Documentation sur Data Infrastructure Insights

Data Infrastructure Insights

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/data-infrastructure-insights/index.html on February 11, 2026. Always check docs.netapp.com for the latest.

Sommaire

Documentation sur Data Infrastructure Insights . . . 1
Que peut m’apporter Data Infrastructure Insights ? . . . 1
Commencer . . . 1
Nouveautés de Data Infrastructure Insights . . . 2
Décembre 2025 . . . 2
Contrôler l’accès aux requêtes avec des requêtes partagées . . . 2
Un meilleur filtrage lors de la gestion des moniteurs . . . 3
Visualisations de tableau de bord plus claires . . . 4
Novembre 2025 . . . 4
Configurez votre page d’accueil personnalisée . . . 4
Restez organisé grâce au regroupement automatique des tableaux de bord . . . 5
Octobre 2025 . . . 5
Santé de l’infrastructure : visibilité instantanée sur les risques liés au stockage et à la structure . . . 5
Moniteurs multi-conditions pour des alertes précises . . . 7
Améliorations des requêtes : aperçu des détails des objets . . . 7
Améliorations de la sécurité de la charge de travail . . . 7
Août 2025 . . . 8
Des données de widgets ciblées à portée de main . . . 8
Exporter et importer des tableaux de bord . . . 8
Intégration cloud améliorée : prise en charge de Google Cloud NetApp Volumes (GCNV) . . . 9
Surveillance améliorée de StorageGRID . . . 9
Prise en charge du système d’exploitation . . . 9
Juin 2025 . . . 9
VM Analyzer : visibilité et dépannage holistiques des machines virtuelles vers le stockage . . . 9
Prise en charge du système d’exploitation . . . 10
Mai 2025 . . . 10
Les nouvelles pages de destination vous permettent de rester dans le flux . . . 10
Améliorations de la sécurité de la charge de travail . . . 11
Exportation asynchrone .CSV . . . 13
Avril 2025 . . . 13
Widgets de limites d’anomalies optimisés par ML pour une résolution proactive des problèmes . . . 13
Optimisez les coûts VMware grâce à la prise en charge du stockage VSAN . . . 14
Les détails des alertes à portée de main . . . 15
Exportation asynchrone de l’analyse forensique de la sécurité de la charge de travail . . . 15
Notifications du collecteur de données regroupées en règles . . . 15
Mars 2025 . . . 16
Navigation contextuelle améliorée pour une gestion efficace des infrastructures . . . 16
Préserver l’historique des ressources supprimées . . . 16
Mise à niveau par simple pression sur un bouton de l’opérateur Kubernetes . . . 17
Tester la connectivité pour les collecteurs de données de sécurité des charges de travail de stockage . . . 18
Prise en charge du système d’exploitation . . . 18
Février 2025 . . . 19
Suivi de l’utilisation de l’API DII : améliorer la sécurité et l’efficacité . . . 19

API de sécurité de la charge de travail pour restreindre les utilisateurs . . . 20
Janvier 2025 . . . 20
Gérez les risques de manière proactive avec Forensics Grouping . . . 20
Contrôle d'accès au tableau de bord . . . 21
Décembre 2024 . . . 22
Présentation de SAN Analyzer : visibilité améliorée pour les charges de travail en mode bloc . . . 22
Optimisez les coûts des machines virtuelles grâce au déclassement intelligent des hôtes et à la récupération des machines virtuelles . . . 23
Découvrez les informations sur les journaux grâce aux graphiques temporels et à la prise en charge des widgets de tableau . . . 24
Novembre 2024 . . . 25
Nouvelle API d'alertes de sécurité de charge de travail . . . 25
Analyser les changements de configuration dans votre environnement . . . 25
Prise en charge de KubeVirt : surveiller les charges de travail des machines virtuelles exécutées dans votre cluster Kubernetes . . . 25
Octobre 2024 . . . 26
Débloquez de nouvelles perspectives grâce aux expressions personnalisées dans les moniteurs . . . 26
Minimiser les interruptions d'alerte pendant la période de maintenance . . . 26
Optimisez la gestion des alertes grâce à de nouvelles règles de notification d'alerte . . . 27
Analyse des journaux dans les tableaux de bord . . . 28
Meilleure observabilité VMware avec VMware Events . . . 28
Mises à jour du collecteur de données : . . . 29
Septembre 2024 . . . 29
Présentation de Data Infrastructure Insights, anciennement Cloud Insights . . . 29
Août 2024 . . . 29
Afficher les données spécifiques à votre plage horaire . . . 29
Analyse du changement et du taux de changement (%) . . . 29
Exporter les résultats de la requête de journal au format .CSV . . . 30
Résoudre les alertes par heure . . . 30
Juillet 2024 . . . 31
AIOps : détection d'anomalies . . . 31
Améliorations de la sécurité de la charge de travail . . . 31
Navigation simplifiée dans le tableau de bord . . . 31
Juin 2024 . . . 32
Prise en charge du système d'exploitation . . . 32
Mai 2024 . . . 32
Résoudre automatiquement les alertes en fonction du temps . . . 32
Avril 2024 . . . 33
Prise en charge iSCSI pour Kubernetes . . . 33
Prise en charge du système d'exploitation . . . 34
Mars 2024 . . . 34
Détails de l'agent de sécurité de la charge de travail . . . 34
Créez des graphiques avec plus de données plus rapidement . . . 34
Février 2024 . . . 35
Améliorations de la convivialité . . . 35

Voir tous les changements dans votre espace de noms . . . 36
Journaux associés aux alertes . . . 37
Collecter les données du commutateur ONTAP . . . 37
API de collecte de données de sécurité de la charge de travail . . . 37
Janvier 2024 . . . 38
Essayez les fonctionnalités de Cloud Insights que vous n'avez pas encore utilisées . . . 38
Dans quelle mesure mes charges de travail sont-elles saines ? . . . 38
Mises à jour du collecteur de données . . . 38
Algorithme ML de détection de ransomware amélioré . . . 38
Fonctionnalité obsolète . . . 39
Décembre 2023 . . . 39
Change Analytics en un coup d'œil . . . 39
Tableau de bord des performances de la charge de travail Kubernetes . . . 40
Détails de la requête sur un seul écran . . . 41
Mises à jour du collecteur de données : . . . 42
Novembre 2023 . . . 42
Sécurité de la charge de travail : suspendre/reprendre un collecteur . . . 42
Informations sur la prise en charge des nœuds de stockage . . . 43
Associer les balises VMware aux annotations Cloud Insights . . . 43
Améliorations de la fiabilité du collecteur Brocade CLI pour le micrologiciel FOS 9.1.1c et supérieur . . . 43
Octobre 2023 . . . 43
Sécurité renforcée de la charge de travail . . . 43
Essais de modules . . . 44
Restreindre l'accès à des domaines spécifiés . . . 44
Mises à jour du collecteur de données . . . 44
Septembre 2023 . . . 45
Trouvez facilement ce que vous voulez dans les journaux . . . 45
Panneau de détails du journal « flottant » . . . 46
Réduire le menu . . . 47
Améliorations du collecteur de données . . . 48
Août 2023 . . . 48
Collecte des journaux Isilon/PowerScale et des données d'analyse avancées . . . 49
Carte de charge de travail améliorée . . . 49
Ajustement de l'utilisation de l'unité gérée Kubernetes . . . 49
Modifications du collecteur/de l'acquisition : . . . 50
Menus améliorés . . . 50
Juillet 2023 . . . 52
Afficher les modifications récentes . . . 52
Améliorations de l'opérateur . . . 52
Aperçu : Récupérer les entrepôts frigorifiques . . . 53
Signature de l'image de l'opérateur . . . 53
Agrégation, mise en forme conditionnelle et plus pour les requêtes . . . 53
API pour l'audit . . . 54
Collecteur de données : Trident Economy . . . 55
Juin 2023 . . . 55

Vérifiez votre utilisation . . . 55
Kubernetes Network Monitoring and Map est disponible pour tous . . . 55
Modifications du collecteur/de l'acquisition : . . . 55
Nouveaux tableaux de bord ONTAP Essentials . . . 56
Moniteurs système supplémentaires . . . 56
Mai 2023 . . . 56
Installation améliorée de l'opérateur de surveillance Kubernetes . . . 56
Virtualisation du stockage . . . 56
Nouveaux paramètres de webhook . . . 57
Rapports sur les données Kubernetes . . . 57
Moniteurs système ONTAP par défaut activés pour les nouveaux clients . . . 57
Avril 2023 . . . 57
Surveillance et cartographie des performances de Kubernetes . . . 57
Tableau de bord de sécurité ONTAP Essentials . . . 58
Récupérez le stockage à froid ONTAP . . . 59
La notification d'abonnement contrôle également les messages de bannière . . . 60
Le reporting a un nouveau look . . . 60
Moniteurs en pause par défaut . . . 60
Vous recherchez l'onglet Mesure de l'API ? . . . 60
Mars 2023 . . . 61
Connexion Cloud pour ONTAP 9.9+ obsolète . . . 61
Janvier 2023 . . . 61
Nouveaux moniteurs de journaux . . . 61
Exportation .CSV pour tous les widgets du tableau de bord . . . 61
Décembre 2022 . . . 61
Découvrez la protection contre les ransomwares et d'autres fonctionnalités de sécurité pendant l'essai de Cloud Insights . . . 61
Les charges de travail Kubernetes ont leur propre page de destination . . . 61
Vérifiez vos sommes de contrôle . . . 62
Améliorations des alertes de journal . . . 62
11 nouveaux moniteurs ONTAP par défaut couvrant SnapMirror pour la continuité des activités . . . 63
Novembre 2022 . . . 63
Plus de 40 nouveaux moniteurs de sécurité, de collecte de données et de CVO ! . . . 63
Octobre 2022 . . . 63
Détection de ransomwares meilleure et plus précise grâce à l'intégration d' ONTAP Autonomous Ransomware Protection . . . 64
Septembre 2022 . . . 64
Moniteurs disponibles en édition de base . . . 64
Tableaux de bord ONTAP Power et StorageGRID . . . 64
Visibilité des seuils en un coup d'œil dans les tableaux . . . 64
Moniteur de sécurité . . . 65
Discutez de n'importe où . . . 65
Des informations plus visibles . . . 65
Nouveaux collecteurs de données . . . 65
Autres mises à jour du collecteur de données . . . 65

Prise en charge du système d'exploitation . . . 65
Août 2022 . . . 66
Cloud Insights a un nouveau look ! . . . 66
Vous ne savez pas par où commencer ? Découvrez ONTAP Essentials ! . . . 66
Les familles de données de stockage sont fusionnées . . . 67
Quelle est la quantité d'énergie utilisée par mon système de stockage ? . . . 68
Fonctionnalités graduées à partir de l'aperçu . . . 69
Comment se porte ma collecte de données ? . . . 69
Jetons API à renouvellement automatique . . . 69
L'édition de base vous offre plus qu'avant . . . 70
Prêt à en savoir plus ? . . . 70
Prise en charge du système d'exploitation . . . 70
Juin 2022 . . . 70
Saturation du cluster Kubernetes et autres détails . . . 70
Quel âge a votre cluster Kubernetes ? . . . 71
Prévision du temps de remplissage de la capacité . . . 71
Qu'est-ce qui a changé dans mon environnement ? . . . 72
Prise en charge du système d'exploitation . . . 73
Agent Telegraf mis à jour . . . 73
Fonctionnalités d'aperçu . . . 73
Mai 2022 . . . 74
Discutez en direct avec le support NetApp . . . 74
Opérateur Kubernetes . . . 74
Gérer les utilisateurs et les invitations avec l'API . . . 75
Alertes de collecte de données . . . 75
Alerte sur les modifications du stockage ONTAP . . . 75
Fonctionnalités d'aperçu . . . 75
Avril 2022 . . . 76
Partagez vos commentaires! . . . 76
Éditeur de tableau de bord mis à jour . . . 76
Surveillance améliorée de votre infrastructure Kubernetes . . . 77
Fonctionnalités d'aperçu . . . 77
Nouveau collecteur de données . . . 78
Autres mises à jour du collecteur de données . . . 78
Mars 2022 . . . 78
Connexion Cloud pour ONTAP 9.9+ . . . 78
Nouveau FSx pour les moniteurs NetApp ONTAP . . . 78
Nouvelles fonctionnalités Cloud Secure accessibles à tous . . . 79
Agent Telegraf mis à jour . . . 79
Mises à jour du collecteur de données . . . 79
Février 2022 . . . 79
Cloud Insights corrige les vulnérabilités d'Apache Log4j . . . 79
Page de détails de l'espace de noms Kubernetes . . . 80
Décembre 2021 . . . 80
Intégration plus poussée pour les systèmes ONTAP . . . 81

