacité, ses seuils et son taux de croissance quotidien.

Par défaut, les événements de capacité ne sont pas générés pour les agrégats racines. De même, les valeurs de seuil utilisées par Unified Manager ne s'appliquent pas aux agrégats racines des nœuds. Seul un représentant du support technique peut modifier les paramètres pour que ces événements soient générés. Lorsque les paramètres sont modifiés par un représentant du support technique, les valeurs de seuil sont appliquées à l'agrégat racine du nœud.

- **Capacité**

  Affiche le graphique de capacité des données et le graphique des copies Snapshot, qui affichent les détails de capacité de l'agrégat :

  - Espace logique utilisé

    La taille réelle des données stockées sur l'agrégat sans appliquer les économies réalisées grâce aux technologies d'efficacité du stockage ONTAP.

  - Utilisé

    La capacité physique utilisée par les données dans l'agrégat.

  - Suralloué

    Lorsque l'espace dans l'agrégat est suralloué, le graphique affiche un indicateur indiquant le volume de surallocation.

  - Avertissement

    Une ligne pointillée s'affiche à l'emplacement du seuil d'alerte, indiquant que l'espace dans l'agrégat est presque plein. Si ce seuil est dépassé, l'événement « Espace presque plein » est généré.

  - Erreur

    Affiche une ligne continue à l'emplacement du seuil d'erreur, indiquant que l'espace dans l'agrégat est plein. Si ce seuil est dépassé, le système génère l'événement « Space Full ».

  - Graphique des 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 de dépassement de la capacité Snapshot par rapport à la réserve Snapshot si la capacité Snapshot utilisée dépasse la réserve Snapshot.

- **Niveau Cloud**

  Affiche l'espace utilisé par les données dans le niveau cloud pour les agrégats compatibles avec FabricPool. Un FabricPool peut être sous licence ou non.

  Lorsque le niveau cloud est dupliqué sur un autre fournisseur de cloud (le « niveau miroir »), les deux

niveaux cloud sont affichés ici.

- **Détails**

  Affiche des informations détaillées sur la capacité.

  - Capacité totale

    Affiche la capacité totale dans l'agrégat.

  - Capacité de données

    Affiche la quantité d'espace utilisée par l'agrégat (capacité utilisée) et la quantité d'espace disponible dans l'agrégat (capacité libre).

  - Réserve Snapshot

    Affiche la capacité Snapshot utilisée et libre de l'agrégat.

  - Capacité surallouée

    Affiche la surallocation de l'agrégat. La surallocation de l'agrégat vous permet de fournir plus de stockage que ce qui est réellement disponible dans un agrégat donné, tant que tout ce stockage n'est pas en cours d'utilisation. 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 suralloué votre agrégat, vous devez surveiller attentivement l'espace disponible et ajouter du stockage selon les besoins pour éviter les erreurs d'écriture dues à un espace insuffisant.

  - Niveau cloud

    Affiche l'espace utilisé par les données dans le niveau cloud pour les agrégats compatibles avec FabricPool. Un FabricPool peut être sous licence ou non. Lorsque le niveau cloud est mis en miroir vers un autre fournisseur de cloud (niveau miroir), les deux niveaux cloud sont affichés ici.

  - Espace cache total

    Affiche l'espace total des disques SSD ou des unités d'allocation ajoutés à un agrégat Flash Pool. Si vous avez activé Flash Pool pour un agrégat mais n'y avez ajouté aucun SSD, l'espace du cache s'affiche à 0 Ko.

    > Ce champ est masqué si Flash Pool est désactivé pour un agrégat.

  - Seuils de l'agrégat

    Affiche les seuils de capacité de l'agrégat suivants :

    - Seuil de remplissage presque complet

      Spécifie le pourcentage auquel un agrégat est presque plein.

    - Seuil plein

      Spécifie le pourcentage auquel un agrégat est plein.

        - Seuil de quasi-surallocation

          Spécifie le pourcentage à partir duquel un agrégat est presque surprovisionné.

        - Seuil de surengagement

          Spécifie le pourcentage à partir duquel un agrégat est suralloué.

    - Autres détails : Taux de croissance quotidien

      Affiche l'espace disque utilisé dans l'agrégat si le taux de variation entre les deux derniers échantillons se maintient pendant 24 heures.

      Par exemple, si un agrégat utilise 10 Go d'espace disque à 14 h et 12 Go à 18 h, le taux de croissance quotidien (Go) de cet agrégat est de 2 Go.

    - Déplacement du volume

      Affiche le nombre d'opérations de déplacement de volume actuellement en cours:

        - Volumes sortants

          Affiche le nombre et la capacité des volumes qui sont déplacés hors de l'agrégat.

      Vous pouvez cliquer sur le lien pour afficher plus de détails, tels que le nom du volume, l'agrégat vers lequel le volume est déplacé, l'état de l'opération de déplacement du volume et l'heure de fin estimée.

        - Volumes entrants

          Affiche le nombre et la capacité restante des volumes en cours de déplacement vers l'agrégat.

    Vous pouvez cliquer sur le lien pour afficher plus de détails, tels que le nom du volume, l'agrégat à partir duquel le volume est déplacé, l'état de l'opération de déplacement du volume et l'heure de fin estimée.

    - Capacité utilisée estimée après le déplacement de volume

      Affiche la quantité estimée d'espace utilisé (en pourcentage et en Ko, Mo, Go, etc.) dans l'agrégat une fois les opérations de déplacement de volume terminées.

- **Aperçu des capacités - Volumes**

  Affiche des graphiques fournissant des informations sur la capacité des volumes contenus dans l'agrégat. L'espace utilisé par le volume (capacité utilisée) et l'espace disponible dans le volume (capacité libre) sont indiqués. Lorsqu'un événement « Espace à risque pour un volume à provisionnement fin » est généré pour des volumes à provisionnement fin, l'espace utilisé par le volume (capacité utilisée) et l'espace disponible dans le volume mais inutilisable (capacité inutilisable) en raison de problèmes de capacité de l'agrégat sont affichés.

  Vous pouvez sélectionner le graphique que vous souhaitez afficher dans les listes déroulantes. Vous pouvez trier les données affichées dans le graphique pour afficher des détails tels que la taille utilisée, la taille provisionnée, la capacité disponible, le taux de croissance quotidien le plus rapide et le taux de croissance le plus lent. Vous pouvez filtrer les données en fonction des machines virtuelles de stockage (SVM) qui contiennent les volumes dans l'agrégat. Vous pouvez également afficher les détails des volumes à provisionnement fin. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur la zone d'intérêt. Par défaut, le graphique affiche les 30 premiers volumes filtrés dans l'agrégat.

Onglet Informations sur le disque

Affiche des informations détaillées sur les disques de l'agrégat sélectionné, notamment le type et la taille du RAID, ainsi que le type de disques utilisés dans l'agrégat. L'onglet affiche également sous forme graphique les groupes RAID et les types de disques utilisés (tels que SAS, ATA, FCAL, SSD ou VMDISK). Vous pouvez afficher des informations supplémentaires, telles que la baie, le tiroir et la vitesse de rotation du disque, en plaçant votre curseur sur les disques de parité et les disques de données.

- **Données**

  Affiche graphiquement des détails sur les disques de données dédiés, les disques de données partagés, ou les deux. Lorsque les disques de données contiennent des disques partagés, des détails graphiques sur les disques partagés sont affichés. Lorsque les disques de données contiennent des disques dédiés et des disques partagés, des détails graphiques sur les disques de données dédiés et les disques de données partagés sont affichés.

  - **Détails du RAID**

    Les détails RAID ne sont affichés que pour les disques dédiés.

    - Type

      Affiche le type RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

    - Taille du groupe

      Affiche le nombre maximal de disques autorisés dans le groupe RAID.

    - Groupes

      Affiche le nombre de groupes RAID dans l'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 détails des disques de données ne sont pas affichés lorsque l'agrégat ne contient que des disques partagés.

    - Disques de parité

      Affiche le nombre et la capacité des disques de parité affectés à un agrégat. Les détails des disques de parité ne sont pas affichés lorsque l'agrégat ne contient que 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 si l'agrégat contient des disques partagés.

  - **Disques de rechange**

    Affiche le type de disque effectif, le nombre et la capacité des disques de données de secours

disponibles pour le nœud dans l'agrégat sélectionné.

> Lorsqu'un agrégat bascule vers le nœud partenaire, Unified Manager n'affiche pas tous les disques de rechange compatibles avec l'agrégat.

- **Cache SSD**

  Fournit des informations détaillées sur les disques SSD de cache dédiés et les disques SSD de cache partagés.

  Les détails suivants concernant les disques SSD dédiés au cache sont affichés :

  - **Détails du RAID**
    - Type

      Affiche le type de RAID (RAID0, RAID4, RAID-DP ou RAID-TEC).

    - Taille du groupe

      Affiche le nombre maximal de disques autorisés dans le groupe RAID.

    - Groupes

      Affiche le nombre de groupes RAID dans l'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 effectif de disque, le nombre et la capacité des disques de secours disponibles pour le nœud dans l'agrégat sélectionné pour le cache.

    > Lorsqu'un agrégat bascule vers le nœud partenaire, Unified Manager n'affiche pas tous les disques de rechange compatibles avec l'agrégat.

    Fournit les détails suivants pour le cache partagé :

  - **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 :

    - Statut

Affiche l'état du pool de stockage, qui peut être sain ou non sain.

- Allocations totales

  Affiche le nombre total d'unités d'allocation et leur taille dans le pool de stockage.

- Taille de l'unité d'allocation

  Affiche la quantité minimale d'espace dans le pool de stockage pouvant être allouée à un agrégat.

- Disques

  Affiche le nombre de disques utilisés pour créer le pool de stockage. Si le nombre de disques indiqué dans la colonne du pool de stockage et celui affiché dans l'onglet Informations sur le disque pour ce pool ne correspondent pas, cela signifie qu'un ou plusieurs disques sont défectueux et que le pool de stockage n'est pas sain.

- Allocation utilisée

  Affiche le nombre et la taille des unités d'allocation utilisées par les agrégats. Vous pouvez cliquer sur le nom de l'agrégat pour afficher ses détails.

- 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.

- **Niveau Cloud**

Affiche le nom du niveau cloud, si vous avez configuré un agrégat compatible FabricPool, et indique l'espace total utilisé. Lorsque le niveau cloud est mis en miroir vers un autre fournisseur de cloud (niveau 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 dans l'agrégat.

  - Type de SnapLock

    Affiche le type de SnapLock de l'agrégat.

- **Niveau Cloud**

  S'il s'agit d'un agrégat compatible FabricPool, les détails du niveau 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 cloud sont affichés ici.

  - Fournisseur

    Affiche le nom du fournisseur de stockage, par exemple, StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage ou Alibaba Cloud Object Storage.

  - Nom

    Affiche le nom du niveau cloud lorsqu'il a été créé par ONTAP.

  - Serveur

    Affiche le nom de domaine complet (FQDN) du niveau cloud.

  - Port

    Le port utilisé pour communiquer avec le fournisseur de cloud.

  - Clé d'accès ou compte

    Affiche la clé d'accès ou le compte pour le niveau cloud.

◦ Nom du conteneur

Affiche le nom du compartiment ou du conteneur du niveau 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. Vous pouvez également cliquer sur le bouton **Exporter** pour générer un rapport au format CSV du graphique affiché.

Vous pouvez sélectionner un type de graphique dans la liste déroulante située en haut du volet Historique. Vous pouvez également consulter les détails d'une période spécifique en sélectionnant 1 semaine, 1 mois ou 1 an. Les graphiques d'historique vous aident à identifier les tendances : par exemple, si l'utilisation de l'agrégat dépasse régulièrement le seuil « Presque plein », vous pouvez prendre les mesures appropriées.

Les graphiques historiques affichent les informations suivantes :

- **Capacité d'agrégat utilisée (%)**

  Affiche la capacité utilisée dans l'agrégat et la tendance d'utilisation de la capacité de l'agrégat en fonction de l'historique d'utilisation sous forme de courbes, en pourcentage, sur l'axe vertical (y). La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'un an. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher une courbe en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende « Capacité utilisée », la courbe « Capacité utilisée » est masquée.

- **Capacité utilisée de l'agrégat par rapport à la capacité totale**

  Affiche, sous forme de graphiques linéaires, la tendance d'utilisation de la capacité de l'agrégat en fonction de l'historique d'utilisation, ainsi que la capacité utilisée et la capacité totale, en octets, kilo-octets, mégaoctets, etc., sur l'axe vertical (y). La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'un an. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher un graphique linéaire en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende Trend Capacity Used, la ligne du graphique Trend Capacity Used est masquée.

- **Capacité d'agrégat utilisée (%) par rapport à la capacité engagée (%)**

  Affiche la tendance d'utilisation de la capacité d'agrégat en fonction de l'historique d'utilisation, ainsi que l'espace engagé, sous forme de courbes, en pourcentage, sur l'axe vertical (y). La période est affichée sur l'axe horizontal (x). Vous pouvez sélectionner une période d'une semaine, d'un mois ou d'un an. Vous pouvez afficher les détails de points spécifiques du graphique en plaçant votre curseur sur une zone particulière. Vous pouvez masquer ou afficher une courbe en cliquant sur la légende appropriée. Par exemple, lorsque vous cliquez sur la légende « Espace engagé », la courbe « Espace engagé » est masquée.

Liste des événements

La liste des événements affiche des détails sur les événements nouveaux et acquittés :

- **Gravité**

  Indique la gravité de l'événement.

- **Événement**

  Affiche le nom de l'événement.

- **Heure de déclenchement**

  Affiche le temps écoulé depuis la génération de l'événement. Si ce temps dépasse une semaine, l'horodatage de la génération de l'événement s'affiche.

Volet Appareils associés

Le volet « Périphériques associés » vous permet d'afficher le nœud de cluster, les volumes et les disques liés à l'agrégat :

- **Nœud**

  Affiche la capacité et l'état de santé du nœud contenant l'agrégat. La capacité indique la capacité utilisable totale par rapport à la capacité disponible.

- **Agrégats dans le nœud**

  Affiche le nombre et la capacité de tous les agrégats du nœud de cluster contenant l'agrégat sélectionné. L'état de santé des agrégats est également affiché, selon le niveau de gravité le plus élevé. Par exemple, si un nœud de cluster contient dix agrégats, dont cinq affichent l'état Warning et les cinq autres l'état Critical, alors l'état affiché est Critical.

- **Volumes**

  Affiche le nombre et la capacité des volumes FlexVol et des volumes FlexGroup dans l'agrégat ; le nombre n'inclut pas les composants FlexGroup. L'état de santé des volumes est également affiché, selon le niveau de gravité le plus élevé.

- **Pool de ressources**

  Affiche les pools de ressources liés à l'agrégat.

- **Disques**

  Affiche le nombre de disques dans l'agrégat sélectionné.

Volet Alertes associées

Le volet « Alertes associées » vous permet de consulter la liste des alertes créées pour l'agrégat sélectionné. Vous pouvez également ajouter une alerte en cliquant sur le lien « Ajouter une alerte » ou modifier une alerte existante en cliquant sur son nom.

Informations connexes

"Affichage des détails du pool de stockage"

Protéger et restaurer les données

Créer et dépanner les relations de protection

Types de protection SnapMirror dans Active IQ Unified Manager

Selon le déploiement de votre topologie de stockage des données, Unified Manager vous permet de configurer plusieurs types de relations de protection SnapMirror. Toutes les variantes de protection SnapMirror offrent une protection de reprise après sinistre avec basculement, mais proposent des capacités différentes en matière de performances, de flexibilité des versions et de protection par copie de sauvegarde multiple.

Traditionnelles SnapMirror relations de protection asynchrones

La protection asynchrone traditionnelle SnapMirror assure une protection miroir par 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 repose sur la réplication par blocs. Cependant, la protection SnapMirror traditionnelle exige que le volume de destination exécute la même version mineure ou une version mineure ultérieure du logiciel ONTAP que le volume source, au sein de la même version majeure (par exemple, version 8.x vers 8.x ou version 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.

SnapMirror Protection asynchrone avec réplication flexible selon la version

SnapMirror La protection asynchrone avec réplication flexible par version fournit une protection miroir de réplication logique entre les volumes source et de destination, même si ces volumes exécutent différentes versions du logiciel ONTAP 8.3 ou version ultérieure (par exemple, de la version 8.3 à 8.3.1, ou de 8.3 à 9.1, ou de 9.2.2 à 9.2).

Dans les relations SnapMirror avec réplication flexible en termes de version, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

En raison de son exécution plus lente, SnapMirror avec protection de réplication flexible par version ne convient pas à une mise en œuvre dans l'une ou l'autre des circonstances suivantes :

- L'objet source contient plus de 10 millions de fichiers à protéger.
- L'objectif de point de récupération pour les données protégées est de deux heures ou moins. (Autrement dit, la destination doit toujours contenir des données répliquées et récupérables qui ne sont pas plus anciennes de deux heures que les données de la source.)

Dans l'un ou l'autre des cas énumérés, l'exécution plus rapide de la protection SnapMirror par défaut, basée sur la réplication de blocs, est requise.

SnapMirror protection asynchrone avec option de réplication flexible selon les versions et de sauvegarde

SnapMirror La protection asynchrone avec réplication flexible des versions et option de sauvegarde assure une protection miroir entre les volumes source et de destination et la possibilité de stocker plusieurs copies

des données mises en miroir à destination.

L'administrateur du stockage peut spécifier quelles copies Snapshot sont répliquées de la source vers la destination et peut également spécifier combien de temps conserver ces copies à la destination, même si elles sont supprimées à la source.

Dans les relations SnapMirror avec une option de réplication flexible en termes de version et de sauvegarde, les opérations de mise en miroir ne s'exécutent pas aussi rapidement que dans les relations SnapMirror traditionnelles.

SnapMirror Réplication unifiée (miroir et archivage)

SnapMirror unified replication vous permet de configurer la reprise après sinistre et l'archivage sur le même volume de destination. Comme avec SnapMirror, la protection unifiée des données effectue un transfert de base la première fois que vous l'utilisez. Un transfert de base dans le cadre de la stratégie de protection unifiée des données par défaut "MirrorAndVault" crée une copie Snapshot du volume source, puis transfère cette copie et les blocs de données auxquels elle fait référence vers le volume de destination. Comme SnapVault, la protection unifiée des données n'inclut pas les anciennes copies Snapshot dans le transfert de base.

SnapMirror Protection synchrone avec synchronisation stricte

SnapMirror La protection synchrone avec la synchronisation « `strict` » garantit que les volumes primaire et secondaire sont toujours une copie conforme l'un de l'autre. En cas d'échec de réplication lors d'une tentative d'écriture de données sur le volume secondaire, les E/S client vers le volume primaire sont interrompues.

SnapMirror protection synchrone avec synchronisation régulière

SnapMirror La protection synchrone avec la synchronisation "regular" n'exige pas que les volumes primaire et secondaire soient toujours des copies conformes l'un de l'autre, garantissant ainsi la disponibilité du volume primaire. En cas d'échec de réplication lors d'une tentative d'écriture de données sur le volume secondaire, les volumes primaire et secondaire se désynchronisent 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 synchrones à partir de la vue Santé : tous les volumes ou de la page de détails Volume / Santé.

SnapMirror active sync

La fonction de synchronisation active SnapMirror est disponible avec ONTAP 9.8 et les versions ultérieures, et vous pouvez l'utiliser pour protéger les applications avec des LUN, ce qui permet aux applications de basculer de manière transparente et assure la continuité des activités en cas de sinistre.

Il vous permet de découvrir et de surveiller les relations synchrones SnapMirror pour les groupes de cohérence (CG) disponibles sur les clusters et les machines virtuelles de stockage depuis Unified Manager. SnapMirror active sync est pris en charge sur les clusters AFF ou les clusters All SAN Array (ASA), où les clusters principal et secondaire peuvent être AFF ou ASA. SnapMirror active sync protège les applications avec des LUN iSCSI ou FCP.

Lorsque vous consultez les volumes et les LUN protégés par la relation de synchronisation active SnapMirror, vous obtenez une vue unifiée des relations de protection, des groupes de cohérence dans l'inventaire des volumes, de la topologie de protection des relations de groupes de cohérence, ainsi que des données historiques de ces relations sur une période pouvant aller jusqu'à un an. Vous pouvez également télécharger le rapport. Vous pouvez également consulter le résumé des relations de groupes de cohérence, rechercher la

prise en charge de ces relations 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 ainsi que de la relation qui les unit, protégés par le groupe de cohérence.

Pour en savoir plus sur SnapMirror active sync, consultez "Documentation ONTAP 9 pour Snapmirror active sync (anciennement SM-BC)".

Configurez les relations de protection dans Unified Manager

Configurez les relations de protection dans Active IQ Unified Manager

Vous devez effectuer plusieurs étapes pour utiliser Unified Manager et OnCommand Workflow Automation afin de configurer des relations SnapMirror et SnapVault pour protéger vos données.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir établi des relations d'égal à égal entre deux clusters ou deux machines virtuelles de stockage (SVM).
- OnCommand Workflow Automation doit être intégré à Unified Manager :
  - "Configurer OnCommand Workflow Automation".
  - "Vérification de la mise en cache de la source de données Unified Manager dans Workflow Automation".

Étapes

1. Selon le type de relation de protection que vous souhaitez créer, procédez comme suit :
   - "Créer une relation de protection SnapMirror".
   - "Créer une relation de protection SnapVault".
2. Si vous souhaitez créer une politique pour la relation, en fonction du type de relation que vous créez, procédez comme suit :
   - "Créer une stratégie SnapVault".
   - "Créer une stratégie SnapMirror".
3. "Créez une planification SnapMirror ou SnapVault".

Configurez une connexion entre Workflow Automation et Active IQ Unified Manager

Vous pouvez configurer une connexion sécurisée entre OnCommand Workflow Automation (WFA) et Unified Manager. La connexion à Workflow Automation vous permet d'utiliser des fonctionnalités de protection telles que les workflows de configuration SnapMirror et SnapVault, ainsi que des commandes pour gérer les relations SnapMirror.

Avant de commencer

- La version installée de Workflow Automation doit être la version 5.1.1P6 ou une version ultérieure.

Le « pack WFA pour la gestion de Clustered Data ONTAP » est inclus dans WFA 5.1.1P6, il

n’est donc plus nécessaire de télécharger ce pack depuis le NetAppStorage Automation Store et de l’installer séparément sur votre serveur WFA comme c’était le cas auparavant. "Téléchargement WFA"

- Vous devez disposer du nom de l’utilisateur de la 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 s’être vu attribuer le rôle d’utilisateur « Integration Schema ».

- Le rôle d’administrateur ou d’architecte doit vous être attribué dans Workflow Automation.
- Vous devez disposer de l’adresse de l’hôte, du numéro de port 443, du nom d’utilisateur et du mot de passe pour la configuration de Workflow Automation.
- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **General** > **Workflow Automation**.
2. Dans la zone **Utilisateur de la base de données** de la **page Workflow Automation**, sélectionnez le nom et saisissez le mot de passe de l’utilisateur de la base de données que vous avez créé pour prendre en charge les connexions à Unified Manager et à Workflow Automation.
3. Dans la zone **Workflow Automation Credentials** de la page, saisissez le nom de l’hôte ou l’adresse IP (IPv4 ou IPv6), ainsi que le nom d’utilisateur et le mot de passe de la configuration Workflow Automation.

   Vous devez utiliser le port du serveur Unified Manager (port 443).

4. Cliquez sur **Enregistrer**.
5. Si vous utilisez un certificat auto-signé, cliquez sur **Oui** pour autoriser le certificat de sécurité.

   La page Workflow Automation s’affiche.

6. Cliquez sur **Oui** pour recharger la web UI et ajouter les fonctionnalités de Workflow Automation.

Informations connexes

"NetApp Documentation : OnCommand Workflow Automation (versions actuelles)"

Vérifiez la mise en cache de la source de données Active IQ Unified Manager dans Workflow Automation

Vous pouvez déterminer si la mise en cache des sources de données de Unified Manager fonctionne correctement en vérifiant si l’acquisition de la source de données réussit dans Workflow Automation. Vous pouvez effectuer cette vérification lorsque vous intégrez Workflow Automation à Unified Manager afin de vous assurer que les fonctionnalités de Workflow Automation sont disponibles après l’intégration.

Avant de commencer

Vous devez disposer du rôle Administrator ou du rôle Architect dans Workflow Automation pour effectuer cette tâche.

Étapes

1. Dans l’interface utilisateur de Workflow Automation, sélectionnez **Execution** > **Data Sources**.

2. Cliquez avec le bouton droit sur le nom de la source de données Unified Manager, puis sélectionnez **Acquire Now**.
3. Vérifiez que l'acquisition se déroule sans erreurs.

   Les erreurs d'acquisition doivent être résolues pour que l'intégration de Workflow Automation avec Unified Manager réussisse.

Comment la réinstallation ou la mise à niveau de OnCommand Workflow Automation affecte Active IQ Unified Manager

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 configurer de nouveau la connexion avec Unified Manager.

Supprimez la configuration OnCommand Workflow Automation d'Active IQ Unified Manager

Vous pouvez supprimer la configuration de OnCommand Workflow Automation de Unified Manager lorsque vous ne souhaitez plus utiliser Workflow Automation.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **General** > **Workflow Automation** dans le menu Setup de gauche.
2. Sur la page **Workflow Automation**, cliquez sur **Remove Setup**.

Effectuer un basculement et un rétablissement de la relation de protection

Effectuez un basculement et un retour en arrière d'une relation de protection dans Active IQ Unified Manager

Lorsqu'un volume source de votre relation de protection est désactivé en raison d'une défaillance matérielle ou d'une catastrophe, vous pouvez utiliser les fonctionnalités de relation de protection d'Unified Manager pour rendre la destination de protection accessible en lecture/écriture et basculer vers ce volume jusqu'à ce que la source soit de nouveau en ligne ; vous pouvez ensuite revenir à la source d'origine lorsqu'elle est disponible pour fournir des données.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré OnCommand Workflow Automation pour effectuer cette opération.

Étapes

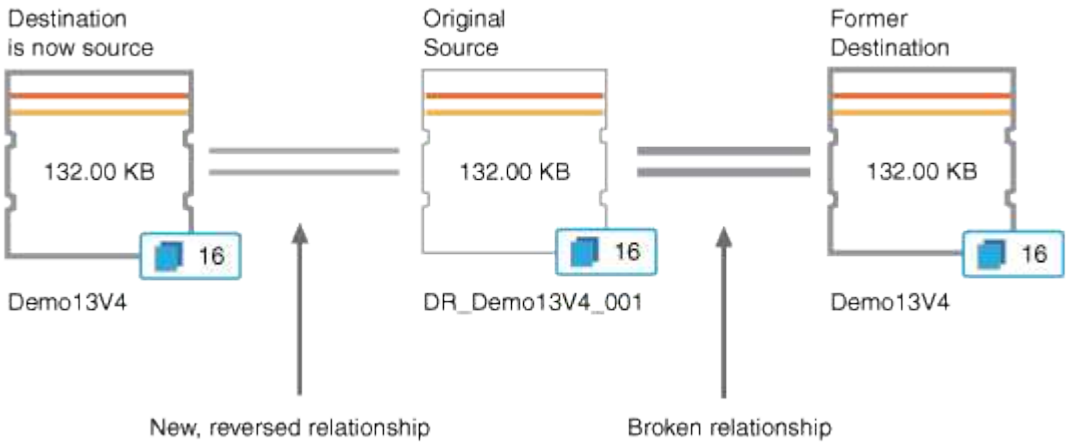
1. "Rompre la SnapMirror relation".

   Vous devez rompre la relation avant de pouvoir convertir le volume de destination d'un volume de protection des données en un volume de lecture/écriture, et avant de pouvoir inverser la relation.

2. "Inverser la relation de protection".

   Lorsque le volume source d'origine est de nouveau disponible, vous pouvez rétablir la relation de protection initiale en restaurant le volume source. Avant de pouvoir restaurer la source, vous devez la synchroniser avec les données écrites sur l'ancienne destination. Vous utilisez l'opération de resynchronisation inverse pour créer une nouvelle relation de protection en inversant les rôles de la relation initiale et en synchronisant le volume source avec l'ancienne destination. Une nouvelle copie Snapshot de référence est créée pour la nouvelle relation.

   La relation inversée ressemble à une relation en cascade :



3. "Rompre la relation SnapMirror inversée".

   Lorsque le volume source d'origine est resynchronisé et peut à nouveau fournir des données, utilisez l'opération de rupture pour rompre la relation inversée.

4. "Supprimer la relation".

   Lorsque la relation inversée n'est plus nécessaire, vous devez la supprimer 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 rétablir la relation d'origine.

Interrompre une relation de protection SnapMirror depuis la page Volume/Santé d'Active IQ Unified Manager

Vous pouvez rompre une relation de protection depuis la page Détails du volume / de l'état et arrêter les transferts de données entre un volume source et un volume de destination dans une relation SnapMirror. Vous pouvez rompre une relation lorsque vous souhaitez migrer des données, pour la reprise après sinistre ou pour tester des applications. Le volume de destination devient un volume en lecture-écriture. Vous ne

pouvez pas rompre une relation SnapVault.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez rompre.
2. Faites un clic droit sur la destination et sélectionnez **Interrompre** 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.

Inverser les relations de protection à partir de la page Détails du volume/de la santé dans Active IQ Unified Manager

Lorsqu'un sinistre rend inutilisable le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour fournir les données en le 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 rétablir la relation dans le sens inverse, en synchronisant les données de la source avec celles du volume de destination en lecture/écriture.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- La relation ne doit pas être une relation SnapVault.
- Une relation de protection doit déjà exister.
- Il faut rompre la relation de protection.
- La source et la destination doivent toutes deux 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 plus récentes que celles de la copie Snapshot commune sont supprimées.
- Les politiques et les planifications créées sur la relation de resynchronisation inverse sont les mêmes que celles de la relation de protection d'origine.

  Si les politiques et les planifications n'existent pas, elles sont créées.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, repérez dans la topologie la relation SnapMirror dont vous souhaitez inverser la source et la destination, puis cliquez dessus avec le bouton droit.
2. Sélectionnez **Resynchronisation inversée** dans le menu.

La boîte de dialogue de resynchronisation inverse s'affiche.

3. Vérifiez que la relation affichée dans la boîte de dialogue **Resynchronisation inverse** est bien celle pour laquelle vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Soumettre**.

   La boîte de dialogue Reverse Resync se ferme et un lien vers une tâche s'affiche en haut de la page de détails Volume / Health.

4. **Facultatif :** Cliquez sur **Afficher les tâches** dans la page de détails **Volume / Health** pour suivre l'état de chaque tâche de resynchronisation inverse.

   Une liste filtrée des tâches s'affiche.

5. **Facultatif :** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

   L'opération de resynchronisation inverse est terminée lorsque toutes les tâches du travail ont été exécutées avec succès.

Supprimez une relation de protection depuis la page Détails du volume/de l'état dans Active IQ Unified Manager

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 avec une destination différente. Cette opération supprime toutes les métadonnées et est irréversible.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, sélectionnez dans la topologie la relation SnapMirror que vous souhaitez supprimer.
2. Faites un clic droit sur le nom de la destination et sélectionnez **Supprimer** dans le menu.

   La boîte de dialogue Supprimer la relation s'affiche.

3. Cliquez sur **Continuer** pour supprimer la relation.

   La relation est supprimée de la page des détails Volume / Santé.

Resynchronisez les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager

Vous pouvez resynchroniser les données d'une relation SnapMirror ou SnapVault qui a été interrompue, puis rendre la destination accessible en lecture/écriture afin que les données de la source correspondent à celles de la destination. Vous pouvez également effectuer une resynchronisation lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, entraînant l'échec des mises à jour SnapMirror ou SnapVault.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, repérez dans la topologie la relation de protection que vous souhaitez resynchroniser et cliquez dessus avec le bouton droit.
2. Sélectionnez **Resynchronize** dans le menu.

   Vous pouvez également, dans le menu **Actions**, sélectionner **Relation** > **Resynchroniser** pour resynchroniser la relation dont vous consultez actuellement les détails.

   La boîte de dialogue Resynchroniser s'affiche.

3. Dans l'onglet **Options de resynchronisation**, sélectionnez une priorité de transfert et le débit de transfert maximal.
4. Cliquez sur **Copies d'instantané source**; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

   La boîte de dialogue « Sélectionner la copie d'instantané source » s'affiche.

5. Si vous souhaitez spécifier une copie 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 **Submit**.

   Vous revenez à la boîte de dialogue Resynchronize.

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 la tâche de resynchronisation.

   La tâche de resynchronisation démarre, vous revenez à la page Détails du volume / de l'état et un lien vers les tâches s'affiche en haut de la page.

9. **Facultatif:** Cliquez sur **Afficher les tâches** dans la page **Détails du volume / de l'état** pour suivre l'état de chaque tâche de resynchronisation.

   Une liste filtrée des tâches s'affiche.

10. **Facultatif :** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page de détails **Volume / Santé**.

    Le travail de resynchronisation est terminé lorsque toutes les tâches du travail se terminent avec succès.

Résoudre l'échec d'une tâche de protection

Résoudre un échec de tâche de protection dans Active IQ Unified Manager

Ce flux de travail illustre comment identifier et résoudre un échec de tâche de protection à partir du tableau de bord Unified Manager.

Avant de commencer

Étant donné que certaines tâches de ce flux de travail nécessitent que vous vous connectiez avec le rôle Administrator, vous devez vous familiariser avec les rôles requis pour utiliser les différentes fonctionnalités.

Dans ce scénario, vous accédez à la page Dashboard pour vérifier si vos tâches de protection présentent des problèmes. Dans la zone Incident de protection, vous remarquez qu'il existe un incident Job Terminated, indiquant une erreur Protection Job Failed sur un volume. Vous examinez cette erreur afin d'en déterminer la cause possible et la solution potentielle.

Étapes

1. Dans le panneau Protection Incidents de la zone Dashboard Unresolved Incidents and Risks, 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 de détails de l'événement relatif à la tâche de protection ayant échoué s'affiche.

2. Consultez le message d'erreur dans le champ Cause de la zone **Summary** pour déterminer le problème et évaluer les actions correctives potentielles.

   Voir "Identifier le problème et effectuer des actions correctives pour une tâche de protection ayant échoué".

Identifiez le problème et effectuez les actions correctives pour un travail de protection ayant échoué dans Active IQ Unified Manager

Vous examinez le message d'erreur d'échec de la tâche dans le champ Cause de la page Event details et déterminez que la tâche a échoué en raison d'une erreur de copie Snapshot. Vous accédez ensuite à la page Volume / Health details pour recueillir davantage d'informations.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Le message d'erreur indiqué dans le champ Cause de la page Détails de l'événement contient le texte suivant concernant la tâche ayant échoué :

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Ce message fournit les informations suivantes :

- La tâche de sauvegarde ou de mise en miroir n'a pas abouti.

  Le travail impliquait une relation de protection entre le volume source `cluster2_src_vol2` sur le serveur

virtuel `cluster2_src_svm` et le volume de destination `managed_svc2_vol3` sur le serveur virtuel nommé `cluster3_dst_svm`.

- Une tâche de copie Snapshot a échoué pour `0426cluster2_src_vol2snap` sur le volume source `cluster2_src_svm:/cluster2_src_vol2`.

Dans ce cas, vous pouvez identifier la cause de l'échec de la tâche et les actions correctives potentielles. Cependant, la résolution de cet échec nécessite d'accéder à l'interface web de System Manager ou aux commandes de l'interface de ligne de commande ONTAP.

Étapes

1. Vous examinez 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 votre volume source.

   Si vous le souhaitez, vous pouvez cliquer sur le lien **Job Details** à la fin du message d'erreur, mais pour les besoins de ce scénario, vous choisissez de ne pas le faire.

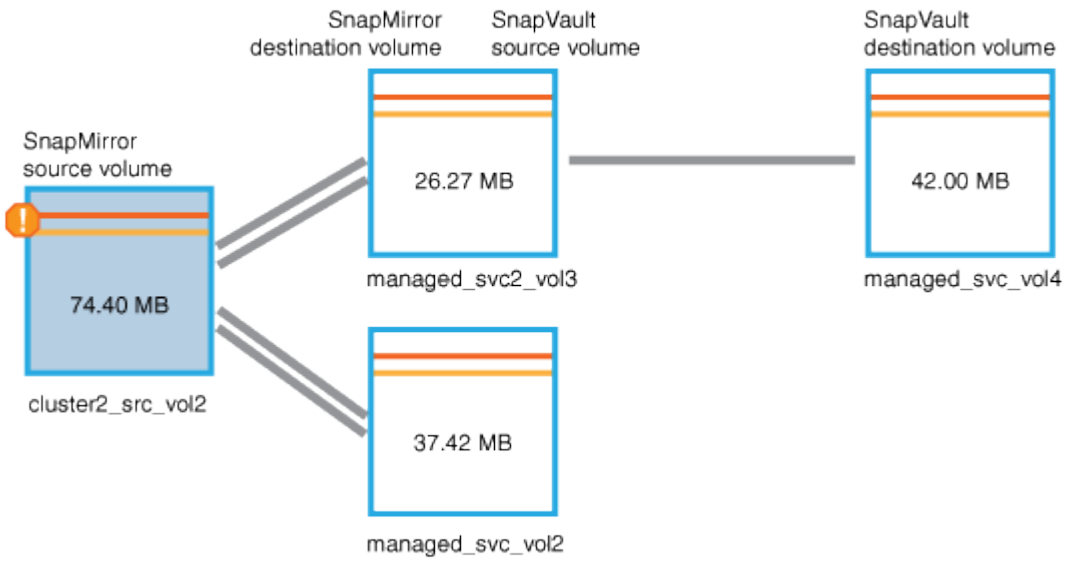
2. Vous décidez d'essayer de résoudre l'événement, vous procédez donc comme suit :
   a. Cliquez sur le bouton **Assign To** et sélectionnez **Me** dans le menu.
   b. Cliquez sur le bouton **Acknowledge** pour ne plus recevoir de notifications d'alerte répétées, si des alertes ont été configurées pour cet événement.
   c. Vous pouvez également ajouter des notes sur l'événement si vous le souhaitez.
3. Cliquez sur le champ **Source** dans le volet **Résumé** pour afficher les détails concernant le volume source.

   Le champ **Source** contient le nom de l'objet source : dans ce cas, le volume sur lequel la tâche de copie Snapshot a été planifiée.

   La page des détails Volume / Santé s'affiche pour `cluster2_src_vol2`, affichant le contenu de l'onglet Protection.

4. En consultant le graphique de topologie de protection, vous voyez une icône d'erreur associée au premier volume de la topologie, qui est le volume source de la relation SnapMirror.

   Vous pouvez également observer les barres horizontales dans l'icône du volume source, indiquant les seuils d'avertissement et d'erreur définis pour ce volume.



5. Vous placez votre curseur sur l'icône d'erreur pour afficher la boîte de dialogue contextuelle indiquant les paramètres de seuil et constater que le volume a dépassé le seuil d'erreur, ce qui indique un problème de capacité.
6. Cliquez sur l'onglet **Capacité**.

   Informations sur la capacité des affichages `cluster2_src_vol2` de volume.
7. Dans le panneau **Capacité**, vous pouvez constater la présence d'une icône d'erreur dans le graphique à barres, indiquant à nouveau que la capacité du volume a dépassé le seuil défini pour ce volume.
8. Sous le graphique de capacité, vous constatez que la croissance automatique du volume a été désactivée et qu'une garantie d'espace du volume a été définie.

   Vous pourriez décider d'activer l'extension automatique, mais dans le cadre de ce scénario, vous décidez d'approfondir la question avant de prendre une décision sur la manière de résoudre le problème de capacité.
9. Vous faites défiler l'écran jusqu'à la liste **Événements** et vous voyez que les événements « Protection Job Failed », « Volume Days Until Full » et « Volume Space Full » ont été générés.
10. Dans la liste **Événements**, vous cliquez sur l'événement **Volume Space Full** pour obtenir plus d'informations, après avoir déterminé que cet événement semble le plus pertinent pour votre problème de capacité.

    La page de 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 les actions correctives suggérées.

    Les actions correctives suggérées ne s'affichent que pour certains événements, vous ne verrez donc pas cette zone pour tous les types d'événements.

    Vous parcourez la liste des actions suggérées que vous pouvez effectuer pour résoudre l'événement « Volume Space Full » :

    - Activer l'extension automatique sur ce volume.
    - Redimensionnez le volume.
    - Activez et exécutez la déduplication sur ce volume.
    - Activez et exécutez la compression sur ce volume.
13. Vous décidez d'activer la croissance automatique du volume, mais pour ce faire, vous devez déterminer l'espace libre disponible sur l'agrégat parent et le taux de croissance actuel du volume :
    a. Consultez l'agrégat parent, `cluster2_src_aggr1`, dans le volet **Appareils associés**.

       Vous pouvez cliquer sur le nom de l'agrégat pour obtenir plus de détails à son sujet.

       Vous déterminez que l'agrégat dispose d'un espace suffisant pour permettre l'augmentation automatique du volume.

    b. En haut de la page, repérez l'icône indiquant un incident critique et consultez le texte situé en dessous.

Vous déterminez que "Jours avant remplissage complet : moins d'un jour | Taux de croissance quotidien : 5,4 %".

14. Accédez à System Manager ou à l'interface de ligne de commande ONTAP pour activer l' `volume autogrow`option.

    Notez les noms du volume et de l'agrégat afin de les avoir à disposition lors de l'activation d'autogrow.

15. Une fois le problème de capacité résolu, retournez à la page de détails **Event** dans Unified Manager et marquez l'événement comme résolu.

Résoudre les problèmes de latence dans Active IQ Unified Manager

Ce flux de travail fournit un exemple de la façon dont vous pouvez résoudre un problème de retard. Dans ce scénario, vous êtes un administrateur ou un opérateur qui accède à la page Unified ManagerDashboard pour vérifier s'il existe des problèmes dans vos relations de protection et, le cas échéant, trouver des solutions.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Sur la page Tableau de bord, vous consultez la zone Incidents et risques non résolus et vous constatez une erreur de décalage SnapMirror dans le volet Protection, sous Risques de protection.

Étapes

1. Dans le volet **Protection** de la page **Tableau de bord**, repérez l'erreur de décalage de la relation SnapMirror et cliquez dessus.

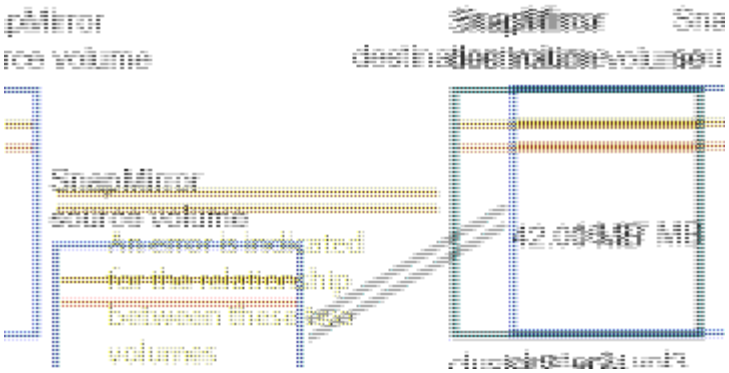
   La page de détails de l'événement correspondant à l'événement d'erreur de décalage s'affiche.

2. Depuis la page de détails de l'**événement**, vous pouvez effectuer une ou plusieurs des tâches suivantes:
   - Consultez le message d'erreur dans le champ Cause de la zone Summary pour déterminer s'il existe une action corrective suggérée.
   - Cliquez sur le nom de l'objet, dans ce cas un volume, dans le champ Source de la zone Summary pour obtenir des détails sur le volume.
   - Recherchez les notes qui auraient pu être ajoutées concernant cet événement.
   - Ajouter une note à l'événement.
   - Attribuer l'événement à un utilisateur spécifique.
   - Accusez réception de l'événement ou résolvez-le.
3. Dans ce scénario, vous cliquez sur le nom de l'objet (dans ce cas, un volume) dans le champ Source de la zone **Summary** pour obtenir des détails sur le volume.

   La page Détails Volume / Santé s'affiche sur l'onglet Protection.

4. Dans l'onglet **Protection**, vous pouvez consulter le diagramme de topologie.

   Vous constatez que le volume présentant l'erreur de décalage est le dernier volume d'une cascade SnapMirror de trois volumes. Le volume que vous avez sélectionné est entouré de gris foncé, et une double ligne orange partant du volume source indique une erreur de relation SnapMirror.



5. Cliquez sur chacun des volumes de la cascade SnapMirror.

   Lorsque vous sélectionnez chaque volume, les informations de protection dans les sections Résumé, Topologie, Historique, Événements, Appareils associés et Alertes associées changent pour afficher les détails relatifs au volume sélectionné.

6. Vous consultez la zone **Résumé** et placez votre curseur sur l'icône d'information dans le champ **Calendrier des mises à jour** pour chaque volume.

   Dans ce scénario, vous constatez que la stratégie SnapMirror est DPDefault et que la planification SnapMirror se met à jour toutes les heures, cinq minutes après l'heure. Vous vous rendez compte que tous les volumes de la relation tentent d'effectuer un transfert SnapMirror en même temps.

7. Pour résoudre le problème de décalage, vous modifiez les planifications de deux des volumes en cascade afin que chaque destination commence un transfert SnapMirror une fois que sa source a terminé un transfert.

Gérer et surveiller les relations de protection

Découvrez comment gérer et surveiller les relations de protection dans Active IQ Unified Manager

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 vers le volume secondaire est définie par un calendrier.

- Synchrone

  La réplication s'effectue simultanément sur le volume primaire et le volume secondaire.

Vous pouvez exécuter jusqu'à 10 tâches de protection simultanément sans impact sur les performances. Vous pourriez constater un certain impact sur les performances lorsque vous exécutez entre 11 et 30 tâches simultanément. Il est déconseillé d'exécuter plus de 30 tâches simultanément.

Consultez l’état de la protection des volumes dans Active IQ Unified Manager

La page Protection des données présente une vue d’ensemble complète des détails de protection des données pour tous les volumes protégés dans un seul cluster, ou pour tous les clusters d’un centre de données.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. Selon que vous souhaitiez 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 seul cluster dans le menu déroulant.
3. Cliquez sur la flèche vers la droite en haut du panneau Protection des données. La page **Protection des données** s’affiche.

Selon que vous ayez sélectionné un seul cluster ou tous les clusters de votre centre de données, cette page affiche l’état de la protection des données des volumes protégés par des copies Snapshot ou par des politiques SnapMirror, ainsi que le nombre de volumes non protégés.

La sélection d’un cluster dans la liste **Cluster individuel** affiche l’état de la protection par snapshot et des relations SnapMirror des volumes protégés de ce cluster.

Lorsque vous cliquez sur les événements de cette page, vous êtes redirigé vers la page des détails de l’événement. Vous pouvez cliquer sur le lien **Tout afficher** pour afficher tous les événements de protection actifs dans la page d’inventaire de gestion des événements. Vous pouvez placer le pointeur de la souris dessus pour afficher les nombres respectifs et les légendes. Vous pouvez cliquer :

- Les histogrammes des volumes non protégés et des volumes protégés par des copies Snapshot permettent d’accéder à la page Volumes et d’afficher les détails.
- Les graphiques à barres de toutes les relations permettent d’accéder à la page Relations, où les détails sont filtrés par le cluster source.

Afficher l’état de protection des volumes protégés par des copies Snapshot

Présentation des copies instantanées : aperçu des volumes protégés par les copies instantanées, tels que :

- Nombre total de volumes protégés et non protégés par des copies Snapshot.
- Le nombre total de volumes qui utilisent ou dépassent l’espace réservé aux copies Snapshot.

L’analyse des copies Snapshot détaille les informations suivantes :

- Événements individuels pour les copies Snapshot, y compris les événements générés au cours des dernières 24 heures.
- Tableau détaillé des volumes protégés et non protégés par les copies Snapshot.
- Volumes utilisant ou non la capacité réservée aux copies Snapshot, et volumes la dépassant.
- Répartition des volumes en fonction du nombre de leurs copies Snapshot.

Points à noter pour les copies Snapshot

- Pour le décompte des volumes protégés par des copies Snapshot, on prend en compte les volumes source et de destination.

- Le nombre de copies Snapshot renvoyées ne concerne que les volumes en ligne et disponibles.
- La plage du graphique pour le nombre de copies Snapshot est dynamique. Elle est générée en fonction du nombre d'instantanés présents dans le cluster sélectionné.
- Pour qu'un volume soit considéré comme protégé, la planification de la copie Snapshot du volume doit être activée.
- La valeur de l'espace réservé aux copies Snapshot est importante pour visualiser la quantité d'espace disque utilisé ou pour calculer l'espace qui peut être récupéré si une ou plusieurs copies Snapshot sont supprimées.

Consulter le statut de protection des SnapMirror relations

SnapMirror Vue d'ensemble : aperçu des volumes protégés par des stratégies SnapMirror, tels que :

- Le nombre de volumes protégés par les politiques SnapMirror respectives, telles que les relations SnapMirror entre volumes, la reprise après sinistre des machines virtuelles de stockage (SVM-DR) et leurs combinaisons.
- Le nombre total de relations SnapMirror subissant un retard de l'objectif de point de récupération (RPO) en fonction de l'état du retard.

SnapMirror Analyse détaille les informations suivantes :

- Événements individuels liés aux relations SnapMirror, y compris ceux survenus au cours des dernières 24 heures
- Le nombre de volumes protégés par chaque type de stratégie SnapMirror.
- Le nombre de relations protégées par les types de relation SnapMirror, tels que Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, le groupe de cohérence SnapMirror active sync et Sync.
- Le nombre de relations saines et malsaines.
- Ventilation du nombre de relations de volume. Vous pouvez basculer entre les graphiques selon le délai de retard du RPO et l'état.
- Seuil de retard pour la relation non gérée. Vous pouvez cliquer sur l'icône des paramètres ( ) pour configurer les paramètres de seuil de retard. Pour plus d'informations, consultez "Configuration des paramètres de seuil de retard pour les relations de protection non gérées".

Points à noter pour les relations SnapMirror

- Pour compter les relations SnapMirror, les volumes sources, activés pour la lecture et l'écriture, sont comptabilisés. Les volumes de destination et les volumes 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 dont les sources et les destinations se trouvent sur le même cluster ou sur des clusters différents.
- La durée du décalage RPO dans la réplication des données est basée sur la relation SnapMirror. L'état est catégorisé comme `ok` « actif », `warning` ou `error` « inactif », selon le seuil de relation défini. Vous pouvez consulter cet état pour déterminer si les paramètres fonctionnent comme prévu ou si vous devez résoudre un problème.
- Si un volume comporte plusieurs relations SnapMirror, chaque type de relation est comptabilisé pour le retard RPO.

- Les relations de volume sont considérées comme défaillantes 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 la configuration MetroCluster

Le panneau **MetroCluster Protection** de la page **Data Protection** affiche le nombre de clusters protégés ou non protégés par MetroCluster via une configuration FC ou IP sur votre site. Cliquer sur les graphiques à barres de ce panneau vous redirige vers la page Clusters, où les détails des clusters sont filtrés selon qu'ils sont protégés ou non protégés. Pour plus d'informations sur la surveillance de votre configuration MetroCluster, consultez "Surveillance des MetroCluster configurations".

Afficher les relations de protection des volumes dans Active IQ Unified Manager

Dans la vue « Relation : toutes les relations » et dans la page « Relations de volume », vous pouvez consulter l'état des relations SnapMirror et SnapVault du volume existant. Vous pouvez également examiner les détails des relations de protection, notamment l'état du transfert et du décalage, les informations sur la source et la destination, le calendrier et les informations sur la stratégie, etc.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez également lancer des commandes de relation à partir de cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Toutes les relations**.

   La vue « Relations : Toutes les relations » s'affiche.

3. Choisissez l'une des méthodes suivantes pour afficher les détails de la protection du volume :

   - Pour consulter les informations actuelles concernant toutes les relations de volume, restez sur la page par défaut **Toutes les relations**.
   - Pour consulter des informations détaillées sur les tendances de transfert du volume au fil du temps, dans le menu Affichage, sélectionnez la vue Relation : État des transferts du dernier mois.
   - Pour consulter des informations détaillées sur l'activité de transfert du volume au jour le jour, dans le menu Affichage, sélectionnez la vue Relation : Taux de transfert du dernier mois.

   > Les vues de transfert de volume affichent des informations uniquement sur les volumes dans des relations asynchrones : les volumes dans des relations synchrones ne sont pas affichés.