Interrogation des journaux . . . 81
Notifications au niveau du collecteur de données. . . . 81
Une plus grande flexibilité des rôles Cloud Secure . . . 81
Prise en charge du système d'exploitation . . . 82
Mises à jour du collecteur de données . . . 82
Novembre 2021 . . . 82
Tableaux de bord adaptatifs . . . 82
Accéder à la base de données de rapports via l'API . . . 83
Tables de pods sur la page de destination de la machine virtuelle . . . 83
Mises à jour du collecteur de données . . . 83
Systèmes d'exploitation supplémentaires pris en charge . . . 84
Octobre 2021 . . . 84
Filtres sur les pages de K8S Explorer . . . 84
Données K8s pour les rapports . . . 84
Le thème sombre est arrivé . . . 85
Assistance au collecteur de données . . . 85
Septembre 2021 . . . 85
Les politiques de performance sont désormais des moniteurs . . . 85
Suggestions de saisie semi-automatique, caractères génériques et expressions dans les moniteurs . . . 86
Agent Telegraf mis à jour . . . 86
Assistance au collecteur de données . . . 86
Août 2021 . . . 87
Nouvelle interface utilisateur de la page d'audit . . . 87
Gestion améliorée des rôles d'utilisateur . . . 87
Juin 2021 . . . 87
Suggestions de saisie semi-automatique, caractères génériques et expressions dans les filtres . . . 87
API disponibles par édition . . . 88
Visibilité des PV et des pods Kubernetes . . . 88
Liens entre le nœud Kubernetes et la VM . . . 89
Les moniteurs d'alerte remplacent les politiques de performance . . . 90
Cloud Secure prend en charge NFS . . . 90
Purge des instantanés Cloud Secure . . . 90
Vitesse de collecte de données Cloud Secure . . . 91
Mai 2021 . . . 91
Agent Telegraf mis à jour . . . 91
Ajouter des actions correctives à une alerte . . . 91
API Cloud Insights pour toutes les éditions . . . 92
Avril 2021 . . . 92
Gestion simplifiée des moniteurs . . . 92
Options d'alerte améliorées à l'aide de Webhooks . . . 93
Identification améliorée des appareils . . . 93
Vous en avez demandé plus ! . . . 93
Plusieurs abonnements dans un seul environnement Cloud Insights . . . 94
Choisissez votre chemin . . . 94
Intégration Cloud Secure . . . 94

Février 2021 . . . 95
Agent Telegraf mis à jour . . . 95
Analyseur de coûts du cloud . . . 95
Interrogation d'objets ayant des valeurs nulles à l'aide de filtres . . . 95
Prise en charge multirégionale . . . 95
Janvier 2021 . . . 96
Mesures ONTAP supplémentaires renommées . . . 96
Nouvel explorateur Kubernetes . . . 97
Décembre 2020 . . . 98
Installation simplifiée de Kubernetes . . . 98
Novembre 2020 . . . 98
Tableaux de bord supplémentaires . . . 98
Renommer les colonnes dans les widgets de tableau . . . 99
Octobre 2020 . . . 99
Extension par défaut des données d'intégration . . . 99
Support technique de l'édition de base . . . 99
API publique Cloud Secure . . . 100
Septembre 2020 . . . 100
Page de requête avec données d'intégration . . . 100
Formatage de l'affichage des unités dans le widget de tableau . . . 100
Page de détails de l'unité d'acquisition . . . 101
Dépendance Docker Cloud Secure supprimée . . . 101
Rapports sur les rôles des utilisateurs . . . 101
Nouvelle catégorie d'API pour l'ingestion de données . . . 102
Août 2020 . . . 102
Surveillance et alerte . . . 102
Juillet 2020 . . . 103
Cloud Secure *Prendre un instantané* Action . . . 103
Mises à jour des métriques/compteurs . . . 104
Détection d'attaques potentielles Cloud Secure . . . 105
Abonnez-vous à l'édition Premium via AWS . . . 106
Widget de tableau amélioré . . . 106
Filtrage des métriques . . . 108
Données de compteur avancées ONTAP . . . 108
Tableaux de bord de compteur avancés . . . 110
En savoir plus . . . 110
Menu des politiques et des violations . . . 110
Agent Telegraf mis à jour . . . 110
Juin 2020 . . . 111
Rapport d'erreurs simplifié du collecteur de données . . . 111
Améliorations des widgets . . . 112
Mai 2020 . . . 113
Rapports sur les rôles des utilisateurs . . . 113
Mises à jour Cloud Secure . . . 113
Regroupement du tableau de bord . . . 113

Épinglage du tableau de bord . . . 114
Mode TV et rafraîchissement automatique . . . 114
Avril 2020 . . . 115
Nouveaux choix de plages horaires du tableau de bord . . . 115
Mises à jour Cloud Secure . . . 115
Heure par défaut du tableau de bord . . . 115
Temps d'agrégation optimisés . . . 115
Formatage automatique de l'unité d'affichage . . . 116
Importer des annotations à l'aide de l'API . . . 116
Sélecteur de widgets plus simple . . . 116
Février 2020 . . . 117
API avec édition Premium . . . 117
Interrogation initiale après l'ajout d'un collecteur de données . . . 117
Duplication de widgets plus facile . . . 118
Authentification unique (SSO) . . . 118
Janvier 2020 . . . 119
Documentation Swagger pour l'API REST . . . 119
Barre de progression des didacticiels sur les fonctionnalités . . . 119
Modifications de l'unité d'acquisition . . . 119
Agrégation temporelle optimisée dans les widgets . . . 119
Processus simplifié de « Mise en route avec Cloud Insights» . . . 119
Data Infrastructure Insights . . . 121
Sécurité . . . 122
Data Infrastructure Insights et sécurité . . . 122
Aperçu de la sécurité . . . 122
Informations et région . . . 124
Quelles informations Data Infrastructure Insights stocke-t-il ? . . . 124
Où sont stockées mes informations ? . . . 125
Plus d'informations . . . 126
Outil d'administration de sécurité . . . 126
Considérations relatives à la mise à niveau et à l'installation . . . 127
Gestion de la sécurité sur l'unité d'acquisition . . . 127
Avant de commencer . . . 127
Utilisation de l'outil SecurityAdmin . . . 127
Spécifier un utilisateur pour exécuter l'outil . . . 129
Mise à jour ou suppression du proxy . . . 130
Récupération de clés externes . . . 132
Crypter un mot de passe à utiliser dans l'API . . . 132
Commencer . . . 136
Premiers pas avec les tutoriels vidéo . . . 136
Liste de contrôle et didacticiels vidéo . . . 136
Tutoriels vidéo . . . 137
Collecte de données . . . 137
Commencer à collecter des données . . . 137
Exigences relatives à l'unité d'acquisition . . . 140

Configuration des unités d'acquisition . . . 142
Configuration d'un agent pour collecter des données (Windows/Linux) . . . 149
Configuration des collecteurs de données . . . 162
Déterminer l'état d'acquisition du collecteur de données . . . 162
Gestion des collecteurs de données configurés . . . 163
Recherche sur un collecteur de données en échec . . . 165
Importation de tableaux de bord . . . 165
Importation depuis la galerie du tableau de bord . . . 166
Importer un tableau de bord exporté . . . 166
Comptes d'utilisateurs et rôles . . . 166
Niveaux d'autorisation . . . 167
Créer des comptes en invitant des utilisateurs . . . 170
Modifier le rôle d'un utilisateur existant . . . 171
Suppression d'utilisateurs . . . 172
Authentification unique (SSO) et fédération d'identité . . . 172
Restreindre l'accès par domaine . . . 175
Liste de référence des collecteurs de données Data Infrastructure Insights . . . 177
S'abonner à Data Infrastructure Insights . . . 181
Édition d'essai . . . 181
Essai via AWS Marketplace . . . 182
Que faire si mon essai a expiré ? . . . 182
Que faire si mon **abonnement** a expiré ? . . . 182
Évaluation du module . . . 182
Estimateur . . . 183
Options d'abonnement . . . 184
Mesure de l'observabilité . . . 184
Mesure de la sécurité de la charge de travail . . . 185
Comment puis-je m'abonner ? . . . 185
Abonnez-vous directement via NetApp Sales . . . 185
Auto-abonnez-vous via AWS Marketplace . . . 185
Afficher le statut de votre abonnement . . . 186
Consultez votre gestion d'utilisation . . . 187
Que se passe-t-il si je dépasse mon utilisation souscrite ? . . . 187
Abonnez-vous directement et évitez l'essai . . . 188
Ajout d'un identifiant d'autorisation . . . 188
Observabilité . . . 189
Création de tableaux de bord . . . 189
Présentation des tableaux de bord . . . 189
Fonctionnalités du tableau de bord . . . 193
Gestion des accès au tableau de bord . . . 227
Bonnes pratiques pour les tableaux de bord et les widgets . . . 228
Exemples de tableaux de bord . . . 231
Travailler avec des requêtes . . . 237
Interrogation des assets et des métriques . . . 237
Créer des requêtes . . . 238

Consultation des requêtes . . . 245
Exportation des résultats de la requête vers un fichier .CSV . . . 245
Modifier ou supprimer une requête . . . 247
Affectation ou suppression de plusieurs applications à des actifs . . . 247
Copie des valeurs du tableau . . . 248
Explorateur de journaux . . . 249
Identifier les appareils inactifs . . . 254
Connaissances . . . 255
Connaissances . . . 255
Perspectives : Les ressources partagées sous pression . . . 255
Aperçu : les espaces de noms Kubernetes manquent d'espace . . . 258
Aperçu : Récupérez le stockage à froid ONTAP . . . 259
Moniteurs et alertes . . . 262
Alertes avec moniteurs . . . 262
Affichage et gestion des alertes des moniteurs . . . 273
Configuration des notifications par e-mail . . . 276
Moniteurs de détection d'anomalies . . . 279
Moniteurs système . . . 283
Notifications Webhook . . . 366
Travailler avec des annotations . . . 379
Définition des annotations . . . 379
Utilisation des annotations . . . 382
Création de règles d'annotation . . . 384
Importation d'annotations . . . 386
Travailler avec des applications . . . 388
Suivi de l'utilisation des actifs par application . . . 388
Création d'applications . . . 389
Résolution automatique des appareils . . . 390
Présentation de la résolution automatique des appareils . . . 390
Règles de résolution des appareils . . . 393
Résolution du périphérique Fibre Channel . . . 396
Résolution du périphérique IP . . . 398
Options de paramétrage dans l'onglet Préférences . . . 400
Exemples d'expressions régulières . . . 401
Informations sur la page des actifs . . . 407
Présentation de la page des ressources . . . 407
Filtrage des objets en contexte . . . 414
Virtualisation du stockage . . . 415
Conseils et astuces pour rechercher des actifs et des alertes . . . 417
Analyse des données . . . 419
Présentation de SAN Analyzer . . . 419
Présentation de VM Analyzer . . . 422
Surveiller la santé de l'infrastructure . . . 424
Rapports . . . 426
Présentation des rapports sur Data Infrastructure Insights . . . 426

Rôles des utilisateurs des rapports sur Data Infrastructure Insights . . . 427
Rapports prédéfinis simplifiés . . . 429
Tableau de bord du gestionnaire de stockage . . . 433
Création d'un rapport (exemple) . . . 436
Gestion des rapports . . . 439
Création de rapports personnalisés . . . 442
Accéder à la base de données de rapports via l'API . . . 450
Publication et dépublication d'annotations pour les rapports . . . 454
Comment les données historiques sont conservées pour les rapports . . . 455
Diagrammes de schéma de reporting des Data Infrastructure Insights . . . 456
Schémas Data Infrastructure Insights pour la création de rapports . . . 509
Kubernetes . . . 511
Présentation du cluster Kubernetes . . . 511
Affiner le filtre . . . 511
Avant d'installer ou de mettre à niveau l'opérateur de surveillance NetApp Kubernetes . . . 512
Choses importantes à noter avant de commencer . . . 513
Installation et configuration de l'opérateur de surveillance Kubernetes . . . 516
Avant d'installer Kubernetes Monitoring Operator . . . 516
Installation de l'opérateur de surveillance Kubernetes . . . 517
Composants de surveillance Kubernetes . . . 519
Mise à niveau vers la dernière version de Kubernetes Monitoring Operator . . . 520
Arrêt et démarrage de l'opérateur de surveillance Kubernetes . . . 521
Désinstallation . . . 521
À propos de Kube-state-metrics . . . 522
Configuration/Personnalisation de l'opérateur . . . 523
Une note sur les secrets . . . 527
Vérification des signatures d'image de l'opérateur de surveillance Kubernetes . . . 527
Dépannage . . . 528
Options de configuration de l'opérateur de surveillance Kubernetes . . . 536
Exemple de fichier AgentConfiguration . . . 536
Page de détails du cluster Kubernetes . . . 554
Nombre d'espaces de noms, de nœuds et de pods . . . 554
Ressources partagées et saturation . . . 554
Espaces de noms . . . 554
Charges de travail . . . 555
La « roue » du cluster . . . 555
Une note sur les jauges . . . 558
Surveillance et cartographie des performances du réseau Kubernetes . . . 558
Prérequis . . . 559
Moniteurs . . . 560
La carte . . . 560
Détails et alertes de charge de travail . . . 562
Recherche et filtrage . . . 562
Étiquettes de charge de travail . . . 563
Plongez en profondeur . . . 564

Analyse des changements Kubernetes . . . 566
Filtration . . . 567
Statut rapide . . . 568
Panneau de détails . . . 569
ONTAP Essentials . . . 571
Aperçu . . . 571
Protection des données . . . 572
Sécurité . . . 573
Alertes . . . 577
Infrastructure . . . 578
Réseautage . . . 579
Charges de travail . . . 579
Administration et autres tâches . . . 581
API Data Infrastructure Insights . . . 581
Conditions requises pour l'accès à l'API . . . 581
Documentation de l'API (Swagger) . . . 581
Jetons d'accès API . . . 582
Type d'API . . . 583
Parcours d'inventaire . . . 584
S'agrandit . . . 584
Données de performance . . . 586
Mesures de performance des objets . . . 588
Données d'historique des performances . . . 588
Objets avec attributs de capacité . . . 589
Utiliser la recherche pour rechercher des objets . . . 590
Désactiver ou révoquer un jeton API . . . 590
Rotation des jetons d'accès API expirés . . . 591
Surveiller votre environnement . . . 592
Audit . . . 592
Digital Advisor Active IQ . . . 595
Sécurité de la charge de travail . . . 598
À propos de la sécurité des charges de travail de stockage . . . 598
Visibilité . . . 598
Protection . . . 598
Conformité . . . 598
Commencer . . . 598
Premiers pas avec la sécurité des charges de travail . . . 598
Exigences relatives à l'agent de sécurité de la charge de travail . . . 599
Déployer des agents de sécurité de charge de travail . . . 603
Suppression d'un agent de sécurité de charge de travail . . . 611
Configuration d'un collecteur d'annuaires utilisateurs Active Directory (AD) . . . 612
Configuration d'un collecteur de serveur d'annuaire LDAP . . . 618
Configuration du collecteur de données ONTAP SVM . . . 623
Dépannage du collecteur de données ONTAP SVM . . . 633
Configuration du collecteur Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP . . . 640

Gestion des utilisateurs . . . 642
Vérificateur de taux d'événements : Guide de dimensionnement des agents . . . 643
Comprendre et examiner les alertes . . . 647
Alerte . . . 647
Options de filtrage . . . 648
La page Détails de l'alerte . . . 649
Prendre un instantané Action . . . 651
Notifications d'alerte . . . 652
Politique de conservation . . . 652
Dépannage . . . 653
criminalistique . . . 653
Forensic - Toutes les activités . . . 654
Présentation de l'utilisateur forensique . . . 664
Politiques de réponse automatisées . . . 665
Politiques relatives aux types de fichiers autorisés . . . 667
Intégration avec la protection autonome contre les ransomwares ONTAP . . . 668
Prérequis . . . 669
Autorisations utilisateur requises . . . 669
Exemple d'alerte . . . 669
Limites . . . 671
Dépannage . . . 671
Intégration avec ONTAP Accès refusé . . . 671
Prérequis . . . 671
Autorisations utilisateur requises . . . 672
Événements d'accès refusé . . . 672
Bloquer l'accès des utilisateurs pour stopper les attaques . . . 673
Conditions préalables au blocage de l'accès utilisateur . . . 673
Comment activer la fonctionnalité ? . . . 674
Comment configurer le blocage automatique de l'accès des utilisateurs ? . . . 674
Comment savoir s'il y a des utilisateurs bloqués dans le système ? . . . 674
Restreindre et gérer manuellement l'accès des utilisateurs . . . 674
Historique des limitations d'accès des utilisateurs . . . 675
Comment désactiver la fonctionnalité ? . . . 675
Restaurer manuellement les adresses IP pour NFS . . . 675
Restaurer manuellement les utilisateurs pour SMB . . . 676
Dépannage . . . 677
Sécurité des charges de travail : simulation de falsification de fichiers . . . 678
Choses à noter avant de commencer . . . 679
Directives : . . . 679
Mesures: . . . 679
Générez les fichiers d'exemple par programmation : . . . 680
Reprendre le collecteur . . . 681
Générez les fichiers d'exemple par programmation : . . . 681
Générer une alerte dans Workload Security . . . 682
Déclenchement de l'alerte plusieurs fois . . . 683

Configuration des notifications par e-mail pour les alertes, les avertissements et l'état de santé de l'agent/collecteur de sources de données . . . 683
Alertes et avertissements d'attaque potentielle . . . 683
Surveillance de la santé des agents et des collecteurs de données . . . 684
Notifications de mise à niveau de l'agent récepteur et du collecteur de données . . . 684
Dépannage . . . 684
Notifications Webhook . . . 684
Notifications de sécurité de la charge de travail à l'aide de webhooks . . . 684
Exemple de webhook de sécurité de charge de travail pour Discord . . . 690
Exemple de webhook de sécurité de charge de travail pour PagerDuty . . . 693
Exemple de webhook de sécurité de charge de travail pour Slack . . . 698
Exemple de webhook de sécurité de charge de travail pour Microsoft Teams . . . 702
API de sécurité de la charge de travail . . . 707
Documentation de l'API (Swagger) . . . 708
Jetons d'accès API . . . 708
Script pour extraire des données via l'API . . . 709
Dépannage du collecteur de données ONTAP SVM . . . 709
Dépannage . . . 717
Dépannage des problèmes généraux Data Infrastructure Insights . . . 717
Problèmes de connexion . . . 717
Autres questions . . . 718
Ressources . . . 718
Dépannage des problèmes d'unité d'acquisition sous Linux . . . 719
Considérations sur les proxys et les pare-feu . . . 721
Ressources . . . 722
Dépannage des problèmes d'unité d'acquisition sous Windows . . . 722
Considérations sur les proxys et les pare-feu . . . 724
Ressources . . . 725
Recherche sur un collecteur de données en échec . . . 725
Matrice de support du collecteur de Data Infrastructure Insights . . . 727
Stockage HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ . . . 727
Amazon AWS EC2 . . . 744
Amazon AWS S3 . . . 750
Azure NetApp Files . . . 754
Commutateurs Fibre Channel Brocade . . . 763
Conseiller réseau Brocade HTTP . . . 774
Brocade FOS REST . . . 778
Commutateurs Cisco MDS et Nexus Fabric . . . 789
Cohésion . . . 797
EMC Celerra (SSH) . . . 806
EMC CLARiiON (NaviCLI) . . . 815
Domaine de données EMC (SSH) . . . 829
CEM ECS . . . 838
Dell EMC Isilon et PowerScale Rest . . . 847
Dell EMC Isilon / PowerScale (CLI) . . . 867

EMC PowerStore REST . . . 884
EMC RecoverPoint (HTTP) . . . 901
EMC ScaleIO et PowerFlex REST . . . 905
Interface de ligne de commande EMC Symmetrix . . . 911
Dell Unisphere REST . . . 929
EMC VNX (SSH) . . . 946
EMC VNXe et Unity Unisphere (CLI) . . . 965
EMC VPLEX . . . 979
EMC XtremIO (HTTP) . . . 988
NetApp Série E . . . 1002
Stockage pur FlashBlade REST . . . 1015
Google Cloud Compute . . . 1026
Volumes Netapp de Google Cloud . . . 1031
HDS HCP (HTTPS) . . . 1041
Gestionnaire de périphériques HiCommand . . . 1046
Centre d’opérations Hitachi . . . 1061
HDS HNAS (CLI) . . . 1078
Stockage HPE Nimble/Alletra 6000 . . . 1087
Huawei OceanStor (REST/HTTPS) . . . 1100
IBM Cleversafe . . . 1120
IBM DS 8K (DSCLI) . . . 1125
IBM PowerVM (SSH) . . . 1137
IBM SVC (CLI) . . . 1140
IBM XIV et A9000 (XIVCLI) . . . 1155
Infinidat Infinibox (HTTP) . . . 1161
Microsoft Azure Compute . . . 1170
Microsoft Hyper-V . . . 1176
Mode NetApp 7 . . . 1186
REST NetApp Série E . . . 1210
Amazon FSx for NetApp ONTAP . . . 1219
Data ONTAP en cluster NetApp ONTAP 8.1.1+ . . . 1242
ASA . . . 1281
NetApp ONTAP REST . . . 1295
NetApp SolidFire 8.1+ . . . 1317
NetApp StorageGRID (HTTPS) . . . 1334
Stockage Nutanix (REST) . . . 1344
OpenStack (API REST / SSH) . . . 1358
Oracle ZFS (HTTPS) . . . 1362
Baie Flash de stockage pure (HTTP) . . . 1377
Red Hat RHV (REST) . . . 1391
Stockage Rubrik . . . 1396
Magasin de données VAST . . . 1406
Centre virtuel NetApp HCI . . . 1417
VMware Cloud sur AWS . . . 1428
VMware vSphere (services Web) . . . 1435

Référence et support . . . 1450
Demande d'assistance . . . 1450
Activation du droit d'assistance . . . 1450
Obtenir des informations d'assistance . . . 1453
Matrice de support du collecteur de Data Infrastructure Insights . . . 1455
Référence du collecteur de données - Infrastructure . . . 1455
Référence spécifique au fournisseur . . . 1455
Configuration du collecteur de données Amazon EC2 . . . 1455
Collecteur de données Amazon FSx for NetApp ONTAP . . . 1458
Configuration du collecteur de données de calcul Azure . . . 1461
Broadcom . . . 1462
Collecteur de données des commutateurs Cisco MDS Fabric . . . 1470
Collecteur de données Cohesity SmartFiles . . . 1473
Dell . . . 1474
Dell EMC . . . 1475
Collecteur de données Fujitsu Eternus . . . 1501
Collecteur de données NetApp Google Compute . . . 1502
Collecteur de données Google Cloud NetApp Volumes . . . 1503
HP Entreprise . . . 1505
Systèmes de données Hitachi . . . 1513
Collecteur de données Infinidat InfiniBox . . . 1522
Collecteur de données Huawei OceanStor . . . 1523
IBM . . . 1524
Collecteur de données Lenovo . . . 1532
Microsoft . . . 1532
NetApp . . . 1535
Collecteur de données Nutanix NX . . . 1576
Collecteur de données Oracle ZFS Storage Appliance . . . 1577
Collecteur de données Pure Storage FlashArray . . . 1580
Collecteur de données de virtualisation Red Hat . . . 1581
Collecteur de données Rubrik CDM . . . 1582
Configuration du collecteur de données VMware VSphere . . . 1584
Référence du collecteur de données - Services . . . 1587
Collecte de données de nœuds . . . 1587
Collecteur de données ActiveMQ . . . 1590
Collecteur de données Apache . . . 1592
Collecteur de données consulaires . . . 1595
Collecteur de données Couchbase . . . 1596
Collecteur de données CouchDB . . . 1598
Collecteur de données Docker . . . 1600
Collecteur de données Elasticsearch . . . 1608
Collecteur de données Flink . . . 1610
Collecteur de données Hadoop . . . 1617
Collecteur de données HAProxy . . . 1622
Collecteur de données JVM . . . 1628

Collecteur de données Kafka . . . 1633
Collecteur de données Kibana . . . 1636
Installation et configuration de l’opérateur de surveillance Kubernetes . . . 1638
Collecteur de données Memcached . . . 1657
Collecteur de données MongoDB . . . 1660
Collecteur de données MySQL . . . 1662
Collecteur de données Netstat . . . 1667
Collecteur de données Nginx . . . 1668
Collecteur de données PostgreSQL . . . 1671
Collecteur de données d’agent de marionnettes . . . 1673
Collecteur de données Redis . . . 1675
Référence d’icône d’objet . . . 1677
Icônes d’infrastructure : . . . 1677
Icônes Kubernetes : . . . 1678
Icônes de surveillance et de carte des performances du réseau Kubernetes : . . . 1678
Mentions légales . . . 1679
Copyright . . . 1679
Marques de commerce . . . 1679
Brevets . . . 1679
Politique de confidentialité . . . 1679
Open source . . . 1679

Documentation sur Data Infrastructure Insights

NetApp Data Infrastructure Insights (anciennement Cloud Insights) est un outil de surveillance de l'infrastructure cloud qui vous offre une visibilité sur l'ensemble de votre infrastructure. Avec Data Infrastructure Insights, vous pouvez surveiller, dépanner et optimiser toutes vos ressources, y compris vos clouds publics et vos centres de données privés.