Surveillez les relations LUN du groupe de cohérence dans Active IQ Unified Manager

Si votre environnement ONTAP prend en charge la synchronisation active SnapMirror pour protéger les applications avec des LUN, vous pouvez visualiser et surveiller ces LUN sur Active IQ Unified Manager.

SnapMirror active sync garantit un objectif de temps de récupération (RTO) nul lors d'un basculement dans les

environnements SAN. Dans un déploiement typique prenant en charge SnapMirror active sync, les LUN sur les volumes sont protégés par des relations de groupe de cohérence.

Ces LUN primaires et secondaires sont des LUN composites, c'est-à-dire une paire de LUN répliquées possédant 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, garantissant ainsi la transparence.

Pour visualiser les LUN composites, les clusters principal et secondaire avec les LUN qui font partie de la relation de groupe de cohérence doivent être ajoutés et découverts dans Unified Manager. Seuls les LUN iSCSI et FCP sont pris en charge.

Pour plus d'informations sur la synchronisation active de SnapMirror, consultez "Documentation ONTAP 9 pour SnapMirror active sync (anciennement SM-BC)".

Pour afficher les LUN composites dans votre environnement, suivez ces étapes :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **LUNs**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Toutes les LUN**.

   La vue « Relation : toutes les LUN » s'affiche.

Vous pouvez consulter les détails du LUN, tels que le nom du LUN, le volume, la VM de stockage hébergeant le LUN, le cluster, le groupe de cohérence et le LUN partenaire. Vous pouvez cliquer sur chacun de ces composants pour accéder à une vue détaillée. En cliquant sur le groupe de cohérence, vous accédez à la page Relationships.

En cliquant sur le LUN partenaire, vous pouvez afficher les détails de sa configuration dans l'onglet SAN de la page Détails de la machine virtuelle de stockage de la machine virtuelle de stockage qui héberge le LUN partenaire. Les informations affichées incluent notamment les initiateurs, les groupes d'initiateurs et d'autres aspects du LUN partenaire.

Vous pouvez effectuer les fonctions standard au niveau de la grille pour trier, filtrer, générer et télécharger des rapports sur les LUN protégées dans votre environnement.

Créez une relation SnapVault à partir de la vue Health: All Volumes dans Active IQ Unified Manager

Vous pouvez utiliser la vue « État : Tous les volumes » pour créer des relations SnapVault pour un ou plusieurs volumes sur la même machine virtuelle de stockage afin d'activer les sauvegardes de données à des fins de protection.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Le menu **Protection** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action: par exemple, si vous ne disposez que de privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le

cluster de destination n’a pas encore été découvert

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans la vue **Santé : Tous les volumes**, sélectionnez un volume que vous souhaitez protéger et cliquez sur **Protéger**.

   Vous pouvez également, pour créer plusieurs relations de protection sur la même machine virtuelle de stockage (SVM), sélectionner un ou plusieurs volumes dans la vue Santé : Tous les volumes, puis cliquer sur **Protéger** dans la barre d’outils.

3. Sélectionnez **SnapVault** dans le menu.

   La boîte de dialogue Configurer la protection s’affiche.

4. Cliquez sur **SnapVault** pour afficher l’onglet **SnapVault** et configurer les informations du volume secondaire.
5. Cliquez sur **Avancé** pour configurer la déduplication, la compression, l’extension automatique et la garantie d’espace selon vos besoins, puis cliquez sur **Appliquer**.
6. Remplissez les zones **Informations sur la destination** et **Paramètres de la relation** dans l’onglet **SnapVault**.
7. Cliquez sur **Appliquer**.

   Vous revenez à la vue Santé: Tous les volumes.

8. Cliquez sur le lien de la tâche de configuration de la protection en haut de la vue **Santé : Tous les volumes**.

   Si vous ne créez qu’une seule relation de protection, la page Détails de la tâche s’affiche ; en revanche, si vous créez plusieurs relations de protection, une liste filtrée de toutes les tâches associées 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 de la tâche associés au travail de configuration de la protection, et pour déterminer quand le travail est terminé.
   - Si vous avez plus d’un emploi :
     i. Cliquez sur une tâche dans la liste des tâches.
     ii. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection, et pour déterminer quand le travail est terminé.
     iii. Utilisez le bouton **Retour** pour revenir à la liste filtrée et afficher une autre tâche.

Créez une relation de protection SnapVault à partir de la page Détails du volume/de l’état dans Active IQ Unified Manager

Vous pouvez créer une relation SnapVault à l’aide de la page des détails du volume et de l’état afin d’activer les sauvegardes de données à des fins de protection sur les volumes.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation pour effectuer cette tâche.

Le menu **Protection** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action: par exemple, si vous ne disposez que de privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Health**, cliquez avec le bouton droit sur un volume dans la vue topologique que vous souhaitez protéger.
2. Sélectionnez **Protéger** > **SnapVault** dans le menu.

   La boîte de dialogue Configurer la protection s'affiche.

3. Cliquez sur **SnapVault** pour afficher l'onglet **SnapVault** et configurer les informations de la ressource secondaire.
4. Cliquez sur **Avancé** pour configurer la déduplication, la compression, l'extension automatique et la garantie d'espace selon vos besoins, puis cliquez sur **Appliquer**.
5. Remplissez la zone **Informations de destination** et la zone **Paramètres de la relation** dans la boîte de dialogue **Configurer la protection**.
6. Cliquez sur **Appliquer**.

   Vous revenez à la page Détails du volume / de l'état de santé.

7. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page de détails **Volume / Health**.

   La page Détails de la tâche s'affiche.

8. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection, et pour déterminer quand le travail est terminé.

   Une fois les tâches terminées, les nouvelles relations s'affichent dans la vue topologique de la page de détails Volume / Health.

Créez une relation SnapMirror à partir de la vue Health : All Volumes dans Active IQ Unified Manager

L'utilisation de la vue « État : Tous les volumes » vous permet de créer simultanément plusieurs relations de protection SnapMirror en sélectionnant plusieurs volumes sur la même machine virtuelle de stockage.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Le menu **Protection** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action: par exemple, si vous ne disposez que de privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Étapes

1. Dans la vue **Santé : Tous les volumes**, sélectionnez le volume que vous souhaitez protéger.

   Vous pouvez également créer plusieurs relations de protection sur le même SVM en sélectionnant un ou plusieurs volumes dans la vue Santé : Tous les volumes, puis en cliquant sur **Protéger** > **SnapMirror** dans la barre d'outils.

   La boîte de dialogue Configurer la protection s'affiche.

2. Cliquez sur **SnapMirror** pour afficher l'onglet **SnapMirror** et configurer les informations de destination.
3. Cliquez sur **Advanced** pour définir la garantie d'espace, si nécessaire, puis cliquez sur **Apply**.
4. Remplissez les sections **Informations sur la destination** et **Paramètres de la relation** dans l'onglet **SnapMirror**.
5. Cliquez sur **Appliquer**.

   Vous revenez à la vue Santé: Tous les volumes.

6. Cliquez sur le lien de la tâche de configuration de la protection en haut de la vue **Santé : Tous les volumes**.

   Si vous ne créez qu'une seule relation de protection, la page Détails de la tâche s'affiche ; en revanche, si vous créez plusieurs relations de protection, une liste de toutes les tâches associées 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 de la tâche associés au travail de configuration de la protection, et pour déterminer quand le travail est terminé.
   - Si vous avez plus d'un emploi :
     i. Cliquez sur une tâche dans la liste des tâches.
     ii. Cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection, et pour déterminer quand le travail est terminé.
     iii. Utilisez le bouton **Retour** pour revenir à la liste filtrée et afficher une autre tâche.

En fonction de la SVM de destination que vous avez spécifiée lors de la configuration ou des options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut prendre l'une des formes suivantes :

- Si vous avez spécifié une SVM de destination qui s'exécute avec la même version d'ONTAP ou une version plus récente que celle du volume source, une relation SnapMirror basée sur la réplication par blocs est le résultat par défaut.
- Si vous avez spécifié une SVM de destination qui s'exécute sous la même version ou une version plus récente d'ONTAP que celle du volume source, mais que vous avez activé la réplication flexible de version dans les paramètres avancés, une relation SnapMirror avec réplication flexible de version est établie.

- Si vous avez spécifié une SVM de destination qui s'exécute sous une version d'ONTAP antérieure à celle du volume source, et que cette version antérieure prend en charge la réplication flexible de version, une relation SnapMirror avec réplication flexible de version est le résultat automatique.

Créez une relation SnapMirror à partir de la page de détails de l'état du volume dans Active IQ Unified Manager

Vous pouvez utiliser la page Détails du volume/de l'état pour créer une relation SnapMirror afin d'activer la réplication des données 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.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Le menu **Protection** ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action: par exemple, si vous ne disposez que de privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Vous pouvez exécuter jusqu'à 10 tâches de protection simultanément sans impact sur les performances. Vous pourriez constater un certain impact sur les performances lorsque vous exécutez entre 11 et 30 tâches simultanément. Il est déconseillé d'exécuter plus de 30 tâches simultanément.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Health**, cliquez avec le bouton droit dans la vue topologique sur le nom d'un volume que vous souhaitez protéger.
2. Sélectionnez **Protéger** > **SnapMirror** dans le menu.

   La boîte de dialogue Configurer la protection s'affiche.

3. Cliquez sur **SnapMirror** pour afficher l'onglet **SnapMirror** et configurer les informations de destination.
4. Cliquez sur **Advanced** pour définir la garantie d'espace, si nécessaire, puis cliquez sur **Apply**.
5. Remplissez la zone **Informations de destination** et la zone **Paramètres de la relation** dans la boîte de dialogue **Configurer la protection**.
6. Cliquez sur **Appliquer**.

   Vous revenez à la page Détails du volume / de l'état de santé.

7. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page de détails **Volume / Health**.

   Les tâches et les détails de la tâche sont affichés sur la page « Détails de la tâche ».

8. Dans la page de détails du **Job**, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails des tâches associés au job de configuration de la protection et pour déterminer quand le job est terminé.
9. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails

Volume / Health.

La nouvelle relation s'affiche dans la vue topologique de la page de détails Volume / Santé.

En fonction de la SVM de destination que vous avez spécifiée lors de la configuration ou des options que vous avez activées dans vos paramètres avancés, la relation SnapMirror résultante peut prendre l'une des formes suivantes :

- Si vous avez spécifié une SVM de destination qui s'exécute avec la même version d'ONTAP ou une version plus récente que celle du volume source, une relation SnapMirror basée sur la réplication par blocs est le résultat par défaut.
- Si vous avez spécifié une SVM de destination qui s'exécute sous la même version ou une version plus récente d'ONTAP que celle du volume source, mais que vous avez activé la réplication flexible de version dans les paramètres avancés, une relation SnapMirror avec réplication flexible de version est établie.
- Si vous avez spécifié une SVM de destination qui exécute une version antérieure de ONTAP, ou une version supérieure à celle du volume source, et que la version antérieure prend en charge la réplication flexible par version, une relation SnapMirror avec réplication flexible par version en résulte automatiquement.

Créez une relation SnapMirror avec la réplication flexible des versions dans Active IQ Unified Manager

Vous pouvez créer une relation SnapMirror avec la réplication flexible des versions. La réplication flexible des versions vous permet de mettre en œuvre la protection SnapMirror même si les volumes source et de destination fonctionnent sous des versions différentes de ONTAP.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- Les SVM source et de destination doivent chacune disposer d'une licence SnapMirror activée.
- Les SVM source et de destination doivent chacune exécuter une version du logiciel ONTAP qui prend en charge la réplication flexible des versions.

SnapMirror avec réplication flexible par version vous permet de mettre en œuvre une protection SnapMirror même dans des environnements de stockage hétérogène où tout le stockage ne fonctionne pas sous une seule version de ONTAP ; cependant, les opérations de mise en miroir effectuées sous SnapMirror avec réplication flexible par version ne s'exécutent pas aussi rapidement qu'avec la réplication par blocs traditionnelle SnapMirror.

Étapes

1. Affichez la boîte de dialogue **Configurer la protection** pour le volume que vous souhaitez protéger.
    - Si vous consultez l'onglet Protection de la page de détails Volume / État, cliquez avec le bouton droit dans la vue topologique portant le nom d'un volume que vous souhaitez protéger et sélectionnez **Protéger** > **SnapMirror** dans le menu.
    - Si vous consultez la vue État : Tous les volumes, repérez un volume que vous souhaitez protéger et cliquez dessus avec le bouton droit de la souris ; sélectionnez ensuite **Protéger** > **SnapMirror** dans le menu. La boîte de dialogue Configurer la protection s'affiche.
2. Cliquez sur **SnapMirror** pour afficher l'onglet **SnapMirror**.

3. Remplissez la zone **Informations de destination** et la zone **Paramètres de la relation** dans la boîte de dialogue **Configurer la protection**.

   Si vous spécifiez une SVM de destination qui s'exécute sous une version d'ONTAP antérieure à celle du volume source que vous protégez, et si cette version antérieure prend en charge la réplication flexible par version, cette tâche configure automatiquement SnapMirror avec la réplication flexible par version.

4. Si vous spécifiez une SVM de destination qui s'exécute sous la même version de ONTAP que celle du volume source, mais que vous souhaitez tout de même configurer SnapMirror avec la réplication flexible par version, cliquez sur **Avancé** pour activer la réplication flexible par version, puis cliquez sur **Appliquer**.
5. Cliquez sur **Appliquer**.

   Vous revenez à la page Détails du volume / de l'état de santé.

6. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page de détails **Volume / Health**.

   Les tâches et les détails du travail s'affichent sur la page « Détails du travail ».

7. Dans la page de détails du **Job**, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails des tâches associés au job de configuration de la protection et pour déterminer quand le job est terminé.
8. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails **Volume / Health**.

   La nouvelle relation s'affiche dans la vue topologique de la page de détails Volume / Santé.

Créez des relations SnapMirror avec la réplication flexible des versions et la fonctionnalité de retour en arrière dans Active IQ Unified Manager

Vous pouvez créer une relation SnapMirror avec une réplication flexible par version et la fonctionnalité d'option de sauvegarde. La fonctionnalité d'option de sauvegarde vous permet de mettre en œuvre la protection SnapMirror et de conserver également plusieurs versions des copies de sauvegarde à l'emplacement de destination.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- Les SVM source et de destination doivent chacune disposer d'une licence SnapMirror activée.
- Les SVM source et de destination doivent chacune disposer d'une licence SnapVault activée.
- Les SVM source et de destination doivent chacune exécuter une version du logiciel ONTAP qui prend en charge la réplication flexible des versions.

La configuration de SnapMirror avec la fonctionnalité d'option de sauvegarde vous permet de protéger vos données grâce aux fonctionnalités de reprise après sinistre de SnapMirror, telles que la capacité de basculement de volume, tout en offrant des fonctionnalités de SnapVault, telles que la protection par plusieurs copies de sauvegarde.

Étapes

1. Affichez la boîte de dialogue **Configurer la protection** pour le volume que vous souhaitez protéger.
   - Si vous consultez l'onglet Protection de la page Détails du volume / de l'état, cliquez avec le bouton

droit dans la vue topologique sur le nom du volume que vous souhaitez protéger et sélectionnez **Protéger** > **SnapMirror** dans le menu.

- Si vous consultez la vue « Intégrité : Tous les volumes », repérez un volume que vous souhaitez protéger et cliquez dessus avec le bouton droit ; puis sélectionnez **Protéger** > **SnapMirror** dans le menu. La boîte de dialogue Configurer la protection s'affiche.

2. Cliquez sur **SnapMirror** pour afficher l'onglet **SnapMirror**.
3. Remplissez la zone **Informations de destination** et la zone **Paramètres de la relation** dans la boîte de dialogue **Configurer la protection**.
4. Cliquez sur **Avancé** pour afficher la boîte de dialogue **Paramètres de destination avancés**.
5. Si la case à cocher **Version-Flexible Replication** n'est pas déjà sélectionnée, cochez-la maintenant.
6. Cochez la case à cocher **With backup option** pour activer l'option de sauvegarde, puis cliquez sur **Appliquer**.
7. Cliquez sur **Appliquer**.

   Vous revenez à la page Détails du volume / de l'état de santé.

8. Cliquez sur le lien de la tâche de configuration de la protection en haut de la page de détails **Volume / Health**.

   Les tâches et les détails du travail s'affichent sur la page « Détails du travail ».

9. Dans la page de détails de **Job**, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails des tâches associés au job de configuration de la protection, et déterminer quand le job est terminé.
10. Une fois les tâches terminées, cliquez sur **Retour** dans votre navigateur pour revenir à la page de détails **Volume / Health**.

    La nouvelle relation s'affiche dans la vue topologique de la page de détails Volume / Santé.

Configurez les paramètres d'efficacité de la destination dans Active IQ Unified Manager

Vous pouvez configurer les paramètres d'efficacité de destination, tels que la déduplication, la compression, l'extension automatique et la garantie d'espace, sur une destination de protection à l'aide de la boîte de dialogue Advanced Destination Settings. Vous utilisez ces paramètres lorsque vous souhaitez optimiser l'utilisation de l'espace sur une destination ou un volume secondaire.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Par défaut, les paramètres d'efficacité correspondent à ceux du volume source, à l'exception des paramètres de compression dans une relation SnapVault, qui sont désactivés par défaut.

Étapes

1. Cliquez sur l'onglet **SnapMirror** ou sur l'onglet **SnapVault** dans la boîte de dialogue **Configurer la protection**, selon le type de relation que vous configurez.
2. Cliquez sur **Avancé** dans la section **Informations sur la destination**.

   La boîte de dialogue Paramètres de destination avancés s'ouvre.

3. Activez ou désactivez les paramètres d'efficacité pour la déduplication, la compression, l'extension automatique et la garantie d'espace, selon vos besoins.
4. Cliquez sur **Appliquer** pour enregistrer vos sélections et revenir à la boîte de dialogue **Configurer la protection**.

Créer des plannings SnapMirror et SnapVault dans Active IQ Unified Manager

Vous pouvez créer des planifications de base ou avancées pour SnapMirror et SnapVault afin d'activer des transferts automatiques de protection des données sur un volume source ou principal, de sorte que les transferts aient lieu plus ou moins fréquemment, selon la fréquence à laquelle les données changent sur vos volumes.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir déjà rempli la section « Informations sur la destination » de la boîte de dialogue « Configurer la protection ».
- Vous devez avoir configuré Workflow Automation pour effectuer cette tâche.

Étapes

1. Dans l'onglet **SnapMirror** ou l'onglet **SnapVault** de la boîte de dialogue **Configurer la protection**, cliquez sur le lien **Créer une planification** dans la zone **Paramètres de relation**.

   La boîte de dialogue Créer une planification s'affiche.

2. Dans le champ **Nom du planning**, saisissez le nom que vous souhaitez donner au planning.
3. Sélectionnez l'une des options suivantes :
   - **De base**

     Sélectionnez si vous souhaitez créer une planification de base de type intervalle.

   - **Avancé**

     Cochez cette case si vous souhaitez créer une planification de type cron.
4. Cliquez sur **Créer**.

   Le nouvel horaire est affiché dans la liste déroulante « Horaire SnapMirror » ou « Horaire SnapVault ».

Étendez la protection à l'aide de relations en cascade ou en éventail dans Active IQ Unified Manager

Vous pouvez étendre la protection 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. Vous pouvez le faire lorsque vous devez copier des données d'un site vers plusieurs sites ou fournir une protection supplémentaire en créant davantage de sauvegardes.

Vous pouvez étendre la protection aux volumes à l'aide d'un groupe de cohérence, qui est un conteneur regroupant plusieurs volumes afin que vous puissiez gérer tous les volumes comme une seule entité. Vous pouvez afficher le groupe de cohérence de synchronisation active SnapMirror et la relation de groupe de

cohérence synchrone dans la page Relations de Unified Manager.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Cliquez sur **Protection** > **Relations**. Vous pouvez également consulter les relations depuis la page de détails du volume.
2. Sur la page **Relations de volume**, sélectionnez la relation SnapMirror à partir de laquelle vous souhaitez étendre la protection.
3. Dans la barre d'actions, cliquez sur **Étendre la protection**.
4. Dans le menu, sélectionnez **Depuis la source** ou **Depuis la destination**, selon que vous créez une relation de diffusion à partir de la source ou une relation en cascade à partir de la destination.
5. Sélectionnez **Avec SnapMirror** ou **Avec SnapVault** selon le type de relation de protection que vous créez.

   La boîte de dialogue **Configurer la protection** s'affiche.

   Cela peut être effectué à partir de la page de détails Relation unifiée / Relation de volume et Volume / Santé.

6. Renseignez les informations comme indiqué dans la boîte de dialogue **Configure Protection**.

Modifiez les relations de protection à partir de la page Relations de volumes dans Active IQ Unified Manager

Vous pouvez modifier les relations de protection existantes pour changer le débit de transfert maximal, la stratégie de protection ou la planification de la protection. Vous pouvez par exemple modifier une relation pour réduire la bande passante utilisée pour les transferts ou augmenter la fréquence des transferts planifiés si les données évoluent fréquemment.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Les volumes sélectionnés doivent être des destinations de relations de protection. Vous ne pouvez pas modifier les relations lorsque des volumes sources, des volumes de partage de charge ou des volumes qui ne sont pas la destination d'une relation SnapMirror ou SnapVault sont sélectionnés.

Étapes

1. Sur la page **Relations entre volumes**, sélectionnez dans la liste des volumes un ou plusieurs volumes du même SVM pour lesquels vous souhaitez modifier les paramètres de relation, puis sélectionnez **Modifier** dans la barre d'outils.

   La boîte de dialogue Modifier la relation s'affiche.

2. Dans la boîte de dialogue **Modifier la relation**, modifiez le taux de transfert maximal, la politique de protection ou le calendrier de protection, selon vos besoins.
3. Cliquez sur **Appliquer**.

Les modifications sont appliquées aux relations sélectionnées.

Modifiez les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager

Vous pouvez modifier les relations de protection existantes pour changer le débit de transfert maximal actuel, la politique de protection ou le calendrier de protection. Vous pouvez, par exemple, modifier une relation pour réduire la bande passante utilisée pour les transferts ou augmenter la fréquence des transferts planifiés si les données changent souvent.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir installé et configuré Workflow Automation.

Les volumes sélectionnés doivent être des destinations de relations de protection. Vous ne pouvez pas modifier les relations lorsque des volumes sources, des volumes de partage de charge ou des volumes qui ne sont pas la destination d'une relation SnapMirror ou SnapVault sont sélectionnés.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Health**, repérez dans la topologie la relation de protection que vous souhaitez modifier et cliquez dessus avec le bouton droit.
2. Sélectionnez **Modifier** dans le menu.

   Vous pouvez également, à partir du menu **Actions**, sélectionner **Relationship** > **Edit** pour modifier la relation dont vous consultez actuellement les détails.

   La boîte de dialogue **Modifier la relation** s'affiche.
3. Dans la boîte de dialogue Modifier la relation, modifiez le taux de transfert maximal, la politique de protection ou la planification de protection, selon vos besoins.
4. Cliquez sur **Appliquer**.

   Les modifications sont appliquées aux relations sélectionnées.

Créez une politique SnapMirror pour optimiser l'efficacité des transferts dans Active IQ Unified Manager

Vous pouvez créer une stratégie SnapMirror pour spécifier la priorité de transfert SnapMirror pour les relations de protection. Les stratégies SnapMirror vous permettent d'optimiser l'efficacité des transferts de la source vers la destination en attribuant des priorités, de sorte que les transferts de priorité inférieure soient planifiés après les transferts de priorité normale.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- Cette tâche suppose que vous avez déjà rempli la section « Informations sur la destination » de la boîte de dialogue « Configurer la protection ».

Étapes

1. À partir de l'onglet **SnapMirror** de la boîte de dialogue **Configurer la protection**, cliquez sur le lien **Créer une stratégie** dans la zone **Paramètres de relation**.

   La boîte de dialogue Créer une stratégie SnapMirror s'affiche.

2. Dans le champ **Nom de la stratégie**, saisissez le nom que vous souhaitez donner 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**, saisissez un commentaire facultatif concernant la politique.
5. Cliquez sur **Créer**.

   La nouvelle stratégie s'affiche dans la liste déroulante de stratégie SnapMirror.

Créez une politique SnapVault pour optimiser l'efficacité des transferts dans Active IQ Unified Manager

Vous pouvez créer une nouvelle stratégie SnapVault pour définir la priorité d'un transfert SnapVault. Vous utilisez des stratégies pour optimiser l'efficacité des transferts du système principal vers le système secondaire dans le cadre d'une relation de protection.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- Vous devez avoir déjà rempli la section « Informations sur la destination » de 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 la relation**.

   L'onglet SnapVault s'affiche.

2. Dans le champ **Nom de la politique**, saisissez le nom que vous souhaitez donner à la politique.
3. Dans le champ **Priorité de transfert**, sélectionnez la priorité de transfert que vous souhaitez attribuer à la stratégie.
4. **Facultatif:** Dans le champ **Comment**, saisissez un commentaire pour la politique.
5. Dans la zone **Étiquette de réplication**, ajoutez ou modifiez une étiquette de réplication, si nécessaire.
6. Cliquez sur **Créer**.

   La nouvelle politique est affichée dans la liste déroulante Créer une politique.

Annuler un transfert depuis la page Relations de volumes dans Active IQ Unified Manager

Vous pouvez interrompre un 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 postérieurs au transfert de base.

Vous pouvez interrompre un transfert s'il entre en conflit avec une autre opération, comme un déplacement de volume.

Vous ne pouvez pas interrompre les relations de volume protégées par le groupe de cohérence.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

L'option d'annulation ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action: par exemple, si vous ne disposez que de privilèges d'opérateur
- Lorsque l'ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert

Vous ne pouvez pas effacer le point de contrôle de redémarrage pour un transfert de base.

Étapes

1. Pour annuler les transferts pour une ou plusieurs relations de protection, depuis la page **Volume Relationships**, sélectionnez un ou plusieurs volumes et, dans la barre d'outils, cliquez sur **Abort**.

   La boîte de dialogue « Annuler 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 Annuler le transfert se ferme et l'état de la tâche d'abandon s'affiche en haut de la page Relations de volume, ainsi qu'un lien vers les détails de la tâche.

4. **Facultatif :** Cliquez sur le lien **View details** pour accéder à la page de détails du **Job** afin d'obtenir des informations supplémentaires et de consulter la progression du job.

Annuler un transfert depuis la page Détails du volume/de l'état dans Active IQ Unified Manager

Vous pouvez interrompre un transfert de protection des données actif lorsque vous souhaitez arrêter une réplication SnapMirror en cours. Vous pouvez également effacer le point de contrôle de redémarrage d'un transfert s'il ne s'agit pas d'un transfert de base. Vous pouvez aussi interrompre un transfert s'il entre en conflit avec une autre opération, comme un déplacement de volume.

Vous ne pouvez pas interrompre les relations de volume protégées par le groupe de cohérence.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

L’option d’annulation ne s’affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action: par exemple, si vous ne disposez que de privilèges d’opérateur
- Lorsque l’ID du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n’a pas encore été découvert

Vous ne pouvez pas effacer le point de contrôle de redémarrage pour un transfert de base.

Étapes

1. Dans l’onglet **Protection** de la page de détails **Volume / Health**, cliquez avec le bouton droit sur la relation dans la vue topologique correspondant au transfert de données que vous souhaitez abandonner, puis sélectionnez **Abort**.

   La boîte de dialogue « Annuler 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 Annuler le transfert se ferme, et l’état de l’opération d’annulation s’affiche en haut de la page Détails du volume/de l’état, accompagné d’un lien vers les détails de la tâche.

4. **Facultatif :** Cliquez sur le lien **View details** pour accéder à la page de détails du **Job** afin d’obtenir des informations supplémentaires et de consulter la progression du job.
5. Cliquez sur chaque tâche pour en afficher les détails.
6. Cliquez sur la flèche Retour de votre navigateur pour revenir à la page de détails **Volume / Health**.

   L’opération d’annulation est terminée lorsque toutes les tâches du job sont accomplies avec succès.

Mettre en veille une relation de protection depuis la page Relations de volume dans Active IQ Unified Manager

Depuis la page Relations entre volumes, 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 contenant une base de données, et que vous voulez vous assurer que son contenu reste stable pendant l’opération de copie Snapshot.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

L’action de suspension ne s’affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas d’effectuer cette action; par exemple, si vous ne disposez que de privilèges d’opérateur
- Lorsque l’ID du volume est inconnu ; par exemple, lorsqu’il existe une relation intercluster et que le cluster de destination n’a pas encore été découvert
- Lorsque vous n’avez pas associé Workflow Automation et Unified Manager

Étapes

1. Pour suspendre les transferts pour une ou plusieurs relations de protection, depuis la page **Relations de volumes**, sélectionnez un ou plusieurs volumes et, dans la barre d'outils, cliquez sur **Suspendre**.

   La boîte de dialogue Quiesce s'affiche.

2. Cliquez sur **Continuer**.

   L'état de la tâche de mise au repos s'affiche en haut de la page des détails du volume/de l'état de santé, avec un lien vers les détails de la tâche.

3. Cliquez sur le lien **Voir les détails** pour accéder à la page de détails du **Job** afin d'obtenir des informations supplémentaires et de consulter la progression du job.
4. **Facultatif:** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

   Le travail de mise au repos est terminé lorsque toutes les tâches du travail ont été exécutées avec succès.

Mettre en veille une relation de protection depuis la page Détails du volume/de la santé dans Active IQ Unified Manager

Vous pouvez suspendre une relation de protection pour empêcher temporairement les transferts de données. Vous pouvez suspendre une relation lorsque vous souhaitez créer une copie Snapshot d'un volume de destination SnapMirror contenant une base de données et que vous voulez vous assurer que son contenu reste stable pendant la copie Snapshot.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

L'action de suspension ne s'affiche pas dans les cas suivants :

- Si les paramètres RBAC ne permettent pas cette action, par exemple si vous ne disposez que de privilèges d'opérateur
- Lorsque l'ID du volume est inconnu, par exemple lorsqu'il existe une relation intercluster et que le cluster de destination n'a pas encore été découvert
- Lorsque vous n'avez pas associé Workflow Automation et Unified Manager

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Health**, cliquez avec le bouton droit sur la relation dans la vue topologique de la relation de protection que vous souhaitez mettre au repos.
2. Sélectionnez **Quiesce** dans le menu.
3. Cliquez sur **Yes** pour continuer.

   L'état de la tâche de mise au repos s'affiche en haut de la page des détails du volume/de l'état de santé, avec un lien vers les détails de la tâche.

4. Cliquez sur le lien **Voir les détails** pour accéder à la page de détails du **Job** afin d'obtenir des informations supplémentaires et de consulter la progression du job.

5. **Facultatif:** Cliquez sur la flèche Précédent de votre navigateur pour revenir à la page de détails **Volume / Health**.

   Le travail de mise au repos est terminé lorsque toutes les tâches du travail ont été exécutées avec succès.

Rompre une relation SnapMirror depuis la page Relations de volumes d'Active IQ Unified Manager

Vous pouvez rompre une relation de protection pour interrompre les transferts de données entre un volume source et un volume de destination dans une relation SnapMirror. Vous pouvez rompre une relation lorsque vous souhaitez migrer des données, pour la reprise après sinistre ou pour les tests d'application. Le volume de destination est modifié en volume en lecture/écriture. Vous ne pouvez pas rompre une relation SnapVault.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Sur la page **Relations entre volumes**, sélectionnez un ou plusieurs volumes avec des relations de protection pour lesquels vous souhaitez arrêter les transferts de données et, dans la barre d'outils, cliquez sur **Interrompre**.

   La boîte de dialogue « Rompre la relation » s'affiche.

2. Cliquez sur **Continuer** pour rompre la relation.
3. Sur la page **Relations de volume**, vérifiez dans la colonne **État de la relation** que la relation est rompue.

   La colonne « État de la relation » est masquée par défaut, vous devrez donc peut-être la sélectionner dans la liste des colonnes à afficher/masquer .

Supprimez une relation de protection depuis la page Volume Relationships dans Active IQ Unified Manager

Depuis la page Relations de volumes, vous pouvez supprimer une relation de protection afin de supprimer définitivement une relation existante entre la source et la destination sélectionnées : par exemple, lorsque vous souhaitez créer une relation avec une destination différente. Cette opération supprime toutes les métadonnées et ne peut pas être annulée.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Sur la page **Relations entre volumes**, sélectionnez un ou plusieurs volumes avec des relations de protection que vous souhaitez supprimer, puis, dans la barre d'outils, cliquez sur **Supprimer**.

La boîte de dialogue Supprimer la relation s'affiche.

2. Cliquez sur **Continuer** pour supprimer la relation.

   La relation est supprimée de la page Relations de volume.

Reprenez les transferts planifiés sur une relation mise en veille depuis la page Relations de volume dans Active IQ Unified Manager

Après avoir mis en pause une relation pour interrompre les transferts planifiés, vous pouvez utiliser **Reprendre** pour les réactiver et ainsi protéger les données du volume source ou principal. Les transferts reprennent à partir d'un point de contrôle s'il en existe un, lors du prochain intervalle de transfert planifié.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Vous ne pouvez sélectionner au maximum que 10 relations mises en pause pour lesquelles reprendre les transferts.

Étapes

1. Dans la page **Relations de volumes**, sélectionnez un ou plusieurs volumes dont les relations sont en pause, puis, dans la barre d'outils, cliquez sur **Reprendre**.
2. Dans la boîte de dialogue **Reprendre**, cliquez sur **Continuer**.

   Vous revenez à la page Relations de volume.

3. Pour consulter les tâches associées et suivre leur progression, cliquez sur le lien de la tâche affiché en haut de la page **Relations de volume**.
4. Effectuez l'une des opérations suivantes :
   - Si un seul job s'affiche, sur la page Job details, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails des tâches associés au job de configuration de la protection et pour déterminer quand le job est terminé.
   - Si plusieurs tâches sont affichées,
     i. Sur la page Jobs, cliquez sur le job dont vous souhaitez afficher les détails.
     ii. Sur la page Détails du travail, cliquez sur **Actualiser** pour mettre à jour la liste des tâches et les détails des tâches associés au travail de configuration de la protection, et pour déterminer quand le travail est terminé. Une fois les travaux terminés, les transferts de données reprennent à l'intervalle de transfert planifié suivant.

Reprenez les transferts sur une relation mise en veille depuis la page Détails du volume/de la santé dans Active IQ Unified Manager

Après avoir mis en pause une relation pour empêcher les transferts planifiés de se produire, vous pouvez utiliser **Resume** sur la page Volume / Health details pour réactiver les transferts planifiés afin que les données du volume source ou principal soient protégées. Les transferts reprennent à partir d'un point de contrôle, s'il en existe un, lors

du prochain intervalle de transfert planifié.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, cliquez avec le bouton droit dans la vue topologique sur une relation mise en veille 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 revenez à la page Détails du volume / de l'état de santé.

3. Pour consulter les tâches associées et suivre leur progression, cliquez sur le lien de la tâche affiché en haut de la page de détails **Volume / Santé**.
4. Dans la page de détails du **Job**, cliquez sur **Refresh** pour mettre à jour la liste des tâches et les détails des tâches associés au job de configuration de la protection et pour déterminer quand le job est terminé.

   Une fois les tâches terminées, les transferts de données reprennent au prochain intervalle de transfert programmé.

Initialisez ou mettez à jour les relations de protection à partir de la page Relations de volumes dans Active IQ Unified Manager

À partir de la page Relations de volumes, vous pouvez effectuer un premier transfert de base sur une nouvelle relation de protection, ou mettre à jour une relation si elle est déjà initialisée et que vous souhaitez effectuer immédiatement une mise à jour incrémentielle manuelle non planifiée.

Vous ne pouvez pas initialiser ni mettre à jour les volumes protégés par des groupes de cohérence.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Depuis la page **Relations entre volumes**, cliquez avec le bouton droit 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 **Initialiser/Mettre à jour**.

   La boîte de dialogue **Initialiser/Mettre à jour** s'affiche.

2. Dans l'onglet **Options de transfert**, sélectionnez une priorité de transfert et le débit de transfert maximal.
3. Cliquez sur **Copies d'instantané source**; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

La boîte de dialogue « Sélectionner la copie d'instantané source » s'affiche.

4. Si vous souhaitez spécifier une copie 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 **Submit**.

   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 démarrer la tâche d'initialisation ou de mise à jour.

   La tâche d'initialisation ou de mise à jour démarre, vous revenez à la page Relations de volumes, et un lien vers les tâches s'affiche en haut de la page.

8. **Facultatif:** Cliquez sur **Afficher les tâches** dans la vue **Santé: Tous les volumes** pour suivre l'état de chaque tâche d'initialisation ou de mise à jour.

   Une liste filtrée des tâches s'affiche.

9. **Facultatif :** Cliquez sur chaque tâche pour en voir les détails.
10. **Facultatif:** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

    L'opération d'initialisation ou de mise à jour est terminée lorsque toutes les tâches se sont achevées avec succès.

Initialisez ou mettez à jour les relations de protection à partir de la page Détails du volume/de l'état dans Active IQ Unified Manager

Vous pouvez effectuer un premier transfert de base 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 incrémentale manuelle et non planifiée pour transférer les données immédiatement.

REMARQUE : Vous ne pouvez pas initialiser ou mettre à jour les volumes protégés par Consistency Groups.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré OnCommand Workflow Automation.

Étapes

1. Dans l'onglet **Protection** de la page de détails **Volume / Santé**, repérez dans la topologie la relation de protection que vous souhaitez initialiser ou mettre à jour, puis cliquez dessus avec le bouton droit.
2. Sélectionnez **Initialiser/Mettre à jour** dans le menu.

   Vous pouvez également, dans le menu **Actions**, sélectionner **Relation** > **Initialiser/Mettre à jour** pour initialiser ou mettre à jour la relation dont vous consultez actuellement les détails.

   La boîte de dialogue Initialiser/Mettre à jour s'affiche.

3. Dans l'onglet **Options de transfert**, sélectionnez une priorité de transfert et le débit de transfert maximal.

4. Cliquez sur **Copies d'instantané source**; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

   La boîte de dialogue « Sélectionner la copie d'instantané source » s'affiche.

5. Si vous souhaitez spécifier une copie 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 **Submit**.

   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 démarrer la tâche d'initialisation ou de mise à jour.

   La tâche d'initialisation ou de mise à jour démarre, vous revenez à la page des détails Volume / Health, et un lien vers les tâches s'affiche en haut de la page.

9. **Facultatif:** Cliquez sur **View Jobs** sur la page de détails **Volume / Health** pour suivre l'état de chaque tâche d'initialisation ou de mise à jour.

   Une liste filtrée des tâches s'affiche.

10. **Facultatif :** Cliquez sur chaque tâche pour en voir les détails.
11. **Facultatif:** Cliquez sur la flèche Précédent de votre navigateur pour revenir à la page de détails **Volume / Health**.

    L'opération d'initialisation ou de mise à jour est terminée lorsque toutes les tâches du job se terminent avec succès.

Resynchronisez les relations de protection à partir de la page Relations de volumes dans Active IQ Unified Manager

Depuis la page Relations de volume, vous pouvez resynchroniser une relation soit pour récupérer après un événement ayant désactivé votre volume source, soit lorsque vous souhaitez remplacer le volume source actuel par un autre volume.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.

Étapes

1. Dans la page **Relations entre volumes**, sélectionnez un ou plusieurs volumes dont les relations sont en pause, puis, dans la barre d'outils, cliquez sur **Resynchroniser**.

   La boîte de dialogue Resynchroniser s'affiche.

2. Dans l'onglet **Options de resynchronisation**, sélectionnez une priorité de transfert et le débit de transfert maximal.

3. Cliquez sur **Copies d'instantané source**; puis, dans la colonne **Copie d'instantané**, cliquez sur **Par défaut**.

   La boîte de dialogue « Sélectionner la copie d'instantané source » s'affiche.

4. Si vous souhaitez spécifier une copie 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 **Submit**.

   Vous revenez à la boîte de dialogue Resynchronize.

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 la tâche de resynchronisation.

   La tâche de resynchronisation démarre, vous revenez à la page Relations de volumes et un lien vers les tâches s'affiche en haut de la page.

8. **Facultatif:** Cliquez sur **Afficher les tâches** sur la page **Relations de volume** pour suivre l'état de chaque tâche de resynchronisation.

   Une liste filtrée des tâches s'affiche.

9. **Facultatif:** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

   L'opération de resynchronisation est terminée lorsque toutes les tâches du travail se terminent avec succès.

Inverser les relations de protection à partir de la page Relations de volume dans Active IQ Unified Manager

Lorsqu'un sinistre rend inutilisable le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour fournir les données en le convertissant en volume accessible 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 du volume de destination accessible en lecture/écriture.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré Workflow Automation.
- La relation ne doit pas être une relation SnapVault.
- Une relation de protection doit déjà exister.
- Il faut rompre la relation de protection.
- La source et la destination doivent toutes deux 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 plus récentes que celles de la copie Snapshot commune sont supprimées.

- Les politiques et les calendriers créés sur les relations de resynchronisation inverse sont identiques à ceux de la relation de protection d'origine.

  Si les politiques et les planifications n'existent pas, elles sont créées.

Étapes

1. Sur la page **Relations entre volumes**, sélectionnez un ou plusieurs volumes avec des relations que vous souhaitez inverser et, dans la barre d'outils, cliquez sur **Inverser la resynchronisation**.

   La boîte de dialogue de resynchronisation inverse s'affiche.

2. Vérifiez que les relations affichées dans la boîte de dialogue **Resynchronisation inverse** sont bien celles pour lesquelles vous souhaitez effectuer l'opération de resynchronisation inverse, puis cliquez sur **Soumettre**.

   L'opération de resynchronisation inverse démarre, vous revenez à la page Relations de volumes et un lien vers les tâches s'affiche en haut de la page.

3. **Facultatif:** Cliquez sur **Afficher les tâches** dans la page **Relations de volume** pour suivre l'état de chaque tâche de resynchronisation inverse.

   Une liste filtrée des tâches liées à cette opération s'affiche.

4. **Facultatif:** Cliquez sur la flèche **Retour** de votre navigateur pour revenir à la page **Relations de volume**.

   L'opération de resynchronisation inverse est terminée lorsque toutes les tâches du travail sont terminées avec succès.

Restaurez les données à l'aide des pages de détails Volume et Volume/Santé dans Active IQ Unified Manager

Vous pouvez restaurer des fichiers, des répertoires ou un volume entier écrasés ou supprimés à partir d'une copie Snapshot en utilisant la fonction de restauration sur les pages de détails Volume et Volume / Health.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Veuillez noter les points suivants :

- Vous ne pouvez pas restaurer un répertoire ou un volume à partir d'un instantané dans l'un des scénarios suivants :
  - L'option **Oui, conserver toutes les copies d'instantané** est sélectionnée.
  - Vous utilisez un compte LDAP pour surveiller le cluster.
  - Vous êtes connecté en tant qu'utilisateur du domaine.
  - Votre compte est configuré pour l'authentification SAML.
  - Vous utilisez le protocole NDMP.

    Pour plus de détails, consultez l'article de la base de connaissances "Comment configurer l'authentification NDMP en mode 'SVM-scope'".

- Il est impossible de restaurer les flux de fichiers NTFS.
- L'option de restauration n'est pas disponible lorsque :
  - L'identifiant du volume est inconnu : par exemple, lorsque vous avez une relation intercluster et que le cluster de destination n'a pas encore été découvert.
  - Le volume est configuré pour la réplication synchrone SnapMirror.

Étapes

1. Dans le volet de navigation de gauche, accédez à **Stockage > Volumes**.
2. Sélectionnez le volume et cliquez sur le bouton **Restaurer**. Vous pouvez également cliquer sur le volume pour accéder à **Détails du volume/de l'état > Actions > Restaurer**. La boîte de dialogue Restaurer s'affiche. Pour plus d'informations sur cette page, consultez "Boîte de dialogue Restore".
3. Sélectionnez le volume et la copie Snapshot à partir desquels vous souhaitez restaurer les données, s'ils sont différents de ceux par défaut.
4. Sélectionnez les éléments que vous souhaitez restaurer, par exemple, le LUN source.

   Vous pouvez restaurer l'intégralité du volume, ou spécifier les dossiers et fichiers que vous souhaitez restaurer.

5. Sélectionnez l'emplacement où vous souhaitez restaurer les éléments sélectionnés : soit **Emplacement d'origine**, soit **Autre emplacement existant**.
6. Si vous sélectionnez un autre emplacement existant, effectuez l'une des opérations suivantes :
   - Dans le champ de texte Chemin de restauration, saisissez le chemin d'accès à l'emplacement où vous souhaitez restaurer les données, puis cliquez sur **Sélectionner un répertoire**.
   - Cliquez sur **Parcourir** pour ouvrir la boîte de dialogue Parcourir les répertoires et suivez les étapes suivantes :
     i. Sélectionnez le cluster de destination, la machine virtuelle de stockage (SVM) et le volume sur lesquels vous souhaitez effectuer la restauration.
     ii. Dans le tableau Nom, sélectionnez un nom de répertoire à restaurer.
     iii. Cliquez sur **Sélectionner un répertoire**.
7. Cliquez sur **Restaurer**.

   Le processus de restauration commence. Une tâche est créée sur le back-end pour mener à bien le processus de restauration.

8. Si vous voulez voir la progression du job, dans le volet de navigation de gauche, accédez à **Protection > Jobs** pour afficher l'état du job de restauration dans la liste des jobs.

> Si une opération de restauration échoue entre des clusters HA Cloud Volumes ONTAP avec une erreur NDMP, vous devrez peut-être ajouter une route AWS explicite dans le cluster de destination afin que celui-ci puisse communiquer avec la LIF de gestion du cluster du système source. Vous effectuez cette étape de configuration à l'aide de la NetApp Console.

Découvrez les pools de ressources dans Active IQ Unified Manager

Les pools de ressources sont des groupes d'agrégats créés par un administrateur de stockage à l'aide d'Unified Manager pour fournir le provisionnement aux applications partenaires pour la gestion des sauvegardes.

Vous pouvez regrouper vos ressources en fonction d'attributs tels que les performances, le coût, l'emplacement physique ou la disponibilité. En regroupant des ressources connexes dans un pool, vous pouvez traiter ce pool comme une seule entité pour la surveillance et le provisionnement. Cela simplifie la gestion de ces ressources et permet une utilisation plus flexible et efficace du stockage.

Lors du provisionnement du stockage secondaire, Unified Manager détermine l'agrégat le plus approprié dans le pool de ressources pour la protection à l'aide des critères suivants :

- L'agrégat est un agrégat de données (et non un agrégat racine) et il est en ligne.
- L'agrégat se trouve sur un nœud du cluster de destination dont la version ONTAP est identique ou supérieure à la version majeure du cluster source.
- Cet agrégat possède le 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 situe dans le seuil de quasi-plein et de quasi-surengagement défini pour l'agrégat (seuil global ou local, selon le cas).
- Le nombre de volumes FlexVol® sur le nœud de destination ne doit pas dépasser la limite de la plateforme.

Créez des pools de ressources dans Active IQ Unified Manager

Vous pouvez utiliser la boîte de dialogue Créer un pool de ressources pour regrouper les agrégats à des fins de provisionnement.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

Les pools de ressources peuvent contenir des agrégats provenant de différents clusters, mais un même agrégat ne peut pas appartenir à différents pools de ressources.

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Resource Pools**.
2. Dans la page **Resource Pools**, cliquez sur **Create**.
3. Suivez les instructions de la boîte de dialogue **Créer un pool de ressources** pour indiquer un nom et une description et pour ajouter des agrégats en tant que membres du pool de ressources que vous souhaitez créer.

Modifier les pools de ressources dans Active IQ Unified Manager

Vous pouvez modifier un pool de ressources existant lorsque vous souhaitez en changer le nom et la description.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Le bouton **Modifier** est activé uniquement lorsqu'un seul pool de ressources est sélectionné. Si plusieurs pools de ressources sont sélectionnés, le bouton **Modifier** est désactivé.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Resource Pools**.
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 description sont affichés dans la liste des pools de ressources.

Afficher l'inventaire du pool de ressources dans Active IQ Unified Manager

Vous pouvez utiliser la page Resource Pools pour consulter l'inventaire des pools de ressources et surveiller la capacité restante pour chaque pool de ressources.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Resource Pools**.

   L'inventaire du pool de ressources est affiché.

Ajouter des membres au pool de ressources dans Active IQ Unified Manager

Un pool de ressources est composé de plusieurs agrégats membres. Vous pouvez ajouter des agrégats aux pools de ressources existants afin d'augmenter l'espace disponible pour le provisionnement des volumes secondaires.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

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** > **Resource Pools**.
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 des pools de ressources.

3. Dans la zone des membres du pool de ressources, cliquez sur **Ajouter**.

   La boîte de dialogue Aggregates s'affiche.

4. Sélectionnez un ou plusieurs agrégats.
5. Cliquez sur **Add**.

   La boîte de dialogue se ferme et les agrégats s'affichent dans la liste des membres du pool de ressources sélectionné.

Supprimez les agrégats des pools de ressources dans Active IQ Unified Manager

Vous pouvez supprimer des agrégats d'un pool de ressources existant : par exemple, lorsque vous souhaitez utiliser un agrégat à d'autres fins.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

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** > **Resource Pools**.
2. Sélectionnez le pool de ressources à partir duquel vous souhaitez supprimer les 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 **Yes** pour continuer.

   Les agrégats sélectionnés sont supprimés du volet Membres.

Supprimer les pools de ressources dans Active IQ Unified Manager

Vous pouvez supprimer les pools de ressources lorsqu'ils ne sont plus nécessaires. Par exemple, vous pouvez redistribuer les agrégats membres d'un pool de ressources vers plusieurs autres pools de ressources, rendant ainsi le pool de ressources d'origine obsolète.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Le bouton **Supprimer** est activé uniquement lorsqu'au moins un pool de ressources est sélectionné.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Resource Pools**.
2. Sélectionnez le pool de ressources que vous souhaitez supprimer.
3. Cliquez sur **Delete**.

   Le pool de ressources est supprimé de la liste des pools de ressources et ses agrégats sont supprimés de la liste des membres.

Surveillez les relations de protection de reprise après sinistre des machines virtuelles de stockage

Découvrez les relations de reprise après sinistre des machines virtuelles de stockage dans Active IQ Unified Manager

Active IQ Unified Manager prend en charge la surveillance des relations de reprise après sinistre des machines virtuelles de stockage, ce qui permet une reprise après sinistre à la granularité d'une machine virtuelle de stockage. La reprise après sinistre des machines virtuelles de stockage permet de récupérer les données présentes dans les volumes constitutifs de la machine virtuelle de stockage ainsi que de restaurer la configuration de la machine virtuelle de stockage.

Une relation DR de machine virtuelle de stockage est créée entre la machine virtuelle de stockage source et la machine virtuelle de stockage de destination afin d'assurer une reprise après sinistre asynchrone. Vous pouvez choisir de répliquer la totalité ou une partie de la configuration de la machine virtuelle de stockage (à l'exclusion de la configuration réseau et de protocole), ainsi que les volumes de données, en fonction de la configuration du cluster.

Une fois la relation de reprise après sinistre de la machine virtuelle de stockage configurée, lorsque la machine virtuelle de stockage source devient indisponible en raison d'une défaillance matérielle ou d'un sinistre environnemental, la machine virtuelle de stockage de destination démarre et fournit l'accès aux données avec une perturbation minimale. De même, lorsque la machine virtuelle de stockage source redevient disponible, elle est resynchronisée avec la machine virtuelle de stockage de destination, puis la source redémarre pour fournir l'accès aux données. Vous pouvez utiliser les commandes SnapMirror pour configurer et gérer la relation de reprise après sinistre de la machine virtuelle de stockage.

Surveillez les machines virtuelles de stockage à l'aide de la page Relationships dans Active IQ Unified Manager

Vous pouvez surveiller les relations de reprise après sinistre de vos VM de stockage depuis la page Relationships de la section PROTECTION de l'INVENTORY. Par défaut, la page Relationships répertorie uniquement les relations de niveau supérieur, car le filtre des relations constituantes est appliqué.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous utilisez des filtres pour visualiser les relations de reprise après sinistre des machines virtuelles de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **PROTECTION** > **Relations**.

   Cette page affiche tous les types de relations : les relations de volume, de groupe de cohérence et de VM de stockage.

2. Cliquez sur **Filtrer**, puis sélectionnez **Type d'objet de relation** et **VM de stockage** 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 entre les constituants pour afficher toutes les relations de protection.