Que peut m'apporter Data Infrastructure Insights ?

Data Infrastructure Insights fournit une surveillance multicloud hybride, vous offrant une observabilité complète de l'infrastructure et des charges de travail.

- Collecteurs de données pour infrastructures et charges de travail hétérogènes, y compris Kubernetes
- Collecteur Telegraf ouvert et API ouvertes pour une intégration facile
- Alertes et notifications complètes
- L'apprentissage automatique pour des informations intelligentes
- Optimiser l'utilisation des ressources
- Tableaux de bord intégrés ou personnalisables avec des filtres avancés pour minimiser le bruit d'affichage afin de répondre aux questions
- Découvrez l'état de santé de vos opérations de stockage ONTAP
- Protégez votre atout commercial le plus précieux – les données – contre la falsification de fichiers ou les attaques de destruction de données

---

Commencer

- Comment puis-je**"commencer"** avec Data Infrastructure Insights?
- Je suis inscrit. Et maintenant, que dois-je faire ?"Acquisition de données" "Configuration des utilisateurs"
- Génial! Et ensuite ?"Préparation des ressources : annotation" "Trouver les ressources souhaitées : interrogation" "Voir les données que vous souhaitez : les tableaux de bord" "Surveillance et alertes" "Sécurisation des données"
- C'est du super truc ! Je suis prêt à**"s'abonner"** .

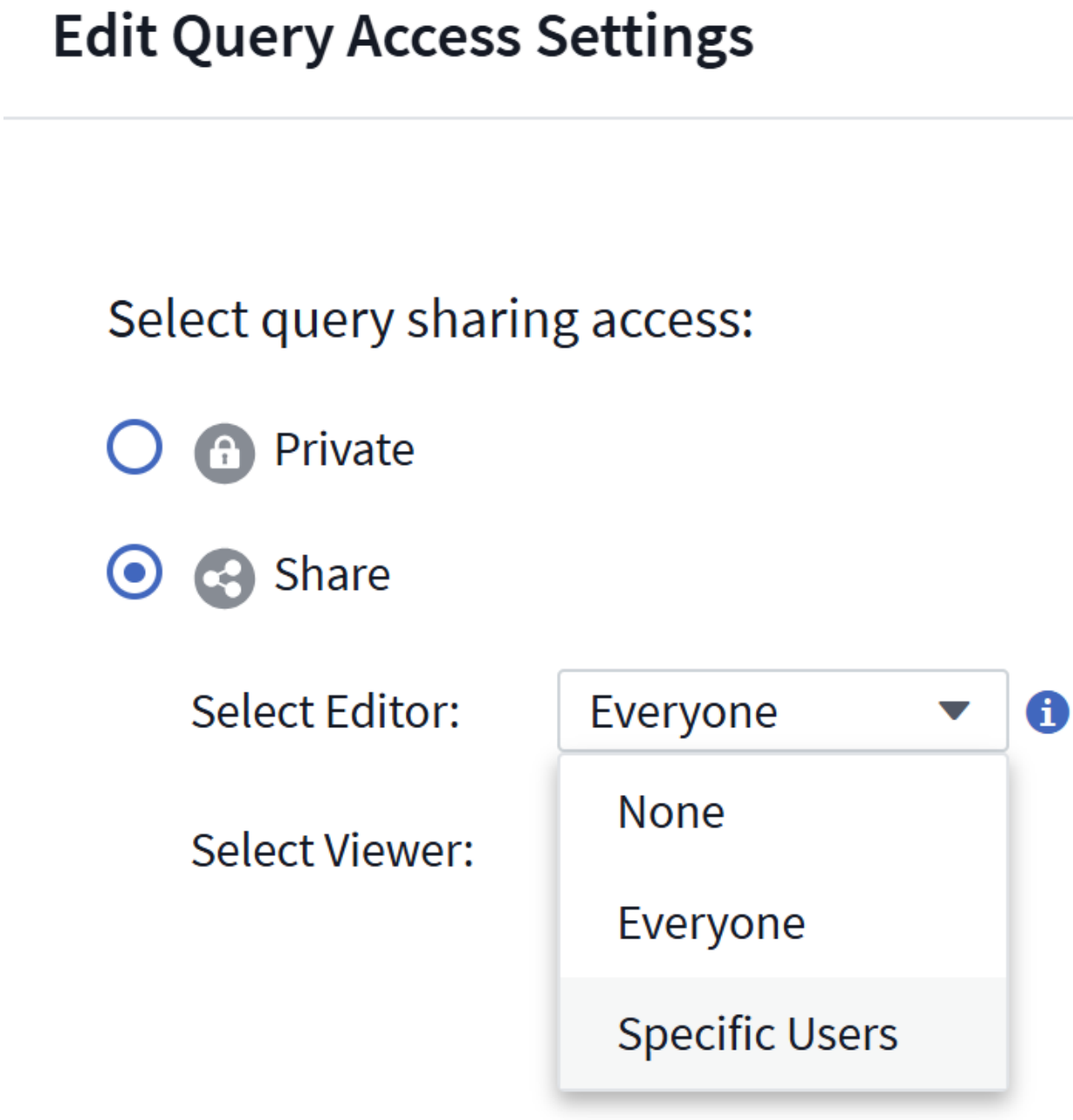
Nouveautés de Data Infrastructure Insights

NetApp améliore et optimise continuellement ses produits et services. Voici quelques-unes des dernières fonctionnalités et fonctionnalités disponibles dans Data Infrastructure Insights (anciennement Cloud Insights).

Décembre 2025

Contrôler l’accès aux requêtes avec des requêtes partagées

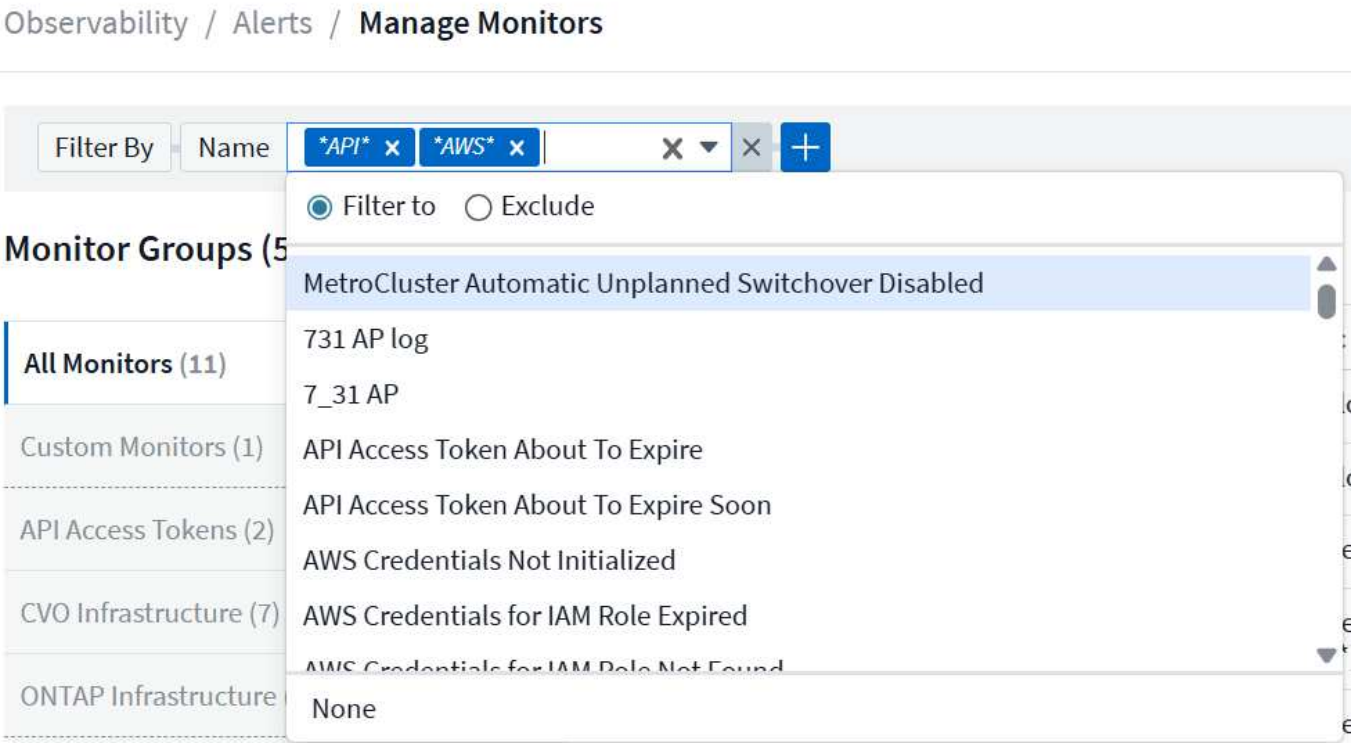
Partagez les requêtes que vous créez grâce à des contrôles d’autorisation précis. Choisissez le mode Visionneuse en lecture seule pour empêcher les modifications ou le mode Édition pour autoriser les modifications. Les requêtes privées sont accessibles aux créateurs, tandis que les requêtes partagées peuvent être utilisées dans les règles d’annotation ou dupliquées pour des cas d’utilisation spécifiques, vous offrant un contrôle total sur la manière dont les requêtes sont utilisées et modifiées au sein de votre organisation.



De plus, les utilisateurs ayant le rôle *Invité* peuvent désormais créer et gérer leurs propres requêtes privées.

Un meilleur filtrage lors de la gestion des moniteurs

Le filtrage des listes et des groupes de surveillance a été amélioré pour ajouter la prise en charge des caractères génériques, les filtres multiples, la fonctionnalité d'inclusion/exclusion, et plus encore.



Visualisations de tableau de bord plus claires

La conception améliorée du tableau de bord vous permet de voir ce qui compte le plus. Amélioration de la clarté visuelle grâce à des bordures ombrées qui séparent les widgets et à la suppression des lignes de séparation pour réduire l'encombrement et vous permettre de vous concentrer sur l'analyse de vos données. Ces améliorations créent une expérience de tableau de bord plus claire et plus intuitive, permettant de repérer plus rapidement et plus facilement les tendances et les anomalies.

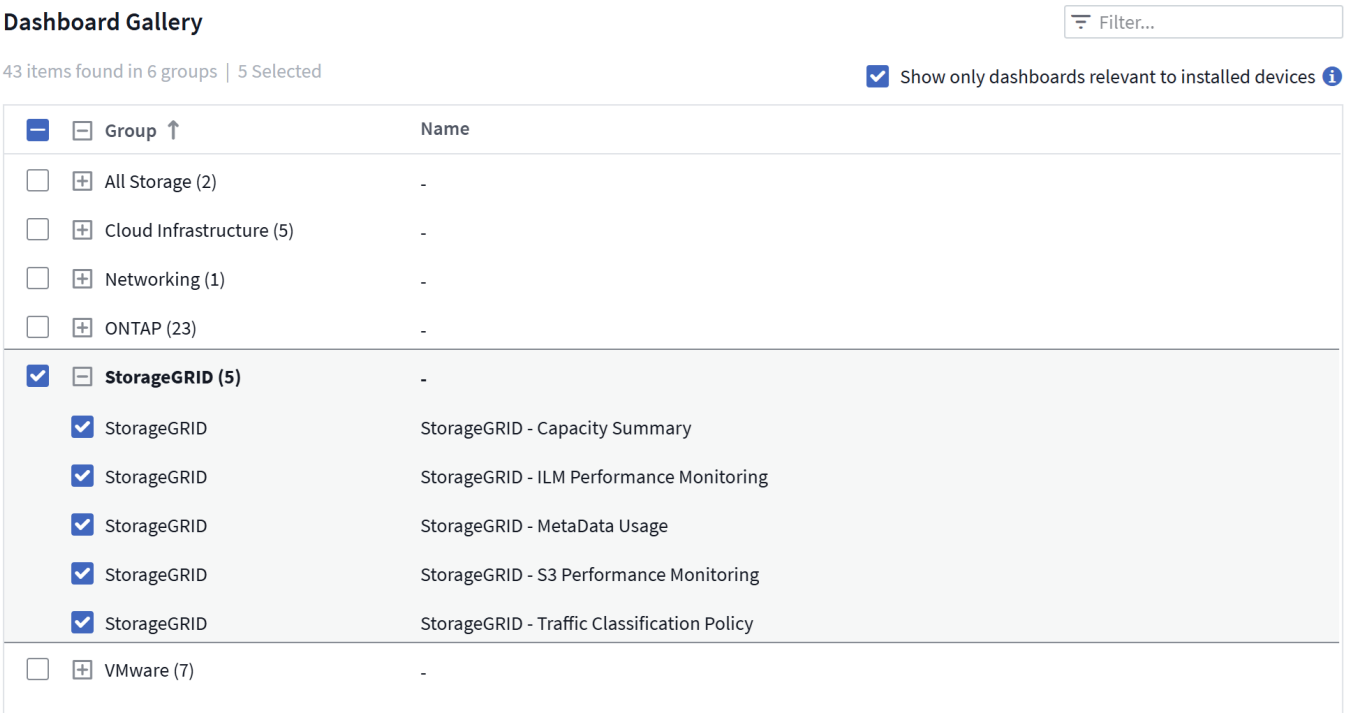
Novembre 2025

Configurez votre page d'accueil personnalisée

Rationalisez votre flux de travail de surveillance quotidien en définissant *n'importe quelle* page Data Infrastructure Insights comme page d'accueil personnalisée. Chaque utilisateur peut sélectionner une page d'accueil différente pour se concentrer sur ce qui est important pour lui : un tableau de bord essentiel, des alertes, l'état de l'infrastructure, la sécurité des charges de travail, ou plus encore.