Cette page affiche uniquement les relations de reprise après sinistre des machines virtuelles de stockage.

Afficher les relations de protection à partir de la page des machines virtuelles de stockage dans Active IQ Unified Manager

La page Machines virtuelles de stockage vous permet de consulter l'état des relations de reprise après sinistre des machines virtuelles de stockage existantes.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez également examiner les détails des relations de protection, y compris l'état du transfert et du retard, ainsi que les détails de la source et de la destination. Vous pouvez programmer des rapports ou télécharger les rapports existants au format dont vous avez besoin. Le bouton **Afficher/Masquer** vous permet d'ajouter les colonnes requises aux rapports, car elles ne sont pas affichées par défaut.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **STOCKAGE** > **VM de stockage**.
2. Dans le menu **AFFICHAGE**, sélectionnez **Relation** > **Toutes les relations**.

   La vue « Relations : Toutes les relations » affiche toutes les machines virtuelles de stockage configurées.

Affichez les machines virtuelles de stockage en fonction de leur état de protection dans Active IQ Unified Manager

Vous pouvez utiliser la page Machines virtuelles de stockage de l'inventaire pour afficher toutes les machines virtuelles de stockage dans Active IQ Unified Manager et filtrer les machines virtuelles de stockage en fonction de leur état de protection.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Une nouvelle colonne Protection Role est ajoutée à la vue des VM de stockage, qui indique si la VM de stockage est protégée ou non protégée.

Si un cluster source n'est pas ajouté à Active IQ Unified Manager, toutes les informations relatives à ce cluster ne sont pas disponibles dans les grilles.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **STOCKAGE** > **VM de stockage**.
2. Dans le menu **AFFICHAGE**, sélectionnez **Santé** > **Toutes les machines virtuelles de stockage**.

   L'état de santé de toutes les machines virtuelles de stockage est affiché.

3. Cliquez sur **Filtrer** 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	**Rôle de protection** est **Non protégé**

Vous ne pouvez pas afficher simultanément les machines virtuelles de stockage protégées et non protégées. Vous devrez supprimer le filtre actuel pour appliquer une nouvelle option de filtrage.

4. Cliquez sur **Appliquer le filtre**.

   La vue « Non enregistrées » affiche toutes les machines virtuelles de stockage qui sont protégées ou non par la reprise après sinistre des machines virtuelles de stockage, en fonction des filtres que vous avez sélectionnés.

Gérer les associations de machines virtuelles de stockage dans Active IQ Unified Manager

Les associations de machines virtuelles de stockage (VM de stockage) sont des mappages d'une VM de stockage source vers une VM de stockage de destination qui sont utilisés 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 cette dernière soit une destination secondaire ou tertiaire. Il est impossible d'utiliser une machine virtuelle de stockage de destination secondaire comme source pour créer une association avec une machine virtuelle de stockage de destination tertiaire.

En tant qu'administrateur d'applications ou administrateur de stockage, vous pouvez consulter les associations de machines virtuelles de stockage dans votre environnement sur la page **Protection** > **Associations de machines virtuelles de stockage**.

Vous pouvez associer les SVMs de trois manières :

- **Associer n'importe quelle VM de stockage** : Vous pouvez créer une association entre n'importe quelle VM de stockage source principale et une ou plusieurs SVM de destination. Cela signifie que toutes les SVM existantes qui nécessitent actuellement une protection, ainsi que toutes les SVM qui seront créées à l'avenir, sont associées aux SVM de destination spécifiées. Par exemple, vous pouvez vouloir sauvegarder des applications de plusieurs sources différentes situées à différents emplacements vers une ou plusieurs SVM de destination dans un seul emplacement.
- **Associer une VM de stockage spécifique** : Vous pouvez créer une association entre une VM de stockage source spécifique et une ou plusieurs VM de stockage de destination spécifiques. Par exemple, si vous fournissez des services de stockage à de nombreux clients dont les données doivent être séparées, vous pouvez utiliser cette option pour associer une VM de stockage source spécifique à une VM de stockage de destination spécifique attribuée uniquement à ce client.
- **Associer à une VM de stockage externe** : Vous pouvez créer une association entre une VM de stockage source et un volume flexible externe d'une VM de stockage de destination.

Créer des associations de machines virtuelles de stockage

L'assistant Créer des associations de machines virtuelles de stockage permet aux applications de protection

partenaires d’associer une machine virtuelle de stockage source à une machine virtuelle de stockage de destination à utiliser avec les relations SnapMirror et SnapVault. Les applications partenaires utilisent ces associations lors du provisionnement initial des volumes de destination afin de déterminer les ressources à sélectionner.dd

Avant de commencer

- La machine virtuelle de stockage que vous associez doit déjà exister.
- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Pour chaque machine virtuelle de stockage source et chaque type de relation, vous ne pouvez choisir qu’une seule machine virtuelle de stockage de destination sur chaque cluster de destination.

La modification des associations à l’aide des fonctions de suppression et de création n’affecte que les opérations de provisionnement futures. Cela ne déplace pas les volumes de destination existants.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Associations de machines virtuelles de stockage**.
2. Sur la page **Associations de machines virtuelles de stockage**, cliquez sur **Créer**.

   L’assistant **Créer des associations de machines virtuelles de stockage** est lancé.

3. Sélectionnez l’une des sources suivantes :
   - **N’importe lequel**

     Choisissez cette option lorsque vous souhaitez créer une association entre toute source de machine virtuelle de stockage principale et une ou plusieurs machines virtuelles de stockage de destination. Cela signifie que toutes les machines virtuelles de stockage existantes qui nécessitent actuellement une protection, ainsi que toutes les machines virtuelles de stockage qui seront créées à l’avenir, sont associées à la machine virtuelle de stockage de destination spécifiée. Par exemple, vous pouvez souhaiter que des applications provenant de plusieurs sources différentes, situées à différents emplacements, soient sauvegardées vers une ou plusieurs machines virtuelles de stockage de destination dans un même emplacement.

   - **Unique**

     Choisissez cette option lorsque vous souhaitez sélectionner une machine virtuelle de stockage source spécifique associée à une ou plusieurs machines virtuelles de stockage de destination. Par exemple, si vous fournissez des services de stockage à de nombreux clients dont les données doivent être séparées les unes des autres, choisissez cette option pour associer une machine virtuelle de stockage source spécifique à une machine virtuelle de stockage de destination spécifique, attribuée uniquement à ce client.

   - **Aucun (Externe)**

     Choisissez cette option lorsque vous souhaitez créer une association entre une machine virtuelle de stockage source et un volume flexible externe d’une machine virtuelle de stockage de destination.

4. Sélectionnez un ou les deux types de relations de protection que vous souhaitez créer :
   - **SnapMirror**
   - **SnapVault**
5. Cliquez sur **Suivant**.

6. Sélectionnez une ou plusieurs destinations de protection de VM de stockage.
7. Cliquez sur **Terminer**.

Supprimer les associations de machines virtuelles de stockage

Vous pouvez supprimer les associations de machines virtuelles de stockage pour les applications partenaires afin de supprimer la relation de provisionnement secondaire entre la machine virtuelle de stockage source et la machine virtuelle de stockage de destination ; par exemple, vous pouvez le faire lorsque la machine virtuelle de stockage de destination est pleine et que vous souhaitez créer de nouvelles associations de protection de machines virtuelles de stockage.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Le bouton **Supprimer** est désactivé tant qu'au moins une association de machine virtuelle de stockage n'est pas sélectionnée. La modification des associations à l'aide des fonctions de suppression et de création n'affecte que les opérations de provisionnement ultérieures ; elle ne déplace pas les volumes de destination existants.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Associations de machines virtuelles de stockage**.
2. Sélectionnez au moins une association de machine virtuelle de stockage.

   Le bouton **Supprimer** est activé.

3. Cliquez sur **Supprimer.**

   Une boîte de dialogue d'avertissement s'affiche.

4. Cliquez sur **Yes** pour continuer.

   La liste ne contient plus l'association de machine virtuelle de stockage sélectionnée.

Exigences relatives aux SVM et aux pools de ressources pour la prise en charge des services de stockage dans Active IQ Unified Manager

Vous pouvez mieux garantir la conformité des applications partenaires si vous respectez certaines exigences d'association SVM et de pool de ressources spécifiques aux services de stockage : par exemple, lorsque vous associez une SVM et créez des pools de ressources dans Unified Manager pour prendre en charge une topologie de protection dans un service de stockage fourni par une application partenaire.

Certaines applications s'associent au serveur Unified Manager pour fournir des services qui configurent et exécutent automatiquement la protection de sauvegarde SnapMirror ou SnapVault entre les volumes sources et les volumes de protection situés dans des emplacements secondaires ou tertiaires. Pour prendre en charge ces services de stockage de protection, vous devez utiliser Unified Manager afin de configurer les associations SVM et les pools de ressources nécessaires.

Pour prendre en charge la protection à saut unique ou en cascade des services de stockage, y compris la réplication à partir d'un volume source SnapMirror ou d'un volume principal SnapVault vers une destination SnapMirror ou vers des volumes de sauvegarde SnapVault situés dans des emplacements secondaires ou

tertiaires, respectez les exigences suivantes :

- Les associations SVM doivent être configurées entre la SVM contenant le volume source SnapMirror ou le volume principal SnapVault et toute SVM sur laquelle réside un volume secondaire ou un volume tertiaire.
  - Par exemple, pour prendre en charge une topologie de protection dans laquelle le volume source Vol_A réside sur SVM_1, 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 de 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, aucune association SnapMirror ou association de sauvegarde SnapVault entre SVM_2 et SVM_3 n'est 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 Vol_B SnapMirror résident tous deux sur SVM_1, vous devez configurer une association SnapMirror entre SVM_1 et SVM_1.
- Les pools de ressources doivent inclure les ressources d'agrégat du cluster disponibles pour les SVM associées.

  Vous configurez les pools de ressources via l'interface utilisateur web de Unified Manager, puis vous affectez via l'application partenaire les nœuds cibles secondaires et tertiaires du service de stockage.

Découvrez les tâches dans Active IQ Unified Manager

Un travail est une série de tâches que vous pouvez surveiller à l'aide d'Unified Manager. L'affichage des travaux et de leurs tâches associées vous permet de déterminer s'ils se sont terminés correctement.

Les tâches sont lancées lorsque vous créez des relations SnapMirror et SnapVault, lorsque vous effectuez une opération sur une relation (rupture, modification, mise en veille, suppression, reprise, resynchronisation et resynchronisation inverse), lorsque vous effectuez des tâches de restauration de données, lorsque vous vous connectez à un cluster, etc.

Lorsque vous lancez une tâche, vous pouvez utiliser la page Tâches et la page Détails de la tâche pour suivre la tâche et l'avancement des opérations associées.

Surveillez les tâches dans Active IQ Unified Manager

Vous pouvez utiliser la page Tâches pour suivre l'état des tâches et consulter leurs propriétés, telles que le type de service de stockage, l'état, l'heure de soumission et l'heure d'achèvement, afin de déterminer si une tâche s'est terminée avec succès.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Tâches**.

   La page Jobs s'affiche.

2. Consultez la colonne **État** pour déterminer l'état des tâches en cours d'exécution.

3. Cliquez sur le nom d'une tâche pour afficher les détails de cette tâche.

   La page Détails de la tâche s'affiche.

Affichez les détails du travail dans Active IQ Unified Manager

Après avoir démarré un job, vous pouvez suivre sa progression depuis la page Détails du job et surveiller les tâches associées afin de détecter d'éventuelles erreurs.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Tâches**.
2. Dans la page Jobs, cliquez sur le nom d'un job dans la colonne **Name** pour afficher la liste des tâches associées à ce job.
3. Cliquez sur une tâche pour afficher des informations supplémentaires dans le volet **Détails de la tâche** et le volet **Messages de la tâche** à droite de la liste des tâches.

Annuler les tâches dans Active IQ Unified Manager

Vous pouvez utiliser la page Tâches pour interrompre une tâche si elle prend trop de temps, rencontre trop d'erreurs ou n'est plus nécessaire. L'interruption est possible uniquement si l'état et le type de la tâche le permettent. Vous pouvez interrompre toute tâche en cours.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Tâches**.
2. Dans la liste des travaux, sélectionnez-en un, puis cliquez sur **Abort**.
3. Lorsque l'invite de confirmation s'affiche, cliquez sur **Oui** pour annuler la tâche sélectionnée.

Réessayez une tâche de protection ayant échoué dans Active IQ Unified Manager

Après avoir pris les mesures nécessaires pour corriger une tâche de protection ayant échoué, vous pouvez utiliser **Réessayer** pour relancer la tâche. La réexécution d'une tâche crée une nouvelle tâche à l'aide de l'ID de tâche d'origine.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous ne pouvez relancer qu'une seule tâche ayant échoué à la fois. La sélection de plusieurs tâches désactive le bouton **Retry**. Seules les tâches de type Protection Configuration et Protection Relationship Operation peuvent être relancées.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Protection** > **Tâches**.
2. Dans la liste des tâches, sélectionnez une seule tâche ayant échoué de type Configuration de protection ou Opération de relation de protection.

   Le bouton **Réessayer** est activé.

3. Cliquez sur **Réessayer**.

   La tâche est redémarrée.

Description des fenêtres et boîtes de dialogue relatives aux relations de protection

Découvrez la page relative aux pools de ressources dans Active IQ Unified Manager

La page Pools de ressources affiche les pools de ressources existants et leurs membres, et vous permet de créer, de surveiller et de gérer des pools de ressources à des fins de provisionnement.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Créer**

  Ouvre la boîte de dialogue Créer un pool de ressources, que vous pouvez utiliser pour créer des pools de ressources.

- **Modifier**

  Vous permet de modifier le nom et la description des pools de ressources que vous créez.

- **Supprimer**

  Permet de supprimer un ou plusieurs pools de ressources.

Liste des pools de ressources

La liste des pools de ressources affiche (sous forme de tableau) les propriétés des pools de ressources existants.

- **Pool de ressources**

  Affiche le nom du pool de ressources.

- **Description**

  Décrit le pool de ressources.

- **Type de SnapLock**

  Affiche le type SnapLock utilisé par les agrégats du pool de ressources. Les valeurs valides pour le type SnapLock sont Compliance, Enterprise et Non-SnapLock. Un pool de ressources ne peut contenir que des agrégats d'un seul type SnapLock.

- **Capacité totale**

  Affiche la capacité totale (en Mo, Go, etc.) du pool de ressources.

- **Capacité utilisée**

  Affiche la quantité d'espace (en Mo, Go, etc.) utilisée dans le pool de ressources.

- **Capacité disponible**

  Affiche la quantité d'espace (en Mo, Go, etc.) disponible dans le pool de ressources.

- **% utilisé**

  Affiche le pourcentage d'espace utilisé dans le pool de ressources.

Boutons de commande de la liste des membres

Les boutons de commande de la liste des membres vous permettent d'effectuer les tâches suivantes :

- **Ajouter**

  Vous permet d'ajouter des membres au pool de ressources.

- **Supprimer**

  Permet de supprimer un ou plusieurs membres du pool de ressources.

Liste des membres

La liste des membres affiche (sous forme de tableau) les membres du pool de ressources et leurs propriétés lorsqu'un pool de ressources est sélectionné.

- **Statut**

  Affiche l'état actuel de l'agrégat membre. L'état peut être Critique (), Erreur (), Avertissement () ou Normal ().

- **Nom de l'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.

  - Restreint

Les opérations limitées (telles que la reconstruction de la parité) sont autorisées, mais l'accès aux données n'est pas autorisé.

- Création

  L'agrégat est en cours de création.

- Destruction en cours

  L'agrégat est en cours de destruction.

- Échec

  L'agrégat ne peut pas être mis en ligne.

- Gelé

  L'agrégat ne traite pas (temporairement) les requêtes.

- Incohérent

  L'agrégat a été marqué comme corrompu; vous devriez contacter le support technique.

- Restriction du fer

  Les outils de diagnostic ne peuvent pas être exécutés sur l'agrégat.

- Montage

  L'agrégat est en cours de montage.

- Partiel

  Au moins un disque a été trouvé pour l'agrégat, mais deux disques ou plus sont manquants.

- Suspension

  L'agrégat est en cours de mise au repos.

- Suspendu

  L'agrégat est au repos.

- Rétabli

  Le retour à une version antérieure d'un agrégat est terminé.

- Non monté

  L'agrégat a été démonté.

- Démontage

  L'agrégat est en cours de mise hors ligne.

- Inconnu

L’agrégat est détecté, mais le serveur Unified Manager n’a pas encore récupéré les informations sur l’agrégat.

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 MB, GB, etc.) de l’agrégat.

- **Capacité utilisée**

  Affiche la quantité d’espace (en Mo, Go, etc.) utilisée dans l’agrégat.

- **Capacité disponible**

  Affiche la quantité d’espace (en Mo, Go, etc.) disponible 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 groupes RAID sont de type RAID-DP.
  - RAID-TEC: Tous les groupes RAID sont de type RAID-TEC.
  - RAID mixte : l’agrégat contient des groupes RAID de différents types de RAID (RAID0, RAID4, RAID-DP et RAID-TEC). Cette colonne est masquée par défaut.

Utilisez la boîte de dialogue Créer un pool de ressources dans Active IQ Unified Manager

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 et supprimer des agrégats de ce pool de ressources.

Nom du pool de ressources

Les zones de texte vous permettent d’ajouter les informations suivantes pour créer un pool de ressources :

Permet de spécifier un nom de pool de ressources.

Description

Permet de décrire un pool de ressources.

Membres

Affiche les membres du pool de ressources. Vous pouvez également ajouter et supprimer des membres.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Ajouter**

  Ouvre la boîte de dialogue Agrégats pour vous permettre d'ajouter des agrégats d'un cluster spécifique au pool de ressources. Vous pouvez ajouter des agrégats provenant de différents clusters, mais un même agrégat ne peut pas être ajouté à plusieurs pools de ressources.

- **Retirer**

  Permet de supprimer les agrégats sélectionnés du pool de ressources.

- **Créer**

  Crée le pool de ressources. Ce bouton n'est pas activé tant que des informations n'ont pas été saisies dans les champs Nom du pool de ressources ou Description.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue Créer un pool de ressources.

Utilisez la boîte de dialogue Modifier le pool de ressources dans Active IQ Unified Manager

Vous pouvez utiliser la boîte de dialogue Modifier le pool de ressources pour modifier le nom et la description d'un pool de ressources existant. Par exemple, si le nom et la description d'origine sont inexacts ou incorrects, vous pouvez les modifier pour plus de précision.

Zones de texte

Les zones de texte vous permettent de modifier les informations suivantes pour le pool de ressources sélectionné :

- **Nom du pool de ressources**

  Permet de saisir un nouveau nom.

- **Description**

  Permet de saisir une nouvelle description.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Sauvegarder**

  Enregistre les modifications apportées au nom et à la description du pool de ressources.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue Modifier le pool de ressources.

Utilisez la boîte de dialogue des agrégats dans Active IQ Unified Manager

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 vous permettent d'effectuer les tâches suivantes :

- **Ajouter**

  Ajoute les agrégats sélectionnés au pool de ressources. Le bouton Ajouter n'est activé que lorsqu'au moins un agrégat est sélectionné.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue Agrégats.

Liste des agrégats

La liste des agrégats affiche (sous forme de tableau) les noms et les propriétés des agrégats surveillés.

- **Statut**

  Affiche l'état actuel d'un volume. L'état peut être Critique (), Erreur (), Avertissement () ou Normal ().

  Vous pouvez placer le pointeur sur l'état pour afficher plus d'informations sur l'événement ou les événements générés pour le volume.

- **Nom de l'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.

  - Restreint

    Les opérations limitées (telles que la reconstruction de la 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 en cours

  L’agrégat est en cours de destruction.

- Échec

  L’agrégat ne peut pas être mis en ligne.

- Gelé

  L’agrégat ne traite pas (temporairement) les requêtes.

- Incohérent

  L’agrégat a été marqué comme corrompu; vous devriez contacter le support technique.

- Restriction du fer

  Les outils de diagnostic ne peuvent pas être exécutés sur l’agrégat.

- Montage

  L’agrégat est en cours de montage.

- Partiel

  Au moins un disque a été trouvé pour l’agrégat, mais deux disques ou plus sont manquants.

- Suspension

  L’agrégat est en cours de mise au repos.

- Suspendu

  L’agrégat est au repos.

- Rétabli

  Le retour à une version antérieure d’un agrégat est terminé.

- Non monté

  L’agrégat est hors ligne.

- Démontage

  L’agrégat est en cours de mise hors ligne.

- Inconnu

  L'agrégat est détecté, mais le serveur Unified Manager n'a pas encore récupéré les informations sur l'agrégat.

- **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. Cette colonne est masquée par défaut.

- **Capacité engagée**

  Affiche l'espace total (en Mo, Go, etc.) alloué à l'ensemble des volumes dans l'agrégat. Cette colonne est masquée par défaut.

- **Capacité utilisée**

  Affiche la quantité d'espace (en Mo, Go, etc.) utilisée dans l'agrégat.

- **Capacité disponible**

  Affiche la quantité d'espace (en Mo, Go, etc.) disponible pour les données dans l'agrégat. Cette colonne est masquée par défaut.

- **Disponible %**

  Affiche le pourcentage d'espace disponible pour les données dans l'agrégat. Par défaut, cette colonne est masquée.

- **% utilisé**

  Affiche le pourcentage d'espace utilisé par les données dans l'agrégat.

- **Type de RAID**

  Affiche le type RAID du volume sélectionné. Le type RAID peut être RAID0, RAID4, RAID-DP, RAID-TEC ou RAID mixte.

Découvrez la page des tâches dans Active IQ Unified Manager

La page Jobs vous permet de consulter l'état actuel et d'autres informations concernant toutes les tâches de protection des applications partenaires en cours d'exécution, ainsi que celles qui sont terminées. Vous pouvez ainsi voir quelles tâches sont toujours en cours et si une tâche a réussi ou échoué.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Abandonner**

  Interrompt la tâche sélectionnée. Cette option est disponible uniquement si la tâche sélectionnée est en cours d'exécution.

- **Réessayer**

  Relance une tâche ayant échoué de type Configuration de protection ou Opération de relation de protection. Vous ne pouvez relancer qu'une seule tâche ayant échoué à la fois. Si plusieurs tâches ayant échoué sont sélectionnées, le bouton **Relancer** est désactivé. Vous ne pouvez pas relancer les tâches de service de stockage ayant échoué.

- **Rafraîchir**

  Actualise la liste des tâches et les informations qui leur sont associées.

Liste des tâches

La liste des tâches affiche, sous forme de tableau, les tâches en cours. Par défaut, la liste affiche uniquement les tâches générées au cours de la semaine écoulée. Vous pouvez utiliser le tri et le filtrage des colonnes pour personnaliser les tâches affichées.

- **Statut**

  Affiche l'état actuel d'une tâche. L'état peut être Erreur (⚠️) ou Normal (✅).

- **ID du travail**

  Affiche le numéro d'identification de la tâche. Par défaut, cette colonne est masquée.

  Le numéro d'identification de la tâche est unique et le serveur l'attribue au démarrage de celle-ci. Vous pouvez rechercher une tâche spécifique en saisissant son numéro d'identification dans le champ de texte fourni par le filtre de colonne.

- **Nom**

  Affiche le nom de la tâche.

- **Type**

  Affiche le type de tâche. Les types de tâches sont les suivants :

  - **Acquisition de cluster**

    Une tâche Workflow Automation redécouvre un cluster.

  - **Configuration de protection**

    Une tâche de protection consiste à lancer des workflows Workflow Automation, tels que des planifications cron, la création de politiques SnapMirror, etc.

  - **Opération de relation de protection**

Une tâche de protection exécute des opérations SnapMirror.

- **Chaîne de flux de travail de protection**

  Une tâche Workflow Automation exécute plusieurs flux de travail.

- **Restaurer**

  Une tâche de restauration est en cours.

- **Nettoyage**

  Cette tâche consiste à nettoyer les artefacts des membres du service de stockage qui ne sont plus nécessaires à des fins de restauration.

- **Conforme**

  Cette tâche consiste à vérifier la configuration des membres du service de stockage afin de s'assurer de leur conformité.

- **Détruire**

  La tâche est en train de détruire un service de stockage.

- **Importer**

  La tâche consiste à importer des objets de stockage non gérés dans un service de stockage existant.

- **Modifier**

  La tâche consiste à modifier les attributs d'un service de stockage existant.

- **S'abonner**

  La tâche consiste à abonner des membres à un service de stockage.

- **Se désabonner**

  La tâche consiste à désinscrire les membres d'un service de stockage.

- **Mise à jour**

  Une tâche de mise à jour de la protection est en cours.

- **Configuration WFA**

  Une tâche Workflow Automation envoie les informations d'identification du cluster et synchronise les caches de la base de données.

- **État**

Affiche l'état d'exécution de la tâche. Les options d'état sont les suivantes :

- **Interrompu**

  La tâche a été abandonnée.

- **Abandon en cours**

  La tâche est en cours d'annulation.

- **Terminé**

  Le travail est terminé.

- **En cours d'exécution**

  La tâche est en cours.

- **Heure de soumission**

  Affiche l'heure de soumission de la tâche.

- **Durée**

  Affiche la durée d'exécution de la tâche. Cette colonne est affichée par défaut.

- **Heure d'achèvement**

  Affiche l'heure de fin de la tâche. Par défaut, cette colonne est masquée.

Découvrez la page des détails du travail dans Active IQ Unified Manager

La page Détails du travail vous permet de consulter l'état et d'autres informations sur des tâches spécifiques de travaux de protection en cours d'exécution, en file d'attente ou terminées. Vous pouvez utiliser ces informations pour suivre la progression des tâches de protection et résoudre les problèmes liés aux échecs des tâches.

Résumé du poste

Le résumé de la tâche affiche les informations suivantes :

- ID de tâche
- Type
- État
- Heure de soumission
- Heure d'achèvement
- Durée

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Rafraîchir**

  Actualise la liste des tâches et les propriétés associées à chaque tâche.

- **Voir les tâches**

Vous ramène à la page Jobs.

Liste des tâches du poste

La liste des tâches affiche, dans un tableau, toutes les tâches associées à un travail spécifique et les propriétés liées à chaque tâche.

- **Heure de début**

  Affiche le jour et l'heure de début de la tâche. Par défaut, les tâches les plus récentes apparaissent en haut de la colonne et les plus anciennes en bas.

- **Type**

  Affiche le type de tâche.

- **État**

  L'état d'une tâche particulière:

  - **Terminé**

    La tâche est terminée.

  - **En file d'attente**

    La tâche est sur le point de s'exécuter.

  - **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 de mise en file d'attente et d'exécution.

- **Statut**

  Affiche l'état de la tâche :

  - **Erreur (❗)**

    La tâche a échoué.

  - **Normal (✅)**

    La tâche a réussi.

  - **Ignoré (↷)**

    Une tâche a échoué, ce qui a entraîné l'omission des tâches suivantes.

- **Durée**

  Affiche le temps écoulé depuis le début de la tâche.

- **Heure d’achèvement**

  Affiche l’heure à laquelle la tâche s’est terminée. Par défaut, cette colonne est masquée.

- **ID de la tâche**

  Affiche le GUID qui identifie une tâche individuelle pour un job. Cette colonne peut être triée et filtrée. Par défaut, cette colonne est masquée.

- **Ordre de dépendance**

  Affiche un entier représentant la séquence des tâches dans un graphe, où la valeur zéro est attribuée à la première tâche. Par défaut, cette colonne est masquée.

- **Volet Détails de la tâche**

  Affiche des informations supplémentaires sur chaque tâche, notamment le nom de la tâche, sa description et, en cas d’échec de la tâche, la raison de cet échec.

- **Volet Messages des tâches**

  Affiche les messages spécifiques à la tâche sélectionnée. Ces messages peuvent inclure la raison de l’erreur et des suggestions pour la résoudre. Certaines tâches n’affichent pas de messages.

Utilisez la boîte de dialogue Paramètres secondaires avancés dans Active IQ Unified Manager

Vous pouvez utiliser la boîte de dialogue Paramètres secondaires avancés pour activer la réplication flexible par version, la sauvegarde multicopie et les paramètres liés à l’espace sur un volume secondaire. Vous pouvez utiliser la boîte de dialogue Paramètres secondaires avancés lorsque vous souhaitez modifier, activer ou désactiver les paramètres actuels.

Les paramètres liés à l’espace maximisent la quantité de données stockées, notamment : la déduplication, la compression des données, l’extension automatique et la garantie d’espace.

La boîte de dialogue comprend les champs suivants :

- **Activer la réplication flexible entre versions**

  Active SnapMirror avec la réplication flexible entre versions. La réplication flexible entre versions permet à SnapMirror de protéger un volume source même si le volume de destination exécute une version antérieure de ONTAP par rapport à celle du volume source.

  - Activer la sauvegarde

    Si la réplication flexible en fonction des versions est activée, elle permet également de transférer vers la destination SnapMirror et d’y conserver plusieurs copies Snapshot des données sources SnapMirror.

- **Activer la déduplication**

  Active la déduplication sur le volume secondaire dans une relation SnapVault afin d’éliminer les blocs de données en double et de réaliser des économies d’espace. Vous pouvez utiliser la déduplication lorsque les économies d’espace atteignent au moins 10 % et que le taux d’écrasement des données n’est pas élevé. 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

    Active la compression transparente des données. Vous pouvez utiliser la compression lorsque le gain d'espace est d'au moins 10 %, que la surcharge potentielle est acceptable et que les ressources système sont suffisantes pour que la compression s'effectue en dehors des heures de pointe. Dans une relation SnapVault, ce paramètre est désactivé par défaut. La compression est disponible uniquement lorsque la déduplication est sélectionnée.

  - Compression en ligne

    Permet de gagner immédiatement de l'espace en compressant les données avant leur écriture sur le disque. Vous pouvez utiliser la compression en ligne lorsque votre système n'a pas plus de 50 % d'utilisation aux heures de pointe et lorsqu'il peut prendre en charge de nouvelles écritures ainsi qu'une charge CPU supplémentaire pendant ces heures. Ce paramètre est disponible uniquement lorsque "Enable Compression" est sélectionné.

- **Activer la croissance automatique**

  Permet d'augmenter automatiquement le volume de destination lorsque le pourcentage d'espace libre est inférieur au seuil spécifié, à condition qu'il y ait de l'espace disponible sur l'agrégat associé.

- **Taille maximale**

  Définit le pourcentage maximal jusqu'auquel un volume peut s'étendre. La valeur par défaut est de 20 % supérieure à la taille du volume source. Un volume ne s'étend pas automatiquement si sa taille actuelle est supérieure ou égale au pourcentage maximal d'extension automatique. Ce champ est activé uniquement lorsque le paramètre d'extension automatique est activé.

- **Taille d'incrément**

  Spécifie le pourcentage d'augmentation automatique du volume avant d'atteindre le pourcentage maximal du volume source.

- **Garantie d'espace**

  Garantit qu'un espace suffisant est alloué sur le volume secondaire pour que les transferts de données réussissent systématiquement. Le paramètre de garantie d'espace peut prendre l'une des valeurs suivantes :

  - Fichier
  - Volume
  - Aucun + Par exemple, vous pouvez avoir un volume de 200 Go qui contient des fichiers totalisant 50 Go ; toutefois, ces fichiers ne contiennent que 10 Go de données. La garantie de volume alloue 200 Go au volume de destination, quel que soit le contenu du volume source. La garantie de fichiers alloue 50 Go pour garantir qu'un espace suffisant est réservé aux fichiers sur le volume source ; dans ce scénario, sélectionner Aucun signifie que seulement 10 Go sont alloués sur le volume de destination pour l'espace réellement utilisé par les données de fichier sur le volume source.

  La garantie d'espace est définie par défaut sur Volume.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Appliquer**

  Enregistre les paramètres d'efficacité sélectionnés et les applique lorsque vous cliquez sur **Appliquer** dans la boîte de dialogue Configurer la protection.

- **Annuler**

  Ignore vos sélections et ferme la boîte de dialogue Paramètres de destination avancés.

Utilisez la boîte de dialogue Paramètres de destination avancés dans Active IQ Unified Manager

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 les paramètres avancés lorsque la garantie d'espace est désactivée sur la source, mais que vous souhaitez l'activer sur la destination. Les paramètres de déduplication, de compression et d'extension automatique dans une relation SnapMirror sont hérités du volume source et ne peuvent pas être modifiés.

Garantie d'espace

Garantit qu'un espace suffisant est alloué sur le volume de destination pour que les transferts de données réussissent toujours. Le paramètre de garantie d'espace peut prendre l'une des valeurs suivantes :

- Fichier
- Volume
- Aucune

Par exemple, vous pouvez avoir un volume de 200 Go contenant des fichiers totalisant 50 Go ; cependant, ces fichiers ne contiennent que 10 Go de données. La garantie de volume alloue 200 Go au volume de destination, quel que soit le contenu du volume source. La garantie de fichier alloue 50 Go afin de garantir un espace suffisant pour les fichiers sources sur le volume de destination ; sélectionner **None** dans ce cas signifie que seuls 10 Go sont alloués sur le volume de destination pour l'espace réellement utilisé par les données des fichiers sur le volume source.

La garantie d'espace est définie par défaut sur Volume.

Utilisez la boîte de dialogue Restaurer dans Active IQ Unified Manager

Vous pouvez utiliser la boîte de dialogue Restaurer pour restaurer des données dans un volume à partir d'une copie Snapshot spécifique.

Restaurer à partir de

La zone « Restaurer à partir de » vous permet de spécifier l'emplacement à partir duquel vous souhaitez restaurer les données.

- **Volume**

  Spécifie le volume à partir duquel vous souhaitez restaurer les données. Par défaut, le volume sur lequel

vous avez lancé la restauration est sélectionné. Vous pouvez sélectionner un autre volume dans la liste déroulante qui contient tous les volumes ayant des relations de protection avec le volume sur lequel vous avez lancé la restauration.

- **copie Snapshot**

  Spécifie la copie Snapshot à utiliser pour restaurer les données. Par défaut, la copie Snapshot la plus récente est sélectionnée. Vous pouvez également choisir une autre copie Snapshot dans la liste déroulante. La liste des copies Snapshot varie selon le volume sélectionné.

- **Liste maximale de 995 fichiers et répertoires**

  Par défaut, la liste affiche un maximum de 995 objets. Vous pouvez décocher cette case si vous souhaitez 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 section « Sélectionner les éléments à restaurer » vous permet de sélectionner soit le volume entier, soit les fichiers et dossiers spécifiques que vous souhaitez restaurer. Vous pouvez sélectionner jusqu'à 10 fichiers, dossiers ou une combinaison des deux. Lorsque le nombre maximal d'éléments est sélectionné, les cases à cocher de sélection des éléments sont désactivées.

- **Champ du chemin**

  Affiche le chemin d'accès aux données que vous souhaitez restaurer. Vous pouvez accéder au dossier et aux fichiers que vous souhaitez restaurer, ou saisir le chemin. Ce champ reste vide tant que vous n'avez pas sélectionné ou saisi un chemin. Si vous cliquez sur  après avoir choisi un chemin, vous remontez d'un niveau dans l'arborescence des répertoires.

- **Liste des dossiers et fichiers**

  Affiche le contenu du chemin que vous avez saisi. Par défaut, le dossier racine est affiché initialement. Cliquer sur le nom d'un dossier affiche son contenu.

Vous pouvez sélectionner les éléments à restaurer comme suit :

- Lorsque vous saisissez le chemin d'accès avec un nom de fichier particulier spécifié dans le champ de chemin, le fichier spécifié s'affiche dans Dossiers et fichiers.
- Lorsque vous saisissez un chemin d'accès sans spécifier de fichier particulier, le contenu du dossier s'affiche dans la liste Dossiers et fichiers, et vous pouvez sélectionner jusqu'à 10 fichiers, dossiers ou une combinaison des deux à restaurer.

  Si un dossier contient plus de 995 éléments, un message s'affiche pour indiquer qu'il y a trop d'éléments à afficher, et si vous poursuivez l'opération, tous les éléments du dossier spécifié sont restaurés. Vous pouvez décocher la case "Répertorier un maximum de 995 fichiers et répertoires" si vous souhaitez afficher tous les objets du volume sélectionné.

Vous ne pouvez pas restaurer les flux de fichiers NTFS.

Restaurer vers

La zone « Restaurer vers » vous permet de spécifier l'emplacement où vous souhaitez restaurer les données.

- **Emplacement d'origine dans Volume_Name**

  Restaure les données sélectionnées dans le répertoire de la source à partir duquel les données ont été initialement sauvegardées.

- **Autre emplacement**

  Restaure les données sélectionnées vers un nouvel emplacement :

  - Chemin de restauration

    Spécifie un autre chemin pour restaurer les données sélectionnées. Le chemin doit déjà exister. Vous pouvez utiliser le bouton **Browse** pour accéder à l'emplacement où vous souhaitez restaurer les données, ou vous pouvez saisir le chemin manuellement au format `cluster://svm/volume/path`.

  - Préserver la hiérarchie des répertoires

    Lorsqu'elle est activée, cette option préserve la structure du fichier ou du répertoire d'origine. Par exemple, si la source est /A/B/C/myFile.txt et la destination est /X/Y/Z, Unified Manager restaure les données en utilisant la structure de répertoires suivante sur la destination : /X/Y/Z/A/B/C/myFile.txt.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Restaurer.

- **Restaurer**

  Applique les sélections que vous avez effectuées et lance le processus de restauration.

Utilisez la boîte de dialogue Parcourir les répertoires dans Active IQ Unified Manager

Vous pouvez utiliser la boîte de dialogue Parcourir les répertoires lorsque vous souhaitez restaurer des données dans un répertoire d'un cluster et d'une SVM différents de la source d'origine. Le cluster et le volume source d'origine sont sélectionnés par défaut.

La boîte de dialogue Parcourir les répertoires vous permet de sélectionner le cluster, le SVM, le volume et le chemin d'accès au répertoire dans lequel vous souhaitez restaurer les données.

- **Cluster**

  Affiche la liste des clusters de destination disponibles pour la restauration. Par défaut, le cluster du volume source d'origine est sélectionné.

- **Liste déroulante SVM**

  Affiche la liste des SVM disponibles pour le cluster sélectionné. Par défaut, la SVM du volume source d'origine est sélectionnée.

- **Volume**

  Affiche la liste de tous les volumes en lecture/écriture d'une SVM sélectionnée. Vous pouvez filtrer les

volumes par nom et par espace disponible. Le volume disposant du plus d'espace est affiché en premier, et ainsi de suite, par ordre décroissant. Par défaut, le volume source d'origine est sélectionné.

- **Zone de texte du chemin d'accès au fichier**

  Permet de saisir le chemin d'accès au fichier dans lequel vous souhaitez restaurer les données. Ce chemin doit déjà exister.

- **Nom**

  Affiche les noms des dossiers disponibles pour le volume sélectionné. Cliquer sur un dossier dans la liste Noms affiche les sous-dossiers, le cas échéant. Les fichiers contenus dans les dossiers ne sont pas affichés. Cliquer sur  après avoir sélectionné un dossier vous fait remonter d'un niveau dans l'arborescence.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Sélectionnez un répertoire**

  Applique vos sélections et ferme la boîte de dialogue Parcourir les répertoires. Si aucun répertoire n'est sélectionné, ce bouton est désactivé.

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Parcourir les répertoires.

Utilisez la boîte de dialogue Configurer la protection dans Active IQ Unified Manager

Vous pouvez utiliser la boîte de dialogue Configurer la protection pour créer des relations SnapMirror et SnapVault pour tous les volumes en lecture, en écriture et de protection des données sur les clusters afin de garantir que les données d'un volume source ou d'un volume principal sont répliquées.

Onglet source

- **Vue topologique**

  Affiche une représentation visuelle de la relation que vous créez. La source dans la topologie est mise en surbrillance par défaut.

- **Informations sur la source**

  Affiche les détails relatifs aux volumes sources sélectionnés, notamment les informations suivantes :

  - Nom du cluster source
  - Nom de la SVM source
  - Taille totale du volume cumulé

    Affiche la taille totale de tous les volumes sources sélectionnés.

  - Taille cumulée utilisée du volume

Affiche la taille cumulée utilisée pour tous les volumes sources sélectionnés.

- Volume source

  Affiche les informations suivantes dans un tableau :

  - Volume source

    Affiche les noms des volumes sources sélectionnés.

  - Type

    Affiche le type de volume.

  - Type de SnapLock

    Affiche le type SnapLock du volume. Les options sont Compliance, Enterprise et Non-SnapLock.

  - Copie instantanée

    Affiche la copie Snapshot utilisée pour le transfert de base. Si le volume source est accessible en lecture/écriture, 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. Cliquer sur la valeur de la copie Snapshot affiche une liste de copies Snapshot parmi lesquelles vous pouvez sélectionner une copie Snapshot existante à utiliser pour le transfert de base. Vous ne pouvez pas sélectionner une autre copie Snapshot par défaut si le type de source est « protection des données ».

onglet SnapMirror

Permet de spécifier un cluster de destination, une machine virtuelle de stockage (SVM) et un agrégat pour une relation de protection, ainsi qu'une convention de nommage pour les destinations lors de la création d'une relation SnapMirror. Vous pouvez également spécifier une stratégie et une planification SnapMirror.

- **Vue topologique**

  Affiche une représentation visuelle de la relation que vous créez. La ressource de destination SnapMirror dans la topologie est mise en surbrillance par défaut.

- **Informations sur la destination**

  Vous permet de sélectionner les ressources de destination pour une relation de protection :

  - Lien avancé

    Ouvre la boîte de dialogue Paramètres de destination avancés lors de la création d'une relation SnapMirror.

  - Cluster

    Répertorie les clusters disponibles en tant qu'hôtes de destination de protection. Ce champ est obligatoire.

  - machine virtuelle de stockage (SVM)

Affiche la liste des SVM disponibles sur le cluster sélectionné. Un cluster doit être sélectionné pour que la liste des SVM s'affiche. Ce champ est obligatoire.

◦ Agrégat

Affiche la liste des agrégats disponibles sur le SVM sélectionné. Un cluster doit être sélectionné pour que la liste des agrégats s'affiche. Ce champ est obligatoire. La liste des agrégats affiche les informations suivantes :

▪ Rang

Lorsque plusieurs agrégats satisfont à toutes les exigences d'une destination, le rang indique la priorité dans laquelle l'agrégat est répertorié, selon les conditions suivantes :

A. Il est préférable d'utiliser un agrégat situé sur un nœud différent de celui du volume source afin de permettre la séparation des domaines de défaillance.
B. Il est préférable d'utiliser un agrégat sur un nœud comportant moins de volumes pour permettre l'équilibrage de charge entre les nœuds d'un cluster.
C. Pour permettre l'équilibrage de la capacité, on privilégie un agrégat disposant de plus d'espace libre que les autres agrégats. Un rang 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 dénomination par défaut appliquée au volume de destination. Vous pouvez accepter la convention proposée ou en créer une personnalisée. Cette convention peut comporter les attributs suivants : %C, %M, %V et %N, où %C correspond au nom du cluster, %M au nom de la SVM, %V au volume source et %N au nom du nœud de destination de la topologie.

Le champ de convention d'appellation est surligné en rouge si votre saisie n'est pas valide. Le fait de cliquer sur le lien "Preview Name" affiche un aperçu de la convention d'appellation que vous avez saisie, et le texte d'aperçu se met à jour dynamiquement à mesure que vous saisissez une convention d'appellation dans le champ de texte. Un suffixe compris entre 001 et 999 est ajouté au nom de destination lors de la création de la relation, remplaçant nnn affiché dans le texte d'aperçu, 001 étant attribué en premier, 002 en deuxième, et ainsi de suite.

- **Paramètres de la relation**

Permet de spécifier le taux de transfert maximal, la stratégie SnapMirror et le planning utilisés par la relation de protection :

◦ Taux de transfert maximal

Spécifie le débit maximal de transfert de données entre les clusters sur le réseau. Si vous choisissez

de ne pas spécifier de débit maximal, le transfert de base entre les relations est illimité.

- SnapMirror stratégie

  Spécifie la stratégie ONTAP SnapMirror pour la relation. La valeur par défaut est DPDefault.

- Créer une stratégie

  Ouvre la boîte de dialogue Créer une stratégie SnapMirror, qui vous permet de créer et d'utiliser une nouvelle stratégie SnapMirror.

- SnapMirror calendrier

  Spécifie la stratégie ONTAP SnapMirror pour la relation. Les planifications disponibles sont : Aucune, 5 min, 8 heures, quotidienne, horaire et hebdomadaire. La valeur par défaut est Aucune, ce qui indique qu'aucune planification n'est associée à la relation. Les relations sans planification n'ont pas de valeurs d'état de décalage, sauf si elles appartiennent à un service de stockage.

- Créer une planification

  Ouvre la boîte de dialogue Créer une planification, qui vous permet de créer une nouvelle planification SnapMirror.

onglet SnapVault

Permet de spécifier un cluster secondaire, une SVM et un agrégat pour une relation de protection, ainsi qu'une convention de dénomination pour les volumes secondaires lors de la création d'une relation SnapVault. Vous pouvez également spécifier une stratégie et une planification SnapVault.

- **Vue topologique**

  Affiche une représentation visuelle de la relation que vous créez. La ressource secondaire SnapVault dans la topologie est mise en surbrillance par défaut.

- **Informations secondaires**

  Vous permet de sélectionner les ressources secondaires pour une relation de protection:

  - Lien avancé

    Ouvre la boîte de dialogue Paramètres secondaires avancés.

  - Cluster

    Répertorie les clusters disponibles en tant qu'hôtes de protection secondaires. Ce champ est obligatoire.

  - machine virtuelle de stockage (SVM)

    Affiche la liste des SVM disponibles sur le cluster sélectionné. Un cluster doit être sélectionné pour que la liste des SVM s'affiche. Ce champ est obligatoire.

  - Agrégat

    Affiche la liste des agrégats disponibles sur le SVM sélectionné. Un cluster doit être sélectionné pour que la liste des agrégats s'affiche. Ce champ est obligatoire. La liste des agrégats affiche les

informations suivantes :

- Rang

  Lorsque plusieurs agrégats satisfont à toutes les exigences d'une destination, le rang indique la priorité dans laquelle l'agrégat est répertorié, selon les conditions suivantes :

  A. Il est préférable d'utiliser un agrégat situé sur un nœud différent de celui du volume principal afin de permettre la séparation des domaines de défaillance.
  B. Il est préférable d'utiliser un agrégat sur un nœud comportant moins de volumes pour permettre l'équilibrage de charge entre les nœuds d'un cluster.
  C. Pour permettre l'équilibrage de la capacité, on privilégie un agrégat disposant de plus d'espace libre que les autres agrégats. Un rang 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 d'appellation par défaut appliquée au volume secondaire. Vous pouvez accepter la convention proposée ou en créer une personnalisée. Cette convention peut comporter les attributs suivants : %C, %M, %V et %N, où %C correspond au nom du cluster, %M au nom de la SVM, %V au volume source et %N au nom du nœud secondaire de la topologie.

Le champ de convention d'appellation est surligné en rouge si votre saisie n'est pas valide. Le fait de cliquer sur le lien « `Preview Name` » affiche un aperçu de la convention d'appellation que vous avez saisie, et le texte d'aperçu se met à jour dynamiquement à mesure que vous saisissez une convention d'appellation dans le champ de texte. Si vous saisissez une valeur non valide, les informations non valides s'affichent sous forme de points d'interrogation rouges dans la zone d'aperçu. Un suffixe compris entre 001 et 999 est ajouté au nom secondaire lorsque la relation est créée, remplaçant le nnn affiché dans le texte d'aperçu, 001 étant attribué en premier, 002 en second, et ainsi de suite.

- **Paramètres de la relation**

  Vous permet de spécifier le taux de transfert maximal, la politique SnapVault et la planification SnapVault utilisés par la relation de protection :

  ◦ Taux de transfert maximal

  Spécifie le débit maximal de transfert de données entre les clusters sur le réseau. Si vous choisissez de ne pas spécifier de débit maximal, le transfert de base entre les relations est illimité.

  ◦ SnapVault Stratégie

  Spécifie la stratégie ONTAP SnapVault pour la relation. La valeur par défaut est XDPDefault.

◦ Créer une stratégie

Ouvre la boîte de dialogue Créer une stratégie SnapVault, qui vous permet de créer et d'utiliser une nouvelle stratégie SnapVault.

◦ SnapVault Calendrier

Spécifie la planification ONTAP SnapVault pour la relation. Les planifications disponibles incluent None, 5min, 8hour, daily, hourly et weekly. La valeur par défaut est None, ce qui indique qu'aucune planification n'est associée à la relation. Les relations sans planification n'ont pas de valeurs d'état de décalage, sauf si elles appartiennent à un service de stockage.

◦ Créer une planification

Ouvre la boîte de dialogue Créer une planification, qui vous permet de créer une planification SnapVault.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Configurer la protection.

- **Appliquer**

  Applique les sélections que vous avez effectuées et lance le processus de protection.

Utilisez la boîte de dialogue Créer une planification dans Active IQ Unified Manager

La boîte de dialogue Créer une planification vous permet de créer une planification de protection de base ou avancée pour les transferts de relations SnapMirror et SnapVault. Vous pouvez créer une nouvelle planification pour augmenter la fréquence des transferts de données en raison de mises à jour fréquentes, ou une planification moins fréquente lorsque les données changent rarement.

Il est impossible de configurer des planifications pour les relations synchrones SnapMirror.

- **Cluster de destination**

  Le nom du cluster que vous avez sélectionné dans l'onglet SnapVault ou l'onglet SnapMirror de la boîte de dialogue Configurer la protection.

- **Nom de la planification**

  Nom que vous fournissez pour la planification. Les noms de planification peuvent contenir les caractères A à Z, a à z, 0 à 9, ainsi que les caractères spéciaux suivants : ! @ # $ % ^ & * ( ) _ -. Les noms de planification ne peuvent pas contenir les caractères suivants : < >.

- **Niveau de base ou avancé**

  Le mode de planification que vous souhaitez utiliser.

Le mode de base comprend les éléments suivants :

- Répéter

  Fréquence à laquelle un transfert planifié a lieu. Les choix incluent horaire, quotidien et hebdomadaire.

- Jour

  Lorsqu'une répétition hebdomadaire est sélectionnée, le jour de la semaine où un transfert a lieu.

- Durée

  Lorsque l'option « Quotidien » ou « Hebdomadaire » est sélectionnée, cela détermine l'heure de la journée à laquelle le transfert a lieu.

  Le mode avancé comprend les éléments suivants :

- Mois

  Liste numérique des mois de l'année, séparés par des virgules. Les valeurs valides vont de 0 à 11, 0 représentant janvier, et ainsi de suite. Cet élément est facultatif. S'il est laissé vide, les transferts sont effectués tous les mois.

- Jours

  Liste numérique séparée par des virgules représentant le jour du mois. Les valeurs valides vont de 1 à 31. Cet élément est facultatif. Si le champ est laissé vide, un transfert a lieu chaque jour du mois.

- Jours de la semaine

  Liste numérique séparée par des virgules représentant les jours de la semaine. Les valeurs valides vont de 0 à 6, 0 représentant le dimanche, et ainsi de suite. Cet élément est facultatif. Laisser le champ vide signifie qu'un transfert a lieu chaque jour de la semaine. Si un jour de la semaine est spécifié mais qu'aucun jour du mois ne l'est, un transfert a lieu uniquement le jour de la semaine indiqué, et non tous les jours.

- Heures

  Liste numérique, séparée par des virgules, représentant le nombre d'heures dans une journée. Les valeurs valides sont comprises entre 0 et 23, 0 représentant minuit. Cet élément est facultatif.

- Minutes

  Liste numérique séparée par des virgules représentant les minutes d'une heure. Les valeurs valides sont comprises entre 0 et 59. Cet élément est obligatoire.

Utilisez la boîte de dialogue Créer une stratégie SnapMirror dans Active IQ Unified Manager

La boîte de dialogue Créer une stratégie SnapMirror vous permet de créer une stratégie pour définir la priorité des transferts SnapMirror. Vous utilisez des stratégies pour optimiser l'efficacité des transferts de la source vers la destination.

- **Cluster de destination**

  Le nom du cluster que vous avez sélectionné dans l'onglet SnapMirror de la boîte de dialogue Configurer

la protection.

- **SVM de destination**

  Le nom de la SVM que vous avez sélectionnée dans l'onglet SnapMirror de la boîte de dialogue Configurer la protection.

- **Nom de la stratégie**

  Le nom que vous attribuez à la nouvelle stratégie. Les noms de stratégie peuvent contenir les caractères A à Z, a à z, 0 à 9, le point (.), le tiret (-) et le trait de soulignement (_).

- **Priorité de transfert**

  La priorité à laquelle un transfert s'exécute pour les opérations asynchrones. Vous pouvez sélectionner Normal ou Low. Les relations de transfert avec des stratégies qui spécifient une priorité de transfert normale s'exécutent avant celles avec des stratégies qui spécifient une priorité de transfert faible.

- **Commentaire**

  Champ facultatif dans lequel vous pouvez ajouter des commentaires sur la stratégie.

- **Redémarrage du transfert**

  Indique l'action de redémarrage à entreprendre lorsqu'un transfert est interrompu par une opération d'annulation ou tout autre type de panne, comme une coupure réseau. Vous pouvez sélectionner l'une des options suivantes :

  - Toujours

    Spécifie qu'une nouvelle copie Snapshot est créée avant le redémarrage d'un transfert, puis que, s'il existe un point de contrôle, le transfert redémarre à partir de ce point de contrôle, suivi d'un transfert incrémentiel depuis la copie Snapshot nouvellement créée.

  - Jamais

    Indique que les transferts interrompus ne sont jamais redémarrés.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

  Annule les sélections et ferme la boîte de dialogue Configurer la protection.

- **Appliquer**

  Applique les sélections que vous avez effectuées et lance le processus de protection.

Utilisez la boîte de dialogue Créer une stratégie SnapVault dans Active IQ Unified Manager

La boîte de dialogue Créer une stratégie SnapVault vous permet de créer une stratégie pour définir la priorité des transferts SnapVault. Vous utilisez des stratégies pour optimiser l'efficacité des transferts du volume principal vers le volume secondaire.

- **Cluster de destination**

  Le nom du cluster que vous avez sélectionné dans l'onglet SnapVault de la boîte de dialogue Configurer la protection.

- **SVM de destination**

  Le nom de la SVM que vous avez sélectionnée dans l'onglet SnapVault de la boîte de dialogue Configurer la protection.

- **Nom de la stratégie**

  Le nom que vous attribuez à la nouvelle stratégie. Les noms de stratégie peuvent contenir les caractères A à Z, a à z, 0 à 9, le point (.), le tiret (-) et le trait de soulignement (_).

- **Priorité de transfert**

  La priorité à laquelle le transfert s'exécute. Vous pouvez sélectionner soit Normal, soit Low. Les relations de transfert avec des règles qui spécifient une priorité de transfert Normal s'exécutent avant celles avec des règles qui spécifient une priorité de transfert Low. Le paramètre par défaut est Normal.

- **Commentaire**

  Champ facultatif dans lequel vous pouvez ajouter un commentaire de 255 caractères maximum sur la politique SnapVault.

- **Ignorer le temps d'accès**

  Indique si les transferts incrémentiels sont ignorés pour les fichiers dont seul le temps d'accès a été modifié.

- **Étiquette de réplication**

  Affiche dans un tableau les règles associées aux copies Snapshot sélectionnées par ONTAP et possédant une étiquette de réplication spécifique dans une stratégie. Les informations et actions suivantes sont également disponibles :

  - Boutons de commande

    Les boutons de commande vous permettent d'effectuer les actions suivantes :

    - Ajouter

      Permet de créer une étiquette de copie Snapshot et un nombre de copies à conserver.

    - Modifier le nombre de rétentions

      Permet de modifier le nombre de copies à conserver d'une étiquette de copie Snapshot existante. Ce nombre doit être compris entre 1 et 251. La somme de tous les nombres de copies à conserver 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 ayant la même stratégie de copie Snapshot locale, une entrée est affichée pour chaque étiquette de la stratégie. Si vous sélectionnez plusieurs volumes ayant deux stratégies de copie Snapshot locales ou plus, le tableau affiche toutes les étiquettes de toutes les stratégies

◦ Calendrier

Affiche la planification associée à chaque étiquette de copie Snapshot. Si une étiquette est associée à plusieurs planifications, celles-ci sont affichées dans une liste séparée par des virgules. Si vous sélectionnez plusieurs volumes portant la même étiquette mais des planifications différentes, la mention « `Various` » s'affiche pour indiquer que plusieurs planifications sont associées aux volumes sélectionnés.

◦ Nombre de rétentions de destination

Affiche le nombre de copies Snapshot portant l'étiquette spécifiée qui sont conservées sur le système secondaire SnapVault. Pour les étiquettes comportant plusieurs planifications, le nombre de copies conservées correspond à la somme des nombres de copies conservées de chaque paire étiquette/planification. Si vous sélectionnez plusieurs volumes avec au moins deux stratégies locales de copie Snapshot, le nombre de copies conservées est vide.

Modifier une relation de protection dans Active IQ Unified Manager

Vous pouvez modifier une relation de protection existante afin de changer le débit de transfert maximal, la politique de protection ou la planification de protection.

Informations sur la destination

- **Cluster de destination**

  Le nom du cluster de destination sélectionné.

- **SVM de destination**

  Le nom du SVM sélectionné

- **Paramètres de la relation**

  Permet de spécifier le taux de transfert maximal, la stratégie SnapMirror et le planning utilisés par la relation de protection :

  ◦ Taux de transfert maximal

  Spécifie le débit maximal auquel les données du transfert de base sont transférées entre les clusters sur le réseau. Lorsqu'elle est sélectionnée, la bande passante du réseau est limitée à la valeur que vous spécifiez. Vous pouvez entrer une valeur numérique, puis sélectionner des kilo-octets par seconde (Ko/s), des mégaoctets par seconde (Mo/s), des gigaoctets par seconde (Go/s) ou des téraoctets par seconde (To/s). Le débit de transfert maximal que vous spécifiez doit être supérieur à 1 Ko/s et inférieur à 4 To/s. Si vous choisissez de ne pas utiliser de débit 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.

  ◦ SnapMirror stratégie

  Spécifie la stratégie ONTAP SnapMirror pour la relation. La valeur par défaut est DPDefault.

◦ Créer une stratégie

Ouvre la boîte de dialogue Créer une stratégie SnapMirror, qui vous permet de créer et d'utiliser une nouvelle stratégie SnapMirror.

◦ SnapMirror calendrier

Spécifie la stratégie ONTAP SnapMirror pour la relation. Les planifications disponibles sont : Aucune, 5 min, 8 heures, quotidienne, horaire et hebdomadaire. La valeur par défaut est Aucune, ce qui indique qu'aucune planification n'est associée à la relation. Les relations sans planification n'ont pas de valeurs d'état de décalage, sauf si elles appartiennent à un service de stockage.

◦ Créer une planification

Ouvre la boîte de dialogue Créer une planification, qui vous permet de créer une nouvelle planification SnapMirror.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

  Annule les sélections et ferme la boîte de dialogue Configurer la protection.

- **Soumettre**

  Applique les sélections que vous avez effectuées et ferme la boîte de dialogue Modifier la relation.

Utilisez la boîte de dialogue Initialiser/Mettre à jour dans Active IQ Unified Manager

La boîte de dialogue Initialiser/Mettre à jour vous permet d'effectuer un premier transfert de base sur une nouvelle relation de protection, ou de mettre à jour une relation si elle est déjà initialisée et que vous souhaitez effectuer une mise à jour manuelle, non planifiée et incrémentale.

Onglet Options de transfert

L'onglet Options de transfert vous permet de modifier la priorité d'initialisation d'un transfert et de modifier la bande passante utilisée pendant les transferts.

- **Priorité de transfert**

  La priorité à laquelle le transfert est exécuté. Vous pouvez choisir entre Normale et Faible. Les relations avec des stratégies qui spécifient une priorité de transfert normale sont exécutées avant celles qui spécifient une priorité de transfert faible. Normale est sélectionnée par défaut.

- **Taux de transfert maximal**

  Spécifie le débit maximal auquel les données sont transférées entre les clusters sur le réseau. Si vous choisissez de ne pas utiliser de débit de transfert maximal, le transfert de base entre les relations est illimité. Si vous sélectionnez plusieurs relations avec des débits de transfert maximaux différents, vous pouvez spécifier l'un des paramètres de débit de transfert maximal suivants :

◦ Utilisez les valeurs spécifiées lors de la configuration ou de la modification de chaque relation

Lorsqu'elle est sélectionnée, les opérations d'initialisation et de mise à jour utilisent le taux de transfert maximal spécifié lors de la création ou de la modification de chaque relation. Ce champ est disponible uniquement lors de l'initialisation ou de la mise à jour de plusieurs relations avec des taux de transfert différents.

◦ Illimité

Indique qu'il n'y a pas de limitation de bande passante pour les transferts entre les relations. Ce champ est disponible uniquement lors de l'initialisation ou de la mise à jour de plusieurs relations avec des débits de transfert différents.

◦ Limiter la bande passante à

Lorsque cette option est sélectionnée, la bande passante réseau est limitée à la valeur que vous spécifiez. Vous pouvez saisir une valeur numérique, puis sélectionner soit kilobytes per second (KBps), Megabytes per second (MBps), Gigabytes per second (GBps) ou Terabytes per second (TBps). Le débit de transfert maximal que vous spécifiez doit être supérieur à 1 KBps et inférieur à 4 TBps.

Onglet Copies Snapshot source

L'onglet Source Snapshot Copies affiche les informations suivantes sur la copie Snapshot source utilisée pour le transfert de base :

- **Volume source**

  Affiche les noms des volumes sources correspondants.

- **Volume de destination**

  Affiche les noms des volumes de destination sélectionnés.

- **Type de source**

  Affiche le type de volume. Ce type peut être Lecture/écriture ou protection des données.

- **copie Snapshot**

  Affiche la copie Snapshot utilisée pour le transfert de données. Cliquer sur la valeur de la copie Snapshot affiche la boîte de dialogue « Sélectionner la copie Snapshot source », dans laquelle vous pouvez sélectionner une copie Snapshot spécifique pour votre transfert, selon le type de relation de protection dont vous disposez et l'opération que vous effectuez. L'option permettant de spécifier une autre copie Snapshot n'est pas disponible pour les sources de type protection des données.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Initialiser/Mettre à jour.

- **Soumettre**

  Enregistre vos sélections et lance la tâche d'initialisation ou de mise à jour.

Utilisez la boîte de dialogue de resynchronisation dans Active IQ Unified Manager

La boîte de dialogue Resynchronize vous permet de resynchroniser les données sur une relation SnapMirror ou SnapVault qui a été précédemment rompue, puis dont le volume de destination a été converti en volume lecture/écriture. Vous pouvez également effectuer une resynchronisation lorsqu'une copie Snapshot commune requise sur le volume source est supprimée, ce qui entraîne l'échec des mises à jour SnapMirror ou SnapVault.

Onglet Options de resynchronisation

L'onglet Options de resynchronisation vous permet de définir la priorité de transfert et le débit de transfert maximal pour la relation de protection que vous resynchronisez.

- **Priorité de transfert**

  La priorité à laquelle le transfert est exécuté. Vous pouvez sélectionner soit Normal, soit Low. Les relations avec des stratégies qui spécifient une priorité de transfert normale s'exécutent avant celles avec des stratégies qui spécifient une priorité de transfert faible.

- **Taux de transfert maximal**

  Spécifie le débit maximal auquel les données sont transférées entre les clusters sur le réseau. Lorsque cette option est sélectionnée, la bande passante réseau est limitée à la valeur que vous spécifiez. Vous pouvez saisir une valeur numérique, puis sélectionner soit des kilooctets par seconde (KBps), des mégaoctets par seconde (MBps), des gigaoctets par seconde (GBps) ou des téraoctets par seconde (TBps). Si vous choisissez de ne pas utiliser de débit de transfert maximal, le transfert de base entre les relations est illimité.

Onglet Copies Snapshot source

L'onglet Source Snapshot Copies affiche les informations suivantes sur la copie Snapshot source utilisée pour le transfert de base :

- **Volume source**

  Affiche les noms des volumes sources correspondants.

- **Volume de destination**

  Affiche les noms des volumes de destination sélectionnés.

- **Type de source**

  Affiche le type de volume : lecture/écriture ou protection des données.

- **copie Snapshot**

  Affiche la copie Snapshot utilisée pour le transfert de données. Cliquer sur la valeur de la copie Snapshot affiche la boîte de dialogue « Select Source Snapshot Copy », dans laquelle vous pouvez choisir une copie Snapshot spécifique pour votre transfert, en fonction du type de relation de protection et de l'opération en cours.

Boutons de commande

- **Soumettre**

  Démarre le processus de resynchronisation et ferme la boîte de dialogue Resynchroniser.

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Resynchronize.

Utilisez la boîte de dialogue Sélectionner la copie d'instantané source dans Active IQ Unified Manager

Vous utilisez la boîte de dialogue Sélectionner la copie Snapshot source pour sélectionner une copie Snapshot spécifique afin de transférer des données entre les relations de protection, ou vous sélectionnez le comportement par défaut, qui varie selon que vous initialisez, mettez à jour ou resynchronisez une relation, et selon que la relation est une SnapMirror ou SnapVault.

Défaut

Permet de sélectionner le comportement par défaut pour déterminer quelle copie Snapshot est utilisée pour initialiser, mettre à jour et resynchroniser les transferts pour les relations SnapVault et SnapMirror.

Si vous effectuez un transfert SnapVault, le comportement par défaut pour chaque opération est le suivant :

Opération	Comportement par défaut de SnapVault lorsque la source est en lecture/écriture	Comportement par défaut de SnapVault lorsque la source est Data Protection (DP)
Initialiser	Crée une nouvelle copie Snapshot et la transfère.	Transfère la dernière copie Snapshot exportée.
Mise à jour	Transfère uniquement les copies Snapshot étiquetées, comme spécifié dans la stratégie.	Transfère la dernière copie Snapshot exportée.
Resynchroniser	Transfère toutes les copies Snapshot étiquetées créées après la plus récente copie Snapshot commune.	Transfère la copie Snapshot la plus récente étiquetée.

Si vous effectuez un transfert SnapMirror, le comportement par défaut de chaque opération est le suivant :

Opération	Comportement de SnapMirror par défaut	Comportement par défaut de SnapMirror lorsque la relation est le deuxième saut dans une cascade de SnapMirror à SnapMirror
Initialiser	Crée une nouvelle copie Snapshot et la transfère ainsi que toutes les copies Snapshot créées avant cette nouvelle copie Snapshot.	Transfère toutes les copies Snapshot à partir de la source.

Opération	Comportement de SnapMirror par défaut	Comportement par défaut de SnapMirror lorsque la relation est le deuxième saut dans une cascade de SnapMirror à SnapMirror
Mise à jour	Crée une nouvelle copie Snapshot et la transfère ainsi que toutes les copies Snapshot créées avant cette nouvelle copie Snapshot.	Transfère toutes les copies Snapshot.
Resynchroniser	Crée une nouvelle copie Snapshot, puis transfère toutes les copies Snapshot depuis la source.	Transfère toutes les copies Snapshot du volume secondaire vers le volume tertiaire et supprime toutes les données ajoutées après la création de la copie Snapshot commune la plus récente.

Snapshot Copy existante

Permet de sélectionner une copie Snapshot existante dans la liste si la sélection d'une copie Snapshot est autorisée pour cette opération.

- **copie Snapshot**

  Affiche les copies Snapshot existantes parmi lesquelles vous pouvez sélectionner un transfert.

- **Date de création**

  Affiche la date et l'heure de création de la copie Snapshot. Les copies Snapshot sont classées de la plus récente à la moins récente, la plus récente apparaissant en haut de la liste.

Si vous effectuez un transfert SnapVault et que vous souhaitez sélectionner une copie Snapshot existante à transférer d'une source vers une destination, le comportement de chaque opération est le suivant :

Opération	SnapVault comportement lors de la spécification d'une copie Snapshot	SnapVault comportement lors de la spécification d'une copie Snapshot dans une cascade
Initialiser	Transfère la copie Snapshot spécifiée.	La sélection de la copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.
Mise à jour	Transfère la copie Snapshot spécifiée.	La sélection de la 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 la 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, le comportement de chaque opération est le suivant :

Opération	SnapMirror comportement lors de la spécification d'une copie Snapshot	SnapMirror comportement lors de la spécification d'une copie Snapshot dans une cascade
Initialiser	Transfère toutes les copies Snapshot présentes sur la source, jusqu'à la copie Snapshot spécifiée.	La sélection de la copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.
Mise à jour	Transfère toutes les copies Snapshot présentes sur la source, jusqu'à la copie Snapshot spécifiée.	La sélection de la 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 copie Snapshot commune la plus récente.	La sélection de la copie Snapshot source n'est pas prise en charge pour les volumes de protection des données.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les tâches suivantes :

- **Soumettre**

  Soumet vos sélections et ferme la boîte de dialogue Sélectionner la copie Snapshot source.

- **Annuler**

  Annule vos sélections et ferme la boîte de dialogue Sélectionner la copie d'instantané source.

Inversion de la resynchronisation dans Active IQ Unified Manager

Lorsqu'une relation de protection est rompue parce que le volume source est désactivé et que la destination devient un volume en lecture/écriture, la resynchronisation inverse vous permet d'inverser le sens de la relation afin que la destination devienne la nouvelle source et la source la nouvelle destination.

Lorsqu'un sinistre rend inutilisable le volume source de votre relation de protection, vous pouvez utiliser le volume de destination pour servir les données en le convertissant en mode lecture/écriture, le temps de réparer ou de remplacer la source, de la mettre à jour et de rétablir la relation. Lors d'une opération de resynchronisation inverse, les données de la source plus récentes que celles de la copie Snapshot commune sont supprimées.

Avant la resynchronisation inverse

Affiche la source et la destination d'une relation avant une opération de resynchronisation inverse.

- **Volume source**

  Le nom et l'emplacement du volume source avant une opération de resynchronisation inverse.

- **Volume de destination**

  Le nom et l'emplacement du volume de destination avant une opération de resynchronisation inverse.

Après 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**

  Le nom et l'emplacement du volume de destination après une opération de resynchronisation inverse.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les actions suivantes :

- **Soumettre**

  Démarre le processus de resynchronisation inverse.

- **Annuler**

  Ferme la boîte de dialogue de resynchronisation inverse sans lancer d'opération de resynchronisation inverse.

Afficher la relation : vue Toutes les relations dans Active IQ Unified Manager

La vue « Relations : Toutes les relations » affiche des informations sur les relations de protection du système de stockage.

Par défaut, lorsque vous accédez à la page Relationships, le rapport affiché inclut les relations de protection de niveau supérieur pour les volumes et les machines virtuelles de stockage. Les commandes en haut de la page vous permettent de sélectionner une vue particulière, d'effectuer des recherches pour localiser des objets spécifiques, de créer et d'appliquer des filtres pour affiner la liste des données affichées, d'ajouter, de supprimer ou de réorganiser les colonnes de la page, et d'exporter les données de la page vers un fichier .csv, .pdf ou .xlsx. Après avoir personnalisé la page, vous pouvez enregistrer les résultats en tant que vue personnalisée, puis planifier la génération et l'envoi régulier par e-mail d'un rapport contenant ces données. Par défaut, lorsque vous sélectionnez le menu **Relationships**, le rapport affiché inclut les 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, par exemple seulement les volumes ou seulement les machines virtuelles de stockage. Le même rapport s'affiche dans la page Storage et uniquement pour l'entité de stockage sélectionnée. Si vous souhaitez afficher les relations de volumes ou de machines virtuelles de stockage, vous pouvez accéder à la page **Storage** > **Volumes** > **Relationship: All Relationships** ou à **Protection** > **Relationships** > **Relationship: All Relationships**, puis utiliser l'option **Relationship Object Type** dans le **Filter** pour filtrer uniquement les données des volumes ou des machines virtuelles de stockage.

La page Relations, qui répertorie toutes les relations de protection, comporte le lien **Afficher dans System Manager** pour le cluster de destination, ce qui vous permet de visualiser les mêmes objets dans ONTAP System Manager.

- **Statut**

  Affiche l'état actuel de la relation de protection.

  Le statut peut être Erreur (), Avertissement (), ou OK ().

- **VM de stockage source**

  Affiche le nom de la SVM source. Vous pouvez afficher plus de détails sur la SVM source en cliquant sur le nom de la SVM.

  Si une SVM existe sur le cluster mais n'a pas encore été ajoutée à l'inventaire de Unified Manager, ou si la SVM a été créée après la dernière actualisation du cluster, ce champ sera vide. Vous devez vous assurer que la SVM existe, ou effectuer une nouvelle découverte du cluster pour actualiser la liste des ressources.

- **Source**

  Affiche le volume source ou la machine virtuelle de stockage source protégés, selon votre sélection. Vous pouvez afficher plus de détails sur le volume source ou la machine virtuelle de stockage source en cliquant sur leur nom.

  Si le message `Resource-key not discovered` s'affiche, cela peut indiquer que le volume existe sur le cluster mais n'a pas encore été ajouté à l'inventaire de 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 de la SVM de destination. Vous pouvez afficher plus de détails sur la SVM de destination en cliquant sur son nom.

- **Destination**

  Affiche le nom du volume de destination ou de la machine virtuelle de stockage en fonction de votre sélection. Vous pouvez afficher plus de détails sur le volume de destination ou la machine virtuelle de stockage en cliquant sur le nom de l'objet correspondant.

- **Type d'objet de relation**

  Affiche le type d'objet utilisé dans la relation, comme une machine virtuelle de stockage, un volume ou un groupe de cohérence. Pour les objets d'une relation de cohérence, la source et les destinations de la relation affichent le groupe de cohérence, et si vous cliquez dessus, vous accédez à la page des LUN pour visualiser la relation.

- **Politique**

  Affiche le nom de la stratégie de protection pour 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 Normal ou Low. Les transferts avec la priorité Normal sont planifiés avant les transferts avec la priorité Low. La valeur par défaut est Normal.

- Ignorer le temps d'accès

  S'applique uniquement aux relations SnapVault. Ce paramètre indique si les transferts incrémentiels ignorent les fichiers dont seul le temps d'accès a été modifié. Les valeurs sont True ou False. La valeur par défaut est False.

- Quand une relation est désynchronisée

  Spécifie l'action qu'ONTAP effectue lorsqu'une relation synchrone ne peut pas être synchronisée. Les relations StrictSync restreignent l'accès au volume principal en cas d'échec de synchronisation avec le volume secondaire. Les relations Sync ne restreignent pas l'accès au volume principal en cas d'échec de synchronisation avec le volume secondaire.

- Limite de tentatives

  Spécifie le nombre maximal de tentatives pour chaque transfert manuel ou planifié d'une relation SnapMirror. La valeur par défaut est 8.

- Commentaires

  Fournit un champ de texte pour les commentaires spécifiques à la politique sélectionnée.

- Étiquette SnapMirror

  Spécifie l'étiquette SnapMirror de la première planification associée à la stratégie de copie Snapshot. L'étiquette SnapMirror est utilisée par le sous-système SnapVault lorsque vous sauvegardez des copies Snapshot vers une destination SnapVault.

- Paramètre de rétention

  Spécifie la durée de conservation des sauvegardes, en fonction du temps ou du nombre de sauvegardes.

- Copies Snapshot réelles

  Spécifie le nombre de copies Snapshot sur ce volume qui correspondent à l'étiquette spécifiée.

- Conserver les Snapshot Copies

  Indique le nombre de copies Snapshot SnapVault qui ne sont pas supprimées automatiquement même si la limite maximale de la stratégie est atteinte. Les valeurs sont True ou False. La valeur par défaut est False.

- Seuil d'avertissement de rétention

  Spécifie la limite de copies Snapshot à partir de laquelle un avertissement est envoyé pour indiquer que la limite de conservation maximale est presque atteinte.

- **Durée du décalage**

  Affiche le temps de décalage des données du miroir par rapport à la source.

  La durée du retard doit être proche de 0 seconde, voire égale à 0 seconde, pour les relations StrictSync.

- **État du retard**

Affiche l'état du retard pour les relations gérées et pour les relations non gérées auxquelles un planning est associé. L'état du retard peut être :

- Erreur

  La durée du retard est supérieure ou égale au seuil d'erreur de retard.

- Avertissement

  La durée du retard est supérieure ou égale au seuil d'alerte de retard.

- OK

  La durée du décalage est dans les limites normales.

- Non applicable

  Le statut de décalage n'est pas applicable aux relations synchrones car il est impossible de configurer une planification.

- **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 avec les parties prenantes**

  Indique si l'objet sélectionné contient des volumes.

- **Type de relation**

  Affiche le type de relation utilisé pour répliquer un volume. Les types de relations incluent :

  - Miroir asynchrone
  - Vault asynchrone
  - Asynchrone MirrorVault
  - StrictSync
  - Synchronisation

- **Statut du transfert**

  Affiche l'état du transfert pour la relation de protection. L'état du transfert peut être l'un des suivants :

  - Annulation en cours

    Les transferts SnapMirror sont activés ; cependant, une opération d'annulation de transfert pouvant inclure la suppression du point de contrôle est en cours.

  - Vérification

    Le volume de destination subit une vérification diagnostique 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 incrémentiels SnapVault.

- Inactif

  Les transferts sont activés et aucun transfert n'est en cours.

- Synchronisé

  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

  SnapMirror est activé pour les transferts. Le volume est actuellement dans la phase de pré-transfert pour les transferts incrémentiels SnapVault.

- En file d'attente

  SnapMirror les transferts sont activés. Aucun transfert n'est en cours.

- Suspendu

  Les transferts SnapMirror sont désactivés. Aucun transfert n'est en cours.

- Suspension

  Un transfert SnapMirror est en cours. Les transferts supplémentaires sont désactivés.

- Transfert

  SnapMirror est activé et un transfert est en cours.

- Transition

  Le transfert asynchrone des données du volume source vers le volume de destination est terminé et la transition vers un fonctionnement synchrone a commencé.

- En attente

  Un transfert SnapMirror a été lancé, mais certaines tâches associées sont en attente de mise en file d'attente.

- **Durée du dernier transfert**

  Affiche le temps nécessaire à l'achèvement du dernier transfert de données.

  La durée du transfert ne s'applique pas aux relations StrictSync, car le transfert doit être simultané.

- **Taille du dernier transfert**

  Affiche la taille, en octets, du dernier transfert de données.

La taille du transfert ne s'applique pas aux relations StrictSync.

- **Médiateurs**

  Affiche le statut du médiateur.

  - Non applicable

    Si le cluster ne prend pas en charge la synchronisation active SnapMirror.

  - Non configuré

    S'il n'est pas configuré, ou s'il est configuré mais que seul le cluster de destination est ajouté et que le cluster source n'est pas ajouté à Unified Manager.

  - Adresse IP du médiateur

    Si cela est configuré et que les clusters source et de destination sont tous deux ajoutés dans Unified Manager.

- **État**

  Affiche l'état de la relation SnapMirror ou SnapVault. L'état peut être Uninitialized, SnapMirrored ou Broken-Off. Si un volume source est sélectionné, l'état de la relation n'est pas applicable et n'est pas affiché.

- **Santé des relations**

  Affiche l'état de santé des relations au sein du cluster.

- **Raison de l'état non sain**

  La raison pour laquelle la relation est dans un état dégradé.

- **Priorité de transfert**

  Affiche la priorité d'exécution d'un transfert. La priorité du transfert est Normale ou Faible. Les transferts de priorité normale sont planifiés avant les transferts de priorité faible.

  La priorité de transfert ne s'applique pas aux relations synchrones car tous les transferts sont traités avec la même priorité.

- **Calendrier**

  Affiche le nom du calendrier de protection attribué à la relation.

  Ce calendrier ne s'applique pas aux relations synchrones.

- **Réplication flexible de version**

  Affiche soit Oui, Oui avec option de sauvegarde, soit Aucun.

- **Cluster source**

  Affiche le nom de domaine complet (FQDN), le nom court ou l'adresse IP du cluster source pour la relation SnapMirror.

- **Nom de domaine complet du cluster source**

  Affiche le nom du cluster source pour la relation SnapMirror.

- **Nœud source**

  Affiche le lien du nom du nœud source pour la relation SnapMirror d'un volume et affiche le lien du nombre de nœuds de la relation SnapMirror lorsque l'objet est une machine virtuelle de stockage ou un groupe de cohérence.

Dans la vue personnalisée, lorsque vous cliquez sur le lien du nom du nœud, vous pouvez afficher et étendre la protection des objets de stockage auxquels appartiennent les volumes de ces groupes de cohérence dans une relation de synchronisation active SnapMirror.

Lorsque vous cliquez sur le lien du nombre de nœuds, vous accédez à la page du nœud présentant les nœuds correspondants associés à cette relation. Si le nombre de nœuds est égal à 0, aucune valeur n'est affichée, car aucun nœud n'est associé à cette relation.

- **Nœud de destination**

  Affiche le lien du nom du nœud de destination pour la relation SnapMirror d'un volume et affiche le lien du nombre de nœuds de relation SnapMirror lorsque l'objet est une Storage VM ou un groupe de cohérence.

  Lorsque vous cliquez sur le lien du nombre de nœuds, vous accédez à la page du nœud présentant les nœuds correspondants associés à cette relation. Si le nombre de nœuds est égal à 0, aucune valeur n'est affichée, car aucun nœud n'est associé à cette relation.

- **Cluster de destination**

  Affiche le nom du cluster de destination pour la relation SnapMirror.

- **Nom de domaine complet du cluster de destination**

  Affiche le nom de domaine complet (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 de volume et de groupe de cohérence pour les clusters et l'ordre des machines virtuelles de stockage, notamment :

  - SnapMirror
  - DR de VM de stockage
  - SnapMirror, reprise après sinistre de la machine virtuelle de stockage
  - Groupe de cohérence
  - SnapMirror, groupe de cohérence.

Informations connexes

- Pour plus d'informations sur la vue **Relation : MetroCluster**, voir "Surveillance des MetroCluster configurations".
- Pour plus d'informations sur la vue **Relation : État des transferts du dernier mois**, voir "Relation : affichage du statut des transferts du dernier mois".

- Pour plus d'informations sur la vue **Relations : Toutes les relations**, voir "Relation : vue du taux de transfert du dernier mois".

Afficher la vue de l'état des transferts du dernier mois dans Active IQ Unified Manager

La vue « Relation : État des transferts du dernier mois » permet d'analyser les tendances de transfert sur une période donnée pour les volumes et les machines virtuelles de stockage dans des relations asynchrones. Cette page indique également si le transfert a réussi ou échoué.

Les commandes situées en haut de la page vous permettent d'effectuer des recherches pour localiser des objets spécifiques, de créer et d'appliquer des filtres pour affiner la liste des données affichées, d'ajouter, de supprimer ou de réorganiser les colonnes sur la page, et d'exporter les données de la page vers un fichier `.csv`, `.pdf`, ou `.xlsx`. Après avoir personnalisé la page, vous pouvez enregistrer les résultats en tant que vue personnalisée, puis planifier la génération et l'envoi régulier par e-mail d'un rapport de ces données. Vous pouvez utiliser l'option **Filter** pour afficher uniquement certains systèmes de stockage, par exemple seulement les volumes ou seulement les Storage VMs. Le même rapport s'affiche dans la page Storage et uniquement pour l'entité de stockage sélectionnée. Par exemple, si vous souhaitez afficher les relations de volume, vous pouvez accéder au rapport **Relationship: Last 1 Month Transfer Status** pour les Storage VMs, soit à partir du menu **Storage** > **Storage VMs** > **Relationship: Last 1 Month Transfer Status**, soit à partir du menu **Protection** > **Relationships** > **Relationship: Last 1 Month Transfer Status**, et utiliser **Filter** pour afficher uniquement les données relatives aux volumes.

- **Volume source**

  Affiche le nom du volume source.

- **Volume de destination**

  Affiche le nom du volume de destination.

- **Type d'opération**

  Affiche le type de transfert de volume.

- **Résultat de l'opération**

  Indique si le transfert de volume a réussi.

- **Heure de début du transfert**

  Affiche l'heure de début du transfert du 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 effectuer le transfert du 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 de la SVM de destination.

- **Cluster de destination**

  Affiche le nom du cluster de destination.

Informations connexes

- Pour plus d'informations sur la vue **Relations : Toutes les relations**, voir "Relation : vue Toutes les relations".
- Pour plus d'informations sur la vue **Relation :MetroCluster**, voir "Surveillance des MetroCluster configurations".
- Pour plus d'informations sur la vue **Relations : Toutes les relations**, voir "Relation : vue du taux de transfert du dernier mois".

Afficher la vue Taux de transfert du dernier mois de la relation dans Active IQ Unified Manager

La vue « Relationship: Last 1 month Transfer Rate » vous permet d'analyser la quantité de données transférée au quotidien pour les volumes dans des relations asynchrones. Cette page fournit également des détails sur les transferts quotidiens et le temps nécessaire pour effectuer l'opération de transfert pour les volumes et les Storage VMs.

Les commandes en haut de la page vous permettent d'effectuer des recherches pour localiser des objets spécifiques, de créer et d'appliquer des filtres pour affiner la liste des données affichées, d'ajouter, de supprimer ou de réorganiser les colonnes sur la page, et d'exporter les données de la page vers un fichier .csv, .pdf ou .xlsx. Après avoir personnalisé la page, vous pouvez enregistrer les résultats en tant que vue personnalisée, puis planifier la génération et l'envoi réguliers par e-mail d'un rapport sur ces données. Par exemple, si vous souhaitez afficher les relations de volume, vous pouvez accéder au menu **Storage** > **Volumes** > **Relationship: Last 1 Month Transfer Rate** ou au menu **Protection** > **Relationships** > **Relationships:Last 1 Month Transfer Rate**, puis utiliser le **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 la date.

Informations connexes

- Pour plus d'informations sur la vue **Relation :MetroCluster**, voir "Surveillance des MetroCluster configurations".
- Pour plus d'informations sur la vue **Relation : État des transferts du dernier mois**, voir "Relation : affichage du statut des transferts du dernier mois".
- Pour plus d'informations sur la vue **Relations : Toutes les relations**, consultez "Relation : vue du taux de transfert du dernier mois"

Générer des rapports personnalisés

Rapports Unified Manager

Découvrez les rapports d'Active IQ Unified Manager

Active IQ Unified Manager (anciennement OnCommand Unified Manager) permet de consulter, personnaliser, télécharger et planifier des rapports pour vos systèmes de stockage ONTAP. Les rapports peuvent fournir des détails sur la capacité, l'état, les performances, la sécurité et les relations de protection du système de stockage.

La nouvelle fonctionnalité de reporting et de planification introduite dans Active IQ Unified Manager 9.6 remplace le moteur de reporting précédent qui a été abandonné dans la version 9.5 de Unified Manager.

La fonction de reporting offre différentes vues de votre réseau, fournissant des informations exploitables sur la capacité, l'état, les performances, la sécurité et les données de protection. Vous pouvez personnaliser ces vues en affichant, masquant et réorganisant les colonnes, en filtrant et triant les données, et en effectuant des recherches dans les résultats. Vous pouvez enregistrer des vues personnalisées pour les réutiliser, les télécharger sous forme de rapports et programmer leur envoi régulier par e-mail.

Vous pouvez télécharger les vues au format Microsoft® Excel et les personnaliser. Vous pouvez utiliser des fonctionnalités Excel avancées, telles que les tris complexes, les filtres multicouches, les tableaux croisés dynamiques et les graphiques. Lorsque vous êtes satisfait du rapport Excel obtenu, vous pouvez importer le fichier Excel afin de l'utiliser chaque fois que le rapport est planifié et partagé.

Outre la génération de rapports à partir de l'interface utilisateur, vous pouvez extraire de Unified Manager des données de santé, de sécurité et de performances à l'aide de ces méthodes supplémentaires :

- Utilisation de la connectivité ODBC (Open Database Connectivity) et des outils ODBC pour accéder directement à la base de données et obtenir des informations sur le cluster
- Exécution des API REST d'Unified Manager pour obtenir les informations que vous souhaitez consulter

Cette version d'Active IQ Unified Manager apporte les améliorations suivantes aux rapports :

- Un courriel contenant un rapport est envoyé selon la planification configurée. Même si vous générez un rapport à la demande, vous recevrez un courriel.
- Le nom du fichier du rapport et les métadonnées du rapport incluent le nom d'hôte à partir duquel le rapport a été généré. Grâce à cette amélioration, même si le nom du fichier est modifié, vous pouvez toujours identifier le nom d'hôte à partir duquel le rapport a été généré.

Points d'accès pour générer des rapports

Découvrez trois façons d'accéder aux fonctionnalités de reporting dans Active IQ Unified Manager

Vous pouvez collecter des informations dans Unified Manager sur vos clusters afin de créer des rapports à partir de l'interface utilisateur, de requêtes de base de données MySQL et des API REST.

Ces sections décrivent la génération de rapports et la planification dans Unified Manager via l'interface utilisateur.

Il existe trois façons d'accéder aux fonctionnalités de création de rapports fournies par Unified Manager :

- Extraction des données directement à partir des pages d'inventaire de l'interface utilisateur.
- Utilisation de Open Database Connectivity (ODBC) et des outils ODBC pour accéder à tous les objets disponibles.
- Exécution des API REST d'Unified Manager pour obtenir les informations que vous souhaitez consulter.

Ces sections décrivent la génération de rapports et la planification dans Unified Manager via l'interface utilisateur.

Accédez aux bases de données pour la création de rapports personnalisés dans Active IQ Unified Manager

Unified Manager utilise une base de données MySQL pour stocker les données des clusters qu'il surveille. Les données sont enregistrées dans différents schémas de la base de données MySQL.

Toutes les données tabulaires des bases de données suivantes sont disponibles :

Base de données	Description
netapp_model	Données relatives aux objets sur les contrôleurs ONTAP.
netapp_model_view	Données relatives aux objets sur les contrôleurs ONTAP, adaptées à l'utilisation d'outils de reporting.
netapp_performance	Compteurs de performances spécifiques au cluster.
ocum	Données et informations de l'application Unified Manager pour la prise en charge du filtrage, du tri et du calcul de certains champs dérivés de l'interface utilisateur.
ocum_report	Données relatives à la configuration de l'inventaire et aux informations sur les capacités.
ocum_report_birt	Vues des données de configuration de l'inventaire et de capacité, adaptées à l'utilisation d'outils de reporting.
opm	Paramètres de configuration des performances et informations sur les seuils.
scalemonitor	Données relatives à l'état et aux problèmes de performances de l'application Unified Manager.
vmware_model	Données d'objets VMware pour les banques de données hébergées sur le stockage NetApp.
vmware_model_view	Vues des données d'objets VMware pour les datastores hébergés sur le stockage NetApp, adaptées à l'utilisation d'outils de reporting.
vmware_performance	Données des compteurs de performance VMware pour les banques de données hébergées sur le stockage NetApp.

Un utilisateur de reporting, c'est-à-dire un utilisateur de base de données disposant du rôle « Schéma de rapport », peut accéder aux données de ces tables. Cet utilisateur dispose d'un accès en lecture seule aux vues de reporting et aux 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'identifiant du cluster.

Utilisez les API REST d'Active IQ Unified Manager pour la génération de rapports

Vous pouvez utiliser les API REST pour faciliter la gestion de vos clusters en consultant les informations relatives à leur état, leur capacité, leurs performances et leur sécurité, enregistrées par Unified Manager.

Les API REST sont accessibles via la page web Swagger. Vous pouvez accéder à la page web Swagger pour afficher la documentation de l'API REST de Unified Manager, ainsi que pour effectuer manuellement un appel d'API. Dans l'interface utilisateur web de Unified Manager, dans la barre de menus, cliquez sur le bouton **Help**, puis sélectionnez **API Documentation**. Pour plus d'informations sur les API REST de Unified Manager, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

Vous devez disposer du rôle d'opérateur, d'administrateur de stockage ou d'administrateur d'application pour accéder aux API REST.

Comprendre les rapports dans Active IQ Unified Manager

Les rapports affichent des informations détaillées sur le stockage, le réseau, la qualité de service et les relations de protection, vous aidant ainsi à identifier et à résoudre les problèmes potentiels avant qu'ils ne surviennent.

Lorsque vous personnalisez une vue, vous pouvez l'enregistrer sous un nom unique pour une utilisation ultérieure. Vous pouvez programmer l'exécution régulière d'un rapport basé sur cette vue et le partager avec d'autres. Vous pouvez également télécharger la vue au format Excel pour la personnaliser à l'aide des fonctionnalités avancées d'Excel, puis importer ce fichier dans Unified Manager. Si vous programmez un rapport à partir de cette vue, celui-ci utilisera le fichier Excel importé pour générer des rapports robustes que vous pourrez partager.

Vous pouvez gérer tous les rapports programmés depuis la page « Planification des rapports ».

> Vous devez disposer du rôle d'administrateur d'applications ou d'administrateur de stockage pour gérer les rapports.

Vous pouvez télécharger les rapports sous forme de fichiers CSV (valeurs séparées par des virgules), Excel ou PDF.

Comprendre la relation entre la vue et le rapport dans Active IQ Unified Manager

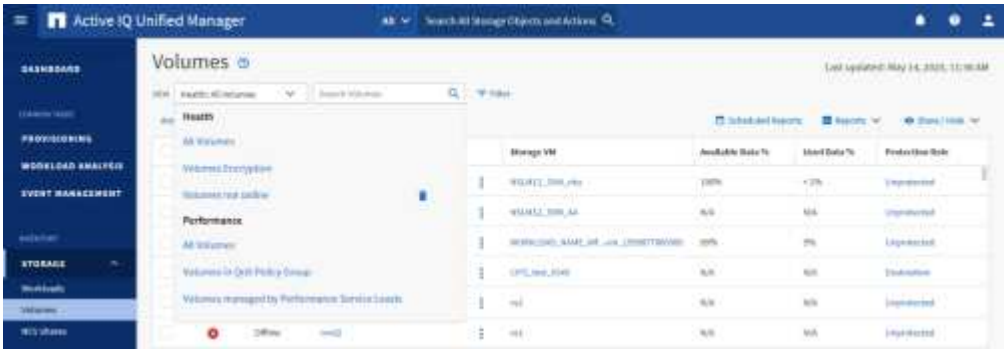
Les pages de visualisation et d'inventaire se transforment en rapports lorsque vous les téléchargez ou les planifiez.

Vous pouvez personnaliser et enregistrer les vues et les pages d'inventaire pour les réutiliser. Presque tout ce que vous pouvez visualiser dans Unified Manager peut être enregistré, réutilisé, personnalisé, programmé et partagé sous forme de rapport.

Dans le menu déroulant « Vue », les éléments comportant l'icône de suppression correspondent aux vues

personnalisées existantes que vous ou un autre utilisateur avez créées. Les éléments sans icône sont les vues par défaut fournies avec Unified Manager. Ces vues par défaut ne peuvent être ni modifiées ni supprimées.

- Si vous supprimez une vue personnalisée de la liste, cela supprime également tous les fichiers Excel ou rapports planifiés qui utilisent cette vue.
- Si vous modifiez une vue personnalisée, les rapports qui utilisent cette vue refléteront la modification lors de leur prochaine génération et de leur envoi par e-mail conformément à la planification des rapports. Lorsque vous modifiez des vues, assurez-vous que vos modifications sont compatibles avec les personnalisations Excel associées utilisées pour les rapports. Si nécessaire, vous pouvez mettre à jour le fichier Excel en le téléchargeant, en apportant les modifications requises, puis en le chargeant comme nouvelle personnalisation Excel pour la vue.



Seuls les utilisateurs ayant le rôle d'administrateur d'application ou d'administrateur de stockage peuvent voir l'icône de suppression, modifier ou supprimer une vue, ou modifier ou supprimer un rapport planifié.

Découvrez les différents types de rapports dans Active IQ Unified Manager

Ce tableau fournit une liste exhaustive 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 de stockage ou de réseau
Capacité	Groupes Agrégats Volumes Qtrees

Type	objet de stockage ou de réseau
Santé	Groupes Nœuds Agrégats Machines virtuelles de stockage Volumes Partages SMB/CIFS Partages NFS
Performances	Groupes Nœuds Agrégats Machines virtuelles de stockage Volumes LUN Espaces de noms NVMe Interfaces réseau (LIFs) Ports
Qualité de service	Groupes de politiques QoS traditionnels Groupes de politiques QoS adaptatives groupes de règles de niveau de service de performances
Relations de protection des volumes (disponibles sur la page Volumes)	Toutes les relations État du transfert du dernier mois Taux de transfert du dernier mois
Sécurité	Machines virtuelles de stockage Groupes

Comprendre les limitations de reporting dans Active IQ Unified Manager

Il existe certaines limitations concernant la nouvelle fonctionnalité de génération de rapports d'Active IQ Unified Manager dont vous devez être conscient.

Rapports existants des versions précédentes d'Unified Manager

Vous pouvez uniquement modifier la planification et les destinataires des rapports existants qui ont été créés et importés (sous forme de fichiers .rptdesign) dans Unified Manager 9.5 et les versions antérieures. Si vous avez personnalisé l'un des rapports standard fournis avec Unified Manager 9.5 ou une version antérieure, ces rapports personnalisés ne sont pas importés dans le nouvel outil de création de rapports.

Si vous devez modifier des rapports existants importés à partir de fichiers .rptdesign, effectuez l'une des opérations suivantes et supprimez le rapport importé :

- Créez une nouvelle vue et planifiez un rapport à partir de cette vue (méthode recommandée)
- Survolez le rapport, copiez le code SQL et récupérez les données à l'aide d'un outil externe

Les vues par défaut peuvent être générées sous forme de rapports sans aucune personnalisation. Vous pouvez utiliser la nouvelle solution de reporting pour recréer tout rapport personnalisé.

Planification et relation de rapport

Vous pouvez créer plusieurs planifications différentes avec n'importe quelle combinaison de destinataires pour chaque rapport enregistré. Cependant, vous ne pouvez pas réutiliser une même planification pour plusieurs rapports.

Protection des rapports

Tout utilisateur disposant des autorisations appropriées peut modifier ou supprimer des rapports. Il est impossible d'empêcher d'autres utilisateurs de supprimer ou de modifier les vues ou les planifications enregistrées.

Rapports d'événements

Bien que vous puissiez personnaliser l'affichage des événements et télécharger le rapport résultant au format CSV, vous ne pouvez pas programmer la génération et la distribution de rapports d'événements récurrents.

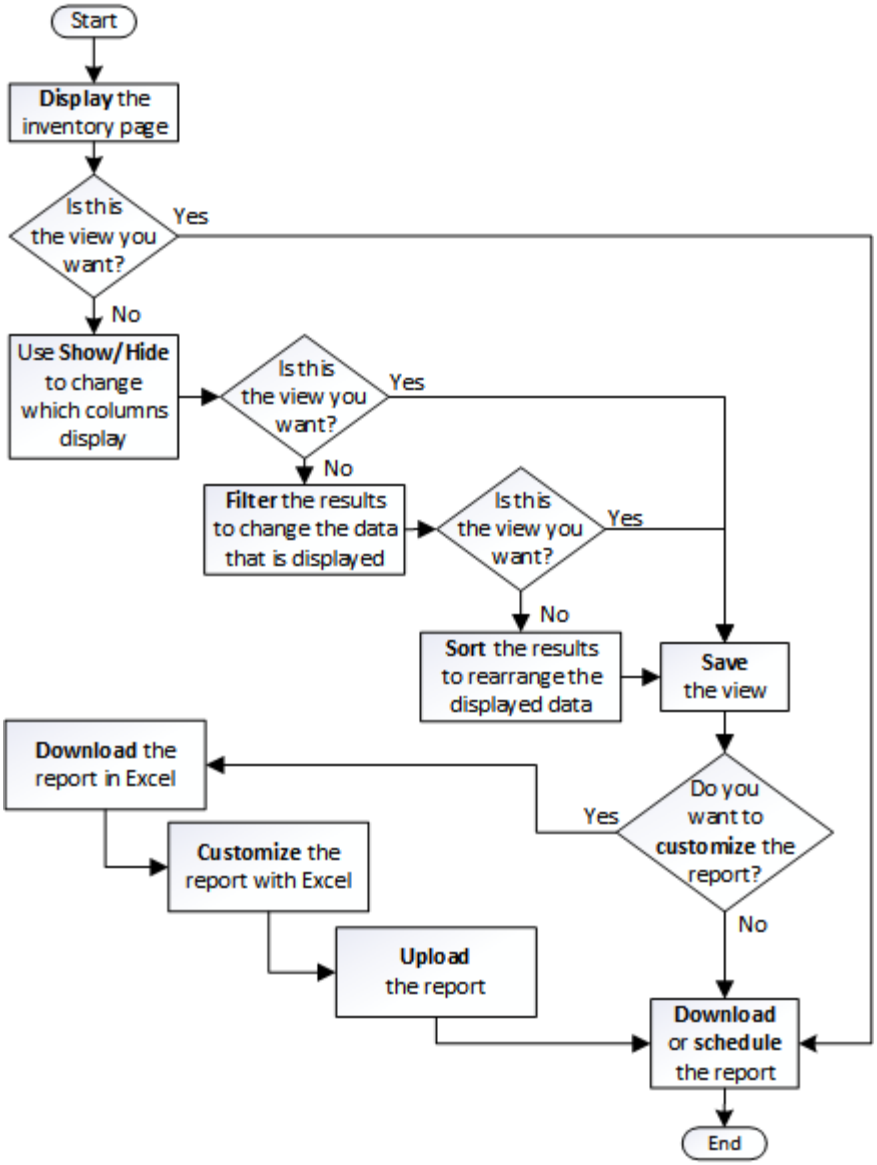
Pièces jointes au rapport

Les rapports ne peuvent pas être inclus dans le corps d'un courriel. À la place, les rapports sont uniquement envoyés en pièces jointes aux formats PDF, Excel ou CSV.

Travailler avec des rapports

Comprendre les flux de travail des rapports dans Active IQ Unified Manager

Arbre de décision décrivant le flux de travail du rapport.



Commencez à créer des rapports dans Active IQ Unified Manager

Créez un exemple de rapport personnalisé pour vous familiariser avec l'exploration des vues et la planification des rapports. Ce rapport de démarrage rapide identifie une liste de volumes que vous pourriez vouloir déplacer vers le niveau cloud, car ils contiennent une quantité importante de données inactives (froides). Vous ouvrirez la vue Performance: All Volumes, la personnaliserez à l'aide de filtres et de colonnes, enregistrerez la vue personnalisée en tant que rapport et planifierez son partage une fois par semaine.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré des agrégats FabricPool et avoir des volumes sur ces agrégats.

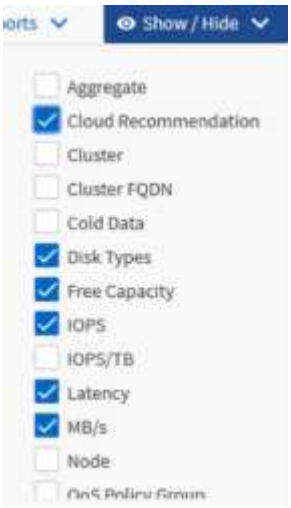
Suivez les étapes ci-dessous pour :

- Ouvrez la vue par défaut

- Personnalisez les colonnes en filtrant et en triant les données
- Enregistrer la vue
- Planifiez la génération d'un rapport pour la vue personnalisée

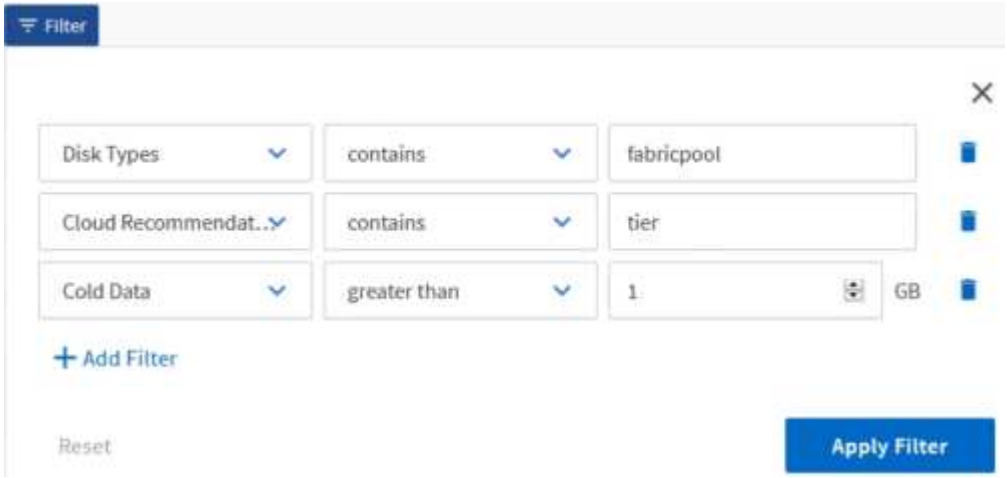
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Performances** > **Tous les volumes**.
3. Cliquez sur **Afficher/Masquer** pour vous assurer que la colonne "Types de disques" apparaît dans la vue.