Restez organisé grâce au regroupement automatique des tableaux de bord

Transformez votre expérience de tableau de bord grâce à un regroupement intelligent qui organise automatiquement les tableaux de bord importés de la galerie en catégories logiques. La nouvelle fonctionnalité de regroupement simplifie l'importation des tableaux de bord et place chaque tableau de bord dans le groupe approprié en fonction de sa fonction et de sa pertinence pour votre environnement.

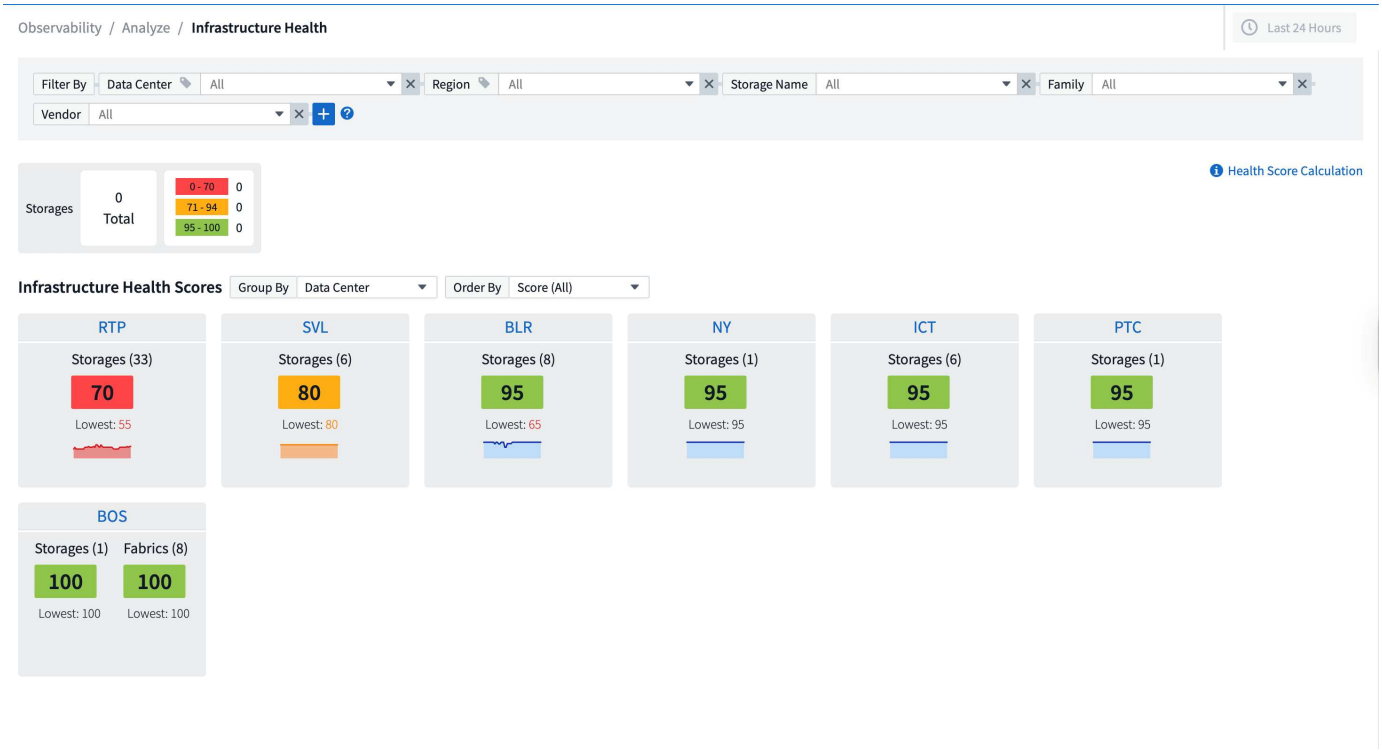


Octobre 2025

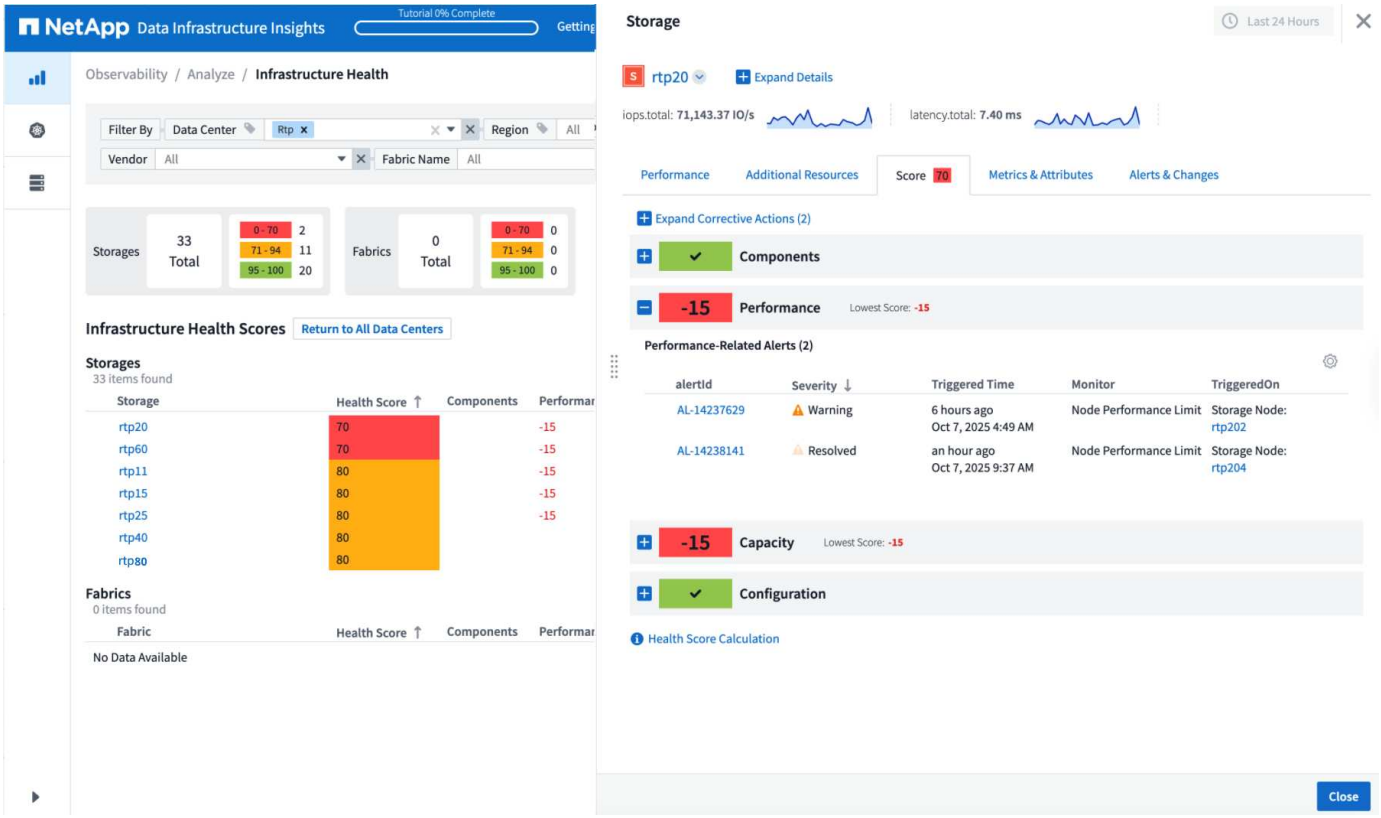
Santé de l'infrastructure : visibilité instantanée sur les risques liés au stockage et à la structure

Bénéficiez d'une visibilité instantanée sur les risques potentiels sur votre stockage et vos infrastructures grâce à notre nouvelle fonctionnalité **Infrastructure Health**. Un tableau de bord unique et codé par couleur vous offre une visibilité unifiée des risques, vous aidant à minimiser les temps d'arrêt et à atténuer rapidement les pertes de revenus.

Les scores inférieurs à 100 indiquent des problèmes potentiels ; plus le score est bas, moins les ressources sont saines. Le regroupement des ressources par centre de données ou par région pour des scores de santé intuitifs et consolidés vous permet de hiérarchiser et de résoudre facilement les problèmes dans les domaines critiques.

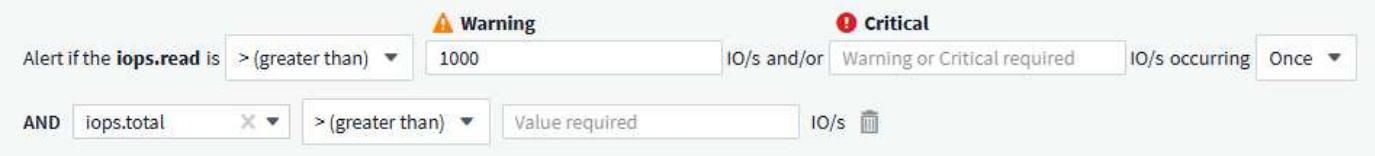


Affichez des informations détaillées dans un panneau coulissant à l'écran en cliquant sur un bouton, en identifiant rapidement les problèmes nécessitant une attention particulière et en gardant vos systèmes sécurisés et résilients.



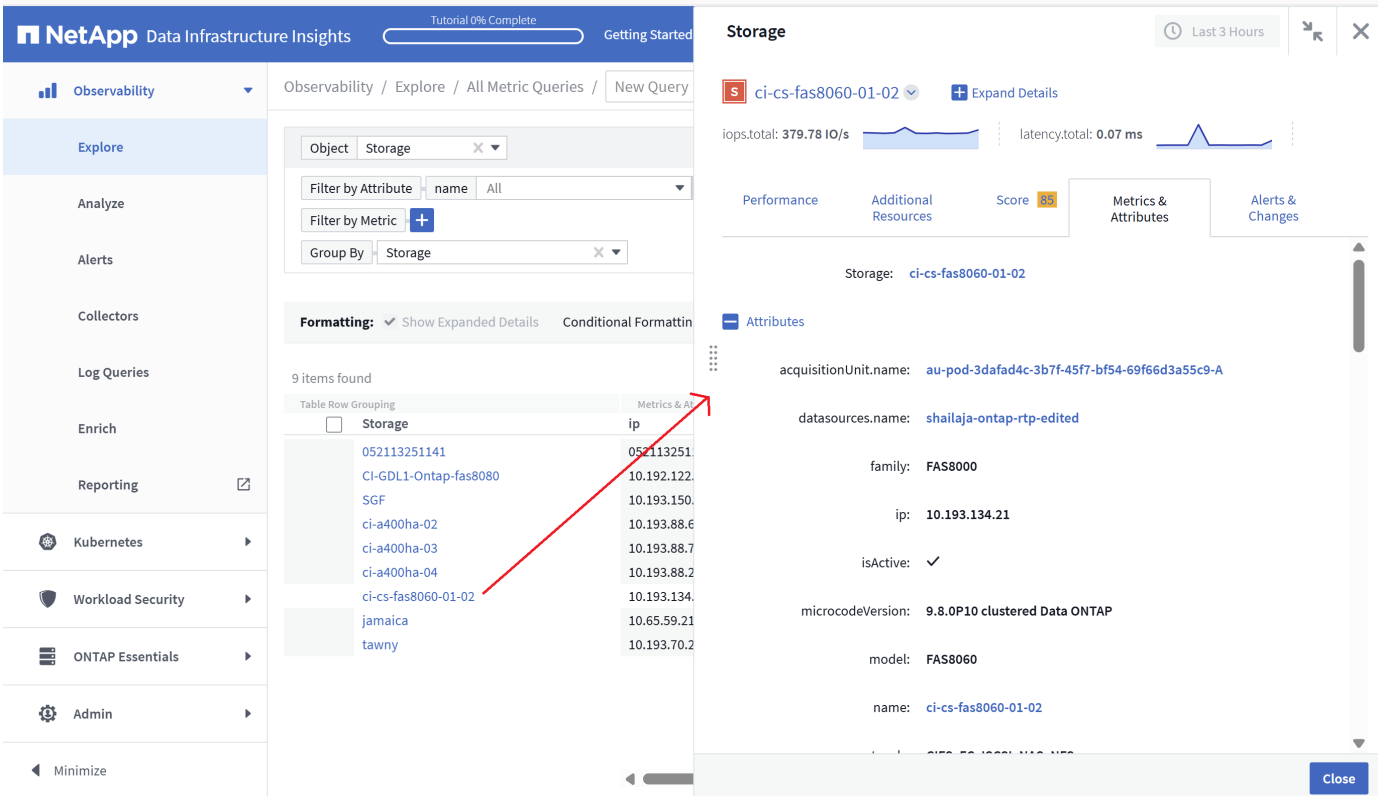
Moniteurs multi-conditions pour des alertes précises

Réduisez le bruit des alertes et améliorez la précision de la surveillance en ajoutant une deuxième condition facultative à n'importe quel moniteur métrique. Les alertes sont déclenchées uniquement lorsque les deux conditions sont remplies, vous offrant ainsi des notifications plus ciblées qui se concentrent sur les scénarios qui comptent le plus pour vous.