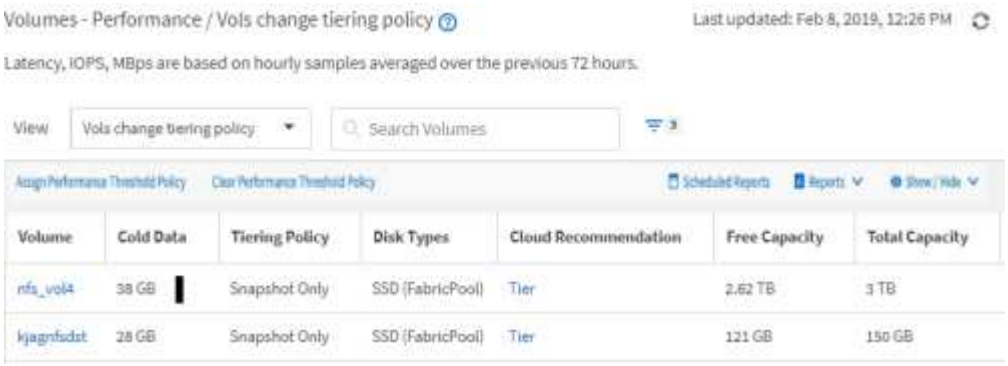
Ajoutez ou supprimez d'autres colonnes pour créer une vue contenant les champs importants pour votre rapport.

4. Faites glisser la colonne « `Disk Types` » à côté de la colonne « `Cloud Recommendation` ».
5. Cliquez sur l'icône de filtre pour ajouter les trois filtres suivants, puis cliquez sur **Appliquer le filtre**:
   - Types de disques contient FabricPool
   - La recommandation Cloud contient un niveau
   - Données froides supérieures à 10 Go



Notez que chaque filtre est combiné avec un ET logique afin que tous les volumes renvoyés répondent à tous les critères. Vous pouvez ajouter jusqu'à cinq filtres.

6. Cliquez en haut de la colonne « Données froides » pour trier les résultats afin que les volumes contenant le plus de données froides apparaissent en haut de la vue.
7. Lorsque la vue est personnalisée, son nom est « Vue non enregistrée ». Nommez la vue de façon à refléter ce qu'elle affiche, par exemple « `Vols change tiering policy` ». Lorsque vous avez terminé, cliquez sur la coche ou appuyez sur **Enter** pour enregistrer la vue sous son nouveau nom.



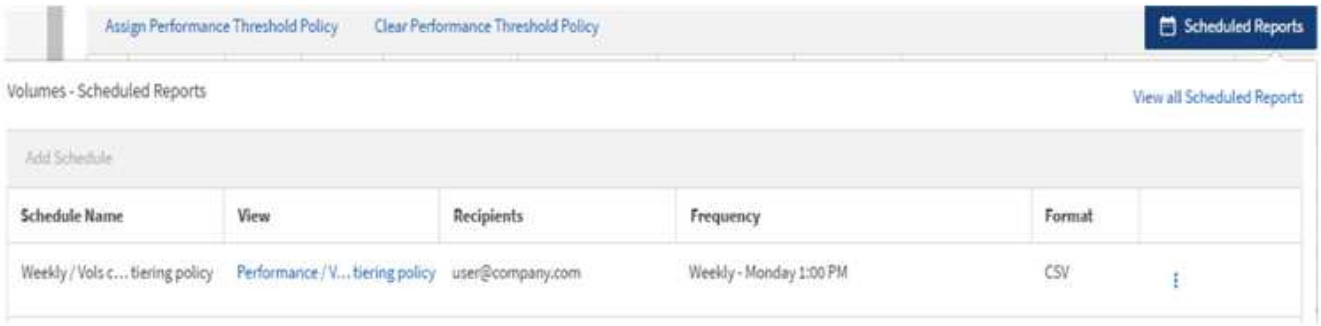
8. Téléchargez le rapport au format **CSV**, **Excel** ou **PDF** pour visualiser le résultat avant de le programmer ou de le partager.

   Ouvrez le fichier avec une application installée, telle que Microsoft Excel (CSV ou Excel) ou Adobe Acrobat (PDF), ou enregistrez le fichier.

   > Vous pouvez personnaliser davantage votre rapport à l'aide de filtres complexes, de tris, de tableaux croisés dynamiques ou de graphiques en téléchargeant la vue sous forme de fichier Excel. Après avoir ouvert le fichier dans Excel, utilisez les fonctionnalités avancées pour personnaliser votre rapport. Lorsque vous êtes satisfait, téléchargez le fichier Excel. Ce fichier, avec ses personnalisations, est appliqué à la vue lors de l'exécution du rapport.

   Pour plus d'informations sur la personnalisation des rapports à l'aide d'Excel, consultez *Exemples de rapports Microsoft Excel*.

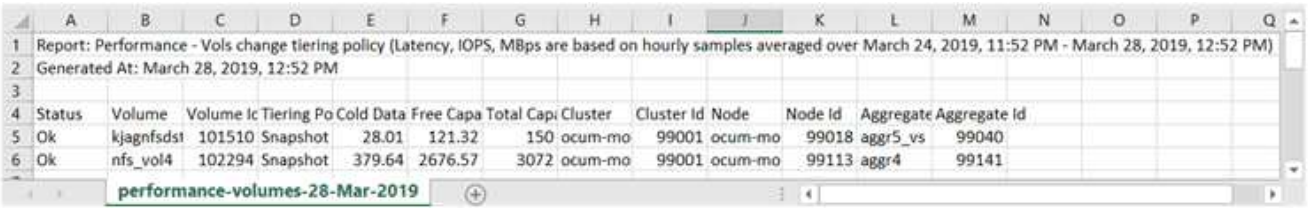
9. Cliquez sur le bouton **Rapports planifiés** sur la page d'inventaire. Tous les rapports planifiés relatifs à l'objet, ici les volumes, apparaissent dans la liste.



10. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page « Planifications des rapports » afin que vous puissiez définir les caractéristiques de la planification du nouveau rapport.
11. Saisissez un nom pour le rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

Le rapport d'exemple 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 Cap	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

Le rapport d'exemple 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								
Ok								

En fonction des résultats présentés dans le rapport, vous pouvez utiliser ONTAP System Manager ou ONTAP CLI pour modifier la stratégie de hiérarchisation en « `auto` » ou « `all` » pour certains volumes afin de décharger davantage de données froides vers le niveau cloud.

Recherchez un rapport planifié dans Active IQ Unified Manager

Vous pouvez rechercher les rapports planifiés par nom, nom de vue, type d'objet ou destinataires.

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Planification des rapports**.
2. Utilisez le champ de texte **Rechercher les rapports planifiés**.

Pour trouver des rapports par …	Essayez …
Nom de la planification	Saisissez une partie du nom du calendrier du rapport.
Nom de la vue	Saisissez une partie du nom de la vue du 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 l'en-tête d'une colonne pour trier les rapports par ordre croissant ou décroissant selon cette colonne, par exemple par nom de planification ou par format.

Personnaliser les rapports

Personnalisez les rapports dans Active IQ Unified Manager

Il existe de nombreuses façons de personnaliser les vues afin de créer un rapport contenant toutes les informations dont vous avez besoin pour gérer vos clusters ONTAP.

Commencez 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 les triant sur une colonne spécifique par ordre croissant ou décroissant.

À partir de Unified Manager 9.8, vous pouvez également télécharger la vue au format Excel pour la personnaliser à l'aide de fonctionnalités avancées. Une fois la personnalisation terminée, importez le fichier Excel personnalisé. Si vous planifiez un rapport à partir de cette vue, celui-ci utilisera le fichier Excel personnalisé pour générer des rapports robustes que vous pourrez partager.

Pour plus d'informations sur la personnalisation des rapports à l'aide d'Excel, consultez *Exemples de rapports Microsoft Excel*.

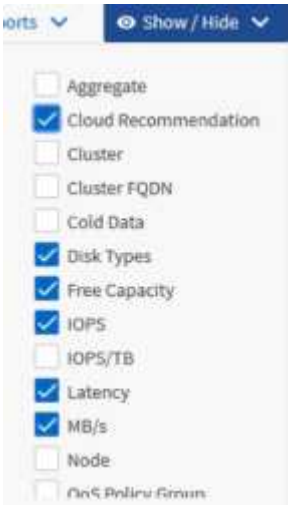
Vous devez disposer du rôle d'administrateur d'applications ou d'administrateur de stockage pour gérer les rapports.

Personnaliser les colonnes d'un rapport dans Active IQ Unified Manager

Utilisez **Afficher/Masquer** pour sélectionner les colonnes à inclure dans votre rapport. Faites glisser les colonnes sur la page d'inventaire pour les réorganiser.

Étapes

1. Cliquez sur **Afficher/Masquer** pour ajouter ou supprimer des colonnes.



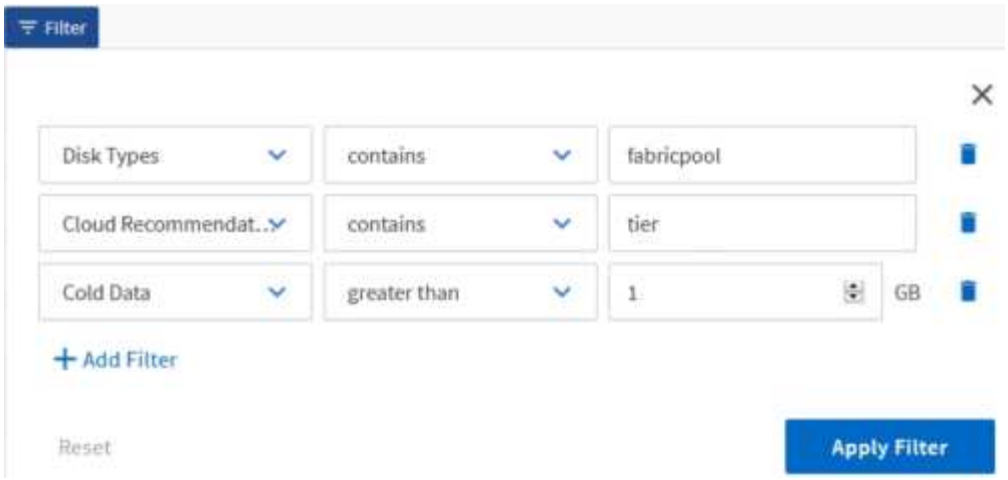
2. Sur la page d'inventaire, faites glisser les colonnes pour les réorganiser dans l'ordre souhaité dans votre rapport.
3. Donnez un nom à la vue non enregistrée pour enregistrer vos modifications.

Filtrer les données dans Active IQ Unified Manager

Filtrez les données pour 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 et affiner les résultats que vous souhaitez afficher, puis cliquez sur **Appliquer le filtre**.



2. Donnez un nom à la vue non enregistrée pour enregistrer vos modifications.

Trier les données dans Active IQ Unified Manager

Pour trier les résultats, cliquez sur une colonne et indiquez l'ordre croissant ou décroissant. Le tri des données permet de prioriser les informations nécessaires à votre rapport.

Étapes

1. Cliquez en haut d'une colonne pour trier les résultats afin que les informations les plus importantes apparaissent en haut de la vue.
2. Donnez un nom à la vue non enregistrée pour enregistrer vos modifications.

Recherchez pour affiner votre affichage dans Active IQ Unified Manager

Une fois que vous avez obtenu l'affichage souhaité, vous pouvez affiner les résultats à l'aide du champ de recherche afin de vous concentrer sur les résultats que vous souhaitez inclure dans le rapport.

Étapes

1. Ouvrez la vue personnalisée ou par défaut que vous souhaitez utiliser comme base pour votre rapport.
2. Saisissez du texte dans le champ de recherche pour affiner les données répertoriées dans la vue. Vous pouvez saisir des données partielles dans n'importe laquelle des colonnes affichées. Par exemple, si vous souhaitez rechercher les nœuds dont le nom contient « US_East », vous pouvez affiner la liste complète des nœuds.

   Les résultats de votre recherche sont enregistrés dans la vue personnalisée et utilisés dans le rapport programmé généré.

3. Donnez un nom à la vue non enregistrée pour enregistrer vos modifications.

Utilisez Excel pour personnaliser votre rapport dans Active IQ Unified Manager

Une fois la vue enregistrée, vous pouvez la télécharger au format classeur Excel (.xlsx). À l'ouverture du fichier Excel, vous pouvez utiliser les fonctionnalités avancées d'Excel pour personnaliser votre rapport.

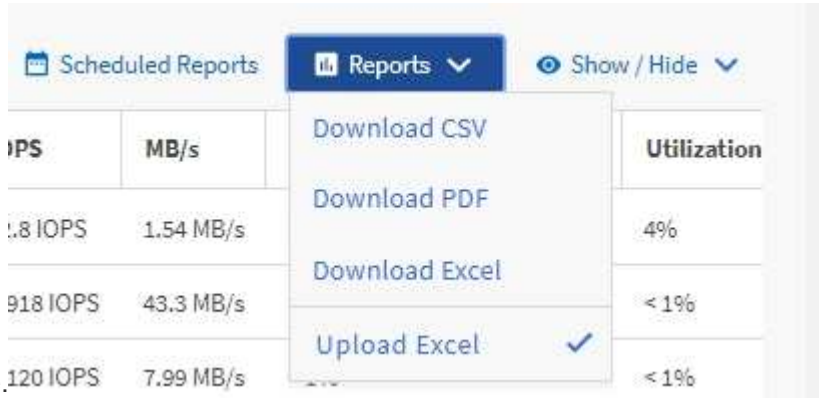
Avant de commencer

Vous pouvez uniquement téléverser un fichier de classeur Excel avec l'extension .xlsx.

Par exemple, voici quelques fonctionnalités avancées d'Excel que vous pouvez utiliser dans votre rapport :

- Tri multicolonnes
- Filtrage complexe
- Tableaux croisés dynamiques
- Graphiques

- Le fichier Excel téléchargé utilise le nom de fichier par défaut de la vue, et non le nom que vous avez enregistré.
  - Le format est `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Par exemple, une vue personnalisée enregistrée nommée `Volumes-not online`a pour nom de fichier `health-volumes-05-May-2020-19-18-00.xlsx`si elle est enregistrée à cette date et à cette heure.
- Vous pouvez ajouter des feuilles au fichier Excel, mais ne modifiez pas les feuilles existantes.
  - Ne modifiez pas les feuilles, les données et les informations existantes. Copiez plutôt les données sur une nouvelle page que vous créerez.
  - Une exception à la règle ci-dessus est que vous pouvez créer des formules sur la page « `data` ». Utilisez les formules de la page data pour créer des graphiques sur de nouvelles pages.
  - Ne nommez pas une nouvelle feuille data ou info.
- Si un fichier Excel personnalisé existe, une coche apparaît à côté de l'élément de menu **Rapports** > **Téléverser 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 pour votre rapport.
2. Sélectionnez **Reports** > **Download Excel**.
3. Enregistrez le fichier. Le fichier est enregistré dans votre dossier Téléchargements.
4. Ouvrez le fichier enregistré dans Excel. Ne déplacez pas le fichier vers un nouvel emplacement ou, si vous travaillez dans un autre emplacement, enregistrez-le de nouveau à son emplacement d'origine en utilisant

le nom de fichier d'origine avant de téléverser le fichier.

5. Personnalisez le fichier à l'aide des fonctionnalités d'Excel, telles que les tris complexes, les filtres multicouches, les tableaux croisés dynamiques ou les graphiques. Pour plus d'informations, consultez la documentation Microsoft® Excel.
6. Sélectionnez **Rapports** > **Importer un fichier Excel** et choisissez le fichier que vous avez modifié. Le fichier téléchargé le plus récemment est importé depuis le même emplacement.
7. Envoyez-vous un rapport de test à l'aide de la fonctionnalité **Rapports programmés**.

Téléchargez les rapports dans Active IQ Unified Manager

Vous pouvez télécharger des rapports et enregistrer les données sur un lecteur local ou réseau en tant que fichier CSV (valeurs séparées par des virgules), fichier Microsoft Excel (.XLSX) ou fichier PDF. Vous pouvez ouvrir les fichiers CSV et XLSX avec des applications de feuille de calcul, telles que Microsoft Excel, et les fichiers PDF avec des lecteurs tels qu'Adobe Acrobat.

Étapes

1. Cliquez sur le bouton **Reports** pour télécharger le rapport dans l'un des formats suivants :

Choisir	À…
Télécharger CSV	Enregistrez le rapport sous forme de fichier de valeurs séparées par des virgules (CSV).
Télécharger PDF	Enregistrez le rapport au format .pdf.
Télécharger Excel	Enregistrez le rapport au format Microsoft Excel (XLSX).

Programmer des rapports

Planifiez des rapports dans Active IQ Unified Manager

Une fois que vous disposez d'une vue que vous souhaitez réutiliser et partager sous forme de rapport, vous pouvez la planifier à l'aide d'Active IQ Unified Manager. Vous pouvez gérer les rapports planifiés, en modifiant les destinataires et la fréquence de distribution pour chaque planification de rapport.

Vous pouvez programmer 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 au format CSV, mais vous ne pouvez pas programmer leur régénération ni leur partage. Vous ne pouvez pas non plus télécharger ni programmer les tableaux de bord, les favoris ou les pages de configuration.

À partir d'Active IQ Unified Manager 9.8, vous pouvez télécharger des vues au format Microsoft® Excel et les personnaliser. Vous pouvez utiliser des fonctionnalités Excel avancées telles que les tris complexes, les filtres multicouches, les tableaux croisés dynamiques et les graphiques. Une fois satisfait du rapport Excel obtenu, vous pouvez importer le fichier Excel pour l'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, soit CSV, PDF ou XSLX. Lorsque vous programmez un rapport pour la première fois, vous pouvez le télécharger et vous désigner comme seul destinataire pour voir le rapport tel que vos

destinataires le verront.

Planifier un rapport

Planifiez un rapport dans Active IQ Unified Manager

Une fois que vous disposez d'une vue ou d'un fichier Excel que vous souhaitez programmer pour une génération et une distribution régulières, vous pouvez programmer le rapport.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré les paramètres du serveur SMTP sur la page **Général** > **Notifications** afin que le moteur de génération de rapports puisse envoyer des rapports sous forme de pièces jointes par e-mail à la liste des destinataires depuis le serveur Unified Manager.
- Le serveur de messagerie doit être configuré pour autoriser l'envoi de pièces jointes avec les e-mails générés.

Suivez les étapes ci-dessous pour tester et planifier la génération d'un rapport pour une vue donnée. Sélectionnez ou personnalisez la vue que vous souhaitez utiliser. La procédure suivante utilise une vue réseau qui affiche les performances de vos interfaces réseau, mais vous pouvez utiliser n'importe quelle vue de votre choix.

Étapes

1. Ouvrez la vue. Cet exemple utilise la vue réseau par défaut qui affiche les performances des LIF. Dans le volet de navigation de gauche, cliquez sur **Réseau > Interfaces réseau**.
2. Personnalisez l'affichage selon vos besoins grâce aux fonctionnalités intégrées de Unified Manager.
3. Après avoir personnalisé l'affichage, vous pouvez lui attribuer 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, consultez "Utiliser Excel pour personnaliser votre rapport".
5. Pour visualiser le résultat avant de le programmer ou de le partager:

Option	Description
Si vous avez utilisé Excel pour personnaliser le rapport	Consultez le fichier Excel déjà téléchargé.
Si vous n'avez pas utilisé Excel pour personnaliser le rapport	Téléchargez le rapport au format **CSV**, **PDF** ou **XLSX**.

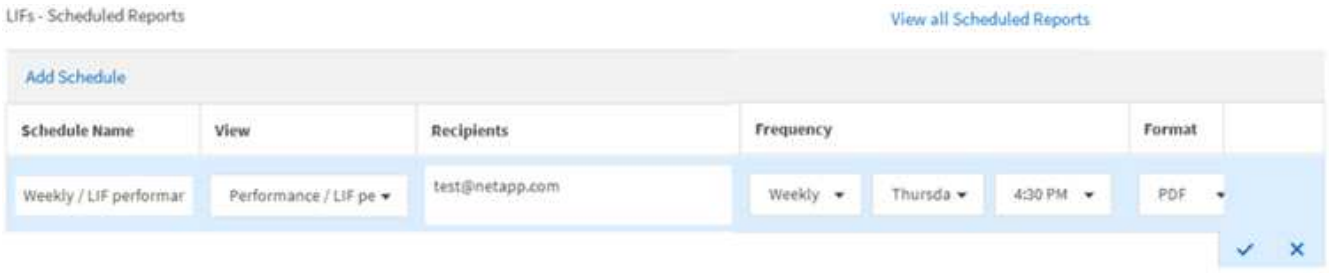
   Ouvrez le fichier avec une application installée, telle que Microsoft Excel (CSV/XSLX) ou Adobe Acrobat (PDF).

6. Si le rapport vous convient, cliquez sur **Rapports programmés**.

7. Sur la page « Planification des rapports », cliquez sur **Ajouter une planification**.
8. Acceptez le nom par défaut, qui est une combinaison du nom de la vue et de la fréquence, ou personnalisez le **nom de la planification**.
9. Pour tester le rapport programmé la première fois, ajoutez uniquement vous-même comme **destinataire**. Une fois satisfait, ajoutez les adresses électroniques de tous les destinataires du rapport.
10. Indiquez 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 dont vous avez personnalisé le contenu à l'aide d'Excel, sélectionnez toujours **XSLX**.

12. Cliquez sur la coche (✓) pour enregistrer la planification du rapport.



Le rapport est envoyé immédiatement à titre de test. Ensuite, il est généré et envoyé par courriel aux destinataires indiqués selon la fréquence programmée.

Planifiez l'importation des rapports .rptdesign dans Active IQ Unified Manager

Vous pouvez planifier des rapports existants créés et importés dans une version antérieure d'Unified Manager.

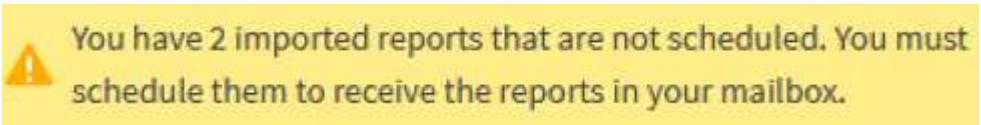
La planification des rapports importés nécessite les éléments suivants :

- rapports de fichiers .rptdesign conçus dans BIRT importés dans une version antérieure de Unified Manager
- applicable lors de la mise à niveau vers Unified Manager 9.6 GA ou version ultérieure

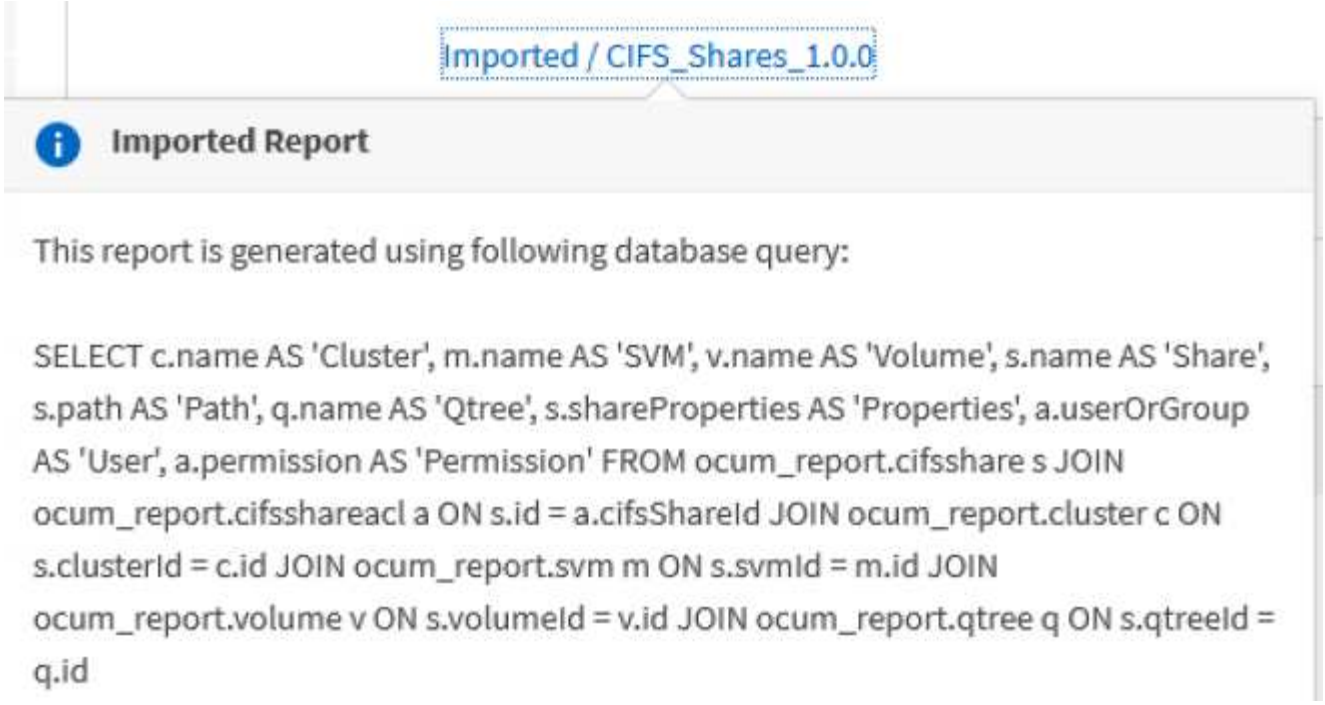
Après la mise à niveau vers Unified Manager 9.6 GA ou une version ultérieure, la page « Planification des rapports » affiche les rapports importés. Vous pouvez modifier la planification de ces rapports afin de spécifier les adresses e-mail des destinataires, la fréquence et le format (PDF ou CSV). Sinon, ces rapports ne peuvent être ni modifiés ni consultés dans l'interface utilisateur de Unified Manager.

Étapes

1. Ouvrez la page « Planification des rapports ». 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 les rapports indésirables à partir de l'icône Plus ⋮.

Gérer les planifications de rapports

Gérer les calendriers de rapports dans Active IQ Unified Manager

Vous pouvez gérer vos planifications de rapports depuis la page « Planifications de rapports ». Vous pouvez consulter, modifier ou supprimer les planifications existantes.

ⓘ **Avant de commencer**

Il n'est pas possible de programmer de nouveaux rapports depuis la page « Planification des rapports ». Vous pouvez uniquement ajouter des rapports planifiés depuis les pages d'inventaire des objets.

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Planification des rapports**.
2. Sur la page des planifications de rapports:

Si vous voulez…	Ensuite…
Afficher une planification existante	Parcourez la liste des rapports existants à l'aide des barres de défilement et des commandes de page.

Si vous voulez…	Ensuite…
Modifier une planification existante	a. Cliquez sur l'icône Plus ⋮ pour la planification 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 ⋮ pour la planification que vous souhaitez utiliser. b. Cliquez sur **Delete**. c. Confirmez votre décision.

Modifier les rapports planifiés dans Active IQ Unified Manager

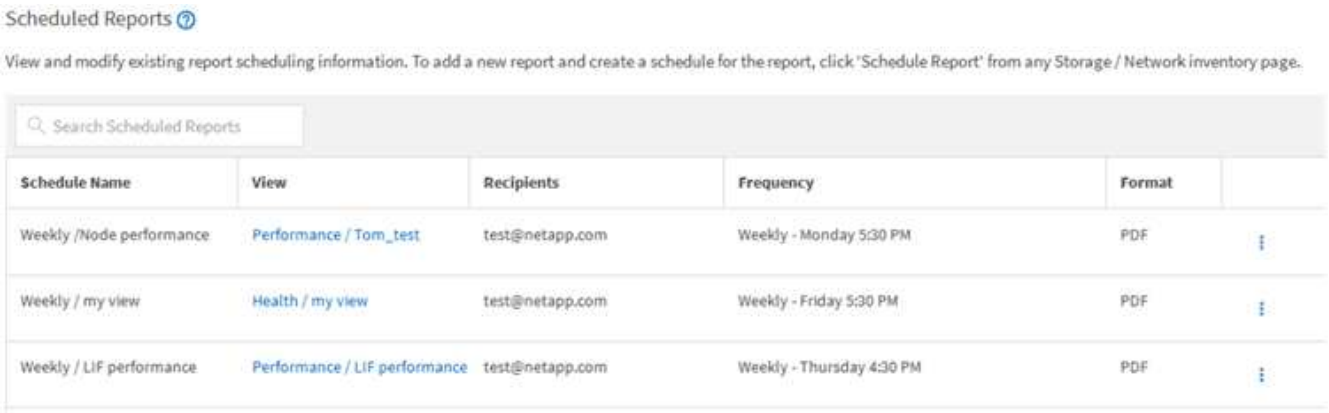
Une fois les rapports programmés, vous pouvez les modifier sur la page « Programmation des rapports ».

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Planification des rapports**.



> Si vous disposez des autorisations appropriées, vous pouvez modifier n'importe quel rapport et sa planification dans le système.

2. Cliquez sur l'icône Plus ⋮ pour l'horaire que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Vous pouvez modifier le **Nom de la planification**, la **liste des destinataires**, la **Fréquence** et le **Format** de la planification du rapport.
5. Une fois terminé, cliquez sur la coche pour enregistrer vos modifications.

Supprimer les rapports planifiés dans Active IQ Unified Manager

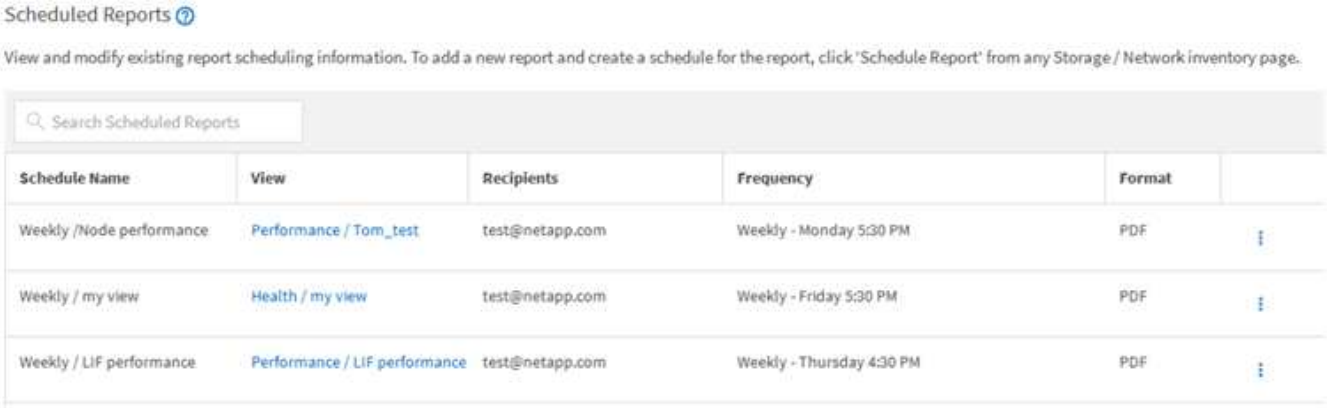
Après avoir programmé les rapports, vous pouvez les supprimer depuis la page « Programmation des rapports ».

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Planification des rapports**.



> Si vous disposez des autorisations appropriées, vous pouvez supprimer n'importe quel rapport et sa planification dans le système.

2. Cliquez sur l'icône Plus ⋮ pour la planification que vous souhaitez supprimer.
3. Cliquez sur **Delete**.
4. Confirmez votre décision.

   Le rapport programmé a été retiré de la liste et ne sera plus généré ni distribué selon la planification établie.

> Si vous supprimez une vue personnalisée de la page d'inventaire, tous les fichiers Excel personnalisés ou les rapports planifiés qui utilisent cette vue sont également supprimés.

Exemples de rapports personnalisés

Comprendre des exemples de rapports personnalisés dans Active IQ Unified Manager

Ces exemples de rapports personnalisés sont couramment utilisés pour vous aider à identifier les problèmes potentiels et à réagir aux incidents potentiels avant que des problèmes ne surviennent.

La liste des rapports présentés dans cette section n'est pas exhaustive et s'enrichira au fil du temps. Vous pouvez suggérer des rapports personnalisés à ajouter à cette section en nous faisant part de vos commentaires sur la documentation.

Vous devez disposer du rôle d'administrateur d'applications ou d'administrateur de stockage pour gérer les rapports.

Personnaliser les rapports de stockage du cluster

Créez un rapport pour visualiser la capacité par modèle de cluster dans Active IQ Unified Manager

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des clusters en fonction du modèle de système de stockage.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant la capacité par modèle de cluster, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport, telles que « `Cluster FQDN` » et « `OS Version` ».
4. Faites glisser « `Total Raw Capacity` », « `Model/Family` » et les trois colonnes d'agrégat près de la colonne « `Cluster` ».
5. Cliquez en haut de la colonne « `Model/Family` » pour trier les résultats par type de cluster.
6. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `Capacity by Cluster Model` ».
7. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez souhaiter augmenter la capacité de certains clusters ou mettre à niveau des modèles de clusters plus anciens.

Identifiez les clusters disposant d'une capacité LUN non allouée dans Active IQ Unified Manager

Vous pouvez créer un rapport pour trouver les clusters ayant la plus grande capacité LUN non allouée, supérieure à 0,5 To, afin d'identifier où vous pouvez ajouter des charges de travail supplémentaires.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les clusters ayant la plus grande

capacité LUN non allouée, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser la colonne « `Unallocated LUN Capacity` » près de la colonne « `HA Pair` ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:
   - Capacité LUN non allouée supérieure à 0,5 To
6. Cliquez en haut de la colonne « `Capacité LUN non allouée` » pour trier les résultats par valeur décroissante de capacité LUN non allouée.
7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `Most unallocated LUN capacity` » et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
10. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez souhaiter utiliser la capacité de LUN non allouée du cluster.

Créez un rapport pour afficher les paires haute disponibilité avec la capacité disponible la plus élevée dans Active IQ Unified Manager

Vous pouvez créer un rapport pour trouver les paires haute disponibilité (HA) ayant la plus grande capacité pour provisionner de nouveaux volumes et LUNs.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les paires HA triées par la capacité disponible la plus élevée afin de provisionner de nouveaux volumes et LUNs, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Clusters**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les clusters**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser la colonne « `Capacité inutilisée de l'agrégat` » près de la colonne « `Paire HA` ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:

◦ Capacité inutilisée de l'agrégat supérieure à 0,5 To

6. Cliquez en haut de la colonne « `Capacité inutilisée agrégée` » pour trier les résultats par valeur décroissante de capacité inutilisée agrégée.
7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `Capacité agrégée la moins utilisée` », et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
10. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez envisager d'équilibrer les paires HA en fonction de la capacité des agrégats.

Créez un rapport pour afficher les nœuds exécutant d'anciennes versions d'ONTAP dans Active IQ Unified Manager

Vous pouvez générer un rapport affichant la version du logiciel ONTAP installée sur tous les nœuds du cluster afin de déterminer quels nœuds doivent être mis à niveau.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Utilisez les étapes suivantes pour créer une vue personnalisée affichant les nœuds exécutant des versions plus anciennes d'ONTAP, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Nœuds**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
3. Faites glisser la colonne « `OS Version` » près de la colonne « `Node` ».
4. Cliquez en haut de la colonne « `OS Version` » pour trier les résultats par version la plus ancienne d'ONTAP.
5. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple, « `Nodes by ONTAP version` ».
6. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
7. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
8. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez envisager de mettre à niveau les nœuds

exécutant des versions plus anciennes d'ONTAP.

Personnaliser les rapports de capacité des agrégats

Créez un rapport pour visualiser les agrégats atteignant leur pleine capacité dans Active IQ Unified Manager

Vous pouvez créer un rapport pour identifier les agrégats qui atteignent leur capacité maximale, afin d'ajouter de la capacité ou de déplacer les charges de travail vers d'autres agrégats.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les agrégats atteignant leur pleine capacité, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:
   - Jours avant saturation inférieurs à 45 jours
5. Cliquez sur le haut de la colonne « `Days to Full` » pour trier les résultats selon le plus petit nombre de jours restants avant d'atteindre la pleine capacité.
6. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple, « `Jours avant la capacité complète de l'agrégat` », et cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats indiqués dans le rapport, il pourrait être judicieux d'augmenter le stockage des agrégats qui atteignent leur pleine capacité. De plus, il pourrait être utile d'augmenter le seuil de « Jours avant saturation » à plus de 7 jours, la valeur par défaut, afin de recevoir des événements vous laissant plus de temps pour réagir lorsque l'espace disponible sur les agrégats devient insuffisant.

Créez un rapport pour afficher les agrégats remplis à 80 % ou plus dans Active IQ Unified Manager

Vous pouvez créer un rapport pour mettre en évidence les agrégats remplis à 80 % ou plus.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les agrégats pleins à 80 % ou plus, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser les colonnes "Available Data %" et "Used Data %" près de la colonne "Aggregate".
5. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **Apply Filter** :
   - Le pourcentage de données utilisées est supérieur à 80%
6. Cliquez en haut de la colonne « `% de données utilisées` » pour trier les résultats par pourcentage de capacité.
7. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « `Agrégats presque pleins` », puis cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
10. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous souhaiterez peut-être déplacer certaines données depuis certains agrégats.

Créez un rapport pour afficher les agrégats surengagés dans Active IQ Unified Manager

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des agrégats, et pour afficher les agrégats en surengagement.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les agrégats qui dépassent le seuil de surallocation, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les agrégats**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « `Overcommitted Capacity %` » près de la colonne « `Aggregate` ».

5. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **Apply Filter** :
   - Le pourcentage de capacité surallouée est supérieur à 100%
6. Cliquez en haut de la colonne "Overcommitted Capacity %" pour trier les résultats par pourcentage de capacité.
7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `Aggregates overcommitted` », et cliquez sur la coche (✓).
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
10. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez souhaiter ajouter davantage de capacité aux agrégats ou déplacer certaines données de certains agrégats.

Personnaliser les rapports de capacité des volumes

Identifiez les volumes proches de leur capacité maximale avec la suppression automatique des instantanés désactivée dans Active IQ Unified Manager

Vous pouvez créer un rapport qui contient la liste des volumes qui approchent de leur capacité maximale avec la fonctionnalité Snapshot Autodelete désactivée. Les résultats peuvent vous aider à identifier les volumes pour lesquels vous pourriez vouloir configurer Snapshot Autodelete.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les colonnes requises dans le bon ordre, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser et déposez les colonnes « `Snapshot 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 avant saturation inférieurs à 30 jours
   - Snapshot Autodelete est désactivé
6. Cliquez en haut de la colonne **Days To Full** pour que les volumes avec le moins de jours restants apparaissent en haut de la liste.

7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'affiche la vue, par exemple "Vols near capacity".
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez vouloir activer Snapshot Autodelete sur les volumes ou trouver un moyen d'augmenter l'espace disponible.

Identifiez les volumes dont le provisionnement fin est désactivé dans Active IQ Unified Manager

Lorsqu'un volume n'est pas à provisionnement fin, il occupe la totalité de l'espace sur le disque telle qu'elle a été définie lors de la création du volume. L'identification des volumes dont le provisionnement fin est désactivé vous aide à décider si vous souhaitez activer le provisionnement fin sur certains volumes.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les colonnes requises dans le bon ordre, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Capacité** > **Tous les volumes**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser et déposez les colonnes « `Used Data %` » et « `Thin Provisioned` » près de la colonne « `Available Data Capacity` ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, **Provisionnement fin** est **Non**, puis cliquez sur **Appliquer le filtre**.
6. Cliquez en haut de la colonne "Used Data %" pour trier les résultats afin que les volumes ayant le pourcentage le plus élevé apparaissent en haut de la liste.
7. Enregistrez la vue avec un nom qui reflète ce qu'elle affiche, par exemple "Vols no thin provisioning".
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
10. Saisissez un nom pour le calendrier du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez souhaiter activer le provisionnement fin sur certains volumes.

Identifiez les volumes qui doivent déplacer des données vers le niveau cloud dans Active IQ Unified Manager

Vous pouvez créer un rapport contenant la liste des volumes qui résident actuellement sur des agrégats FabricPool, qui ont une recommandation cloud de type Tier et qui contiennent une grande quantité de données froides. Ce rapport peut vous aider à décider si vous devez modifier la stratégie de hiérarchisation de certains volumes en « auto » ou « all » afin de transférer davantage de données froides (inactives) vers le niveau cloud.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez avoir configuré des agrégats FabricPool et avoir des volumes sur ces agrégats.

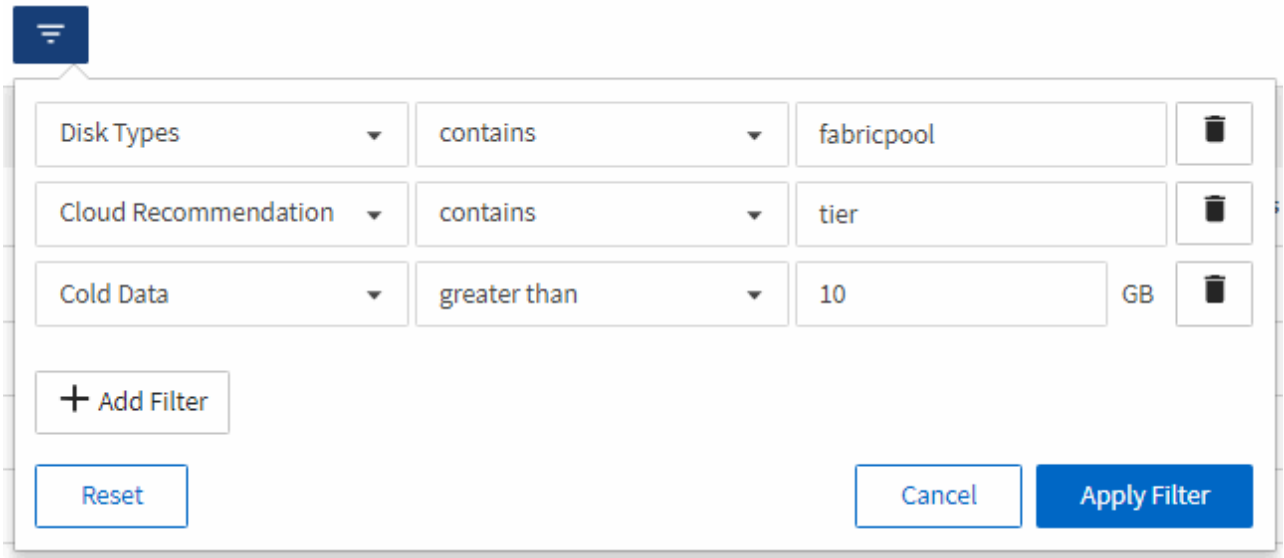
Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les colonnes requises dans le bon ordre, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Performances** > **Tous les volumes**.
3. Dans le sélecteur de colonnes, assurez-vous que la colonne « `Disk Type` » apparaît dans la vue.

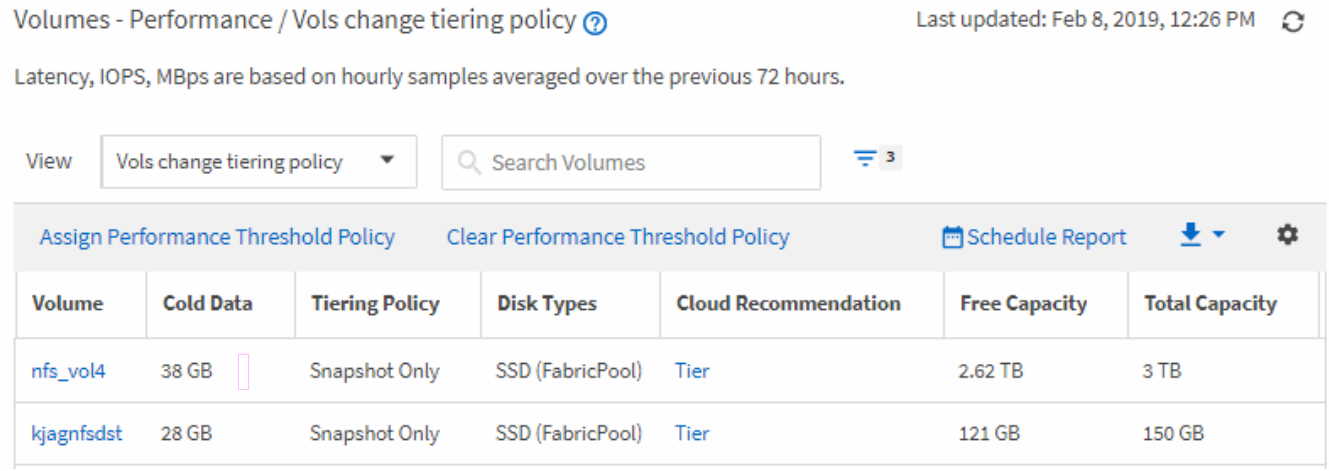
   Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Faites glisser et déposez la colonne « `Type de disque` » près de la colonne « `Recommandation cloud` ».
5. Cliquez sur l'icône de filtre, ajoutez les trois filtres suivants, puis cliquez sur **Apply Filter** :
   - Le type de disque contient FabricPool
   - La recommandation Cloud contient un niveau
   - Données froides supérieures à 10 Go



6. Cliquez en haut de la colonne « Données froides » pour que les volumes contenant le plus de données froides apparaissent en haut de la vue.

7. Enregistrez la vue sous un nom reflétant son contenu, par exemple « `Vols change tiering policy` ».



8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
10. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

En fonction des résultats présentés dans le rapport, vous pouvez utiliser System Manager ou l'interface de ligne de commande ONTAP pour modifier la stratégie de hiérarchisation en « `auto` » ou « `all` » pour certains volumes afin de décharger davantage de données froides vers le niveau cloud.

Personnaliser les rapports de capacité Qtree

Créez un rapport pour afficher les qtrees presque pleins dans Active IQ Unified Manager

Vous pouvez créer un rapport pour analyser la capacité de stockage et l'utilisation des qtrees, et pour visualiser les qtrees qui sont presque pleins.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les qtrees presque pleins, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Qtrees**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
3. Faites glisser la colonne « `Disk Used %` » près de la colonne « `Qtrees` ».
4. Cliquez sur l'icône de filtre, ajoutez les filtres suivants, puis cliquez sur **Apply Filter** :
   - Le pourcentage d'utilisation du disque est supérieur à 75%

5. Cliquez en haut de la colonne “Disk Used %” pour trier les résultats par pourcentage de capacité.
6. Enregistrez la vue sous un nom spécifique qui reflète ce qu’elle affiche, par exemple « `Qtrees presque pleins` », puis cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports programmés** sur la page d’inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

En fonction des résultats présentés dans le rapport, vous pourriez vouloir ajuster les limites strictes et souples du disque (si elles sont définies) ou équilibrer les données entre les qtrees.

Personnaliser les rapports de partage NFS

Personnalisez les rapports de partage NFS dans Active IQ Unified Manager

Vous pouvez personnaliser les rapports de partage NFS pour analyser les informations relatives aux règles et aux politiques d’export NFS des volumes sur vos systèmes de stockage. Par exemple, vous pouvez personnaliser les rapports pour afficher les volumes dont les chemins de montage sont inaccessibles et les volumes avec les règles d’export par défaut.

Créez un rapport pour afficher les volumes dont le chemin de montage est inaccessible dans Active IQ Unified Manager

Vous pouvez générer un rapport pour identifier les volumes dont le chemin de montage est inaccessible.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée pour les volumes dont le chemin de montage est inaccessible, puis planifiez la génération d’un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **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 sous un nom spécifique qui reflète ce qu’elle affiche, par exemple « `Volumes avec un chemin de montage inaccessible` », puis cliquez sur la coche (✓).
5. Cliquez sur le bouton **Rapports programmés** sur la page d’inventaire.
6. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page « Planifications des

rapports » afin que vous puissiez définir les caractéristiques de la planification du nouveau rapport.

7. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous souhaiterez peut-être corriger les chemins de montage inaccessibles.

Créez un rapport pour visualiser les volumes en utilisant la règle d'export par défaut dans Active IQ Unified Manager

Vous pouvez créer un rapport pour trouver les volumes qui utilisent les règles d'export par défaut.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée pour les volumes utilisant les règles d'export par défaut, puis planifiez 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 « `règles d'export` » près de la colonne « `Volume` ».
4. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:
   - Les règles d'export contiennent une valeur par défaut
5. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `Volumes avec une règle d'export par défaut` » et cliquez sur la coche (✓).
6. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
7. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page « Planifications des rapports » afin que vous puissiez définir les caractéristiques de la planification du nouveau rapport.
8. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez souhaiter configurer une règle d'export.

Personnaliser les rapports de VM de stockage

Personnalisez les rapports de machines virtuelles de stockage dans Active IQ Unified Manager

Vous pouvez créer des rapports sur les machines virtuelles de stockage (SVM) afin d'analyser les informations sur les volumes et d'afficher l'état général 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 arrêtées.

Créez un rapport pour visualiser les machines virtuelles de stockage atteignant la limite maximale de volumes dans Active IQ Unified Manager

Vous pouvez générer un rapport pour identifier les SVM qui atteignent la limite de volume maximale.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les machines virtuelles de stockage qui atteignent la limite de volume maximale, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Machines virtuelles de stockage**.
2. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
3. Faites glisser les colonnes « `Volume Count` » et « `Maximum Allowed Volumes` » près de la colonne « `Storage VM` ».
4. Cliquez en haut de la colonne « Volumes maximums autorisés » pour trier les résultats par nombre de volumes le plus élevé.
5. Enregistrez la vue avec un nom spécifique qui reflète ce que la vue affiche, par exemple « `SVMs atteignant le nombre maximal de volumes` » et cliquez sur la coche (✓).
6. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
7. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
8. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez vouloir équilibrer les volumes attribués aux machines virtuelles de stockage ou, si possible, utiliser ONTAP System Manager pour modifier le nombre maximal de volumes autorisés.

Créez un rapport pour afficher les machines virtuelles de stockage arrêtées dans Active IQ Unified Manager

Vous pouvez générer un rapport affichant la liste de toutes les SVM arrêtées.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée affichant les machines virtuelles de stockage arrêtées, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Machines virtuelles de stockage**.
2. Dans le menu Affichage, sélectionnez **Santé** > **Toutes les machines virtuelles de stockage**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas inclure dans le rapport.
4. Faites glisser la colonne « `State` » 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. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `SVM arrêtés` », puis cliquez sur la coche (✓).
7. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
8. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pouvez chercher à comprendre pourquoi la SVM est arrêtée afin de déterminer s'il faut redémarrer les SVM arrêtées.

Personnaliser les rapports de relation de volume

Personnalisez les rapports de relations de volume dans Active IQ Unified Manager

Le rapport d'inventaire des relations de volume vous permet d'analyser les détails de l'inventaire du stockage dans un cluster, de comprendre le niveau de protection requis pour les volumes et de filtrer les détails des volumes en fonction de la source de panne, du modèle et des calendriers.

Créez un rapport pour regrouper les relations de volume par source de défaillance dans Active IQ Unified Manager

Vous pouvez créer un rapport qui regroupe les volumes en fonction de la raison pour laquelle la relation se trouve dans un état non sain.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée qui regroupe les volumes par source de défaillance, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Toutes les relations**.
3. Sélectionnez **Afficher/Masquer** pour vous assurer que les colonnes « `Relationship Health` » et « `Unhealthy Reason` » apparaissent dans la vue.

Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Faites glisser les colonnes « Relationship Health » et « Unhealthy Reason » près de la colonne « State ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:
   - L'état de la relation est mauvais
6. Cliquez sur le haut de la colonne « `Raison de l'état non sain` » pour regrouper les relations de volume par source de défaillance.
7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « `Relations de volume par défaillance` ».
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pouvez analyser la source et l'impact de chaque type de défaillance.

Créez un rapport pour regrouper les relations de volume par problème dans Active IQ Unified Manager

Vous pouvez créer un rapport qui regroupe les relations de volume par problème.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée qui regroupe les relations de volume par problème, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Toutes les relations**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser la colonne "Unhealthy Reason" près de la colonne "State".
5. Cliquez en haut de la colonne « `Unhealthy Reason` » pour regrouper les volumes par problème.
6. Enregistrez la vue sous un nom spécifique qui reflète son contenu, par exemple « `Relations Vol par problème` ».
7. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
8. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pouvez analyser la source et l'impact de chaque type de problème.

Créez un rapport pour visualiser les tendances des transferts de volume à intervalles réguliers dans Active IQ Unified Manager

Vous pouvez créer un rapport affichant les tendances des transferts de volume à des intervalles de temps spécifiques.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée des volumes à des intervalles de temps spécifiques, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Statut des transferts du dernier mois**.
3. Sélectionnez **Afficher/Masquer** pour supprimer les colonnes que vous ne souhaitez pas voir apparaître dans le rapport.
4. Faites glisser la colonne Transfer Duration près de la colonne « `Operational Result` ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:
   - Heure de fin du transfert au cours des 7 derniers jours
6. Cliquez en haut de la colonne « `Durée du transfert` » pour trier les volumes par intervalle de temps.
7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple "Volumes par durée".
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Saisissez un nom pour la planification du rapport, définissez la fréquence sur **Hebdomadaire** et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pouvez analyser les intervalles de temps de transfert.

Créez un rapport pour visualiser les transferts de volume ayant échoué ou réussi dans Active IQ Unified Manager

Vous pouvez générer un rapport affichant l'état des transferts de volume. Ce rapport permet de visualiser les transferts de volume réussis et ceux ayant échoué.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée permettant d'afficher les transferts qui ont échoué et ceux qui ont réussi, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Statut des transferts 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 “Operation Result” près de la colonne “State”.
5. Cliquez en haut de la colonne “Operation Result” pour trier les volumes par statut.
6. Enregistrez la vue sous un nom spécifique qui reflète ce qu’elle affiche, par exemple “Volumes par statut de transfert”.
7. Cliquez sur le bouton **Rapports programmés** sur la page d’inventaire.
8. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D’après les résultats présentés dans le rapport, vous pouvez consulter l’état du transfert.

Créez un rapport pour afficher les transferts de volume en fonction de la taille de transfert dans Active IQ Unified Manager

Vous pouvez créer un rapport pour visualiser les transferts de volume en fonction de la taille du transfert.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée des transferts de volume en fonction de la taille du transfert, puis planifiez la génération d’un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Taux de transfert du dernier mois**.
3. Cliquez sur l’en-tête de la colonne « `Volume total transféré` » pour trier les transferts de volume par taille.
4. Enregistrez la vue sous un nom spécifique qui reflète ce qu’elle affiche, par exemple “Volumes par taille de transfert”.
5. Cliquez sur le bouton **Rapports programmés** sur la page d’inventaire.
6. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D’après les résultats présentés dans le rapport, vous pouvez étudier les relations entre les volumes en fonction de la taille du transfert.

Créez un rapport pour visualiser les transferts de volume regroupés par jour dans Active IQ Unified Manager

Vous pouvez générer un rapport pour visualiser les transferts de volume regroupés par jour.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes ci-dessous pour créer une vue personnalisée des transferts de volume regroupés par jour, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Relation** > **Taux de transfert du dernier mois**.
3. Cliquez en haut de la colonne « `Jour` » pour trier les transferts de volume par jour.
4. Enregistrez la vue sous un nom spécifique qui reflète son contenu, par exemple « Transferts de volume par jour ».
5. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
6. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pouvez analyser les transferts de volumes par jour.

Personnaliser les rapports de performance des volumes

Créez un rapport pour identifier les volumes présentant un taux élevé de données froides sur un agrégat non FabricPool dans Active IQ Unified Manager

Vous pouvez créer un rapport pour afficher les volumes comportant une grande quantité de données inactives sur un agrégat non-FabricPool. Cela peut vous aider à identifier les volumes à déplacer vers un agrégat FabricPool.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Utilisez les étapes suivantes pour créer une vue personnalisée pour les volumes comportant une grande quantité de données froides sur un agrégat pour lequel FabricPool n'est pas activé, puis planifiez la génération d'un rapport pour cette vue.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Performances** > **Tous les volumes**.
3. Sélectionnez **Show/Hide** pour vous assurer que la colonne « `Disk Type` » apparaît dans la vue.

   Ajoutez ou supprimez d'autres colonnes pour créer une vue importante pour votre rapport.

4. Faites glisser la colonne « `Disk Type` » près de la colonne « `Cold Data` ».
5. Cliquez sur l'icône de filtre, ajoutez le filtre suivant, puis cliquez sur **Appliquer le filtre**:
   - Données froides supérieures à 100 Go
   - Le type de disque contient SSD

6. Cliquez en haut de la colonne « `Type de disque` » pour trier les volumes par type de disque afin que le type de disque SSD (FabricPool) soit en bas.
7. Enregistrez la vue sous un nom spécifique qui reflète ce qu'elle affiche, par exemple « Volumes de données froides non FabricPool ».
8. Cliquez sur le bouton **Rapports programmés** sur la page d'inventaire.
9. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

   Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pouvez identifier les volumes qui sont de bons candidats pour un transfert vers des agrégats FabricPool.

Exemples de rapports Microsoft Excel

Comprendre des exemples de rapports Microsoft Excel dans Active IQ Unified Manager

Ces exemples de rapports Microsoft Excel ont pour but de présenter les options de création de rapports disponibles grâce aux fonctionnalités avancées d'Excel.

Les fonctionnalités avancées d'Excel permettent de créer une grande variété de rapports adaptés à vos besoins. Pour plus d'informations sur l'utilisation d'Excel, consultez la documentation du produit.

ⓘ Vous devez disposer du rôle d'administrateur d'applications ou d'administrateur de stockage pour gérer les rapports.

Créez un rapport pour afficher un tableau et un graphique de capacité agrégée dans Active IQ Unified Manager

Vous pouvez créer un rapport pour analyser la capacité dans un fichier Excel en utilisant les totaux additionnés et le format de graphique en colonnes groupées.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes suivantes pour ouvrir une vue Health: All Aggregates, télécharger la vue dans Excel, créer un graphique de capacité disponible, téléverser le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Sélectionnez **Reports** > **Download Excel**.



Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

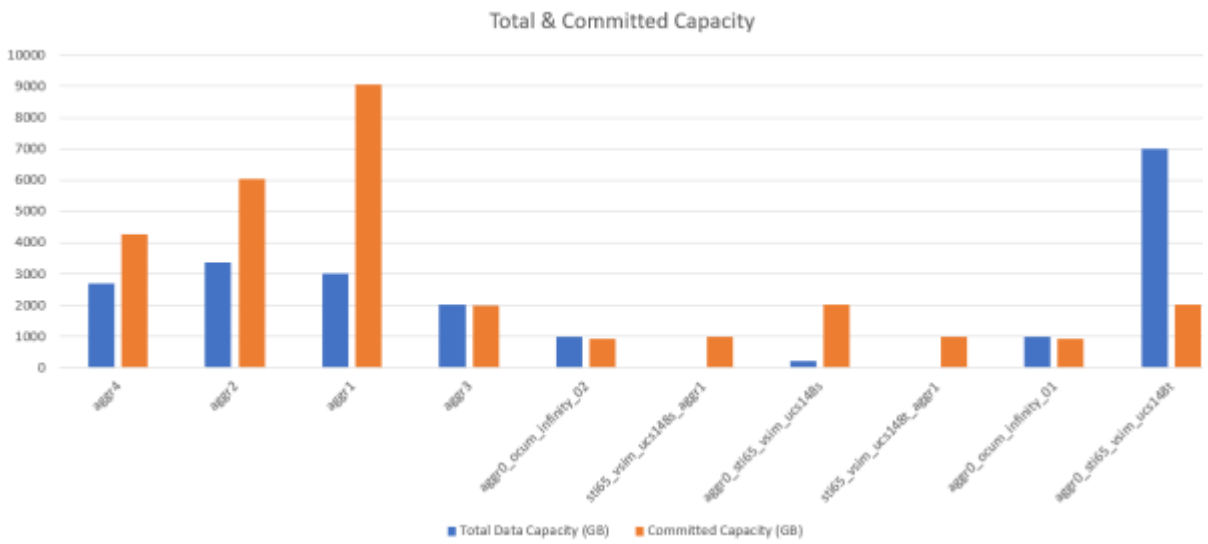
3. Si nécessaire, cliquez sur **Activer la modification**.
4. Dans Excel, ouvrez le fichier téléchargé.
5. Créez une nouvelle feuille (⊕) après la `data` feuille et nommez-la **Total Data Capacity**.
6. Ajoutez les colonnes suivantes dans la nouvelle feuille « Capacité totale des données » :
   a. Capacité totale des données (Go)
   b. Capacité engagée (GB)
   c. Capacité de données utilisée (GB)
   d. Capacité de données disponible (Go)
7. Dans la première ligne de chaque colonne, saisissez la formule suivante, en veillant à ce qu'elle fasse référence à la feuille de données (data!) et aux spécificateurs de colonne et de ligne corrects pour les données capturées (Total Data Capacity extrait les données de la colonne E, lignes 2 à 20).
   a. =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 calcule le total de chaque colonne en fonction des données actuelles.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. Sur la feuille de données, sélectionnez les colonnes **Capacité totale des données (Go)** et **Capacité engagée (Go)**.
2. Sélectionnez **Graphiques recommandés** dans le menu **Insertion** et sélectionnez le graphique **Colonnes groupées**.
3. Faites un clic droit sur le graphique et sélectionnez **Déplacer le graphique** pour déplacer le graphique vers la `Total Data Capacity` feuille.
4. Les menus **Design** et **Format**, disponibles lorsque le graphique est sélectionné, vous permettent de personnaliser son apparence.
5. Une fois satisfait(e), enregistrez le fichier avec vos modifications. Ne modifiez ni le nom ni l'emplacement

du fichier.

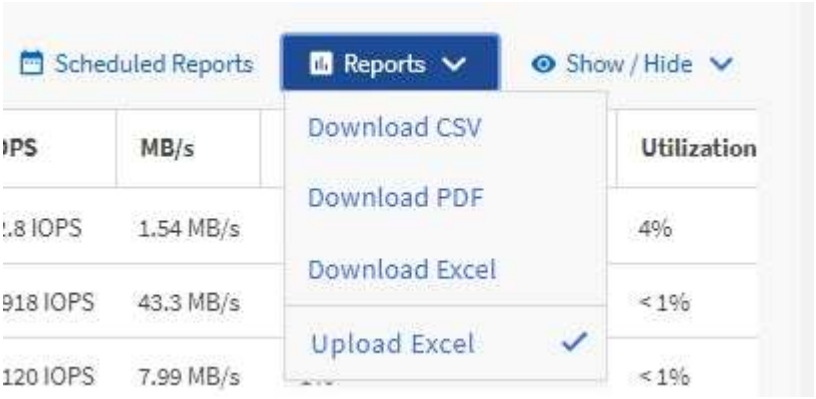


6. Dans Unified Manager, sélectionnez **Rapports** > **Importer Excel**.

   Assurez-vous d'être 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 **Submit**.

   Une coche apparaît à côté de l'élément de menu **Rapports** > **Importer Excel**.



10. Cliquez sur **Scheduled Reports**.
11. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.

    Sélectionnez le format **XLSX** pour le rapport.

12. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

Au vu des résultats présentés dans le rapport, il peut être utile d'examiner comment utiliser au mieux la capacité disponible sur l'ensemble de votre réseau.

Afficher les graphiques comparant la capacité totale agrégée à la capacité disponible dans Active IQ Unified Manager

Vous pouvez créer un rapport pour analyser la capacité de stockage totale et la capacité engagée sous forme de graphique Excel.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes suivantes pour ouvrir une vue Health: All Aggregates, télécharger la vue dans Excel, créer un graphique de capacité totale et engagée, charger le fichier Excel personnalisé et planifier le rapport final.

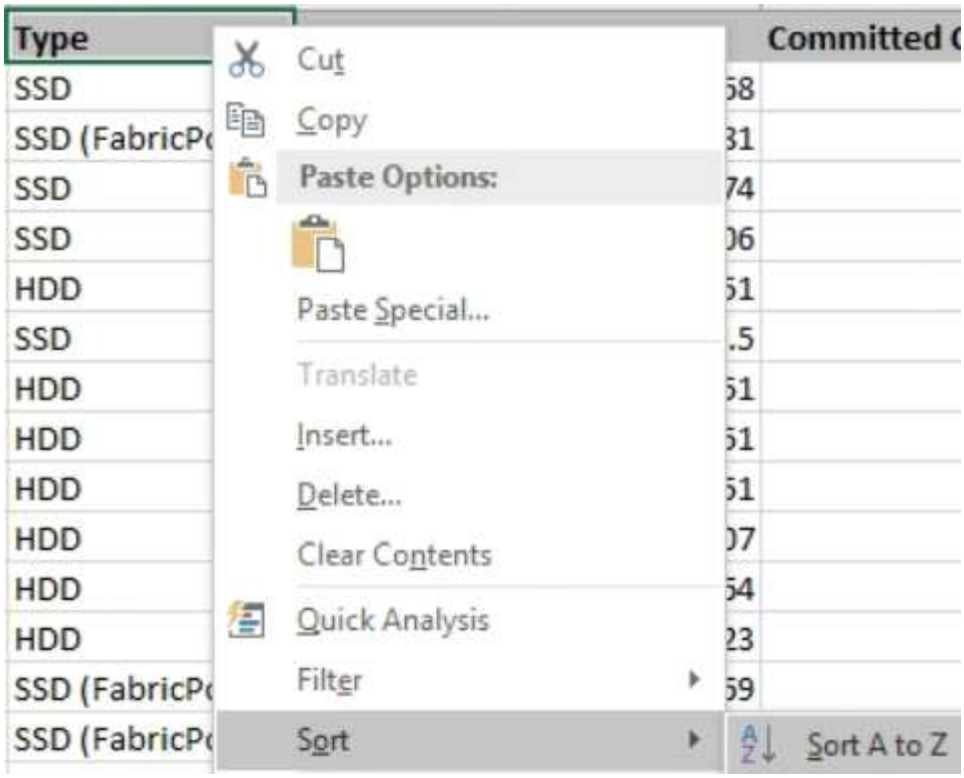
Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Sélectionnez **Reports** > **Download 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. Dans la feuille de données, cliquez avec le bouton droit sur la colonne Type et sélectionnez **Trier** > **Trier de A à Z**.

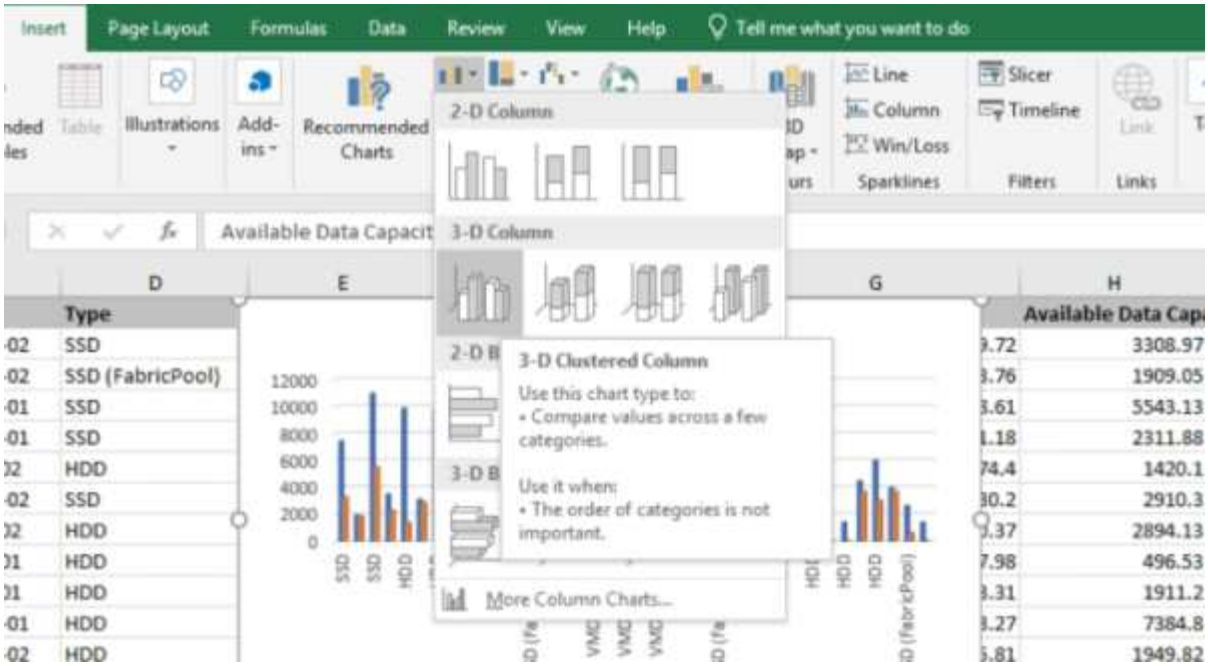


Cela permettra de classer vos données par type de stockage, par exemple :

- disque dur
- Hybride
- SSD
- SSD (FabricPool)

6. Sélectionnez les colonnes `Type`, `Total Data Capacity`, et `Available Data Capacity`.
7. Dans le menu **Insérer**, sélectionnez un `3-D column` graphique.

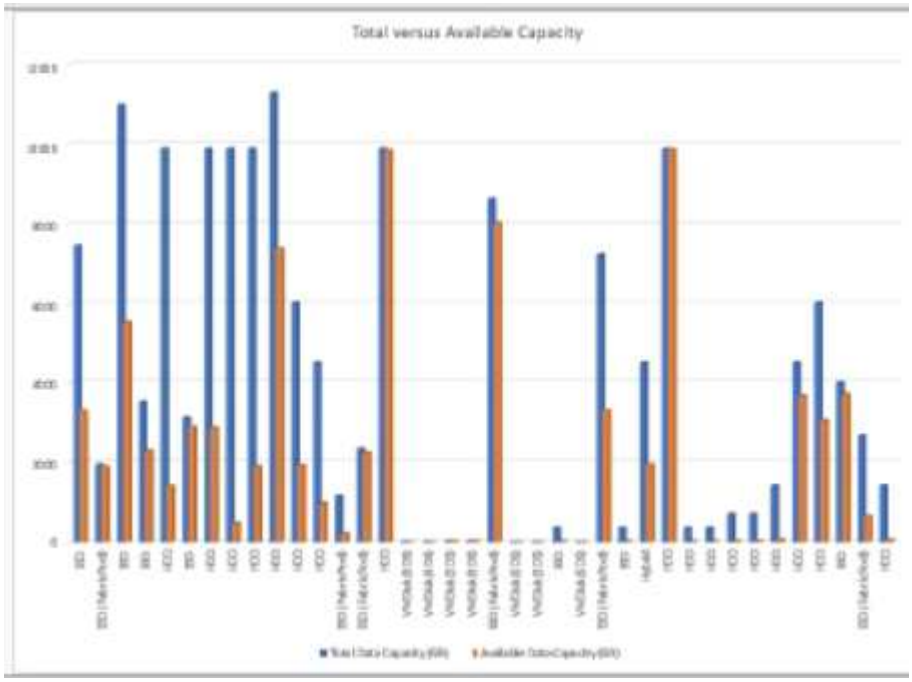
   Le graphique figure sur la fiche technique.



8. Faites un clic droit sur le graphique et sélectionnez **Déplacer le graphique**.
9. Sélectionnez **Nouvelle feuille** et nommez la feuille **Tableaux de stockage total**.

> Assurez-vous que la nouvelle feuille apparaisse après les feuilles d'informations et de données.

10. Intitulez le graphique **Capacité totale versus capacité disponible**.
11. Les menus **Design** et **Format**, disponibles lorsque le graphique est sélectionné, vous permettent de personnaliser son apparence.
12. Une fois satisfait(e), enregistrez le fichier avec vos modifications. Ne modifiez ni le nom ni l'emplacement du fichier.

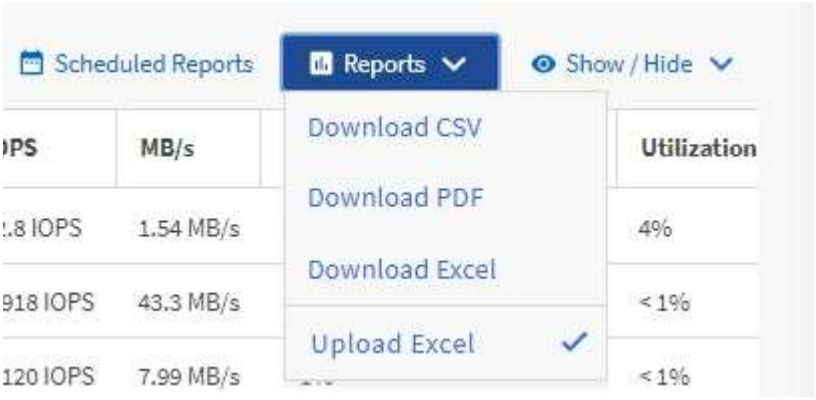


13. Dans Unified Manager, sélectionnez **Rapports** > **Importer Excel**.

    Assurez-vous d'être 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 **Submit**.

    Une coche apparaît à côté de l'élément de menu **Rapports** > **Importer Excel**.



17. Cliquez sur **Scheduled Reports**.
18. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.

    Sélectionnez le format **XLSX** pour le rapport.

19. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez envisager d'équilibrer la charge sur vos agrégats.

Créez un rapport pour afficher les graphiques de capacité de volume disponibles dans Active IQ Unified Manager

Vous pouvez créer un rapport pour analyser la capacité de volume disponible dans un graphique Excel.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes suivantes pour ouvrir une vue « Health: All Volumes », télécharger la vue dans Excel, créer un graphique de capacité disponible, téléverser le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.

2. Sélectionnez **Reports** > **Download Excel**.



   Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

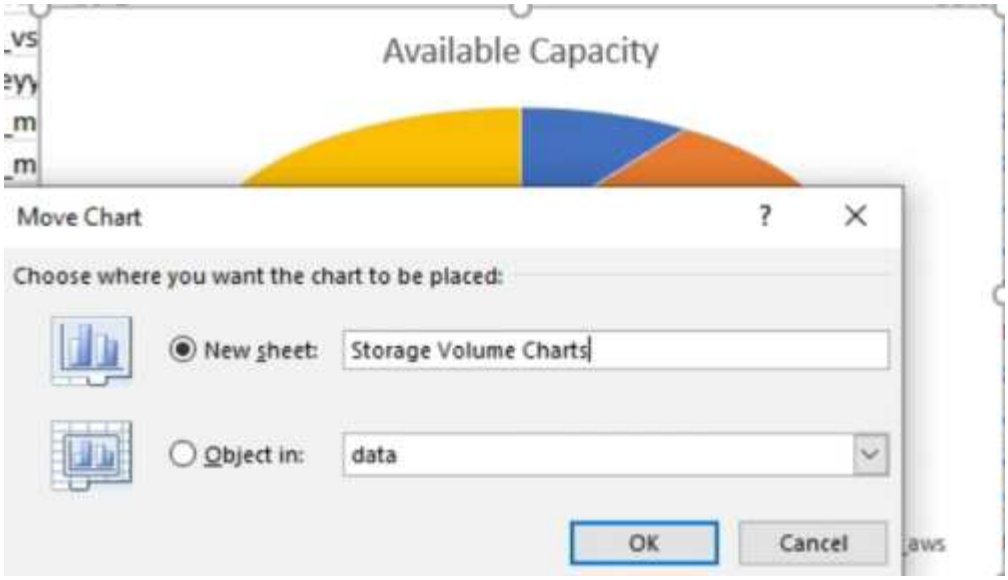
3. Si nécessaire, cliquez sur **Activer la modification**.
4. Dans Excel, ouvrez le fichier téléchargé.
5. Sur la `data` feuille, sélectionnez les données que vous souhaitez utiliser dans les colonnes `Volume` et `Available Data` %.
6. Dans le menu **Insérer**, sélectionnez un `3-D piechart`.

   Le graphique indique les volumes présentant le plus grand espace disponible. Il figure sur la fiche technique.

   > Selon la configuration de votre réseau, la sélection de colonnes entières ou d'un trop grand nombre de lignes de données peut rendre votre graphique circulaire illisible. Cet exemple utilise un graphique circulaire 3-D, mais vous pouvez utiliser n'importe quel type de graphique. Choisissez le graphique qui représente le mieux les données que vous souhaitez recueillir.

7. Intitulez le graphique **Capacité disponible**.
8. Faites un clic droit sur le graphique et sélectionnez **Déplacer le graphique**.
9. Sélectionnez **Nouvelle feuille** et nommez-la **Graphiques des volumes de stockage**.

   > Assurez-vous que la nouvelle feuille apparaisse après les feuilles d'informations et de données.

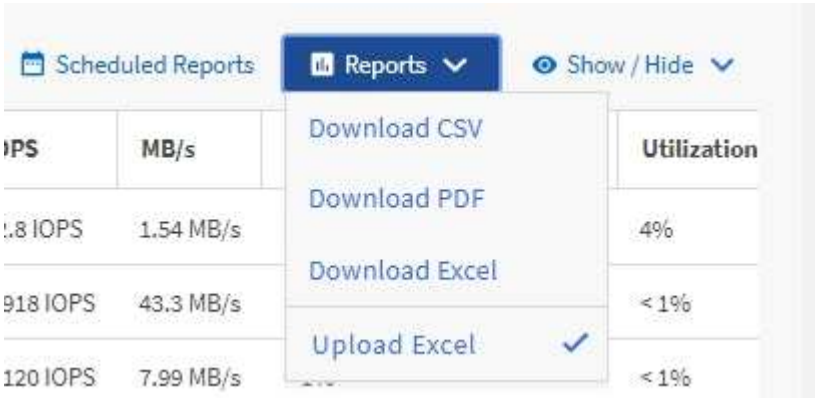


10. Les menus **Design** et **Format**, disponibles lorsque le graphique est sélectionné, vous permettent de personnaliser son apparence.
11. Une fois que vous êtes satisfait, enregistrez le fichier avec vos modifications.
12. Dans Unified Manager, sélectionnez **Rapports** > **Importer Excel**.

    Assurez-vous d'être 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 **Submit**.

    Une coche apparaît à côté de l'élément de menu **Rapports** > **Importer Excel**.



16. Cliquez sur **Scheduled Reports**.
17. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page **Planifications des rapports** afin de définir les caractéristiques de la planification du nouveau rapport.
18. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Sélectionnez le format **XLSX** pour le rapport.

Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez envisager d'équilibrer la charge sur vos volumes.

Créez un rapport pour afficher les agrégats présentant le plus grand nombre d'IOPS disponibles dans Active IQ Unified Manager

Ce rapport indique quels agrégats disposent du plus grand nombre d'IOPS disponibles par type d'agrégat et sur lesquels vous pouvez provisionner de nouvelles charges de travail.

Avant de commencer

- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Suivez les étapes suivantes pour ouvrir une vue « Health: All Volumes », télécharger la vue dans Excel, créer un graphique de capacité disponible, téléverser le fichier Excel personnalisé et planifier le rapport final.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Agrégats**.
2. Sélectionnez **Performances : Tous les agrégats** dans le menu déroulant **Affichage**.
3. Sélectionnez **Afficher/Masquer** pour afficher la colonne `Available IOPS` et masquer les colonnes `Cluster FQDN`, `Inactive Data Reporting`, et `Threshold Policy`.
4. Faites glisser et déposez les colonnes `Available IOPS` et `Free Capacity` à côté de la colonne `Type`.
5. Nommez et enregistrez la vue personnalisée `Available IOPS Per Aggr`.
6. Sélectionnez **Reports** > **Download Excel**.



   Selon votre navigateur, vous devrez peut-être cliquer sur **OK** pour enregistrer le fichier.

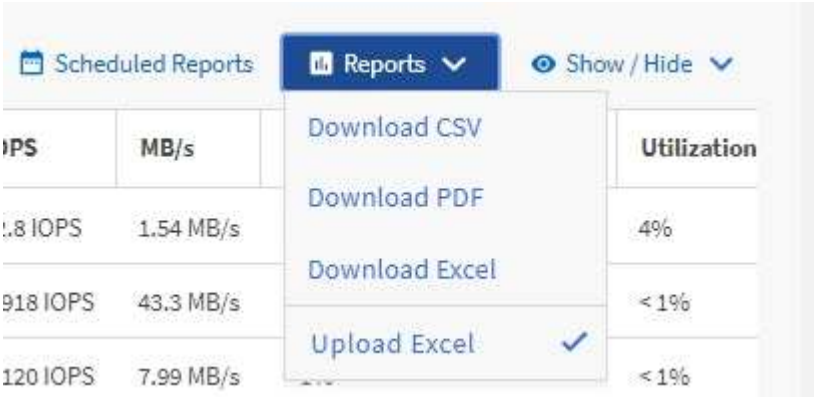
7. Si nécessaire, cliquez sur **Activer la modification**.
8. Dans Excel, ouvrez le fichier téléchargé.
9. Sur la feuille de données, cliquez sur le petit triangle en haut à gauche de la feuille pour sélectionner la feuille entière.

10. Dans l'onglet **Données**, sélectionnez **Trier** dans le menu `Sort & Filter area`.
11. Définissez les niveaux de tri suivants :
    a. Spécifiez le **Tri par** comme `Available IOPS` (IOPS), le **Tri sur** comme `Cell Values`, et l'**Ordre** comme `Largest to Smallest`.
    b. Cliquez sur **Ajouter un niveau**.
    c. Spécifiez **Tri par** comme `Type`, **Tri sur** comme `Cell Values`, et **Ordre** comme `Z to A`.
    d. Cliquez sur **Ajouter un niveau**.
    e. Spécifiez **Trier par** comme `Free Capacity (GB)`, le **Tri sur** comme `Cell Values`, et l'**Ordre** comme `Largest to Smallest`.
    f. Cliquez sur **OK**.
12. Enregistrez et fermez le fichier Excel.
13. Dans Unified Manager, sélectionnez **Rapports** > **Importer Excel**.

    Assurez-vous d'être 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-ci `performance-aggregates-<date>.xlsx`.
15. Cliquez sur **Ouvrir**.
16. Cliquez sur **Submit**.

    Une coche apparaît à côté de l'élément de menu **Rapports** > **Importer Excel**.



17. Cliquez sur **Scheduled Reports**.
18. Cliquez sur **Ajouter une planification** pour ajouter une nouvelle ligne à la page Planifications des rapports afin de définir les caractéristiques de la planification du nouveau rapport.
19. Saisissez un nom pour la planification du rapport et remplissez les autres champs du rapport, puis cliquez sur la coche (✓) à la fin de la ligne.

    Sélectionnez le format **XLSX** pour le rapport.

    Le rapport est envoyé immédiatement à titre de test. Ensuite, le rapport est généré et envoyé par courriel aux destinataires indiqués, selon la fréquence spécifiée.

D'après les résultats présentés dans le rapport, vous pourriez envisager de provisionner les nouvelles charges

de travail sur les agrégats disposant du plus grand nombre d’IOPS disponibles.

Gérer le stockage à l'aide des API REST

Premiers pas avec Active IQ Unified Manager

Démarrer avec les API REST d'Active IQ Unified Manager

Active IQ Unified Manager fournit un ensemble d'API permettant de gérer vos ressources de stockage sur les systèmes de stockage pris en charge via une interface de service Web RESTful pour toute intégration tierce.

Dans ces rubriques, vous trouverez des informations sur les API d'Unified Manager, des exemples de flux de travail pour résoudre des problèmes spécifiques, ainsi que des exemples de code. Grâce à ces informations, vous pourrez créer des clients RESTful des solutions logicielles NetApp Manageability pour gérer les systèmes NetApp. Les API sont basées sur le style architectural Representational State Transfer (REST). Les quatre opérations REST Create, Read, Update et Delete (également appelées CRUD) sont prises en charge.

Consultez "Active IQ Unified Manager" pour obtenir des ressources supplémentaires et des détails sur les avantages de l'API REST Active IQ Unified Manager.

Identifier les utilisateurs prévus des API REST d'Active IQ Unified Manager

Les sujets abordés ici sont destinés aux développeurs qui créent des applications interagissant avec le logiciel Active IQ Unified Manager via des API REST.

Les administrateurs et architectes de stockage peuvent se référer à ces informations pour acquérir une compréhension de base de la manière dont les API REST de Unified Manager peuvent être utilisées pour créer des applications clientes afin de gérer et de surveiller les systèmes de stockage NetApp.

Vous devez utiliser ces informations si vous souhaitez utiliser le fournisseur de stockage, le cluster ONTAP et les API d'administration de la gestion pour gérer votre stockage.

Vous devez posséder l'un des rôles suivants : opérateur, administrateur de stockage ou administrateur d'application. Vous devez connaître l'adresse IP ou le nom de domaine complet du serveur Unified Manager sur lequel vous souhaitez exécuter les API REST.

Gérez l'accès à l'API et les catégories d'Active IQ Unified Manager

Les API Active IQ Unified Manager vous permettent de gérer et de provisionner les objets de stockage de votre environnement. Vous pouvez également accéder à l'interface utilisateur Web de Unified Manager pour effectuer certaines de ces opérations.

Construisez une URL pour accéder directement aux API REST

Vous pouvez accéder directement aux API REST via un langage de programmation, tel que Python, C#, C++, JavaScript, etc. Saisissez le nom de l'hôte ou l'adresse IP et l'URL pour accéder aux API REST au format suivant :

https://<hostname>/api

Le port par défaut est 443. Vous pouvez configurer le port en fonction des besoins de votre

environnement.

Accédez à la page de documentation de l'API en ligne

Vous pouvez accéder à la page de contenu de référence *API Documentation*, fournie avec le produit, pour afficher la documentation de l'API et émettre manuellement un appel d'API (dans l'interface, par exemple Swagger). Vous pouvez accéder à cette documentation en cliquant sur **Menu Bar** > **Help button** > **API Documentation**

Vous pouvez également saisir le nom de l'hôte ou l'adresse IP et l'URL pour accéder à la page de l'API REST au format suivant

https://<hostname>/docs/api/

Catégories

Les appels d'API sont organisés de manière fonctionnelle selon les domaines ou les catégories. Pour trouver une API spécifique, cliquez sur la catégorie d'API correspondante.

Les API REST fournies avec Unified Manager vous permettent d'effectuer des fonctions d'administration, de surveillance et de provisionnement. Ces API sont regroupées dans les catégories suivantes.

- **centre de données**

  Cette catégorie regroupe les API qui vous aident à gérer et à analyser le stockage du centre de données à l'aide d'outils tels que Work Flow Automation et Ansible. Les API REST de cette catégorie fournissent des informations sur les clusters, les nœuds, les agrégats, les volumes, les LUN, les partages de fichiers, les espaces de noms et les autres éléments de votre centre de données.

- **serveur de gestion**

  Les API de la catégorie **management-server** contiennent les API `jobs, system,` et `events`. Les tâches sont des opérations planifiées pour une exécution asynchrone, liées à la gestion des objets de stockage ou des charges de travail sur Unified Manager. L'API `events` renvoie les événements de votre centre de données, et l'API `system` renvoie les détails de l'instance Unified Manager.

- **fournisseur de stockage**

  Cette catégorie contient toutes les API de provisionnement requises pour gérer et provisionner les partages de fichiers, les LUN, les niveaux de service de performance et les stratégies d'efficacité du stockage. Les API vous permettent également de configurer les points de terminaison d'accès, les annuaires Active Directory, ainsi que d'attribuer des niveaux de service de performance et des stratégies 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, la consultation des certificats du magasin de confiance pour les sources de données Unified Manager et la gestion des clusters ONTAP en tant que sources de données pour Unified Manager.

- **passerelle**

  Unified Manager vous permet d'invoquer les API REST ONTAP via les API de la catégorie gateway et de gérer les objets de stockage dans votre centre de données.

- **sécurité**

  Cette catégorie contient des API permettant de gérer les utilisateurs d'Unified Manager.

Comprendre les services REST proposés dans Active IQ Unified Manager

Vous devez connaître les services et opérations REST proposés avant de commencer à utiliser les API Active IQ Unified Manager.

Les API de provisionnement et d'administration utilisées pour configurer le serveur d'API prennent en charge les opérations de lecture (GET) ou d'écriture (POST, PATCH, DELETE). Voici quelques exemples d'opérations GET, PATCH, POST et DELETE prises en charge par les API :

- Exemple pour GET : `GET /datacenter/cluster/clusters` récupère les détails du cluster dans votre centre de données. Le nombre maximal d'enregistrements renvoyés par l'opération `GET` est de 1000.

  Les API vous permettent de filtrer, trier et ordonner les enregistrements selon les attributs pris en charge.

- Exemple pour 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'une SVM à l'aide de sa clé unique.
- Exemple de DELETE : `DELETE /storage-provider/access-endpoints/{key}`supprime un point de terminaison d'accès d'un LUN, d'un SVM ou d'un partage de fichiers à l'aide de sa clé unique.

Les opérations REST pouvant être effectuées via les API dépendent du rôle de l'utilisateur : opérateur, administrateur de stockage ou administrateur d'application.

Rôle utilisateur	Méthode REST prise en charge
Opérateur	Accès en lecture seule aux données. Les utilisateurs disposant de ce rôle peuvent exécuter toutes les requêtes GET.
Administrateur de stockage	Accès en lecture à toutes les données. Les utilisateurs disposant de ce rôle peuvent exécuter toutes les requêtes GET. De plus, ils disposent d'un accès en écriture (pour exécuter des requêtes PATCH, POST et DELETE) afin d'effectuer des activités spécifiques, telles que la gestion des objets de service de stockage et des options de gestion du stockage.
Administrateur d'application	Accès en lecture et en écriture à toutes les données. Les utilisateurs disposant de ce rôle peuvent exécuter des requêtes GET, PATCH, POST et DELETE pour toutes les fonctions.

Pour plus d'informations sur toutes les opérations REST, consultez la *documentation de l'API en ligne*.

Comprendre les numéros de version de l'API dans Active IQ Unified Manager

Les URI de l'API REST dans Active IQ Unified Manager spécifient un numéro de version. Par exemple, `/v2/datacenter/svm/svms.` le numéro de version `v2` dans `/v2/datacenter/svm/svms` indique la version de l'API utilisée dans une version spécifique. Ce numéro de version minimise l'impact des modifications de l'API sur le logiciel client en renvoyant une réponse que ce dernier peut traiter.

La partie numérique de ce numéro de version est incrémentale par rapport aux versions. Les URI comportant 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 correspondent toujours à 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 (en fonction de l'entier incrémentiel) disponible dans votre instance Unified Manager.

Pour toutes les requêtes, vous devez demander explicitement la version de l'API que vous souhaitez utiliser. Lorsque le numéro de version est indiqué, le service ne renvoie pas d'éléments de réponse que votre application n'est pas conçue pour traiter. Dans les requêtes REST, vous devez inclure le paramètre de version. Les versions antérieures des API finissent par être dépréciées après quelques versions. Dans cette version, la version `v1` des API est dépréciée.

Comprendre le modèle de ressources de stockage ONTAP dans Active IQ Unified Manager

Les ressources de stockage dans ONTAP peuvent être globalement classées en *ressources de stockage physiques* et *ressources de stockage logiques*. Pour gérer efficacement vos systèmes ONTAP à l'aide des API fournies dans Active IQ Unified Manager, vous devez comprendre le modèle de ressources de stockage et la relation entre les différentes ressources de stockage.

- **Ressources de stockage physiques**

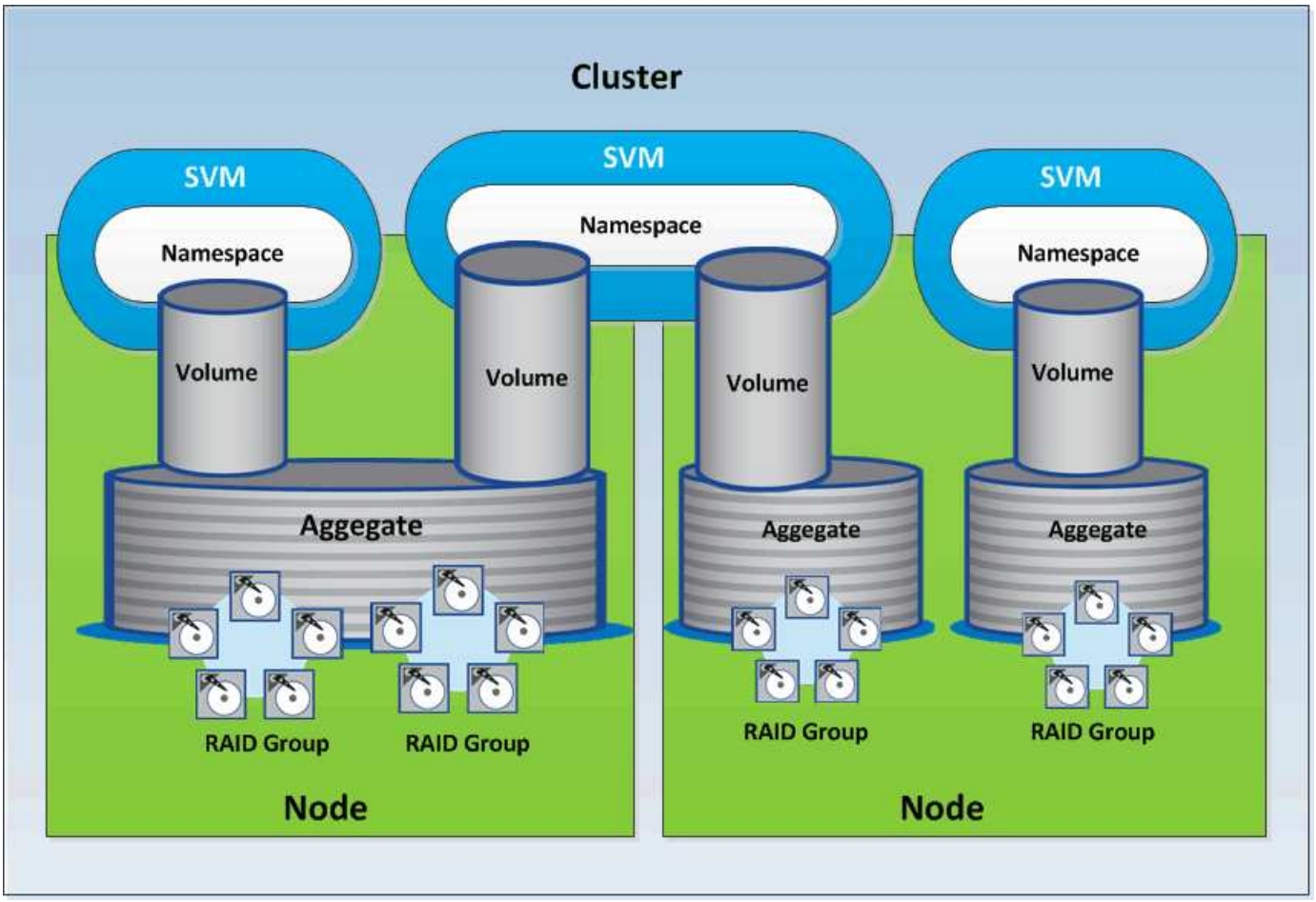
  Désigne les objets de stockage physique fournis par ONTAP. Les ressources de stockage physique comprennent les disques, les clusters, les contrôleurs de stockage, les nœuds et les agrégats.

- **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 existent indépendamment de toute ressource de stockage physique spécifique telle qu'un disque, une baie LUN ou un agrégat.

  Les ressources de stockage logique comprennent les volumes de tous types et les qtrees, ainsi que les fonctionnalités et les configurations que vous pouvez utiliser avec ces ressources, telles que les copies Snapshot, la déduplication, la compression et les quotas.

L'illustration suivante montre les ressources de stockage dans un cluster à 2 nœuds :



Accès à l'API REST et authentification dans Active IQ Unified Manager

Accédez et authentifiez les API REST dans Active IQ Unified Manager

L'API REST Active IQ Unified Manager est accessible à l'aide de n'importe quel client REST ou de toute plateforme de programmation capable d'émettre des requêtes HTTP avec un mécanisme d'authentification HTTP de base.

Exemple de requête et de réponse :

- **Demande**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Réponse**

```
{
  "records": [
```

```
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 13924095,
          "serial_number": "701424000157"
        },
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
```

```
          "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
          "name": "fas8040-206-21-02",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 14012386,
          "serial_number": "701424000564"
        }
      ],
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-
00a0985badbb"
        }
      }
    },
```

- *IP address/hostname* est l'adresse IP ou le nom de domaine complet (FQDN) du serveur API.
- Port 443

443 est le port HTTPS par défaut. Vous pouvez personnaliser le port HTTPS, si nécessaire.
Pour effectuer des requêtes HTTP depuis un navigateur web, vous devez utiliser des plugins de navigateur pour l'API REST. Vous pouvez également accéder à l'API REST via des plateformes de script telles que cURL et Perl.

Authentification

Unified Manager prend en charge le schéma d'authentification HTTP de base pour les API. Afin de garantir la sécurité des échanges d'informations (requêtes et réponses), 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 d'autorité de certification).

Vous devez configurer l'accès utilisateur au serveur API pour appeler les API REST. Les utilisateurs peuvent être des utilisateurs locaux (profils utilisateur stockés dans la base de données locale) ou des utilisateurs

LDAP (si vous avez configuré le serveur API pour l'authentification via LDAP). Vous pouvez gérer l'accès des utilisateurs en vous connectant à l'interface utilisateur de Unified Manager Administration Console.

Découvrez les codes d'état HTTP d'Active IQ Unified Manager

Lors de l'exécution des API ou du dépannage des problèmes, vous devez connaître les différents codes d'état HTTP et codes d'erreur utilisés par les API d'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 en cas d'exécution réussie des appels API synchrones.
201	Créé	Création de nouvelles ressources par appels synchrones, comme la configuration d'Active Directory.
202	Accepté	Renvoyé lors de l'exécution réussie d'appels asynchrones pour des fonctions de provisionnement, telles que la création de LUN et de partages de fichiers.
400	Requête invalide	Indique un échec de validation des données saisies. L'utilisateur doit corriger les données saisies, par exemple les clés valides dans le corps de la requête.
401	Requête non autorisée	Vous n'êtes pas autorisé à consulter la ressource/Non autorisé.
403	Requête interdite	L'accès à la ressource que vous tentiez de consulter est interdit.
404	Ressource introuvable	La ressource que vous tentiez d'atteindre est introuvable.
405	Méthode non autorisée	Méthode non autorisée.
429	Trop de requêtes	Renvoyé lorsque l'utilisateur envoie trop de requêtes dans un laps de temps donné.

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 peut être temporaire ou permanente. Par exemple, si vous exécutez une `GET` ou `GET ALL` opération et que vous recevez cette erreur, il est recommandé de répéter cette opération au moins cinq fois. En cas d'erreur permanente, le code d'état renvoyé reste 500. Si l'opération réussit, le code d'état renvoyé est 200.

Suivez les pratiques recommandées pour l'utilisation des API Active IQ Unified Manager

Lorsque vous utilisez les API dans Active IQ Unified Manager, vous devez suivre certaines pratiques recommandées.

- Tous les types de contenu de réponse doivent être au format suivant pour une exécution valide :

```
application/json
```

- Le numéro de version de l'API n'est pas lié au numéro de version du produit. Vous devez utiliser la dernière version de l'API disponible pour votre instance Unified Manager. Pour plus d'informations sur les versions de l'API Unified Manager, consultez la section « `Gestion des versions de l'API REST dans Active IQ Unified Manager` ».
- Lors de la mise à jour des valeurs d'un tableau à l'aide d'une API Unified Manager, vous devez mettre à jour l'intégralité de la chaîne de valeurs. Vous ne pouvez pas ajouter de valeurs à un tableau. Vous pouvez uniquement remplacer un tableau existant.
- Vous pouvez utiliser des opérateurs de filtre, tels que le pipe (|) et le caractère générique (*), pour tous les paramètres de requête, à l'exception des valeurs de type double, par exemple IOPS et performance dans les API de métriques.
- Évitez d'interroger des objets en utilisant une combinaison des opérateurs de filtre caractère générique (*) et barre verticale (|). Cela pourrait renvoyer un nombre incorrect d'objets.
- Lors de l'utilisation de valeurs pour le filtre, assurez-vous que la valeur ne contient aucun `?` caractère. Cela permet d'atténuer les risques d'injection SQL.
- Notez que la `GET`requête (all) pour n'importe quelle API renvoie un maximum de 1 000 enregistrements. Même si vous exécutez la requête en définissant le `max_records`paramètre sur une valeur supérieure à 1 000, seuls 1 000 enregistrements sont renvoyés.
- Pour effectuer des tâches administratives, il est recommandé d'utiliser l'interface utilisateur d'Unified Manager.

Dépannez à l'aide des journaux système dans Active IQ Unified Manager

Les journaux système vous permettent d'analyser les causes des pannes et de résoudre les problèmes pouvant survenir lors de l'exécution des API.

Pour résoudre les problèmes liés aux appels d'API, veuillez récupérer les journaux à l'emplacement suivant.

Emplacement du journal	Utiliser
`/var/log/ocie/access_log.log`	Contient tous les détails des appels API, tels que le nom d'utilisateur de l'utilisateur qui invoque l'API, l'heure de début, la durée d'exécution, le statut et l'URL. Ce fichier journal vous permet de vérifier les API fréquemment utilisées ou de résoudre les problèmes liés aux flux de travail de l'interface graphique. Il vous permet également de dimensionner l'analyse 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 d'API.
`/var/log/ocie/server.log`	Contient tous les journaux de déploiement des serveurs Wildfly et les journaux relatifs au démarrage/arrêt des services. Vous pouvez utiliser ce fichier journal pour trouver la cause première de tout problème survenant lors du démarrage, de l'arrêt ou du déploiement du serveur Wildfly.
`/var/log/ocie/au.log`	Contient les journaux relatifs à l'unité d'acquisition. Vous pouvez utiliser ce fichier journal lorsque vous avez créé, modifié ou supprimé des objets dans ONTAP, mais que ces modifications ne sont pas reflétées dans les API REST Active IQ Unified Manager.

Comprenez comment Active IQ Unified Manager utilise les objets Job pour le traitement asynchrone

Active IQ Unified Manager fournit l' `jobs`API qui récupère des informations sur les tâches exécutées lors de l'utilisation d'autres API. Vous devez comprendre le fonctionnement du traitement asynchrone à l'aide de l'objet Job.

Certains appels d'API, notamment ceux utilisés pour ajouter ou modifier des ressources, peuvent prendre plus de temps à s'exécuter que d'autres appels. Unified Manager traite ces requêtes de longue durée de manière asynchrone.

Requêtes asynchrones décrites à l'aide de l'objet Job

Après un appel API asynchrone, le code de réponse HTTP 202 indique que la requête a été validée et acceptée, mais pas encore terminée. La requête est traitée comme une tâche en arrière-plan qui continue de s'exécuter après la réponse HTTP initiale au client. La réponse inclut l'objet Job associé à la requête, ainsi que son identifiant unique.

Interroger l'objet Job associé à une requête API

L'objet Job renvoyé dans la réponse HTTP contient plusieurs propriétés. Vous pouvez interroger la propriété state pour déterminer si la requête a été complétée avec succès. Un objet Job peut se trouver dans l'un des états suivants :

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

Il existe deux techniques que vous pouvez utiliser lors de l'interrogation d'un objet Job pour détecter un état terminal de la tâche, soit la réussite, soit l'échec :

- Requête d'interrogation standard : l'état actuel de la tâche est renvoyé immédiatement.
- Requête d'interrogation longue : lorsque l'état de l'emploi passe à `NORMAL, ERROR,` ou `PARTIAL_FAILURES.`

Étapes d'une requête asynchrone

Vous pouvez utiliser la procédure générale suivante pour effectuer un appel d'API asynchrone :

1. Effectuez l'appel API asynchrone.
2. Recevez une réponse HTTP 202 indiquant l'acceptation réussie de la requête.
3. Extrayez l'identifiant de l'objet Job du corps de la réponse.
4. Dans une boucle, attendez que l'objet Job atteigne l'état terminal `NORMAL, ERROR,` ou `PARTIAL_FAILURES.`
5. Vérifiez l'état final du Job et récupérez son résultat.

Découvrez l'exemple de programme serveur Hello API dans Active IQ Unified Manager

Le *Hello API server* est un exemple de programme illustrant comment appeler une API REST dans Active IQ Unified Manager à l'aide d'un client REST simple. Ce programme vous fournit des informations de base sur le serveur API au format JSON (le serveur ne prend en charge que le `application/json`format).