Améliorations des requêtes : aperçu des détails des objets

La sélection d'une ligne dans la liste de résultats d'une requête d'objet ouvre un panneau de détails pour l'objet sélectionné. Affichez rapidement les métriques et les attributs (vue par défaut pour les requêtes d'objet), les alertes et les modifications, les performances et les scores d'intégrité, ou explorez les ressources associées. Toutes les informations pertinentes sur les objets sont à portée de main.



Améliorations de la sécurité de la charge de travail

Deux nouvelles API vous offrent plus de contrôle sur votre environnement Workload Security :

1. Afficher et gérer les groupes avec *GET /rest/v1/cloudsecure/activities/groups*.
2. Mettre en pause et reprendre les collecteurs de données avec *POST /rest/v1/cloudsecure/collectors/{collector-uuid}/status*

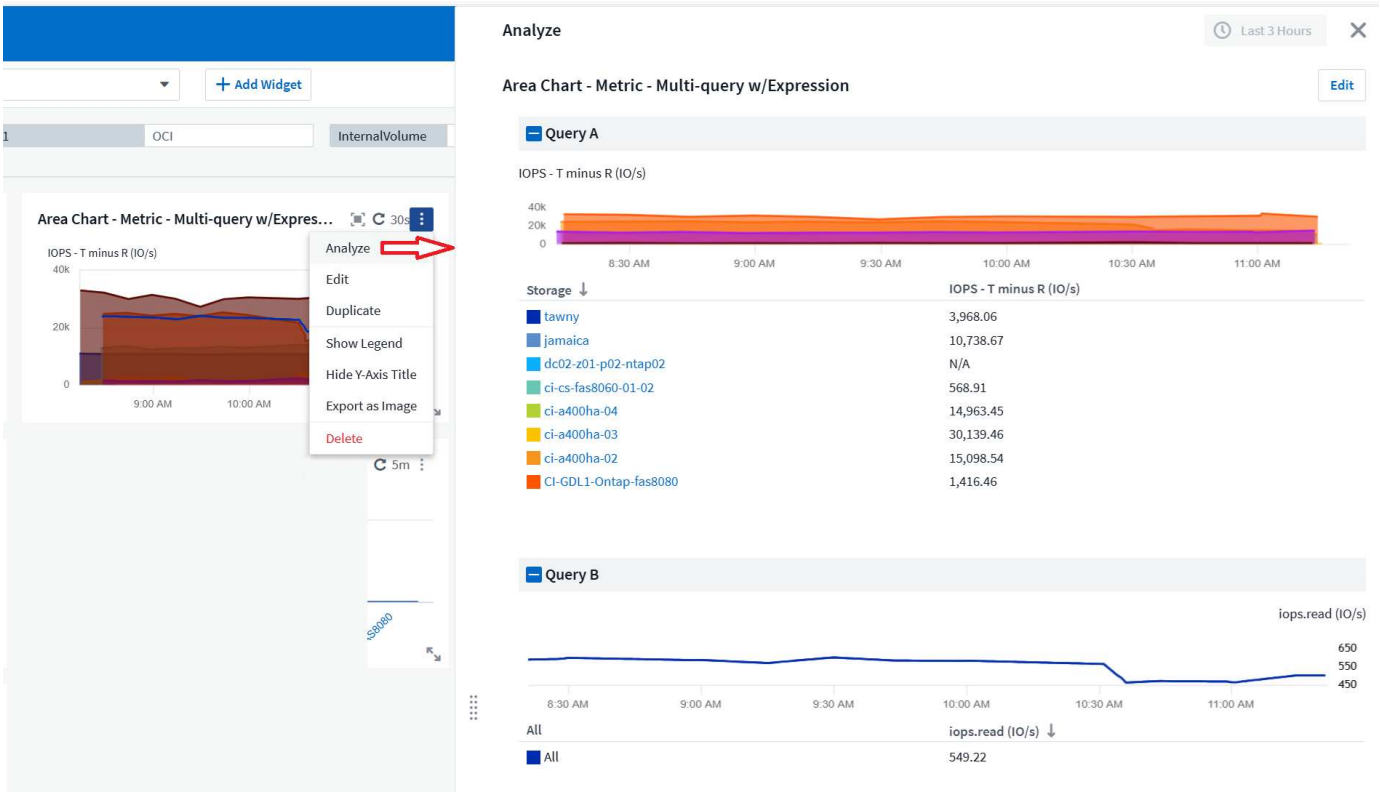
De plus, les contrôles d'autorisation des rôles de sécurité de la charge de travail sont désormais encore plus

sécurisés. En raison de la sécurité améliorée, certains utilisateurs existants peuvent rencontrer des problèmes d'autorisation lors de l'ajout d'un collecteur. Confirmez les autorisations de l'utilisateur en suivant les instructions dans le"documentation" .

Août 2025

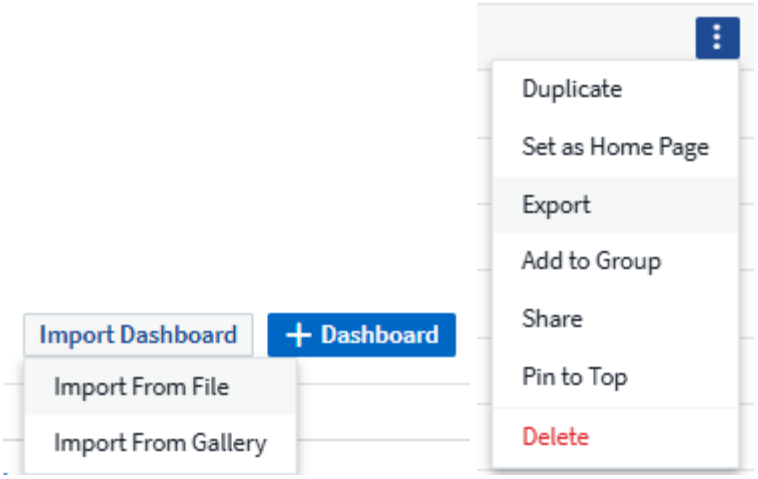
Des données de widgets ciblées à portée de main

La nouvelle fonctionnalité **Analyser** présente dans la plupart des widgets vous permet d'examiner de plus près les données d'un widget à la fois. Cliquez simplement sur le bouton « Analyser » d'un widget pour ouvrir une vue détaillée, dans laquelle vous pouvez explorer de manière interactive les données sous-jacentes et zoomer pour obtenir des informations plus approfondies, sans quitter le contexte de votre tableau de bord.



Exporter et importer des tableaux de bord

Si vous gérez plusieurs locataires et avez développé un tableau de bord utile, vous pouvez exporter le tableau de bord et l'importer vers un autre locataire.



Intégration cloud améliorée : prise en charge de Google Cloud NetApp Volumes (GCNV)

- Google Cloud NetApp Volumes* (GCNV) est désormais entièrement pris en charge en tant que collecteur de données dans DII, complétant ainsi notre écosystème de surveillance du cloud hybride. Bénéficiez d'une visibilité sur les objets de stockage critiques tels que les organisations, les pools et les volumes dans l'ensemble de l'infrastructure. Vous pouvez désormais suivre tous vos environnements de stockage, sur site ou dans le cloud, à partir d'une seule plateforme.

Surveillance améliorée de StorageGRID

La collecte des journaux StorageGRID est désormais activée par défaut, fournissant des données de suivi des événements à DII, et nous avons étendu la surveillance StorageGrid avec plus de 50 alertes par défaut, un suivi des événements en temps réel et de nouveaux tableaux de bord pour simplifier les opérations complexes de la grille de stockage. Gardez une longueur d'avance sur les problèmes grâce à des informations plus approfondies sur les politiques de circulation et les performances des compartiments.

Prise en charge du système d'exploitation

Les systèmes d'exploitation suivants sont désormais pris en charge avec les unités d'acquisition Data Infrastructure Insights , en plus de ceux"déjà pris en charge" :

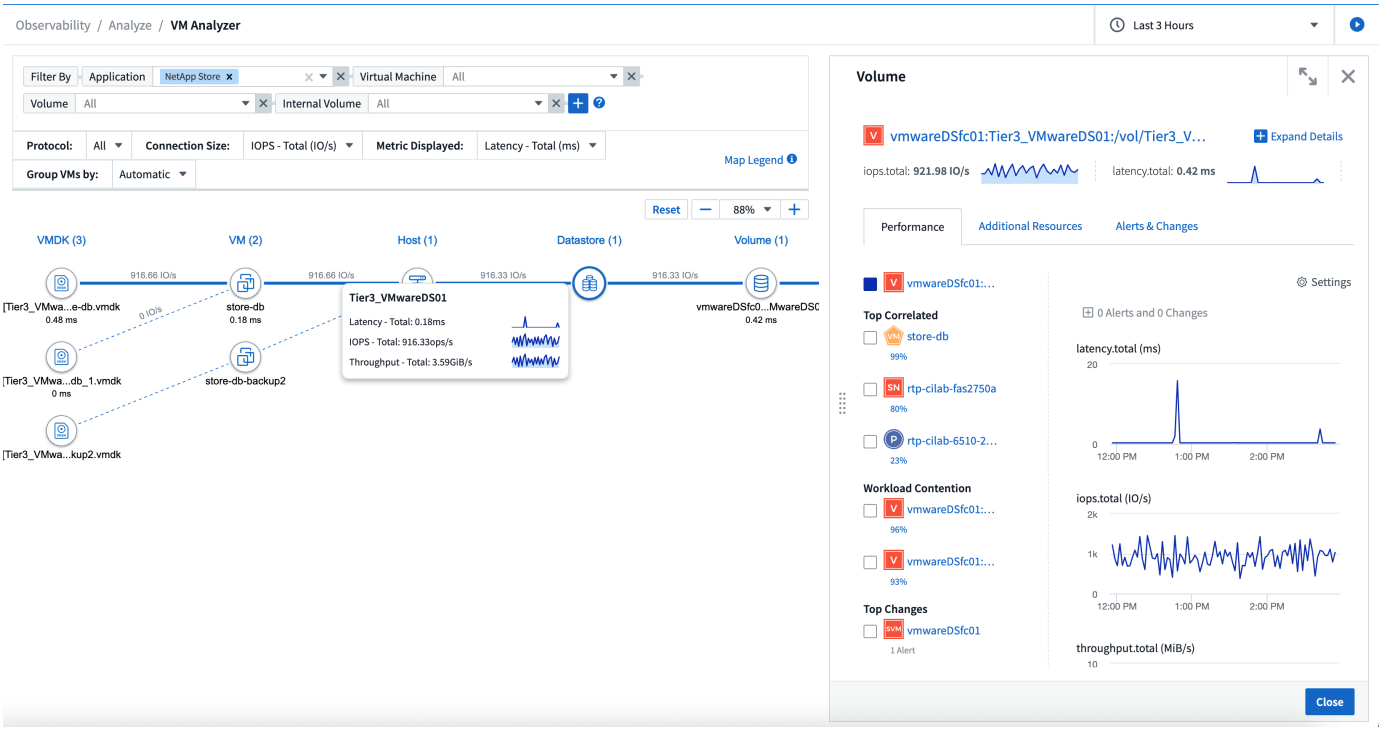
- AlmaLinux (64 bits) 10
- Red Hat (64 bits) 10
- Rocky (64 bits) 9.6

Juin 2025

VM Analyzer : visibilité et dépannage holistiques des machines virtuelles vers le stockage

La fonctionnalité **VM Analyzer** de DII fournit une vue complète de bout en bout de vos environnements virtualisés. VM Analyzer simplifie le dépannage en cartographiant l'intégralité du chemin depuis les machines virtuelles vers le stockage, permettant aux utilisateurs d'identifier rapidement les problèmes de performances sur les disques virtuels, les machines virtuelles, les hôtes, les banques de données, les volumes et le stockage. Grâce à une vue topologique intuitive, un filtrage et des mesures de performances détaillées, les administrateurs peuvent facilement identifier les goulots d'étranglement, analyser les déséquilibres de trafic et

optimiser les performances globales de stockage.



Prise en charge du système d’exploitation

Les systèmes d’exploitation suivants sont désormais pris en charge avec les unités d’acquisition Data Infrastructure Insights , en plus de ceux"déjà pris en charge" :

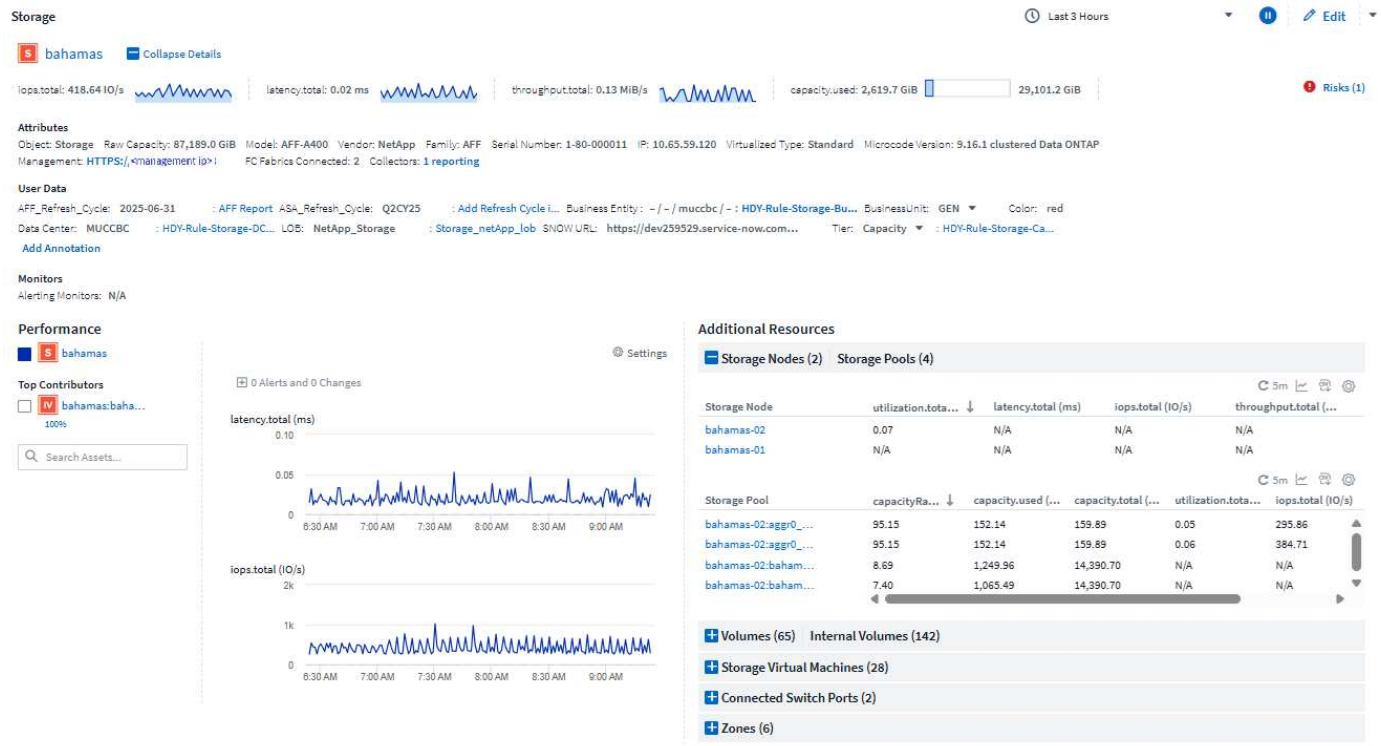
- Debian (64 bits) 12
- Oracle Enterprise Linux (64 bits) 9.6
- Red Hat (64 bits) 9,6

Mai 2025

Les nouvelles pages de destination vous permettent de rester dans le flux

Les pages de destination repensées présentent tout ce dont vous avez besoin : données récapitulatives, graphiques de performances, corrélations, alertes et modifications, ainsi que ressources clés, dans une seule vue.

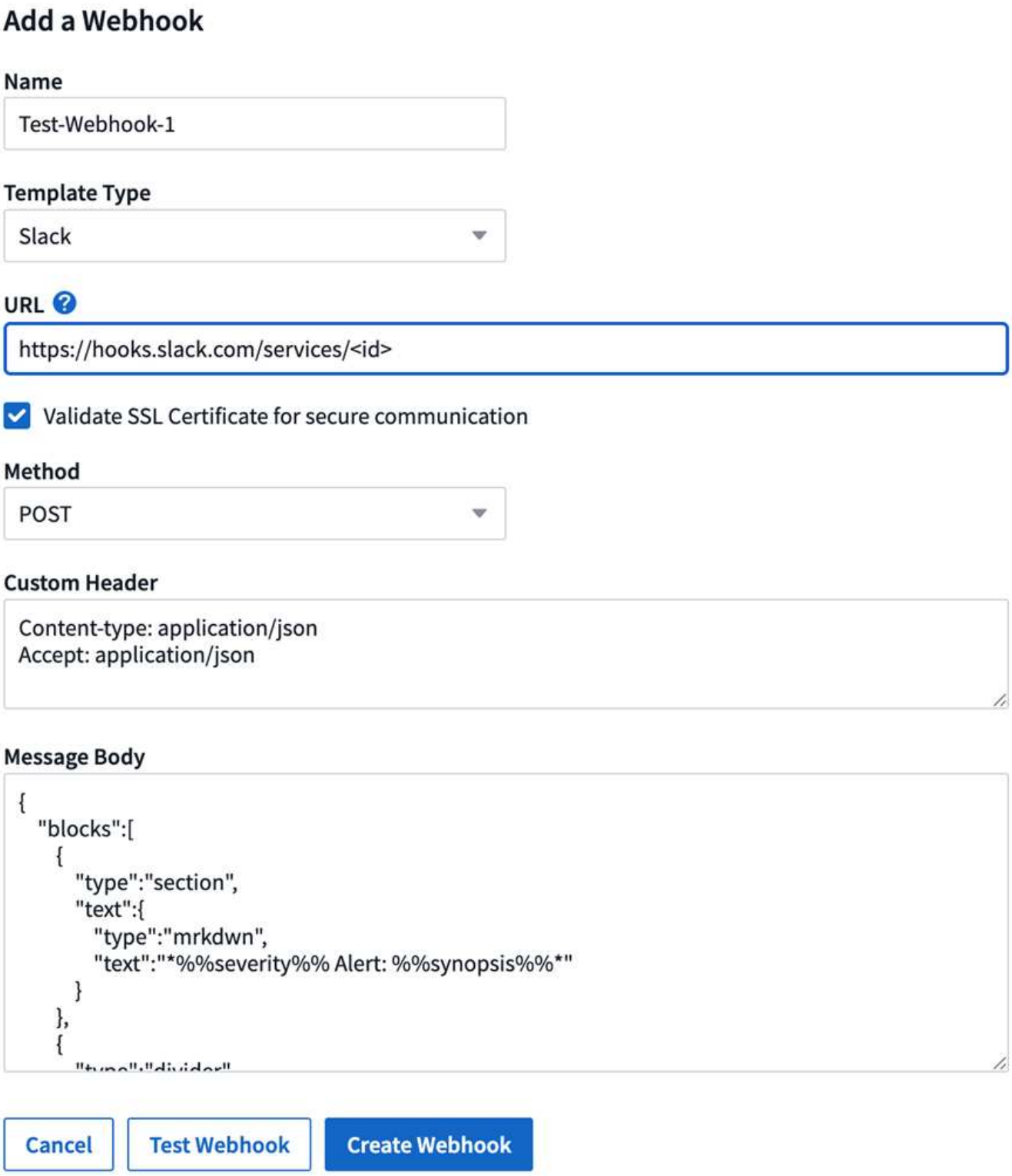
Vous pouvez désormais résoudre les problèmes plus rapidement et rester concentré, sans passer d’un onglet à l’autre ni perdre le contexte.



Améliorations de la sécurité de la charge de travail

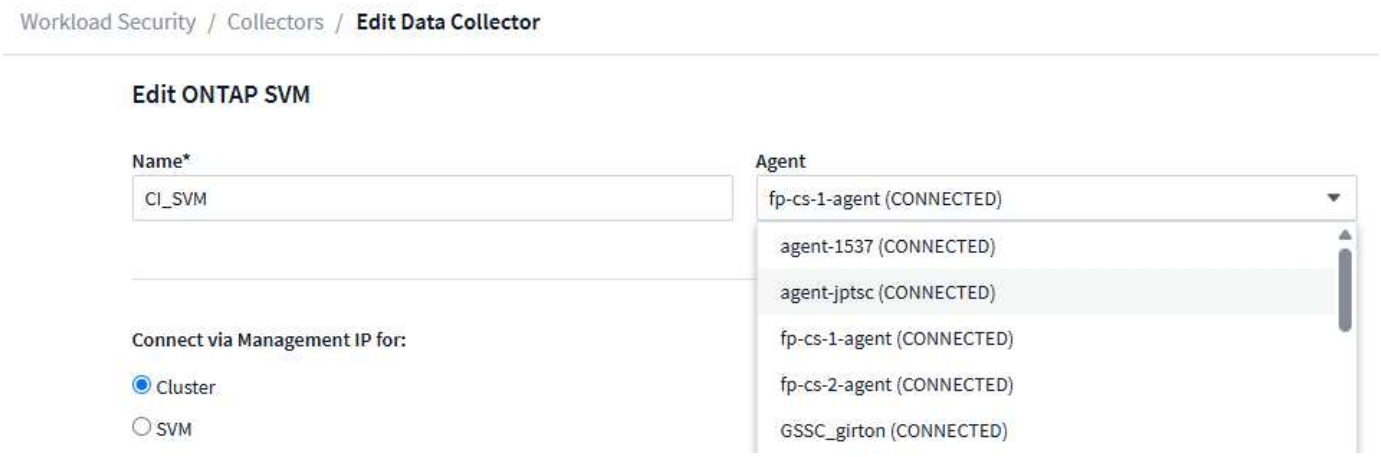
Webhooks désormais disponibles pour les alertes de sécurité des charges de travail

Workload Security prend désormais en charge les notifications webhook prêtes à l'emploi vers des outils tels que Slack, PagerDuty, Teams, etc. De plus, nous proposons des modèles personnalisables qui vous permettent de personnaliser le message ou de l'intégrer à tout autre SIEM ou application tierce. Acheminez les alertes critiques directement vers vos flux de travail de sécurité existants, afin que votre équipe puisse enquêter et réagir plus rapidement.



Migrer les collecteurs de sécurité de la charge de travail entre les agents

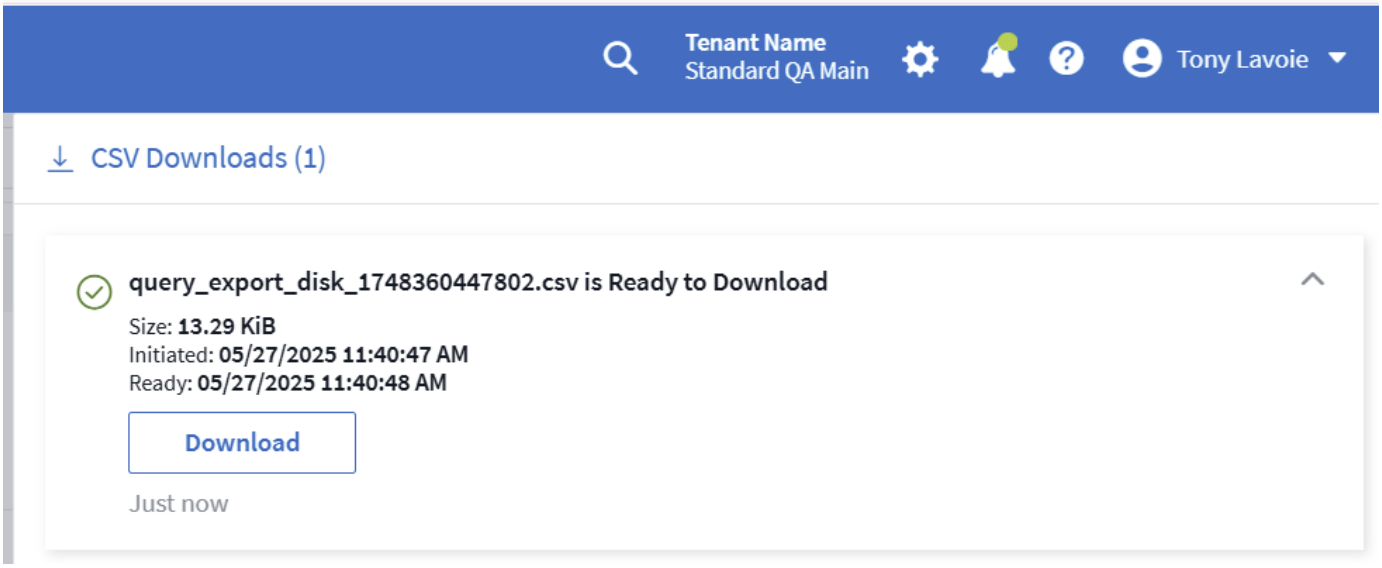
Vous pouvez facilement migrer un collecteur Workload Security d'un agent à un autre, permettant ainsi un équilibrage efficace de la charge des collecteurs entre les agents. La migration est aussi simple que de modifier le collecteur et de sélectionner l'agent de destination dans la liste.