L'URI utilisée est : `https://<hostname>/api/datacenter/svm/svms`. Ce code d'exemple prend les paramètres d'entrée suivants :

- L'adresse IP ou le FQDN du serveur 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 également utiliser d'autres scripts tels que Jersey et RESTEasy afin de développer un client REST Java pour Active IQ Unified Manager. Veuillez prendre en compte les points suivants concernant l'exemple de code :

- Utilise une connexion HTTPS à Active IQ Unified Manager pour appeler l'URI REST spécifié
- Ignore le certificat fourni par Active IQ Unified Manager
- Ignore la vérification du nom de l'hôte lors de la négociation
- Utilisation `javax.net.ssl.HttpsURLConnection` pour une connexion URI
- Utilise une bibliothèque tierce (`org.apache.commons.codec.binary.Base64`) pour construire la chaîne encodée en Base64 utilisée dans l'authentification de base HTTP

Pour compiler et exécuter l'exemple de code, vous devez utiliser le compilateur Java 1.8 ou une version ultérieure.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.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 de Unified Manager

Comprendre les catégories des API REST d'Active IQ Unified Manager

Les API REST pour Active IQ Unified Manager sont répertoriées dans cette section, en fonction de leurs catégories.

Vous pouvez consulter, depuis votre instance Unified Manager, la page de documentation en ligne qui inclut 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 inclut uniquement les informations dont vous avez besoin pour localiser l'appel sur la page de documentation. Après avoir localisé un appel d'API spécifique, vous pouvez consulter tous les détails de cet appel, notamment les paramètres d'entrée, les formats de sortie,

les codes d'état HTTP et le type de traitement de la requête.

Les informations suivantes sont incluses pour chaque appel d'API au sein d'un flux de travail afin de faciliter la localisation de l'appel sur la page de documentation :

- Catégorie

  Les appels d'API sont organisés sur la page de documentation en domaines ou catégories fonctionnelles. Pour trouver un appel d'API spécifique, faites défiler la page jusqu'en bas, puis cliquez sur la catégorie d'API correspondante.

- verbe HTTP (appel)

  Le verbe HTTP identifie l'action effectuée sur une ressource. Chaque appel d'API s'effectue au moyen d'un seul verbe HTTP.

- Chemin

  Le chemin détermine la ressource spécifique qu'utilise l'action dans le cadre de l'exécution d'un appel. La chaîne de chemin est ajoutée à l'URL principale pour former l'URL complète identifiant la ressource.

Gérez les objets de stockage dans un centre de données à l'aide des API dans Active IQ Unified Manager

Les API REST de la `datacenter` catégorie vous permettent de gérer les objets de stockage de votre centre de données, tels que les clusters, les nœuds, les agrégats, les machines virtuelles de stockage, les volumes, les LUN, les partages de fichiers et les espaces de noms. Ces API permettent d'interroger la configuration des objets, et certaines d'entre elles vous permettent également d'effectuer des opérations d'ajout, de suppression ou de modification de ces objets.

La plupart de ces API sont des requêtes GET qui permettent l'agrégation inter-clusters avec prise en charge du filtrage, du tri et de la pagination. Lors de leur exécution, ces API renvoient des données issues de la base de données. Par conséquent, les objets nouvellement créés doivent être détectés lors du cycle d'acquisition suivant pour apparaître dans la réponse.

Pour consulter les détails d'un objet spécifique, vous devez saisir son identifiant unique pour afficher ses détails. Par exemple, pour les informations sur les métriques et les analyses des objets de stockage, consultez "Affichage des indicateurs de performance".

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-
2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

Les commandes CURL, les exemples, les requêtes et les réponses aux API sont disponibles sur votre interface Swagger API. Vous pouvez filtrer et trier les résultats selon des paramètres spécifiques, comme indiqué dans Swagger. Ces API vous permettent de filtrer les résultats pour des objets de stockage spécifiques, tels que cluster, volume ou storage VM.

API pour les objets de stockage de votre centre de données

Verbe HTTP	Chemin	Description

GET	`/datacenter/cluster/clusters`
	
	`/datacenter/cluster/clusters/{key}`
		Cette méthode permet de consulter les détails des clusters ONTAP du centre de données. L'API renvoie des informations, telles que l'adresse IPv4 ou IPv6 du cluster, des informations sur le nœud, telles que l'état du nœud, la capacité de performance et la paire High Availability (HA), et indique si le cluster est un All SAN Array.

GET	`/datacenter/cluster/licensing/licenses` `/datacenter/cluster/licensing/licenses/{key}`	Affiche les détails des licences installées sur les clusters de votre centre de données. Vous pouvez filtrer les résultats selon les critères souhaités. Les informations affichées incluent la clé de licence, la clé de cluster, la date d'expiration et l'étendue de la licence. Vous pouvez saisir une clé de licence pour obtenir les détails d'une licence spécifique.

GET	`/datacenter/cluster/nodes`
	
	`/datacenter/cluster/nodes/{key}`
		Cette méthode vous permet de consulter les détails des nœuds du centre de données. Vous pouvez consulter des informations sur le cluster, l'état de santé du nœud, la capacité de performance et la paire de haute disponibilité (HA) du nœud.

GET	`/datacenter/protocols/cifs/shares`
	
	`/datacenter/protocols/cifs/shares/{key}`
		Cette méthode permet de consulter les détails des partages CIFS du centre de données. Outre les informations relatives au cluster, aux SVM et aux volumes, elle fournit également des données sur les listes de contrôle d'accès (ACL).

Verbe HTTP	Chemin	Description
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	Vous pouvez utiliser cette méthode pour consulter les détails des règles d'export des services NFS pris en charge. Vous pouvez interroger les règles d'export d'un cluster ou d'une machine virtuelle de stockage et réutiliser la clé de règles d'export pour le provisionnement de partages de fichiers NFS. Pour plus d'informations sur l'attribution et la réutilisation des règles d'export pour les charges de travail, consultez « Provisionnement de partages de fichiers CIFS et NFS ».
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Cette méthode vous permet de visualiser l'ensemble des agrégats du centre de données ou un agrégat spécifique pour le provisionnement des charges de travail sur ceux-ci ou leur surveillance. Des informations telles que les détails du cluster et des nœuds, la capacité de performance utilisée, l'espace disponible et utilisé, ainsi que l'efficacité du stockage sont renvoyées.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Vous pouvez utiliser cette méthode pour afficher l'ensemble des LUN dans tout le centre de données. Vous pouvez afficher des informations sur le LUN, telles que les détails du cluster et des SVM, les règles QoS et les igroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Cette méthode permet de consulter le détail de toutes les politiques QoS applicables aux objets de stockage du centre de données. Elle renvoie des informations telles que les détails du cluster et de la SVM, les détails de la politique fixe ou adaptative, et le nombre d'objets auxquels cette politique s'applique.

Verbe HTTP	Chemin	Description
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Vous pouvez utiliser cette méthode pour afficher les détails du qtree dans l'ensemble du data center pour tous les volumes FlexVol ou les volumes FlexGroup. Cette méthode renvoie des informations telles que les détails du cluster et de la SVM, le volume FlexVol et les règles d'export.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Cette méthode permet de visualiser l'ensemble des volumes du centre de données. Des informations sur les volumes, telles que les détails des SVM et des clusters, les règles de QoS et d'export, ainsi que le fait que le volume soit de type lecture-écriture, protection des données ou partage de charge, sont renvoyées. Pour les volumes FlexVol et FlexClone, vous pouvez consulter les informations relatives aux agrégats respectifs. Pour un volume FlexGroup, la requête renvoie la liste des agrégats qui le composent.

Verbe HTTP	Chemin	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Vous pouvez attribuer des groupes d'initiateurs (igroups) autorisés à accéder à des cibles LUN spécifiques. Si un igroup existe déjà, vous pouvez l'attribuer. Vous pouvez également créer des igroups et les attribuer aux LUN.
		
		Vous pouvez utiliser ces méthodes pour interroger, créer, supprimer et modifier respectivement les igroups.
		
		Points à noter:
		
		• `POST`: Lors de la création d'un igroup, vous pouvez désigner la VM de stockage à laquelle vous souhaitez affecter l'accès.
		• `DELETE`: Vous devez fournir la clé de l'igroup comme paramètre d'entrée pour supprimer un igroup spécifique. Si vous avez déjà affecté un igroup à un LUN, vous ne pouvez pas supprimer cet igroup.
		• `PATCH`: Pour modifier un igroup particulier, vous devez fournir la clé igroup comme paramètre d'entrée. Vous devez également indiquer la propriété à mettre à jour, ainsi que sa valeur.

Verbe HTTP	Chemin	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		Vous pouvez utiliser ces méthodes pour afficher, créer, supprimer et modifier des machines virtuelles de stockage (VM de stockage).
		
		• `POST:` Vous devez saisir l'objet de machine virtuelle 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 spécifique.
		
		• `PATCH:` Vous devez fournir la clé de la machine virtuelle de stockage pour modifier une machine virtuelle de stockage spécifique. Vous devez également saisir les propriétés que vous souhaitez mettre à jour, ainsi que leurs valeurs.

Points à noter:

Si vous avez activé le provisionnement des workloads basé sur les SLO dans votre environnement, lors de la création de la machine virtuelle de stockage, assurez-vous qu'elle prend en charge tous les protocoles nécessaires au provisionnement des LUN et des partages de fichiers sur celle-ci, par exemple, CIFS ou SMB, NFS, FCP et iSCSI. Les flux de travail de provisionnement risquent d'échouer si la machine virtuelle de stockage ne prend pas en charge les services requis. Il est recommandé d'activer également sur la machine virtuelle de stockage les services correspondant aux types de workloads respectifs.

Si vous avez activé le provisionnement des workloads basé sur les SLO dans votre environnement, vous ne pouvez pas supprimer la machine virtuelle de stockage sur laquelle des workloads de stockage ont été provisionnés. Lorsque vous supprimez une machine virtuelle de stockage sur laquelle un serveur CIFS ou SMB a été configuré, cette API supprime également le serveur CIFS ou SMB, ainsi que la configuration Active Directory locale. Toutefois, le nom du serveur CIFS ou SMB reste présent dans la configuration Active Directory, que vous devez supprimer manuellement du serveur Active Directory.

API pour les éléments de réseau de votre centre de données

Les API suivantes de la catégorie datacenter récupèrent des informations sur les ports et les interfaces réseau de votre environnement, notamment 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 les informations relatives à tous les ports Ethernet de votre environnement de centre de données. Avec une clé de port comme paramètre d'entrée, vous pouvez consulter les informations de ce port spécifique. Les informations récupérées incluent notamment les détails du cluster, le domaine de diffusion, les détails du port, tels que l'état, la vitesse et le type, ainsi que si le port est activé.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des interfaces FC dans votre environnement de centre de données. En spécifiant une clé d'interface comme paramètre d'entrée, vous pouvez afficher les informations de cette interface spécifique. Les informations, telles que les détails du cluster, du nœud d'origine et du port d'attache, sont récupérées.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Récupère des informations sur tous les ports FC utilisés dans les nœuds de votre environnement de centre de données. En utilisant une clé de port comme paramètre d'entrée, vous pouvez afficher les informations de ce port spécifique. Des informations telles que les détails du cluster, la description du port, le protocole pris en charge et l'état du port sont récupérées.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Vous pouvez utiliser cette méthode pour afficher les détails des interfaces IP dans votre environnement de data center. Avec une clé d'interface comme paramètre d'entrée, vous pouvez afficher les informations de cette interface spécifique. Les informations récupérées incluent notamment les détails du cluster, de l'IPspace, du nœud d'origine et l'activation ou non du basculement.

Accédez aux API ONTAP via un accès proxy dans Active IQ Unified Manager

Les API de passerelle vous offrent l'avantage 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 API Gateway est activée dans l'interface web de Unified Manager.

Les API REST de Unified Manager ne prennent en charge qu'un ensemble limité d'actions à effectuer sur les sources de données de Unified Manager, à savoir les clusters ONTAP. Vous pouvez utiliser les autres fonctionnalités via les API ONTAP. Les API de passerelle permettent à Unified Manager de servir d'interface de relais pour acheminer toutes les requêtes d'API à exécuter sur les clusters ONTAP qu'il gère, sans vous connecter individuellement à chaque cluster de data center. Unified Manager sert de point de gestion unique pour exécuter les API sur les clusters ONTAP gérés par votre instance de Unified Manager. La fonctionnalité API Gateway permet à Unified Manager de constituer un plan de contrôle unique à partir duquel vous pouvez gérer plusieurs clusters ONTAP, sans vous y connecter individuellement. Les API de passerelle vous permettent de rester connecté à Unified Manager et de gérer les clusters ONTAP en exécutant des opérations d'API REST ONTAP.

Tous les utilisateurs peuvent exécuter une requête à l'aide de l'opération GET. Les administrateurs d'applications peuvent exécuter toutes les opérations REST ONTAP.

La passerelle sert de proxy pour acheminer les requêtes API en conservant l'en-tête et le corps des requêtes dans le même format que dans les API ONTAP. Vous pouvez utiliser vos identifiants Unified Manager et exécuter les opérations spécifiques pour accéder aux clusters ONTAP et les gérer sans avoir à transmettre les identifiants de chaque cluster. Elle continue de gérer l'authentification et l'administration des clusters, mais redirige les requêtes API pour qu'elles s'exécutent directement sur le cluster concerné. La réponse renvoyée par les API est identique à celle renvoyée par les API REST ONTAP correspondantes 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 en fonction de l'UUID du cluster, ou identifiant unique universel (UUID). Les API de passerelle récupèrent uniquement les clusters pris en charge par ONTAP 9.5 ou version ultérieure, et ajoutés à Unified Manager via HTTPS.

Verbe HTTP	Chemin (URL)	Description

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (non disponible sur Swagger)
 	
`HEAD` (non disponible sur Swagger)
	`/gateways/{uuid}/{path}`
	
	La valeur de {uuid} doit être remplacée par l'UUID du cluster sur lequel l'opération REST doit être effectuée. Assurez-vous également que cet UUID correspond à un cluster pris en charge par ONTAP 9.5 ou version ultérieure, et ajouté à Unified Manager via HTTPS. {path} doit être remplacé par l'URL REST ONTAP. Vous devez supprimer `/api/` de l'URL.
		Il s'agit d'une API proxy à point d'accès unique, prenant en charge les opérations POST, DELETE, PATCH et GET pour toutes les API REST ONTAP. Aucune restriction ne s'applique à l'une quelconque des API tant qu'elle est prise en charge par ONTAP. La fonctionnalité de tunneling ou de proxy ne peut pas être désactivée.
		
		La méthode `OPTIONS` renvoie toutes les opérations prises en charge par une API REST ONTAP. Par exemple, si une API ONTAP ne prend en charge que l'opération `GET`, l'exécution de la méthode `OPTIONS` à l'aide de cette API de passerelle renvoie `GET` comme réponse. Cette méthode n'est pas prise en charge dans Swagger, mais peut être exécutée avec d'autres outils d'API.
		
		La `OPTIONS` méthode détermine si une ressource est disponible. Cette opération peut être utilisée pour consulter les métadonnées d'une ressource dans les en-têtes de réponse HTTP. Cette méthode n'est pas prise en charge par Swagger, mais peut être exécutée dans d'autres outils API.

Comprendre le tunneling de l'API Gateway

Les API de passerelle vous permettent de gérer les objets ONTAP via Unified Manager. Unified Manager gère les clusters et les informations d'authentification, puis redirige les requêtes vers le point de terminaison REST ONTAP. L'API de passerelle transforme l'URL et les liens HATEOAS (Hypermedia as the Engine of Application State) dans l'en-tête et le corps de la réponse avec l'URL de base de la passerelle API. L'API de passerelle agit comme l'URL de base du proxy à laquelle vous ajoutez l'URL REST ONTAP et exécutez le point de terminaison REST ONTAP requis.

Pour qu'une API ONTAP s'exécute correctement via la passerelle API, l'API doit être prise en charge par cette version du cluster ONTAP sur laquelle elle est exécutée. L'exécution d'une API qui n'est pas prise en charge sur le cluster ONTAP ne renvoie aucun résultat.

Dans cet exemple, l'API de passerelle (URL de base du proxy) est : `/gateways/{uuid}/`

L'API ONTAP utilisée est la suivante : `/storage/volumes`. Vous devez ajouter l'URL REST de l'API ONTAP comme valeur du paramètre path.

Lors de l'ajout du chemin, assurez-vous d'avoir supprimé le « /`" symbol at the beginning of the URL. For the API `/storage/volumes, add 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 balise /api de l'URL REST ONTAP est supprimée de l'URL ajoutée, tandis que celle de l'API de passerelle est conservée.

Exemple de commande cURL

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

L'API renvoie la liste des volumes de stockage de ce cluster. Le format de la réponse est identique à celui que vous obtenez lorsque vous exécutez la même API depuis ONTAP. Les codes d'état renvoyés sont les codes d'état REST d'ONTAP.

Définir l'étendue de l'API

Toutes les API ont un contexte défini dans la portée du cluster. Les API qui fonctionnent sur la base des machines virtuelles de stockage ont également le cluster comme portée, c'est-à-dire que les opérations d'API sont exécutées sur une machine virtuelle de stockage particulière au sein d'un cluster géré. Lorsque vous exécutez l' `/gateways/{uuid}/{path}`API, veillez à saisir l'UUID du cluster (UUID de la source de données Unified Manager) pour le cluster sur lequel vous exécutez l'opération. Pour définir le contexte sur une machine virtuelle de stockage particulière dans ce cluster, saisissez 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 comme filtre dans l'en-tête de chaîne, et l'opération s'exécute dans la portée de cette machine virtuelle de stockage à l'intérieur de ce cluster.

Exemple de commande cURL

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-
00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-
SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f"
-H "Authorization: Basic <Base64EncodedCredentials>"
```

Pour plus d'informations sur l'utilisation des API REST ONTAP, consultez "Automatisation de l'API REST ONTAP"

Effectuez des tâches administratives à l'aide des API dans Active IQ Unified Manager

Vous pouvez utiliser les API de la administration catégorie pour modifier les

paramètres de sauvegarde, vérifier les informations des fichiers de sauvegarde et les certificats de cluster, et également gérer les clusters ONTAP en tant que sources de données d'Active IQ Unified Manager.

Vous devez disposer du rôle Application Administrator pour exécuter ces opérations. Vous pouvez également utiliser l'interface utilisateur web de Unified Manager pour configurer ces paramètres.

Verbe HTTP	Chemin	Description

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Vous pouvez utiliser la `GET` méthode pour consulter les paramètres de la planification des sauvegardes configurée par défaut dans Unified Manager. Vous pouvez vérifier les éléments suivants :
		• Si la planification est activée ou désactivée
		• Fréquence de la sauvegarde programmée (quotidienne ou hebdomadaire)
		• Heure de la sauvegarde
		• Nombre maximal de fichiers de sauvegarde à conserver dans l'application
		
		L'heure de la sauvegarde est exprimée dans le fuseau horaire du serveur.
		
		Les paramètres de sauvegarde de la base de données sont disponibles par défaut sur Unified Manager, et vous ne pouvez pas créer de planification de sauvegarde. Cependant, vous pouvez utiliser la `PATCH`méthode pour modifier les paramètres par défaut.

Verbe HTTP	Chemin	Description
GET	/admin/backup-file-info	Un fichier de vidage de sauvegarde est généré chaque fois que la planification de sauvegarde est modifiée pour Unified Manager. Vous pouvez utiliser cette méthode pour vérifier si le fichier de sauvegarde est généré conformément aux paramètres de sauvegarde modifiés et si les informations du fichier correspondent aux paramètres modifiés.
GET	/admin/datasource-certificate	Cette méthode permet de consulter le certificat de la source de données (cluster) dans le magasin de certificats de confiance. La validation du certificat est requise avant d'ajouter un cluster ONTAP comme source de données pour 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 de l'hôte, son nom d'utilisateur et son mot de passe. Pour modifier et supprimer un cluster géré comme source de données par Unified Manager, utilisez la clé de cluster ONTAP.

Gérer les utilisateurs dans Active IQ Unified Manager à l'aide des API

Vous pouvez utiliser les API de la `security` catégorie pour contrôler l'accès des utilisateurs aux objets de cluster sélectionnés dans Active IQ Unified Manager. Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données. Vous pouvez également ajouter des utilisateurs ou des groupes distants appartenant à un serveur d'authentification. En fonction des privilèges des rôles que vous attribuez aux utilisateurs, ils peuvent gérer les objets de stockage ou afficher les données dans Unified Manager.

Vous devez disposer du rôle Application Administrator pour exécuter ces opérations. Vous pouvez également utiliser l'interface utilisateur web de Unified Manager pour configurer ces paramètres.

Les API de cette `security` catégorie utilisent le paramètre « users », c'est-à-dire le nom d'utilisateur, et non le paramètre « key » comme identifiant unique de l'entité utilisateur.

Verbe HTTP	Chemin	Description

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Vous pouvez utiliser ces méthodes pour obtenir les informations des utilisateurs ou ajouter un nouvel utilisateur à Unified Manager.
		
		Vous pouvez attribuer des rôles spécifiques aux utilisateurs en fonction de leur type d'utilisateur. Lors de l'ajout d'utilisateurs, vous devez fournir les mots de passe de l'utilisateur local, de l'utilisateur de maintenance et de l'utilisateur de la base de données.

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	La méthode GET permet de récupérer toutes les informations d'un utilisateur, telles que son nom, son adresse e-mail, son rôle et son type d'autorisation. La méthode PATCH permet de mettre à jour ces informations. La méthode DELETE permet de supprimer l'utilisateur.

Consultez les indicateurs de performance à l'aide des API dans Active IQ Unified Manager

Active IQ Unified Manager met à votre disposition un ensemble d'API sous la catégorie `/datacenter` qui vous permettent de visualiser les données de performance de vos clusters et objets de stockage dans un centre de données. Ces API récupèrent les données de performance des différents objets de stockage tels que les clusters, les nœuds, les LUN, les volumes, les agrégats, les machines virtuelles de stockage, les interfaces FC, les ports FC, les ports Ethernet et les interfaces IP.

Les `/metrics` et `/analytics` API offrent différentes vues des indicateurs de performance, grâce auxquelles vous pouvez explorer différents niveaux de détail pour les objets de stockage suivants dans votre centre de données :

- clusters
- nœuds
- machines virtuelles de stockage
- agrégats

- volumes
- LUN
- Interfaces FC
- Ports FC
- ports Ethernet
- Interfaces IP

Le tableau suivant compare les API `/metrics` et `/analytics` en ce qui concerne les caractéristiques des données de performance récupérées.

Métriques	**Analytique**
Détails de performance pour un objet unique. Par exemple, l' `/datacenter/cluster/clusters/{key}/metrics`API exige que la clé du cluster soit saisie comme paramètre de chemin pour récupérer les métriques de ce cluster spécifique.	Détails des performances de plusieurs objets du même type dans un centre de données. Par exemple, l' `/datacenter/cluster/clusters/analytics` API récupère les métriques globales de tous les clusters d'un centre de données.
Exemple de métriques de performance pour un objet de stockage en fonction du paramètre d'intervalle de temps pour la récupération.	La valeur agrégée globale des performances pour un certain type d'objet de stockage sur une période donnée (supérieure à 72 heures).
Les informations de base de l'objet sont récupérées, telles que celles d'un nœud ou d'un cluster.	Aucun détail précis n'a été récupéré.
Les compteurs cumulés, tels que le minimum, le maximum, le 95e percentile et les valeurs de performance moyennes sur une période donnée, sont extraits pour un seul objet, comme les compteurs de lecture, d'écriture, de total et autres.	Une seule valeur agrégée est affichée pour tous les objets du même type.

Métriques	Analytique
La plage horaire et les données d'échantillonnage sont basées sur le calendrier suivant : la plage horaire des données. Les exemples peuvent être 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m. Vous obtenez des échantillons d'une heure si la plage est supérieure à 3 jours (72 hr) ; sinon, il s'agit d'échantillons de 5 minutes. La période pour chaque plage horaire est la suivante : • 1h: métriques de la dernière heure échantillonnées sur 5 minutes. • 12h: Métriques des 12 dernières heures échantillonnées toutes les 5 minutes. • 1j: Métriques sur la journée la plus récente, échantillonnées toutes les 5 minutes. • 2d: Métriques sur les 2 derniers jours échantillonnées toutes les 5 minutes. • 3d: Métriques sur les 3 derniers jours échantillonnées toutes les 5 minutes. • 15j: Métriques des 15 derniers jours échantillonnées sur 1 heure. • 1 sem.: Métriques sur la semaine la plus récente échantillonnées sur 1 heure. • 1m: Métriques du mois le plus récent échantillonnées sur 1 heure. • 2m: Métriques des 2 derniers mois échantillonnées sur 1 heure. • 3m: Métriques sur les 3 derniers mois échantillonnées sur 1 heure. • 6m: Métriques des 6 derniers mois échantillonnées sur 1 heure. Valeurs disponibles : 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m Valeur par défaut : 1h	Plus de 72 heures. La durée sur laquelle cet échantillon est calculé est représentée au format de la norme ISO-8601.

Exemple de sortie pour les API de métriques

Par exemple, l' `/datacenter/cluster/nodes/{key}/metrics` API récupère les détails suivants (entre autres) pour un nœud :

> Le 95e percentile dans la valeur récapitulative indique que 95 % des échantillons collectés pour la période ont une valeur de compteur inférieure à la valeur spécifiée comme 95e percentile.

```
{
```

```
      "iops": {
        "local": {
          "other": 100.53,
          "read": 100.53,
          "total": 100.53,
          "write": 100.53
        },
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "latency": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "performance_capacity": {
        "available_iops_percent": 0,
        "free_percent": 0,
        "system_workload_percent": 0,
        "used_percent": 0,
        "user_workload_percent": 0
      },
      "throughput": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "timestamp": "2018-01-01T12:00:00-04:00",
      "utilization_percent": 0
    }
  ],
  "start_time": "2018-01-01T12:00:00-04:00",
  "summary": {
    "iops": {
      "local_iops": {
        "other": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "read": {
```

```
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "total": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "write": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        }
      },
```

Exemple de sortie pour les API analytiques

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 en détail les API `/metrics` et `/analytics`.

> Les IOPS et les indicateurs de performance renvoyés par ces API sont des valeurs doubles, par exemple `100.53`. Le filtrage de ces valeurs flottantes par le caractère pipe (|) et le caractère générique (*) n'est pas pris en charge.

Verbe HTTP	Chemin	Description
`GET`	`/datacenter/cluster/clusters/{key}/metrics`	Récupère les données de performance (échantillon et résumé) d'un cluster spécifié par le paramètre d'entrée de la clé du cluster. Les informations renvoyées comprennent la clé et l'UUID du cluster, la plage horaire, les IOPS, le débit et le nombre d'échantillons.
`GET`	`/datacenter/cluster/clusters/analytics`	Récupère des mesures de performance de haut niveau pour tous les clusters d'un centre de données. Vous pouvez filtrer vos résultats selon les critères requis. Les valeurs renvoyées incluent les IOPS agrégées, le débit et la période de collecte (en heures).

Verbe HTTP	Chemin	Description
GET	/datacenter/cluster/nodes/{key}/metrics	Récupère les données de performance (échantillon et résumé) d'un nœud spécifié par le paramètre d'entrée de la clé du nœud. Les informations renvoyées comprennent l'UUID du nœud, la plage horaire, un résumé des IOPS, du débit, de la latence et des performances, le nombre d'échantillons collectés et le pourcentage d'utilisation.
GET	/datacenter/cluster/nodes/analytics	Récupère des indicateurs de performance de haut niveau pour tous les nœuds d'un centre de données. Vous pouvez filtrer les résultats selon les critères souhaités. Les informations renvoyées comprennent les clés des nœuds et des clusters, ainsi que les valeurs telles que les IOPS agrégées, le débit et la période de collecte (en heures).
GET	/datacenter/storage/aggregates/{key}/metrics	Récupère les données de performance (échantillon et résumé) d'un agrégat spécifié par le paramètre d'entrée de la clé d'agrégat. Les informations renvoyées comprennent la plage temporelle, le résumé des IOPS, la latence, le débit et la capacité de performance, le nombre d'échantillons collectés pour chaque compteur et le pourcentage d'utilisation.
GET	/datacenter/storage/aggregates/analytics	Récupère des indicateurs de performance de haut niveau pour tous les agrégats d'un centre de données. Vous pouvez filtrer les résultats selon les critères souhaités. Les informations renvoyées comprennent les clés des agrégats et des clusters, ainsi que les valeurs telles que les IOPS agrégées, le débit et la période de collecte (en heures).

Verbe HTTP	Chemin	Description

GET	`/datacenter/storage/luns/{key}/metrics`
	
	`/datacenter/storage/volumes/{key}/metrics`
		Récupère les données de performance (échantillon et résumé) d'un LUN ou d'un partage de fichiers (volume) spécifié par le paramètre d'entrée de la clé LUN ou de volume. Les informations renvoyées comprennent le résumé des valeurs minimales, maximales et moyennes des IOPS en lecture, en écriture et totales, la latence et le débit, ainsi que le nombre d'échantillons collectés pour chaque compteur.

GET	`/datacenter/storage/luns/analytics`
	
	`/datacenter/storage/volumes/analytics`
		Récupère des indicateurs de performance de haut niveau pour tous les LUN ou volumes d'un centre de données. Vous pouvez filtrer vos résultats selon les critères requis. Des informations, telles que les clés des machines virtuelles de stockage et des clusters, 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 performance (échantillon et résumé) d'une machine virtuelle de stockage spécifiée par le paramètre d'entrée de la clé de la machine virtuelle de stockage. Un résumé des IOPS basé sur chaque protocole pris en charge, tels que `nvmf`, `fcp`, `iscsi`, et `nfs`, ainsi que le débit, la latence et le nombre d'échantillons collectés sont renvoyés.
GET	`/datacenter/svm/svms/analytics`	Récupère des indicateurs de performance de haut niveau pour toutes les machines virtuelles de stockage d'un centre de données. Vous pouvez filtrer vos résultats selon les critères requis. Les informations renvoyées incluent l'UUID de la machine virtuelle de stockage, les IOPS agrégées, la latence, le débit et la période de collecte (en heures).

Verbe HTTP	Chemin	Description
GET	/datacenter/network/ethernet/ports/{key}/metrics	Récupère les indicateurs de performance d'un port Ethernet spécifique, indiqué par le paramètre d'entrée de la clé de port. Lorsqu'un intervalle (plage de temps) est fourni dans la plage prise en charge, l'API renvoie les compteurs cumulés, tels que les valeurs de performance minimales, maximales et moyennes sur la période considérée.
GET	/datacenter/network/ethernet/ports/analytics	Récupère les indicateurs de performance de haut niveau de tous les ports Ethernet de votre environnement de centre de données. Les informations renvoyées incluent notamment la clé et l'UUID du cluster et du nœud, le débit, la période de collecte et le pourcentage d'utilisation des ports. Vous pouvez filtrer le résultat à l'aide des paramètres disponibles, tels que la clé du port, le pourcentage d'utilisation, le nom et l'UUID du cluster et du nœud, etc.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Récupère les indicateurs de performance d'une interface FC réseau spécifique, indiquée par le paramètre d'entrée de la clé d'interface. Lorsqu'un intervalle (plage de temps) est fourni dans la plage prise en charge, l'API renvoie les compteurs cumulés, tels que les valeurs de performance minimales, maximales et moyennes sur la période considérée.

Verbe HTTP	Chemin	Description
GET	/datacenter/network/fc/interfaces/analytics	Récupère les indicateurs de performance de haut niveau de tous les ports Ethernet de l'environnement de votre centre de données. Les informations renvoyées incluent notamment la clé et l'UUID du cluster et de l'interface FC, le débit, les IOPS, la latence et la machine virtuelle de stockage. Vous pouvez filtrer le résultat à l'aide des paramètres disponibles, tels que le nom et l'UUID du cluster et de l'interface FC, la machine virtuelle de stockage, le débit, etc.
GET	/datacenter/network/fc/ports/{key}/metrics	Récupère les indicateurs de performance d'un port FC spécifique indiqué par le paramètre d'entrée de la clé de port. Lorsqu'un intervalle (plage de temps) est fourni dans la plage prise en charge, l'API renvoie les compteurs cumulés, tels que les valeurs de performance minimales, maximales et moyennes sur la période considérée.
GET	/datacenter/network/fc/ports/analytics	Récupère les indicateurs de performance de haut niveau de tous les ports FC de votre environnement de centre de données. Les informations renvoyées comprennent notamment la clé et l'UUID du cluster et du nœud, le débit, la période de collecte et le pourcentage d'utilisation des ports. Vous pouvez filtrer le résultat à l'aide des paramètres disponibles, tels que la clé du port, le pourcentage d'utilisation, le nom et l'UUID du cluster et du nœud, etc.

Verbe HTTP	Chemin	Description
GET	/datacenter/network/ip/interfaces/{key}/metrics	Récupère les indicateurs de performance d'une interface IP réseau, conformément au paramètre d'entrée de la clé d'interface. Lorsqu'un intervalle (plage de temps) est fourni dans la plage prise en charge, l'API renvoie des informations telles que le nombre d'échantillons, les compteurs cumulés, le débit et le nombre de paquets reçus et transmis.
GET	/datacenter/network/ip/interfaces/analytics	Récupère les indicateurs de performance de haut niveau de toutes les interfaces IP réseau de votre environnement de centre de données. Les informations renvoyées incluent notamment la clé et l'UUID du cluster et de l'interface IP, le débit, les IOPS et la latence. Vous pouvez filtrer le résultat à l'aide des paramètres disponibles, tels que le nom et l'UUID du cluster et de l'interface IP, les IOPS, la latence, le débit, etc.

Affichez les tâches et les détails du système à l'aide des API dans Active IQ Unified Manager

Vous pouvez utiliser l `jobs`API de la catégorie `management-server` pour consulter les détails d'exécution des opérations asynchrones. L `system`API de la catégorie `management-server` vous permet de consulter les détails de l'instance dans votre environnement Active IQ Unified Manager.

Voir les offres d'emploi

Dans Active IQ Unified Manager, les opérations, telles que l'ajout et la modification de ressources, sont effectuées par des appels d'API synchrones et asynchrones. Les appels planifiés pour une exécution asynchrone peuvent être suivis par un objet Job créé pour cet appel. Chaque objet Job possède une clé unique d'identification. Chaque objet Job renvoie l'URI de l'objet Job pour vous permettre d'accéder à la tâche et d'en suivre la progression. Vous pouvez utiliser cette API pour récupérer les détails de chaque exécution.

Cette API vous permet d'interroger tous les objets Job de votre centre de données, y compris les données historiques. Par défaut, l'interrogation de tous les jobs renvoie les détails des 20 derniers jobs déclenchés via l'interface web et l'API. Utilisez les filtres intégrés pour afficher des jobs spécifiques. Vous pouvez également utiliser la clé Job pour consulter les détails d'un job spécifique et exécuter le prochain ensemble d'opérations sur les ressources.

Catégorie	Verbe HTTP	Chemin	Description
serveur de gestion	GET	`/management-server/jobs`	Renvoie les détails de toutes les tâches. Sans ordre de tri, le dernier objet Job soumis apparaît en premier.
serveur de gestion	GET	`/management-server/jobs/{key}` Saisissez la clé du job de l'objet Job pour afficher les détails spécifiques de ce job.	Renvoie les détails de l'objet Job spécifique.

Afficher les détails du système

En utilisant l' `/management-server/system`API, vous pouvez interroger les détails spécifiques à votre instance Unified Manager. L'API renvoie des informations sur le produit et les services, telles que la version d'Unified Manager installée sur votre système, son UUID, le nom du fournisseur, le système d'exploitation hôte, ainsi que le nom, la description et l'état des services exécutés sur l'instance Unified Manager.

Catégorie	Verbe HTTP	Chemin	Description
serveur de gestion	GET	`/management-server/system`	Aucun paramètre d'entrée n'est requis pour exécuter cette API. Les informations système de l'instance Unified Manager actuelle sont renvoyées par défaut.

Gérez les événements et les alertes à l'aide des API dans Active IQ Unified Manager

Les `events`, `alerts` et `scripts` API de la catégorie `management-server` vous permettent de gérer les événements, les alertes et les scripts associés aux alertes dans votre environnement Active IQ Unified Manager.

Afficher et modifier les événements

Unified Manager reçoit les événements générés sur ONTAP pour les clusters qu'il surveille et gère. Grâce à ces API, vous pouvez consulter, résoudre et mettre à jour les événements générés pour vos clusters.

En exécutant la `GET` méthode de l' `/management-server/events`API, vous pouvez interroger les événements de votre centre de données, y compris les données historiques. Utilisez les filtres intégrés, tels que le nom, le niveau d'impact, la zone d'impact, la gravité, l'état, le nom de la ressource et le type de ressource, pour afficher des événements spécifiques. Les paramètres de type de ressource et de zone renvoient des informations sur l'objet de stockage sur lequel l'événement s'est produit, et la zone d'impact renvoie des informations sur le problème pour lequel l'événement est généré, comme la disponibilité, la capacité, la configuration, la sécurité, la protection et les performances.

En exécutant l'opération PATCH pour cette API, vous pouvez activer le workflow de résolution pour

l'événement. Vous pouvez vous attribuer un événement ou l'attribuer à un autre utilisateur et en accuser réception. Après avoir effectué les étapes nécessaires sur les ressources pour résoudre le problème qui a déclenché l'événement, vous pouvez utiliser cette API pour marquer l'événement comme résolu.

Pour plus d'informations sur les événements, voir "Découvrez les événements de la plateforme Active IQ".

Catégorie	Verbe HTTP	Chemin	Description
serveur de gestion	GET	`/management-server/events` `/management-server/events/{key}`	Lorsque vous exécutez la méthode Get ALL, le corps de la réponse contient les détails de tous les événements de votre centre de données. Lorsque vous récupérez les détails d'un événement à l'aide d'une clé spécifique, vous pouvez consulter les informations relatives à un événement particulier et exécuter les opérations suivantes sur les ressources. Le corps de la réponse contient alors les détails de cet événement.
serveur de gestion	CORRECTIF	`management-server/events/{key}`	Utilisez cette API pour attribuer un événement ou modifier son état en accusé de réception ou résolu. Vous pouvez également l'utiliser pour vous attribuer l'événement ou l'attribuer à un autre utilisateur. Il s'agit d'une opération synchrone.

Gérer les alertes

Les événements sont générés automatiquement et en continu. Unified Manager génère une alerte uniquement lorsqu'un événement répond à certains critères de filtrage. 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 envoyer automatiquement des notifications lorsque des événements spécifiques ou des événements de certains niveaux de gravité se produisent.

Pour plus d'informations sur les alertes, consultez "Découvrez les alertes".

Catégorie	Verbe HTTP	Chemin	Description
serveur de gestion	GET	`/management-server/alerts` `/management-server/alerts/{key}`	Consultez toutes les alertes existantes dans votre environnement ou une alerte spécifique à l'aide de la clé d'alerte. Vous pouvez visualiser les informations relatives aux alertes générées dans votre environnement, telles que la description, l'action, l'adresse e-mail de notification, l'événement et le niveau de gravité.
serveur de 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 auquel l'alerte s'applique, indiquer si l'alerte est activée et si vous émettez des traps SNMP. Vous pouvez ajouter des détails supplémentaires pour lesquels vous souhaitez générer l'alerte, tels que l'action, l'adresse e-mail de notification, les détails du script, si vous ajoutez un script d'alerte, etc.
serveur de gestion	PATCH et DELETE	`management-server/events/{key}`	Vous pouvez utiliser ces méthodes pour modifier et supprimer des alertes spécifiques. Vous pouvez modifier différents attributs, tels que la description, le nom et l'activation ou la désactivation de l'alerte. Vous pouvez supprimer une alerte lorsqu'elle n'est plus nécessaire.

Lors de la sélection d'une ressource pour l'ajout d'une alerte, veuillez noter que la sélection d'un cluster ne sélectionne pas automatiquement les objets de stockage qu'il contient. Par exemple, si vous créez une alerte pour tous les événements critiques de tous les clusters, vous ne recevrez d'alertes que pour les événements critiques des clusters. Vous ne recevrez pas

d’alertes pour les événements critiques sur les nœuds, les agrégats, etc.

Gérer les scripts

Grâce à l' `/management-server/scripts`API, vous pouvez également associer une alerte à un script qui s’exécute 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 s’exécute. Vous pouvez charger des scripts personnalisés et tester leur exécution lorsqu’une alerte est générée. Vous pouvez associer une alerte à votre script afin que celui-ci s’exécute lorsqu’une alerte est déclenchée pour un événement dans Unified Manager.

Pour plus d’informations sur les scripts, voir "Gérer les scripts".

Catégorie	Verbe HTTP	Chemin	Description
serveur de gestion	GET	`/management-server/scripts`	Utilisez cette API pour interroger tous les scripts existants dans votre environnement. Utilisez les fonctions de filtrage et de tri standard pour afficher uniquement les scripts souhaités.
serveur de gestion	POST	`/management-server/scripts`	Utilisez cette API pour ajouter une description au script et télécharger le fichier de script associé à une alerte.

Gérer les workloads

Visualisez les charges de travail de stockage à l’aide des API dans Active IQ Unified Manager

Les API listées ici vous permettent de consulter une liste consolidée des charges de travail de stockage pour tous les clusters ONTAP de votre centre de données. Elles fournissent également une vue récapitulative du nombre de charges de travail de stockage provisionnées dans votre environnement Active IQ Unified Manager, ainsi que de leurs statistiques de capacité et de performances (IOPS).

Afficher les charges de travail du stockage

Vous pouvez utiliser la méthode suivante pour visualiser toutes les charges de travail de stockage dans tous les clusters de votre centre de données. Pour plus d’informations sur le filtrage de la réponse en fonction de colonnes spécifiques, consultez la documentation de référence de l’API disponible dans votre instance Unified Manager.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/workloads`

Résumé des charges de travail de stockage

Vous pouvez utiliser la méthode suivante pour évaluer la capacité utilisée, la capacité disponible, les IOPS utilisées, les IOPS disponibles et le nombre de charges de travail de stockage gérées par chaque Performance Service Level. Les charges de travail de stockage affichées peuvent concerner n'importe quelle LUN, partage de fichiers NFS ou partage CIFS. L'API fournit une vue d'ensemble des charges de travail de stockage, une vue d'ensemble des charges de travail de stockage provisionnées par Unified Manager, une vue d'ensemble du centre de données, ainsi qu'une vue d'ensemble de l'espace total, utilisé et disponible et des IOPS dans le centre de données, en fonction des Performance Service Levels attribués. Les informations reçues en réponse à cette API sont utilisées pour alimenter le tableau de bord de l'interface utilisateur de Unified Manager.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/workloads-summary`

Gérez les points de terminaison d'accès à l'aide des API dans Active IQ Unified Manager

Vous devez créer des points de terminaison d'accès ou des interfaces logiques (LIF), nécessaires au provisionnement des machines virtuelles de stockage (SVM), des LUN et des partages de fichiers. Vous pouvez consulter, créer, modifier et supprimer les points de terminaison d'accès des SVM, des LUN ou des partages de fichiers dans votre environnement Active IQ Unified Manager.

Afficher les points de terminaison d'accès

Vous pouvez consulter la liste des points de terminaison d'accès de votre environnement Unified Manager en procédant comme suit. Pour obtenir la liste des points de terminaison d'accès d'une SVM, d'un LUN ou d'un partage de fichiers spécifique, vous devez saisir l'identifiant unique de cette SVM, de ce LUN ou de ce partage de fichiers. Vous pouvez également saisir la clé unique du point de terminaison d'accès pour récupérer les détails de ce point de terminaison d'accès particulier.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Ajouter des points de terminaison d'accès

Vous pouvez créer des points de terminaison d'accès personnalisés et leur attribuer les propriétés requises. Vous devez saisir les détails du point de terminaison d'accès que vous souhaitez créer comme paramètres d'entrée. Vous pouvez utiliser cette API, System Manager ou ONTAP CLI pour créer un point de terminaison d'accès sur chaque nœud. Les adresses IPv4 et IPv6 sont prises en charge pour la création de points de terminaison d'accès.

Pour le provisionnement des LUN et des partages de fichiers, vous devez configurer votre SVM avec un nombre minimal de points d'accès par nœud. Il est recommandé de configurer votre SVM avec au moins deux points d'accès par nœud : l'un prenant en charge les protocoles CIFS et/ou NFS, et l'autre les protocoles iSCSI ou FCP.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

Supprimer les points de terminaison d'accès

Vous pouvez supprimer un point de terminaison d'accès spécifique en utilisant la méthode suivante. Vous devez fournir la clé du point de terminaison d'accès comme paramètre d'entrée pour supprimer un point de terminaison d'accès particulier.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	`/storage-provider/access-endpoints/{key}`

Modifier les points de terminaison d'accès

Vous pouvez modifier un point de terminaison d'accès et mettre à jour ses propriétés en utilisant la méthode suivante. Vous devez fournir la clé du point de terminaison d'accès pour modifier un point de terminaison d'accès particulier. Vous devez également indiquer la propriété à mettre à jour, ainsi que sa valeur.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/access-endpoints/{key}`

Gérez les mappages Active Directory à l'aide des API dans Active IQ Unified Manager

Vous pouvez utiliser les API listées ici pour gérer les mappages Active Directory sur la SVM, nécessaires au provisionnement des partages CIFS sur les SVM. Ces mappages Active Directory doivent être configurés pour associer les SVM à ONTAP.

Afficher les mappages Active Directory

Vous pouvez consulter les détails de configuration des mappages Active Directory d'une SVM en procédant comme suit. Pour afficher les mappages Active Directory sur une SVM, vous devez saisir la clé SVM. Pour interroger les détails d'un mappage particulier, vous devez saisir la clé du mappage.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Ajouter un mappage Active Directory

Vous pouvez créer des mappages Active Directory sur une SVM en utilisant la méthode suivante. Vous devez saisir les détails du mappage en tant que paramètres d'entrée.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/active-directories-mappings`

Gérez les partages de fichiers à l'aide des API dans Active IQ Unified Manager

Vous pouvez utiliser l' `/storage-provider/file-shares`API pour visualiser, ajouter, modifier et supprimer les volumes de partage de fichiers CIFS et NFS dans votre environnement de centre de données.

Avant le provisionnement des volumes de partage de fichiers, assurez-vous que la SVM a été créée et provisionnée avec les protocoles pris en charge. Si vous attribuez des niveaux de service de performance (PSL) ou des stratégies d'efficacité du stockage (SEP), les PSL ou les SEP doivent être créés avant la création des partages de fichiers, lors du provisionnement.

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 comme source de données dans 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 ajoutés automatiquement et manuellement à votre instance Unified Manager. Vous pouvez afficher les détails d'un partage de fichiers spécifique en exécutant cette API avec la clé du partage de fichiers.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Ajouter des partages de fichiers

Vous pouvez utiliser la méthode suivante pour ajouter des partages de fichiers CIFS et NFS dans votre SVM. Vous devez saisir les détails du partage de fichiers que vous souhaitez créer 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 les paramètres des règles d'export sont fournis, des partages CIFS ou des partages de fichiers NFS sont créés. Si vous ne fournissez pas les valeurs des paramètres ACL, aucun partage CIFS n'est créé, et des partages NFS sont créés par défaut, ce qui donne accès à tous.

Création de volumes de protection des données : Lorsque vous ajoutez des partages de fichiers à votre SVM, le type du volume monté est, par défaut, `rw` (lecture-écriture). Pour créer des volumes de protection des données (DP), spécifiez `dp` comme valeur du paramètre `type`.

Supprimer les partages de fichiers

Vous pouvez utiliser la méthode suivante pour supprimer un partage de fichiers spécifique. Vous devez saisir la clé du 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.

Pour modifier un partage de fichiers spécifique, vous devez fournir la clé du partage de fichiers. Vous devez également indiquer la propriété à mettre à jour, ainsi que sa valeur.

Veuillez noter que vous ne pouvez modifier qu'une seule propriété lors d'un seul appel à cette API. Pour effectuer plusieurs modifications, vous devez exécuter cette API autant de fois que nécessaire.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares/{key}`

Gérez les LUN à l'aide des API dans Active IQ Unified Manager

Vous pouvez utiliser l' `/storage-provider/luns`API pour afficher, ajouter, modifier et supprimer les LUN dans votre environnement de centre de données.

Avant de provisionner les LUN, assurez-vous que la SVM a été créée et provisionnée avec les protocoles pris en charge. Si vous attribuez des niveaux de service de performances (PSL) ou des stratégies d'efficacité du stockage (SEP) lors du provisionnement, les PSL ou les SEP doivent être créés avant la création de la LUN.

Afficher les LUN

Vous pouvez utiliser la méthode suivante pour afficher les LUN dans votre environnement Unified Manager. Lorsque vous avez ajouté un cluster ONTAP comme source de données dans Active IQ Unified Manager, les charges de travail de stockage de ces clusters sont automatiquement ajoutées à votre instance Unified Manager. Cette API récupère tous les LUN ajoutés automatiquement et manuellement à votre instance Unified Manager. Vous pouvez afficher les détails d'un LUN spécifique en exécutant cette API avec la clé du LUN.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

Ajouter des LUNs

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 spécifiez une valeur pour le paramètre optionnel `volume_name_tag`, cette valeur sera utilisée lors de la création du LUN pour nommer le volume. Cette étiquette facilite la recherche du volume. Si vous fournissez la clé du volume dans la requête, l'étiquetage est ignoré.

Supprimer des LUN

Vous pouvez utiliser la méthode suivante pour supprimer un LUN spécifique. Vous devez fournir la clé LUN pour supprimer un LUN particulier.

Si vous avez créé un volume dans ONTAP puis provisionné des LUN via Unified Manager sur ce volume, lorsque vous supprimez 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 un LUN et mettre à jour ses propriétés. Vous devez fournir la clé du LUN pour modifier un LUN particulier. Vous devez également indiquer la propriété du LUN que vous souhaitez mettre à jour, ainsi que sa valeur. Pour mettre à jour des baies de LUN à l'aide de cette API, vous devez consulter les recommandations dans « `Recommendations for using the APIs` ».

Vous ne pouvez modifier qu'une seule propriété à la fois lors d'un appel à cette API. Pour effectuer plusieurs modifications, vous devez exécuter cette API autant de fois que nécessaire.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/luns/{key}`

Gérez les niveaux de service de performance à l'aide des API dans Active IQ Unified Manager

Vous pouvez consulter, créer, modifier et supprimer des niveaux de service de performance en utilisant les API du fournisseur de stockage sur votre Active IQ Unified Manager.

Afficher les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour afficher les Performance Service Levels afin de les attribuer aux charges de travail de stockage. L'API répertorie tous les Performance Service Levels définis par le système et créés par l'utilisateur, et récupère les attributs de tous les Performance Service Levels. Si vous souhaitez interroger un Performance Service Level spécifique, vous devez saisir l'identifiant unique du Performance Service Level pour en récupérer les détails.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Ajouter des niveaux de service de performances

Vous pouvez utiliser la méthode suivante pour créer des niveaux de service de performance personnalisés et les affecter à vos charges de travail de stockage si les niveaux de service de performance définis par le système ne répondent pas aux objectifs de niveau de service (SLO) requis. Saisissez les détails du niveau de service de performance que vous souhaitez créer. Pour les propriétés IOPS, assurez-vous de saisir une plage de valeurs valide.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/performance-service-levels`

Supprimer les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour supprimer un Performance Service Level spécifique. Vous ne pouvez pas supprimer un Performance Service Level s'il est attribué à un workload, ou s'il s'agit du seul Performance Service Level disponible. Pour supprimer un Performance Service Level particulier, vous devez fournir son ID unique en tant que paramètre d'entrée.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	`/storage-provider/performance-service-levels/{key}`

Modifier les niveaux de service de performance

Vous pouvez utiliser la méthode suivante pour modifier un niveau de service de performance et mettre à jour ses propriétés. Vous ne pouvez pas modifier un niveau de service de performance défini par le système ou affecté à un workload. Pour modifier un niveau de service de performance particulier, vous devez fournir son identifiant unique. Vous devez également saisir la propriété IOPS à mettre à jour, ainsi qu'une valeur valide.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/performance-service-levels/{key}`

Afficher les capacités de l'agrégat en fonction des Performance Service Levels

Vous pouvez utiliser la méthode suivante pour interroger les capacités des agrégats en fonction des niveaux de service de performance. Cette API renvoie la liste des agrégats disponibles dans votre centre de données

et indique les capacités en termes de niveaux de service de performance qui peuvent être prises en charge par ces agrégats. Lors du provisionnement de workloads sur un volume, vous pouvez consulter la capacité d'un agrégat à prendre en charge un niveau de service de performance particulier et provisionner des workloads en fonction de cette capacité. La possibilité de spécifier l'agrégat n'est disponible que lorsque vous provisionnez un workload à l'aide des API. Cette fonctionnalité n'est pas disponible dans l'interface utilisateur Web de Unified Manager.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Gérez les politiques d'efficacité du stockage à l'aide des API dans Active IQ Unified Manager

Vous pouvez consulter, créer, modifier et supprimer des politiques d'efficacité du stockage à l'aide des API du fournisseur de stockage.

Veuillez noter les points suivants :

- Il n'est pas obligatoire d'attribuer une Storage Efficiency Policy lors de la création d'un workload sur Unified Manager.
- Vous ne pouvez pas dissocier une stratégie d'efficacité du stockage d'un workload après qu'une stratégie lui a été attribuée.
- Si un workload comporte des paramètres de stockage spécifiés sur des volumes ONTAP, tels que la déduplication et la compression, ces paramètres peuvent être remplacés par les paramètres spécifiés dans la stratégie d'efficacité du stockage que vous appliquez lorsque vous ajoutez les workloads de stockage dans Unified Manager.

Consultez les politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour consulter les Storage Efficiency Policies avant de les affecter aux workloads de stockage. Cette API répertorie toutes les Storage Efficiency Policies définies par le système et créées par l'utilisateur, et récupère les attributs de toutes les Storage Efficiency Policies. Si vous souhaitez interroger une Storage Efficiency Policy spécifique, vous devez saisir l'ID unique de la stratégie afin d'en récupérer les détails.

Catégorie	Verbe HTTP	Chemin

fournisseur de stockage	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Ajouter des politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour créer des stratégies d'efficacité du stockage personnalisées et

les affecter à vos workloads de stockage si les stratégies définies par le système ne répondent pas aux exigences de provisionnement de vos workloads de stockage. Saisissez les détails de la stratégie d'efficacité du stockage que vous souhaitez créer comme paramètres d'entrée.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/storage-efficiency-policies`

Supprimer les politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour supprimer une Storage Efficiency Policy spécifique. Vous ne pouvez pas supprimer une Storage Efficiency Policy si elle est affectée à un workload, ou s'il s'agit de la seule Storage Efficiency Policy disponible. Vous devez fournir l'ID unique de la Storage Efficiency Policy comme paramètre d'entrée pour supprimer une Storage Efficiency Policy particulière.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	SUPPRIMER	`/storage-provider/storage-efficiency-policies/{key}`

Modifier les politiques d'efficacité du stockage

Vous pouvez utiliser la méthode suivante pour modifier une stratégie d'efficacité du stockage et mettre à jour ses propriétés. Vous ne pouvez pas modifier une stratégie d'efficacité du stockage définie par le système ou attribuée à un workload. Pour modifier une stratégie d'efficacité du stockage particulière, vous devez fournir son identifiant unique. De plus, vous devez fournir la propriété que vous souhaitez mettre à jour, ainsi que sa valeur.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/storage-efficiency-policies/{key}`

Flux de travail courants pour la gestion du stockage

Comprendre les flux de travail API courants pour la gestion du stockage dans Active IQ Unified Manager

Les flux de travail courants fournissent aux développeurs d'applications clientes des exemples de la manière dont les API Active IQ Unified Manager peuvent être appelées par une application cliente pour exécuter des fonctions courantes de gestion du stockage. Cette section présente quelques-uns de ces exemples de flux de travail.

Les flux de travail décrivent certains cas d'utilisation courants de la gestion du stockage ainsi que des exemples de code à utiliser. Chaque tâche est décrite à l'aide d'un processus de flux de travail comprenant un ou plusieurs appels d'API.

Comprendre les appels d'API utilisés dans les flux de travail

Vous pouvez consulter la page de documentation en ligne depuis 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 utilisé dans les exemples de workflow de ce document comprend uniquement les informations dont vous avez besoin pour localiser l'appel dans la page de documentation. Après avoir localisé un appel d'API spécifique, vous pouvez consulter les détails complets de l'appel, notamment les paramètres d'entrée, les formats de sortie, les codes d'état HTTP et le type de traitement de la requête.

Les informations suivantes sont incluses pour chaque appel d'API au sein d'un flux de travail afin de faciliter la localisation de l'appel sur la page de documentation :

- Catégorie : Les appels d'API sont organisés sur la page de documentation en domaines ou catégories fonctionnellement liés. Pour trouver un appel d'API spécifique, faites défiler la page jusqu'en bas et cliquez sur la catégorie d'API correspondante.
- Verbe HTTP (appel) : le verbe HTTP identifie l'action effectuée sur une ressource. Chaque appel d'API est exécuté via un seul verbe HTTP.
- Chemin : le chemin détermine la ressource spécifique à laquelle l'action s'applique dans le cadre de l'exécution d'un appel. La chaîne de chemin est ajoutée à l'URL de base pour former l'URL complète identifiant la ressource.

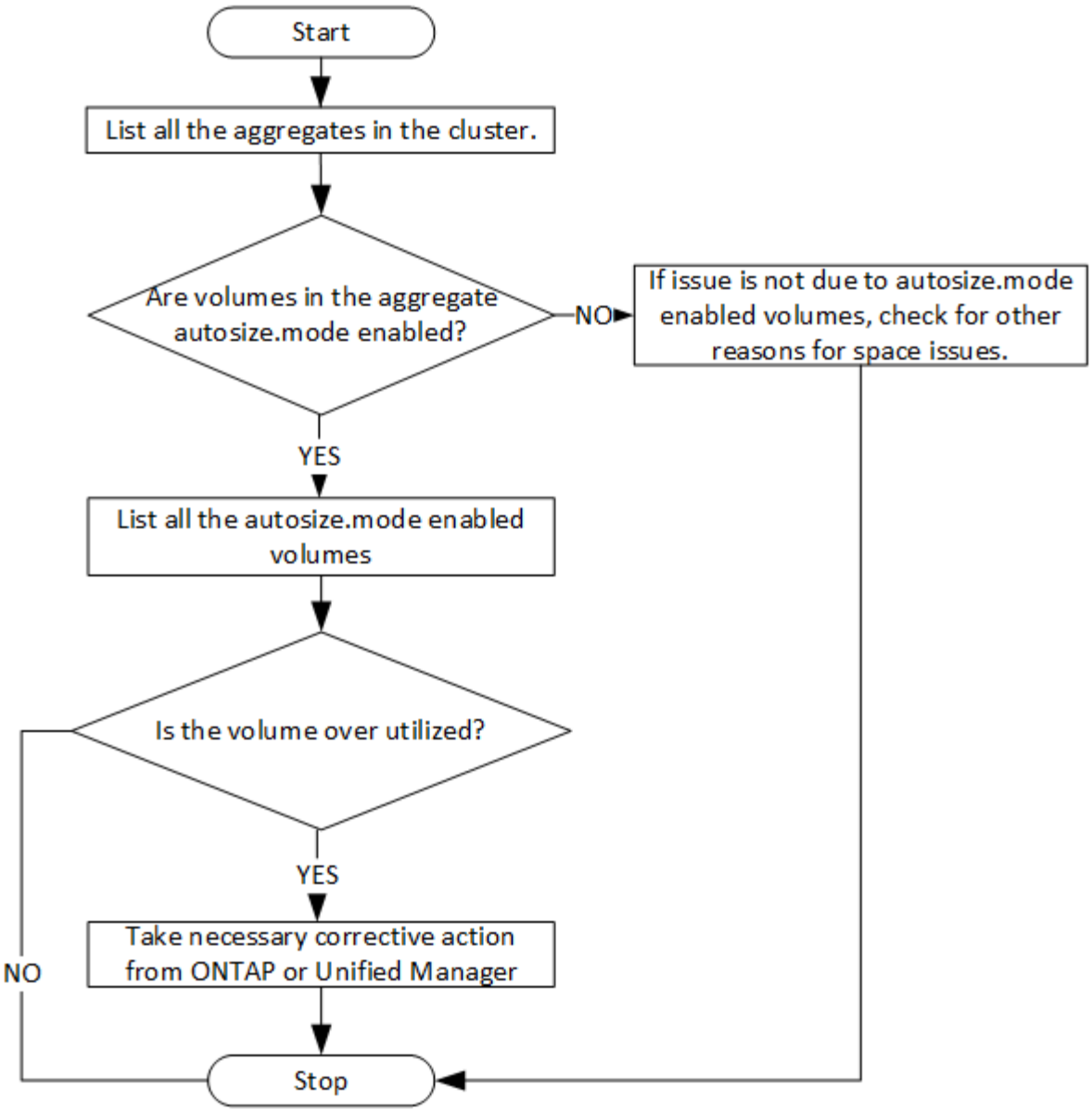
Déterminez les problèmes d'espace dans les agrégats à l'aide des API Active IQ Unified Manager

Vous pouvez utiliser les API du centre de données dans Active IQ Unified Manager pour surveiller la disponibilité et l'utilisation de l'espace dans vos volumes. Vous pouvez déterminer les problèmes d'espace dans votre volume et identifier les ressources de stockage surutilisées ou sous-utilisées.

Les API des centres de données pour les agrégats récupèrent les informations pertinentes concernant l'espace disponible et utilisé, ainsi que les paramètres d'efficacité des économies d'espace. Vous pouvez également filtrer les informations récupérées en fonction d'attributs spécifiques.

Pour identifier un éventuel manque d'espace dans vos agrégats, vérifiez si des volumes de votre environnement ont le mode de dimensionnement automatique activé. Vous devrez ensuite repérer les volumes surutilisés et prendre les mesures correctives nécessaires.

L'organigramme suivant illustre le processus de récupération des informations relatives aux volumes dont le mode de dimensionnement automatique est activé :



Ce flux suppose que les clusters ont déjà été créés dans ONTAP et ajoutés à Unified Manager.

1. Obtenez la clé du cluster, sauf si vous connaissez sa valeur :

Catégorie	Verbe HTTP	Chemin
centre de données	GET	`/datacenter/cluster/clusters`

2. En utilisant la clé du cluster comme paramètre de filtre, interrogez les agrégats de ce cluster.

Catégorie	Verbe HTTP	Chemin
centre de données	GET	`/datacenter/storage/aggregates`

3. À partir de la réponse, analysez l'utilisation de l'espace des agrégats et identifiez ceux qui présentent des problèmes d'espace. Pour chaque agrégat concerné, récupérez sa clé à partir de la même sortie JSON.

4. À l'aide de chaque clé d'agrégation, filtrez tous les volumes dont la valeur du paramètre autosize.mode est définie sur `grow`.

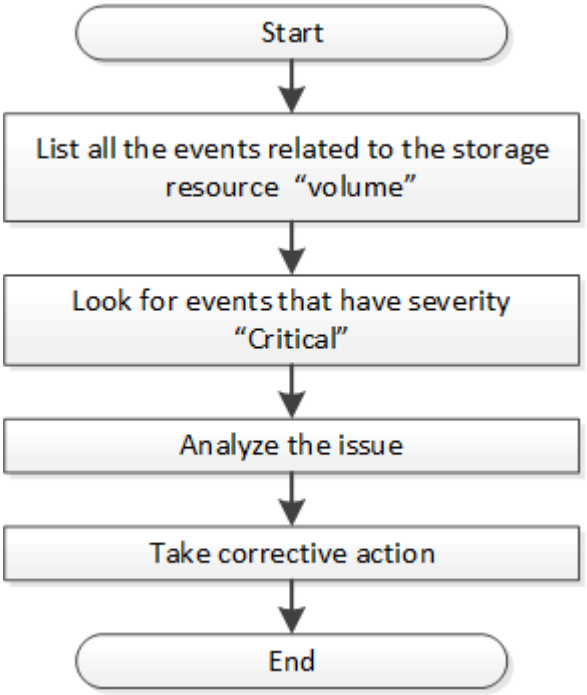
Catégorie	Verbe HTTP	Chemin
centre de données	GET	`/datacenter/storage/volumes`

5. Analysez quels volumes sont surutilisés.
6. Pour résoudre les problèmes d'espace dans votre volume, effectuez toute action corrective nécessaire, comme le déplacement du volume entre les agrégats. Vous pouvez effectuer ces actions depuis l'interface utilisateur web d'ONTAP ou de Unified Manager.

Déterminez les problèmes liés aux objets de stockage à l'aide des API d'événements d'Active IQ Unified Manager

Lorsqu'un objet de stockage de votre centre de données dépasse un seuil, vous recevez une notification concernant cet événement. Grâce à cette notification, vous pouvez analyser le problème et prendre des mesures correctives à l'aide des `events` API.

Ce processus prend pour exemple un volume comme objet ressource. Vous pouvez utiliser les `events` APIs pour récupérer la liste des événements liés à un volume, analyser les problèmes critiques de ce volume, puis prendre des mesures correctives pour résoudre le problème.



Suivez ces étapes pour identifier les problèmes de votre volume avant de prendre des mesures correctives.

Étapes

1. Analysez les notifications d'événements critiques d'Active IQ Unified Manager pour les volumes de votre centre de données.
2. Interrogez tous les événements pour les volumes en utilisant les paramètres suivants dans l'API /management-server/events:

```
"resource_type": "volume"
"severity": "critical"
```

Catégorie	Verbe HTTP	Chemin
serveur de gestion	GET	/management-server/events

3. Consultez la sortie et analysez les problèmes dans les volumes spécifiques.
4. Effectuez les actions nécessaires à l'aide des API REST ou de l'interface utilisateur Web de Unified Manager pour résoudre les problèmes.

Dépannez les volumes ONTAP à l'aide des API de passerelle Active IQ Unified Manager

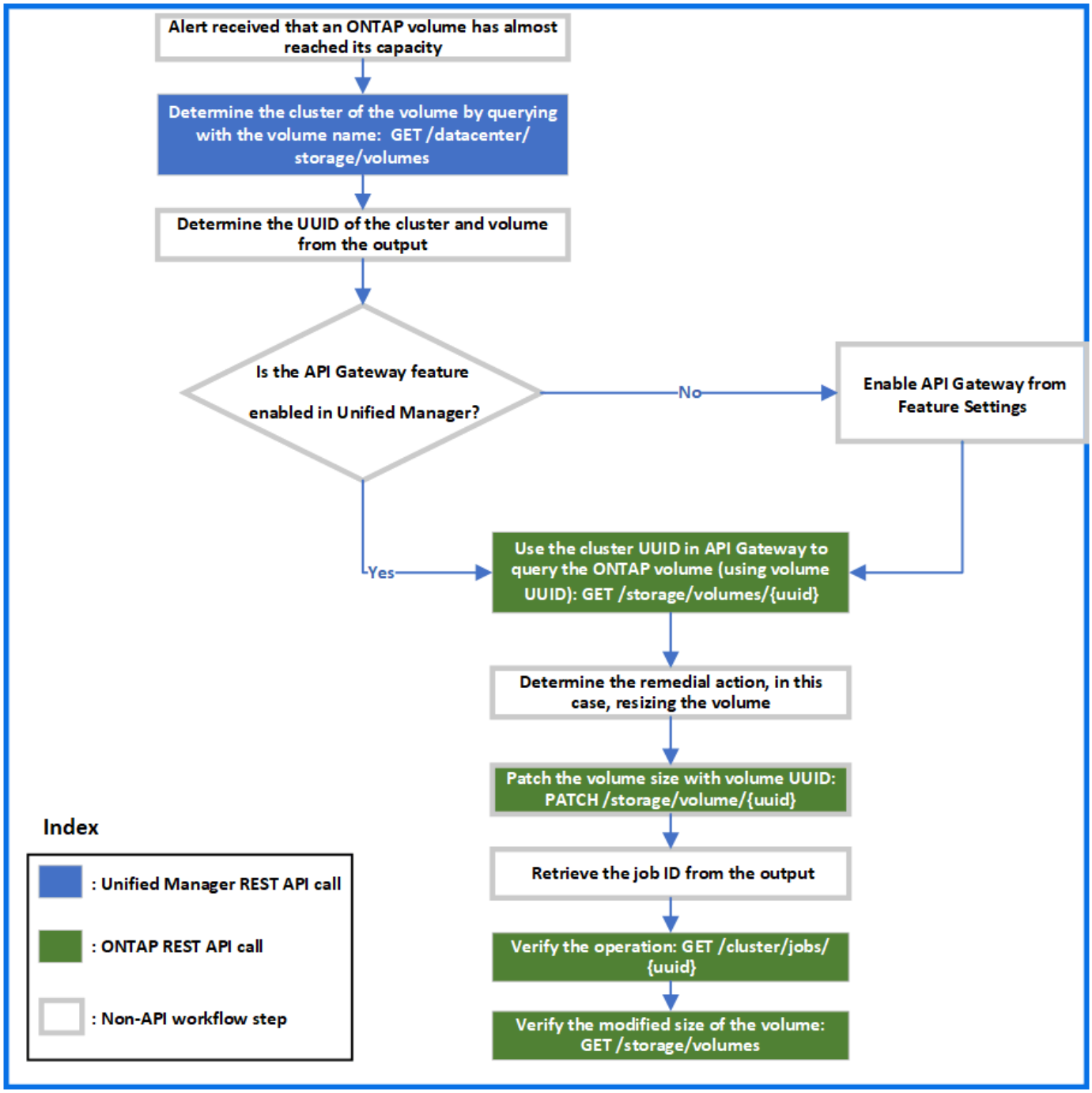
Les API de passerelle servent à invoquer les API ONTAP afin d'interroger des informations sur vos objets de stockage ONTAP et de prendre des mesures correctives pour résoudre les problèmes signalés.

Ce flux de travail illustre une utilisation dans laquelle un événement est déclenché lorsqu'un volume ONTAP atteint presque sa capacité maximale. Il montre également comment résoudre ce problème en combinant Active IQ Unified Manager et les API REST ONTAP.

Avant d'exécuter les étapes du flux de travail, assurez-vous des points suivants :

- Vous connaissez les API de passerelle et leur mode d'utilisation. Pour plus d'informations, consultez "Accès aux API ONTAP via un accès proxy".
- Vous connaissez l'utilisation des API REST ONTAP. Pour plus d'informations sur l'utilisation des API REST ONTAP, consultez "Documentation de l'automatisation ONTAP".
- Vous êtes un administrateur d'applications.
- Le cluster sur lequel vous souhaitez exécuter les opérations de l'API REST est pris en charge avec ONTAP 9.5 ou version ultérieure, et le cluster est ajouté à Unified Manager via HTTPS.

Le diagramme suivant illustre chaque étape du flux de travail pour dépanner le problème d'utilisation de la capacité des volumes ONTAP.



Le flux de travail couvre les points d'invocation des API REST de Unified Manager et de ONTAP.

1. Notez le nom du volume indiqué par l'événement signalant 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
centre de données	GET	`/datacenter/storage/volumes`

3. Récupérez l'UUID du cluster et l'UUID du volume à partir de la sortie.

4. Dans l'interface utilisateur web de Unified Manager, accédez à **General** > **Feature Settings** > **API Gateway** pour vérifier si la fonctionnalité API Gateway est activée. Si ce n'est pas le cas, les API de la catégorie Gateway ne sont pas disponibles pour que vous les appeliez. Activez la fonctionnalité si elle est désactivée.
5. Utilisez l'UUID du cluster pour exécuter l'API ONTAP `/storage/volumes/{uuid}` via la passerelle API. La requête renvoie les détails du volume lorsque l'UUID du volume est transmis comme paramètre d'API.

   Pour exécuter les API ONTAP via la passerelle API, les informations d'identification de Unified Manager sont transmises en interne pour l'authentification, et vous n'avez pas besoin d'effectuer une étape d'authentification supplémentaire pour l'accès à chaque cluster.

Catégorie	Verbe HTTP	Chemin
Unified Manager: passerelle ONTAP : stockage	GET	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 du cluster sur lequel l'opération REST doit être effectuée. {path} doit être remplacé par l'URL REST ONTAP /storage/volumes/{uuid}.

   L'URL ajoutée est : `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

   Lors de l'exécution de l'opération GET, l'URL générée est: `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

   Exemple de commande cURL

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. À partir des résultats, déterminez la taille, l'utilisation et la mesure corrective à prendre. Dans ce flux de travail, la mesure corrective consiste à redimensionner le volume.
7. Utilisez l'UUID du cluster et exécutez l'API ONTAP suivante via la passerelle API pour redimensionner le volume. Pour plus d'informations sur les paramètres d'entrée des API de la passerelle et d'ONTAP, consultez l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager: passerelle ONTAP : stockage	CORRECTIF	API de passerelle: `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

Outre l'UUID du cluster et l'UUID du volume, vous devez saisir une valeur pour le paramètre size afin de redimensionner le volume. Veillez à saisir la valeur *en octets*. Par exemple, si vous souhaitez augmenter la taille d'un volume de 100 Go à 120 Go, saisissez la valeur du paramètre size à la fin de la requête `-d {\"size\": 128849018880}"`.

Exemple de commande cURL

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H
    "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
    {\"size\": 128849018880}"
```

La sortie JSON renvoie un UUID de tâche.

8. Vérifiez si la tâche s'est exécutée correctement à l'aide de l'UUID de la tâche. Utilisez l'UUID du cluster et l'UUID de la tâche pour exécuter l'API ONTAP suivante via la passerelle API. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, consultez l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager: passerelle ONTAP : cluster	GET	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 des API de la passerelle et de ONTAP, consultez l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager: passerelle ONTAP : stockage	GET	API de passerelle: `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

Le résultat affiche une taille de volume accrue de 120 Go.

Flux de travail pour la gestion des workloads

Provisionnez et modifiez les charges de travail de stockage dans Active IQ Unified Manager

Avec Active IQ Unified Manager, vous pouvez provisionner et modifier les charges de travail de stockage (LUN, partages de fichiers NFS et partages CIFS). Le provisionnement comprend plusieurs étapes, de la création de la machine virtuelle de stockage (SVM) à l'application des niveaux de service de performance et des stratégies

d'efficacité du stockage aux charges de travail. La modification des charges de travail consiste à ajuster des paramètres spécifiques et à activer des fonctionnalités supplémentaires.

Les flux de travail suivants sont décrits :

- Flux de travail pour le provisionnement de machines virtuelles de stockage (SVM) dans Unified Manager.

  Cette procédure doit être effectuée avant le provisionnement des LUN ou des partages de fichiers sur Unified Manager.

- Provisionnement de partages de fichiers.
- Provisionnement des 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 de stockage).
- Modification d'un partage de fichiers NFS pour prendre en charge le protocole CIFS
- Modification des charges de travail pour faire passer la QoS à AQoS

Pour chaque flux de travail de provisionnement (LUN et partages de fichiers), assurez-vous d'avoir terminé le flux de travail de vérification des SVM sur les clusters.

Vous devez également prendre connaissance des recommandations et des limitations avant d'utiliser chaque API dans les flux de travail. Les détails pertinents des API sont disponibles dans leurs sections respectives, répertoriées dans les concepts et références associés.

Vérifiez les SVM sur les clusters ONTAP à l'aide des API d'Active IQ Unified Manager

Avant de provisionner des partages de fichiers ou des LUN, vous devez vérifier si des machines virtuelles de stockage (SVM) ont été créées sur les clusters.

Le workflow suppose que les clusters ONTAP ont été ajoutés à Unified Manager et que la clé du cluster a été obtenue. Les clusters doivent disposer des licences requises pour le provisionnement des LUN et des partages de fichiers sur ceux-ci.

1. Vérifiez si une SVM a été créée dans le cluster.

Catégorie	Verbe HTTP	Chemin
centre de données	GET	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

Exemple de cURL

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si la clé SVM n'est pas renvoyée, créez la SVM. Pour créer les SVM, vous avez besoin de la clé du cluster

sur lequel vous provisionnez la SVM. Vous devez également spécifier le nom de la SVM. Suivez ces étapes.

Catégorie	Verbe HTTP	Chemin
centre de données	GET	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Obtenez la clé du cluster.

Exemple de cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. À partir du résultat, récupérez la clé du cluster, puis utilisez-la comme valeur d'entrée pour créer le SVM.

> Lors de la création de la SVM, assurez-vous qu'elle prend en charge tous les protocoles nécessaires au provisionnement des LUN et des partages de fichiers, tels que CIFS, NFS, FCP et iSCSI. Les processus de provisionnement risquent d'échouer si la SVM ne prend pas en charge les services requis. Il est recommandé d'activer également sur la SVM les services correspondant aux types de charges de travail concernés.

Catégorie	Verbe HTTP	Chemin
centre de données	POST	`/datacenter/svm/svms`

Exemple de cURL

Saisissez 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 le SVM que vous avez créé.

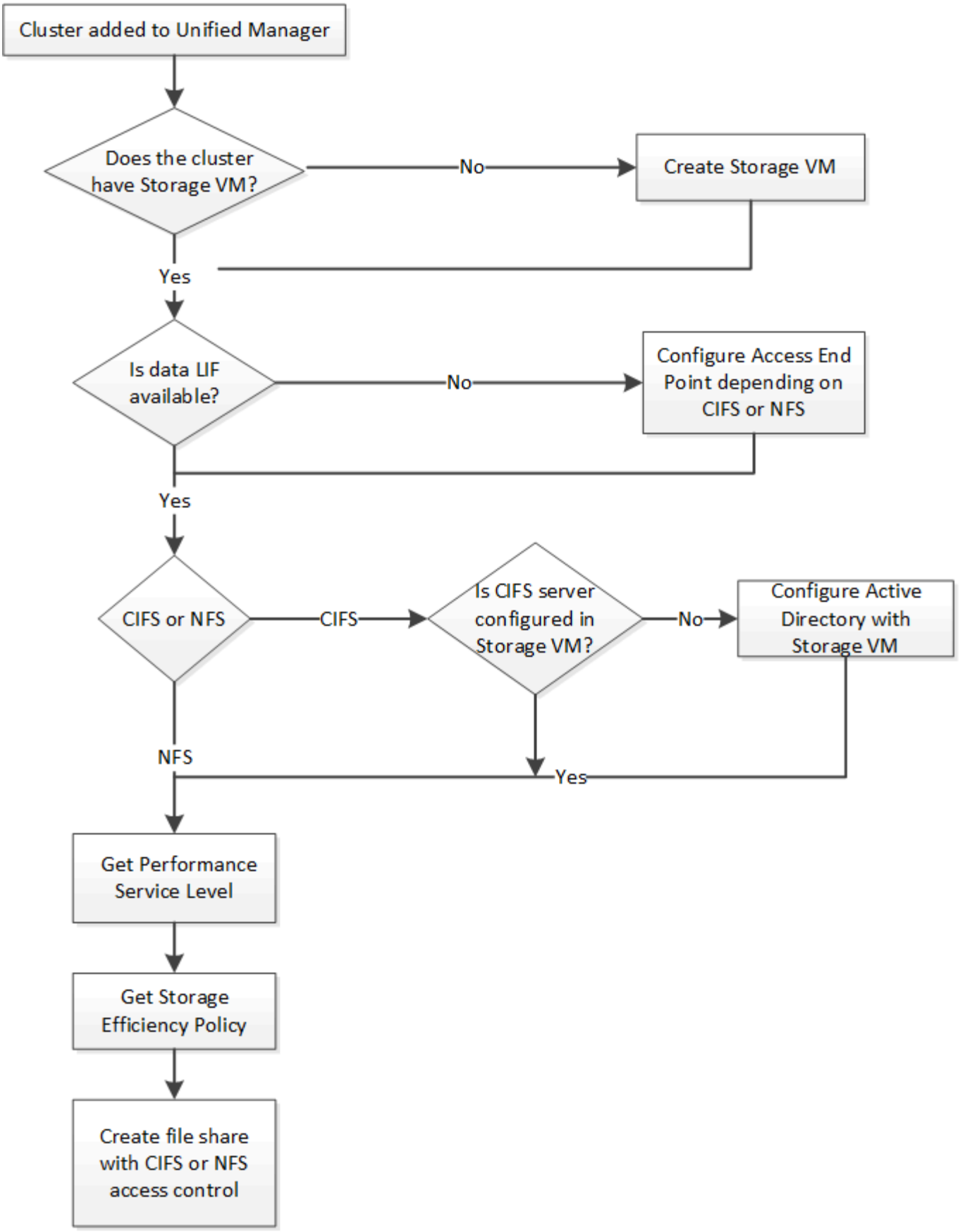
4. Vérifiez la création du SVM à l'aide de la clé de l'objet de tâche pour la requête. Si le SVM est créé avec succès, la clé du SVM est renvoyée dans la réponse.

Catégorie	Verbe HTTP	Chemin
serveur de gestion	GET	`/management-server/jobs/{key}`

Provisionnez des partages de fichiers CIFS et NFS à l'aide des API d'Active IQ Unified Manager

Vous pouvez provisionner des partages CIFS et des partages de fichiers NFS sur vos Storage Virtual Machines (SVM) à l'aide des API de provisionnement fournies dans le cadre d'Active IQ Unified Manager. Ce workflow de provisionnement décrit en détail les étapes permettant de récupérer les clés des SVM, des Performance Service Levels et des Storage Efficiency Policies avant de créer les partages de fichiers.

Le diagramme suivant illustre chaque étape d'un processus de provisionnement de partage de fichiers. Il inclut le provisionnement des partages CIFS et des partages de fichiers NFS.



Assurez-vous de ce qui suit :

- Les clusters ONTAP ont été ajoutés à Unified Manager et la clé du cluster a été obtenue.
- Des SVM ont été créés sur les clusters.
- Les SVM prennent en charge les services CIFS et NFS. Le provisionnement des partages de fichiers peut échouer si les SVM ne prennent pas en charge les services requis.
- Le port FCP est en ligne pour le provisionnement des ports.

1. Déterminez si des LIF de données ou des points de terminaison d'accès sont disponibles sur la SVM sur laquelle vous souhaitez créer le partage CIFS. Obtenez la liste des points de terminaison d'accès disponibles sur la SVM :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

Exemple de cURL

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si votre point de terminaison d'accès figure dans la liste, obtenez la clé du point de terminaison d'accès, sinon créez le point de terminaison d'accès.

Veillez à créer des points d'accès sur lesquels le protocole CIFS est activé. Le provisionnement des partages CIFS échoue si vous n'avez pas créé de point d'accès avec le protocole CIFS activé.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

Exemple de cURL

Vous devez saisir, en tant que paramètres d'entrée, les détails du point de terminaison d'accès que vous souhaitez créer.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
```

```
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le point de terminaison d'accès que vous avez créé.

3. Vérifiez le point de terminaison d'accès :

Catégorie	Verbe HTTP	Chemin
serveur de gestion	GET	`/management-server/jobs/{key}`

4. Déterminez si vous devez créer un partage CIFS ou un partage de fichiers NFS. Pour créer un partage CIFS, suivez les étapes suivantes :

   a. Déterminez si le serveur CIFS est configuré sur votre SVM, c'est-à-dire si un mappage Active Directory est créé sur le SVM.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/active-directories-mappings`

   b. Si le mappage Active Directory est créé, prenez la clé, sinon, créez le mappage Active Directory sur la SVM.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/active-directories-mappings`

Exemple de cURL

Vous devez saisir les détails nécessaires à la création du mappage Active Directory, en tant que paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/storage-provider/active-
directories-mappings" -H "accept: application/json" -H "Content-Type:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
\"dns\": \"10.000.000.000\",
```

```
\"domain\": \"example.com\",
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+
Il s'agit d'un appel synchrone et vous pouvez vérifier la création du mappage Active Directory dans le résultat. En cas d'erreur, le message d'erreur s'affiche afin de vous permettre de résoudre le problème et de relancer la requête.

5. Obtenez la clé SVM de la SVM sur laquelle vous souhaitez créer le partage CIFS ou le partage de fichiers NFS, comme décrit dans la rubrique du flux de travail *Vérification des SVM sur les clusters*.
6. Obtenez la clé du Performance Service Level en exécutant l'API suivante et en récupérant la clé dans la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/performance-service-levels`

Vous pouvez récupérer les détails des niveaux de service de performance définis par le système en définissant le paramètre d'entrée `system_defined` sur `true`. À partir de la sortie, obtenez la clé du niveau de service de performance que vous souhaitez appliquer au partage de fichiers.

7. Si vous le souhaitez, obtenez la clé de la stratégie d'efficacité du stockage que vous souhaitez appliquer au partage de fichiers en exécutant l'API suivante et en récupérant la clé dans la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/storage-efficiency-policies`

8. Créez le partage de fichiers. Vous pouvez créer un partage de fichiers qui prend en charge à la fois CIFS et NFS en spécifiant la liste de contrôle d'accès et les règles d'export. Les sous-étapes suivantes fournissent des informations si vous souhaitez créer un partage de fichiers pour prendre en charge un seul des protocoles sur le volume. Vous pouvez également mettre à jour un partage de fichiers NFS pour inclure la liste de contrôle d'accès après avoir créé le partage NFS. Pour plus d'informations, consultez la rubrique *Modifying storage workloads*.

   a. Pour créer uniquement un partage CIFS, rassemblez les informations relatives à la liste de contrôle d'accès (ACL). Pour créer le partage CIFS, fournissez des valeurs valides pour les paramètres d'entrée suivants. Pour chaque groupe d'utilisateurs que vous attribuez, une ACL est créée lorsqu'un partage CIFS/SMB est provisionné. Selon les valeurs que vous saisissez pour l'ACL et le mappage 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'exemple

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. Pour créer uniquement un partage de fichiers NFS, rassemblez les informations relatives aux règles d'export. Pour créer le partage de fichiers NFS, veuillez fournir des valeurs valides pour les paramètres d'entrée suivants. En fonction des valeurs que vous fournissez, les règles d'export sont associées au partage de fichiers NFS lors de sa création.

> Lors du provisionnement du partage NFS, vous pouvez soit créer des règles d'export en fournissant toutes les valeurs requises, soit fournir la clé des règles d'export et réutiliser des règles d'export existantes. Si vous souhaitez réutiliser des règles d'export pour la machine virtuelle de stockage, vous devez ajouter la clé des règles d'export. Si vous ne connaissez pas cette clé, vous pouvez récupérer la clé des règles d'export à l'aide de l' `/datacenter/protocols/nfs/export-policies`API. Pour créer de nouvelles règles, vous devez saisir les règles comme indiqué dans l'exemple suivant. Pour les règles saisies, l'API tente de rechercher des règles d'export existantes en faisant correspondre l'hôte, la machine virtuelle de stockage et les règles. S'il existe des règles d'export, elles sont utilisées. Sinon, de nouvelles règles d'export sont créées.

Une commande cURL avec des valeurs d'exemple

```
"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 les règles d'export, indiquez les valeurs valides pour les paramètres d'entrée obligatoires des 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 Job que vous pouvez utiliser pour vérifier le partage de fichiers que vous avez créé . Vérifiez la création du partage de fichiers en utilisant la clé d'objet Job renvoyée lors de l'interrogation de la tâche :

Catégorie	Verbe HTTP	Chemin
serveur de gestion	GET	`/management-server/jobs/{key}`

À la fin de la réponse, vous verrez 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	GET	`/storage-provider/file-shares/{key}`

Exemple de sortie JSON

Vous pouvez constater que la méthode POST `/storage-provider/file-shares` appelle en interne toutes les API nécessaires à chacune des fonctions et crée l'objet. Par exemple, elle appelle l' `/storage-provider/performance-service-levels/`API permettant d'attribuer le niveau de service de performance au 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": {}
```

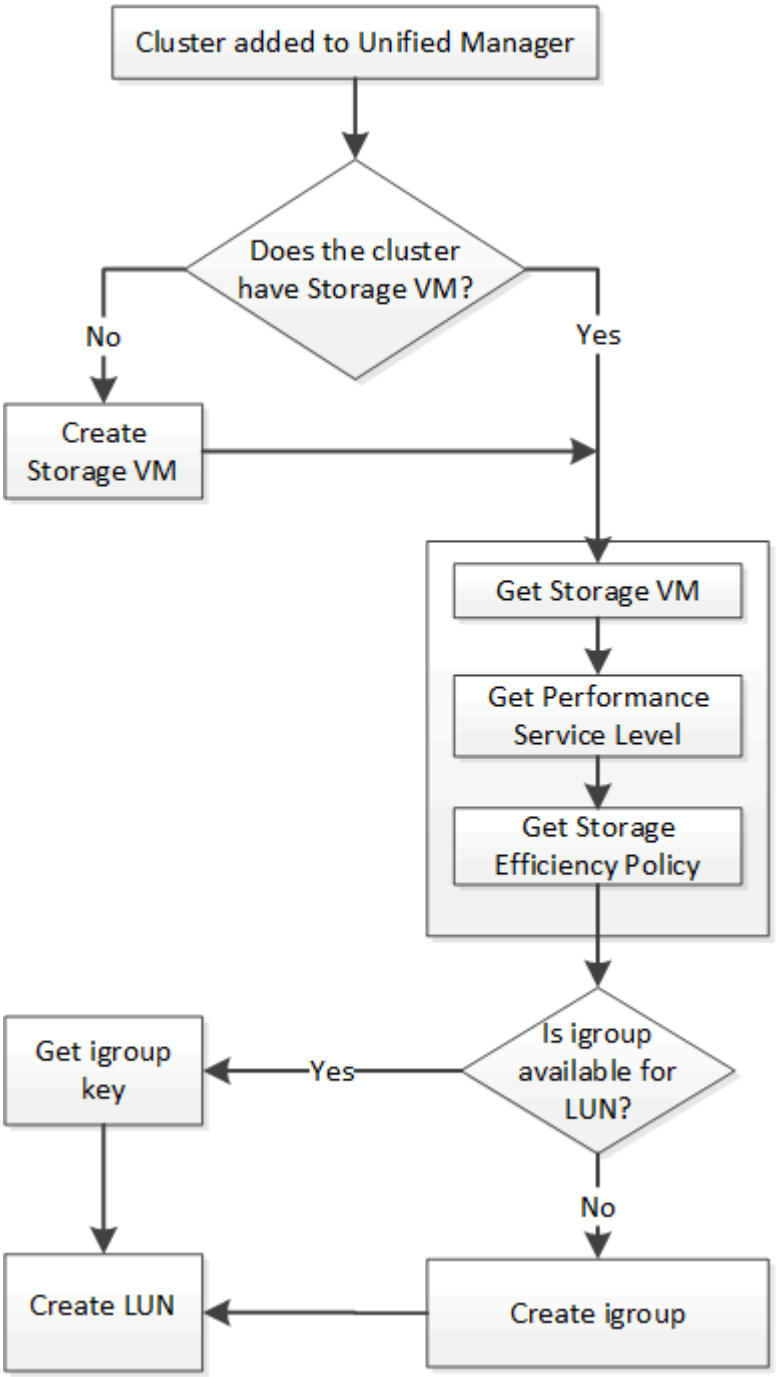
```
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "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"
        }
    }
}
```

Provisionnez des LUN à l'aide des API Active IQ Unified Manager

Vous pouvez provisionner des LUN sur vos machines virtuelles de stockage (SVM) à l'aide des API de provisionnement fournies dans le cadre d'Active IQ Unified Manager. Ce workflow de provisionnement détaille les étapes de récupération des clés des SVM, des niveaux de service de performance et des stratégies d'efficacité du stockage avant la création de la LUN.

Le diagramme suivant illustre les étapes d'un workflow de provisionnement de LUN.



Ce workflow suppose que les clusters ONTAP ont été ajoutés à Unified Manager et que la clé du cluster a été obtenue. Le workflow suppose également que les SVM ont déjà été créées sur les clusters.

1. Obtenez la clé SVM pour la SVM sur laquelle vous souhaitez créer la LUN, comme décrit dans la rubrique de workflow *Vérification des SVM sur les clusters*.
2. Obtenez la clé du Performance Service Level en exécutant l'API suivante et en récupérant la clé dans la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/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, obtenez la clé du niveau de service de performance que vous souhaitez appliquer au LUN.

3. Si vous le souhaitez, obtenez la clé de la stratégie d'efficacité du stockage que vous souhaitez appliquer sur le LUN en exécutant l'API suivante et en récupérant la clé dans la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/storage-efficiency-policies`

4. Déterminez si des groupes d'initiateurs (igroups) ont été créés pour accorder l'accès à la cible LUN que vous souhaitez créer.

Catégorie	Verbe HTTP	Chemin
centre de données	GET	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Vous devez saisir la valeur du paramètre pour indiquer la SVM pour laquelle l'igroup dispose d'un accès autorisé. De plus, si vous souhaitez interroger un igroup particulier, saisissez son nom (clé) comme paramètre d'entrée.

5. Dans la sortie, si vous trouvez l'igroup auquel vous souhaitez accorder l'accès, récupérez la clé. Sinon, créez l'igroup.

Catégorie	Verbe HTTP	Chemin
centre de données	POST	`/datacenter/protocols/san/igroups`

Vous devez saisir les détails de l'igroup que vous souhaitez créer en tant que paramètres d'entrée. Il s'agit d'un appel synchrone ; vous pouvez vérifier la création de l'igroup dans la sortie. En cas d'erreur, un message s'affiche pour vous permettre de résoudre le problème et de relancer l'API.

6. Créez le LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/luns`

Pour créer le LUN, assurez-vous d'avoir ajouté les valeurs récupérées en tant que paramètres d'entrée

obligatoires.

> La politique d'efficacité du stockage est un paramètre facultatif pour la création de LUN.

Exemple de cURL

Vous devez saisir tous les détails de la LUN que vous souhaitez créer comme paramètres d'entrée.

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le LUN que vous avez créé.

7. Vérifiez la création du LUN à l'aide de la clé de l'objet Job renvoyée lors de l'interrogation du Job :

Catégorie	Verbe HTTP	Chemin
serveur de gestion	GET	`/management-server/jobs/{key}`

À la fin de la réponse, vous voyez la clé de la LUN créée.

8. Vérifiez la création du LUN en exécutant l'API suivante avec la clé renvoyée :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/luns/{key}`

Exemple de sortie JSON

Vous pouvez constater que la méthode POST de `/storage-provider/luns` appelle en interne toutes les API nécessaires à chacune des fonctions et crée l'objet. Par exemple, elle appelle l' `/storage-provider/performance-service-levels/`API permettant d'attribuer le niveau de service de performance au LUN.

== Étapes de dépannage en cas d'échec de la création ou du mappage d'un LUN

Une fois ce processus terminé, il est possible que la création de votre LUN échoue. Même si la LUN est créée avec succès, le mappage de la LUN avec l'igroup peut échouer en raison de l'indisponibilité d'une LIF SAN ou d'un point de terminaison d'accès sur le nœud où vous créez la LUN. En cas d'échec, 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 cette défaillance.

1. Créez un point de terminaison d'accès prenant en charge le protocole ISCSI/FCP sur la SVM sur laquelle vous avez tenté de créer le LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

Exemple de cURL

Vous devez saisir, comme paramètres d'entrée, les détails du point de terminaison d'accès que vous souhaitez créer.

> Assurez-vous que, dans le paramètre d'entrée, vous avez ajouté l'adresse pour indiquer le nœud principal de la LUN et ha_address pour indiquer le nœud partenaire du nœud principal. Lorsque vous exécutez cette opération, elle crée des points de terminaison d'accès sur le nœud principal et le nœud partenaire.

2. Interrogez la tâche avec la clé d'objet Job renvoyée dans la sortie JSON pour vérifier qu'elle s'est exécutée avec succès pour ajouter les points de terminaison d'accès sur la SVM et que les services iSCSI/FCP ont été activés sur la SVM.

Catégorie	Verbe HTTP	Chemin
serveur de gestion	GET	`/management-server/jobs/{key}`

Exemple de sortie JSON

À la fin du résultat, vous pouvez voir la clé des points de terminaison d'accès créés. Dans le résultat suivant, la valeur « name » : « accessEndpointKey » indique le point de terminaison d'accès créé sur le nœud principal du LUN, dont la clé est 9c964258-14ef-11ea-95e2-00a098e32c28. La valeur « name » : « accessEndpointHAKey » indique le point de terminaison d'accès créé sur le nœud partenaire du nœud principal, dont la clé est 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modifiez la LUN pour mettre à jour le mappage de l'igroup. Pour plus d'informations sur la modification du flux de travail, consultez « `Modifying storage workloads` ».

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/lun/{key}`

Dans le champ de saisie, spécifiez la clé igroup avec laquelle vous souhaitez mettre à jour le mappage de LUN, ainsi que la clé LUN.

Exemple de cURL

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier si le mappage a réussi.

4. Vérifiez le mappage LUN en interrogeant avec la clé LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/luns/{key}`

Exemple de sortie JSON

Dans la sortie, vous pouvez voir que le LUN a été mappé avec succès avec l'igroup (clé d19ec2fa-fec7-11e8-b23d-00a098e32c28) avec lequel il a été initialement provisionné.

Modifier les workloads de stockage

Modifiez les charges de travail de stockage à l'aide des API dans Active IQ Unified Manager

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 prend pour exemple la mise à jour des niveaux de service de performance pour les LUN et les partages de fichiers.

> Le flux de travail suppose que le LUN ou le partage de fichiers a été provisionné avec des niveaux de service de performance.

Modifier les partages de fichiers

Lors de la modification d'un partage de fichiers, vous pouvez mettre à jour les paramètres suivants :

- Capacité ou taille.
- Configuration en ligne ou hors ligne.
- Politique d'efficacité du stockage.
- Niveau de service de performance.
- Paramètres de la liste de contrôle d'accès (ACL).
- Paramètres des règles d'export. Vous pouvez également supprimer les paramètres des règles d'export et rétablir les règles d'export par défaut (vides) sur le partage de fichiers.

> Lors d'une exécution unique de l'API, vous ne pouvez mettre à jour qu'un seul paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performance à un partage de fichiers. Vous pouvez utiliser la même procédure pour mettre à jour toute autre propriété d'un partage de fichiers.

1. Obtenez la clé du partage CIFS ou du partage de fichiers NFS du partage de fichiers que vous souhaitez mettre à jour. Cette API interroge tous les partages de fichiers de votre centre de données. Ignorez cette étape si vous connaissez déjà la clé du partage de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/file-shares`

2. Consultez les détails du partage de fichiers en exécutant l'API suivante avec la clé de partage de fichiers que vous avez obtenue.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/file-shares/{key}`

Consultez 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 performance que vous souhaitez attribuer à ce partage de fichiers. Aucune stratégie n'y est actuellement associée.

Catégorie	Verbe HTTP	Chemin
Niveaux de service de performance	GET	`/storage-provider/performance-service-levels`

Vous pouvez récupérer les détails des niveaux de service de performances définis par le système en définissant le paramètre d'entrée `system_defined` sur `true`. À partir de la sortie, obtenez la clé du niveau de service de performances que vous souhaitez appliquer au partage de fichiers.

4. Appliquez le niveau de service de performance au partage de fichiers.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares/{key}`

Dans les données d'entrée, vous devez spécifier uniquement le paramètre que vous souhaitez mettre à jour, ainsi que la clé du partage de fichiers. Dans ce cas, il s'agit de la clé du Performance Service Level.

Exemple de cURL

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares"`-H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
\"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

La sortie JSON affiche un objet Job que vous pouvez utiliser pour vérifier si les points de terminaison d'accès sur les nœuds d'origine et partenaires ont bien été créés.

5. Vérifiez si le Performance Service Level a été ajouté au partage de fichiers à l'aide de la clé d'objet Job affichée dans votre résultat.

Catégorie	Verbe HTTP	Chemin
Serveur de gestion	GET	`/management-server/jobs/{key}`

En interrogeant l'objet Job par son ID, vous pouvez vérifier si le partage de fichiers a bien été mis à jour. En cas d'échec, identifiez la cause et relancez l'API. Une fois la création réussie, interrogez le partage de fichiers pour visualiser l'objet modifié :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/file-shares/{key}`

Consultez 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'un LUN, vous pouvez modifier les paramètres suivants :

- Capacité ou taille
- Paramètre en ligne ou hors ligne
- Politique d'efficacité du stockage
- Niveau de service de performances
- Mappage de LUN

Lors d'une exécution unique de l'API, vous ne pouvez mettre à jour qu'un seul paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performance à un LUN. Vous pouvez utiliser la même procédure pour mettre à jour toute autre propriété d'un LUN.

1. Obtenez la clé LUN de la LUN que vous souhaitez mettre à jour. Cette API renvoie les détails de toutes les LUN de votre centre de données. Ignorez cette étape si vous connaissez déjà la clé LUN.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	GET	`/storage-provider/luns`

2. Consultez les détails du LUN en exécutant l'API suivante avec la clé LUN que vous avez obtenue.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	GET	`/storage-provider/luns/{key}`

Consultez les détails du LUN dans la sortie. Vous constaterez qu'aucun niveau de service de performance n'est attribué à ce LUN.

Exemple de sortie JSON

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Obtenez la clé du niveau de service de performance que vous souhaitez attribuer à la LUN.

Catégorie	Verbe HTTP	Chemin
Niveaux de service de performance	GET	`/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, obtenez la clé du niveau de service de performance que vous souhaitez appliquer au LUN.

4. Appliquez le niveau de service de performances sur le LUN.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	`/storage-provider/lun/{key}`

Dans le champ de saisie, vous devez indiquer uniquement le paramètre à mettre à jour, ainsi que la clé LUN. Dans ce cas, il s'agit de la clé de Performance Service Level.

Exemple de cURL

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-
953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-
Type: application/json" H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" }"
```

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier le LUN que vous avez mis à jour.

5. Consultez les détails du LUN en exécutant l'API suivante avec la clé LUN que vous avez obtenue.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	GET	`/storage-provider/luns/{key}`

Consultez les détails du LUN dans la sortie. Vous pouvez constater que le Performance Service Level est attribué à ce LUN.

Exemple de sortie JSON

```
     "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
```

Modifier un partage de fichiers NFS pour prendre en charge CIFS à l'aide des API d'Active IQ Unified Manager

Vous pouvez modifier un partage de fichiers NFS pour qu'il prenne en charge le protocole CIFS. Lors de la création d'un partage de fichiers, il est possible de spécifier à la fois les paramètres de liste de contrôle d'accès (ACL) et les règles d'export pour le même partage de fichiers. Toutefois, si vous souhaitez activer CIFS sur le même volume que celui où vous avez créé un partage de fichiers NFS, vous pouvez mettre à jour les paramètres ACL de ce partage de fichiers pour prendre en charge CIFS.

Avant de commencer

1. Un partage de fichiers NFS doit avoir été créé avec uniquement les détails des règles d'export. Pour plus d'informations, consultez les sections *Gestion des partages de fichiers* et *Modification des charges de travail de stockage*.

2. Vous devez disposer de la clé de partage de fichiers pour exécuter cette opération. Pour plus d'informations sur la consultation des détails du partage de fichiers et la récupération de la clé de partage de fichiers à l'aide de l'ID de tâche, consultez *Provisioning CIFS and NFS file shares*.

Ceci s'applique à un partage de fichiers NFS que vous avez créé en ajoutant uniquement des règles d'export et non des paramètres ACL. Vous modifiez le partage de fichiers NFS pour y inclure les paramètres ACL.

Étapes

1. Sur le partage de fichiers NFS, effectuez une `PATCH` opération avec les détails de l'ACL pour autoriser l'accès CIFS.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares`

Exemple de cURL

En fonction des privilèges d'accès que vous attribuez au groupe d'utilisateurs, comme illustré dans l'exemple suivant, une liste de contrôle d'accès (ACL) est créée et attribuée au partage de fichiers.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

Exemple de sortie JSON

L'opération renvoie le Job ID du Job qui exécute la mise à jour.

2. Vérifiez si les paramètres ont été correctement ajoutés en consultant les détails du partage de fichiers correspondant.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	GET	`/storage-provider/file-shares/{key}`

Exemple de sortie JSON

```
"access_control": {
        "acl": [
```

```
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
```

```
                    ],
                    "rw_rule": [
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
```

Vous pouvez voir la liste de contrôle d'accès (ACL) attribuée ainsi que les règles d'export au même partage de fichiers.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques de commerce, aux brevets et plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NETAPP, le logo NETAPP et les marques figurant sur la page NetApp Trademarks sont des marques de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp peut être trouvée à :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Informations relatives aux droits d'auteur et aux licences de tiers utilisées dans ce produit.

"Avis concernant Active IQ Unified Manager 9.18"

Informations sur le copyright

Copyright © 2026 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.