Exportation asynchrone .CSV

L'exportation de données au format .CSV peut prendre de quelques secondes à plusieurs heures, selon la quantité de données à exporter. Data Infrastructure Insights exporte désormais ces données de manière asynchrone, ce qui vous permet de continuer à travailler pendant la compilation du fichier .CSV.

Affichez vos exportations .CSV en sélectionnant l'icône « Cloche » dans la barre d'outils en haut à droite.



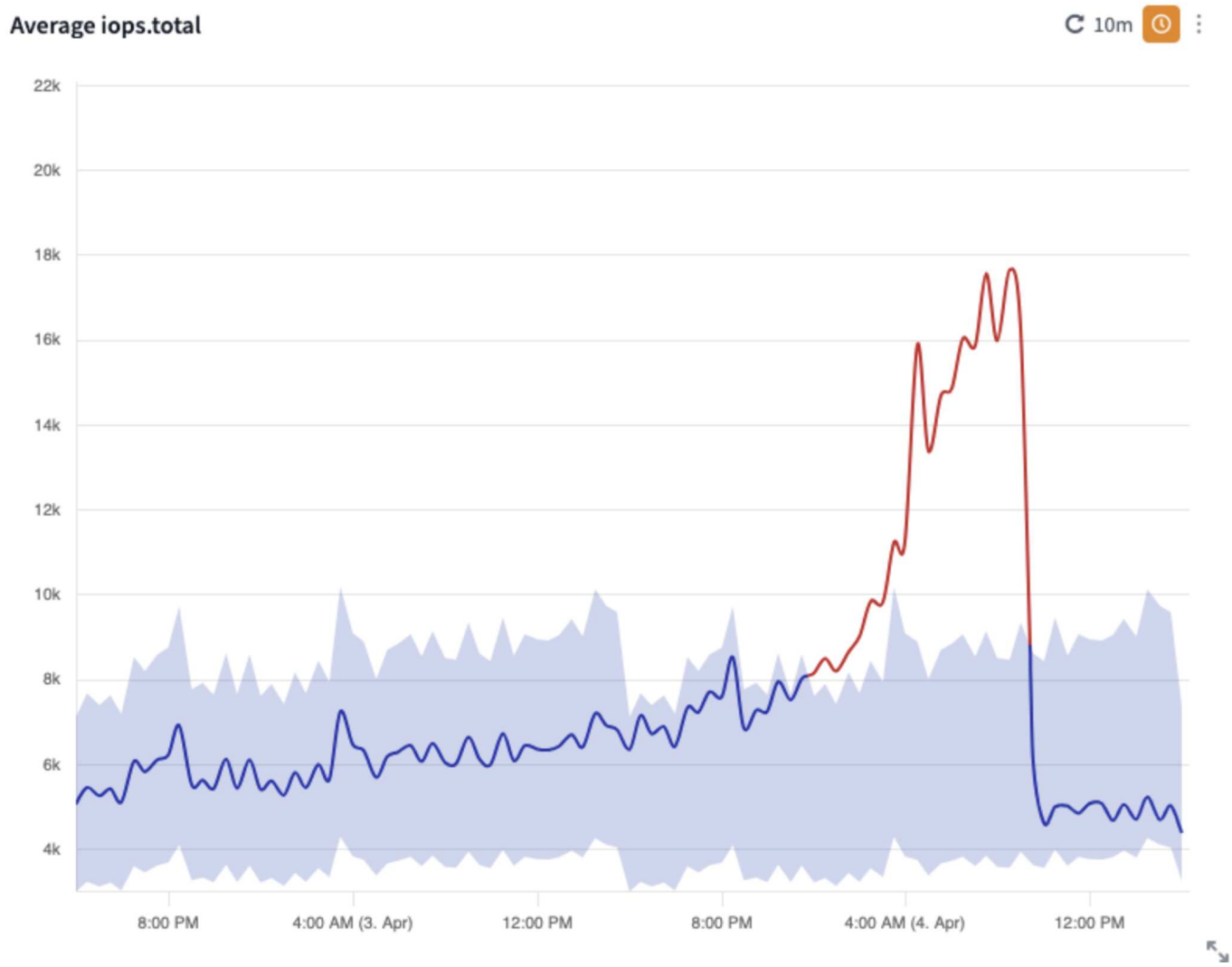
Avril 2025

Widgets de limites d'anomalies optimisés par ML pour une résolution proactive des problèmes

Pour résoudre les problèmes de performances avec les widgets de graphique linéaire ou spline, vous pouvez désormais afficher les limites de comportement attendues à côté des mesures réelles, ce qui vous permet de faire la distinction entre les tendances de mesures normales et anormales.

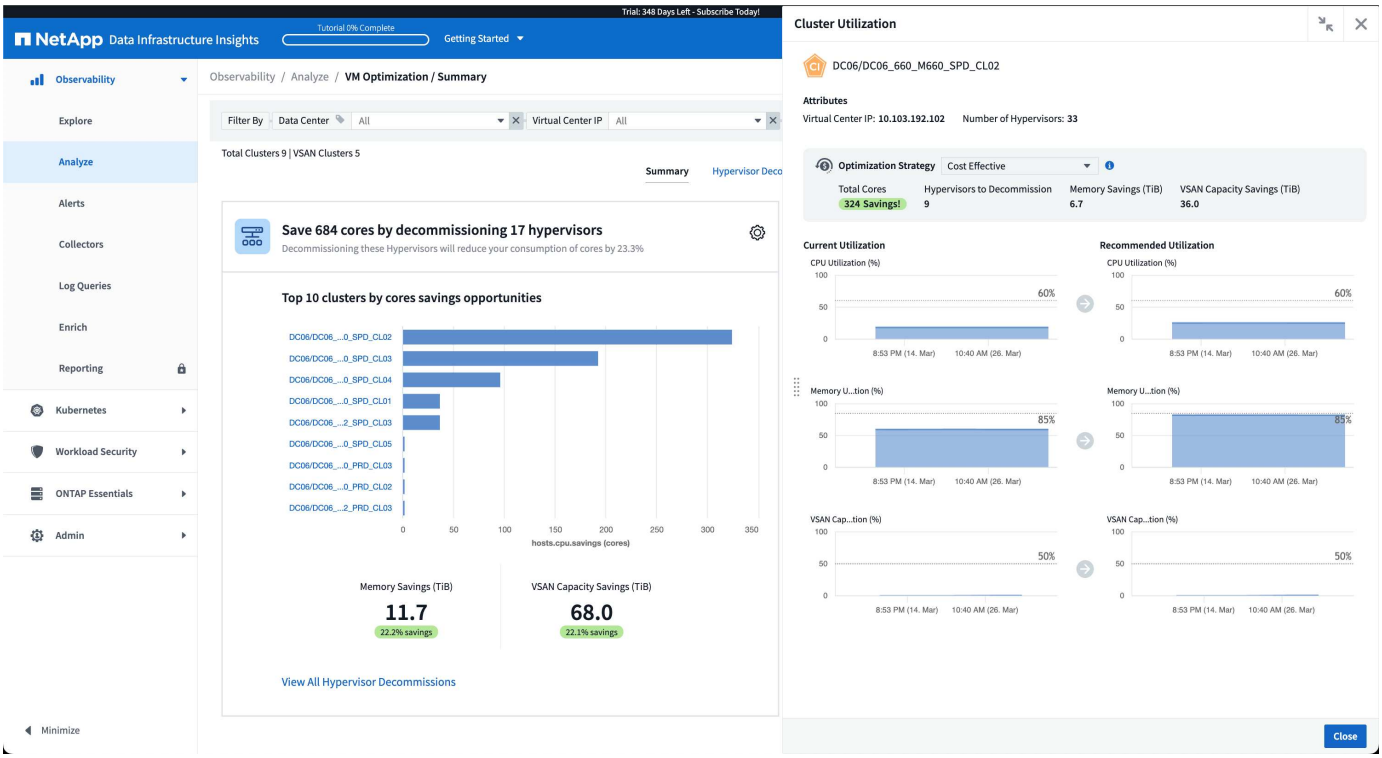
L'apprentissage automatique DII avec analyse des données saisonnières établit des seuils intelligents basés sur des modèles historiques. Lorsque les mesures s'écartent des plages attendues, le système les met en

évidence comme des anomalies, ce qui permet une identification rapide des problèmes, réduit le temps moyen de résolution et résout les problèmes avant qu'ils n'affectent les opérations.



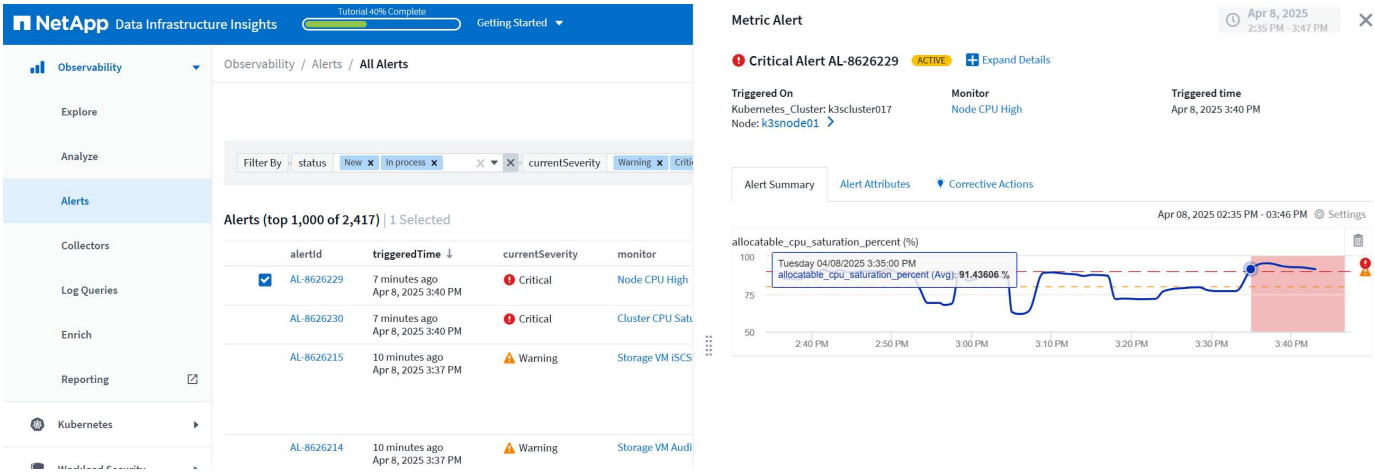
Optimisez les coûts VMware grâce à la prise en charge du stockage VSAN

Notre fonctionnalité d'optimisation de machine virtuelle inclut désormais la prise en charge des environnements VMWare avec stockage VSAN. Outre l'utilisation du processeur et de la mémoire, l'analyse prend désormais en compte le stockage VSAN local pour les recommandations de récupération, vous aidant ainsi à réduire davantage les coûts de licence.



Les détails des alertes à portée de main

Enquêter sur les alertes est plus facile que jamais grâce au nouveau panneau coulissant. Sélectionnez une alerte pour afficher les détails de cette alerte et basculez facilement entre les alertes sans perdre votre place lors de l'examen des problèmes.



Exportation asynchrone de l'analyse forensique de la sécurité de la charge de travail

L'exportation de données médico-légales peut prendre de quelques secondes à plusieurs heures, selon la quantité de données à exporter. Workload Security exporte ces données de manière asynchrone, ce qui vous permet de continuer à travailler pendant la compilation du fichier .CSV.

Notifications du collecteur de données regroupées en règles

Si vous avez configuré des notifications sur les collecteurs de données, à partir du 15 avril, ces notifications

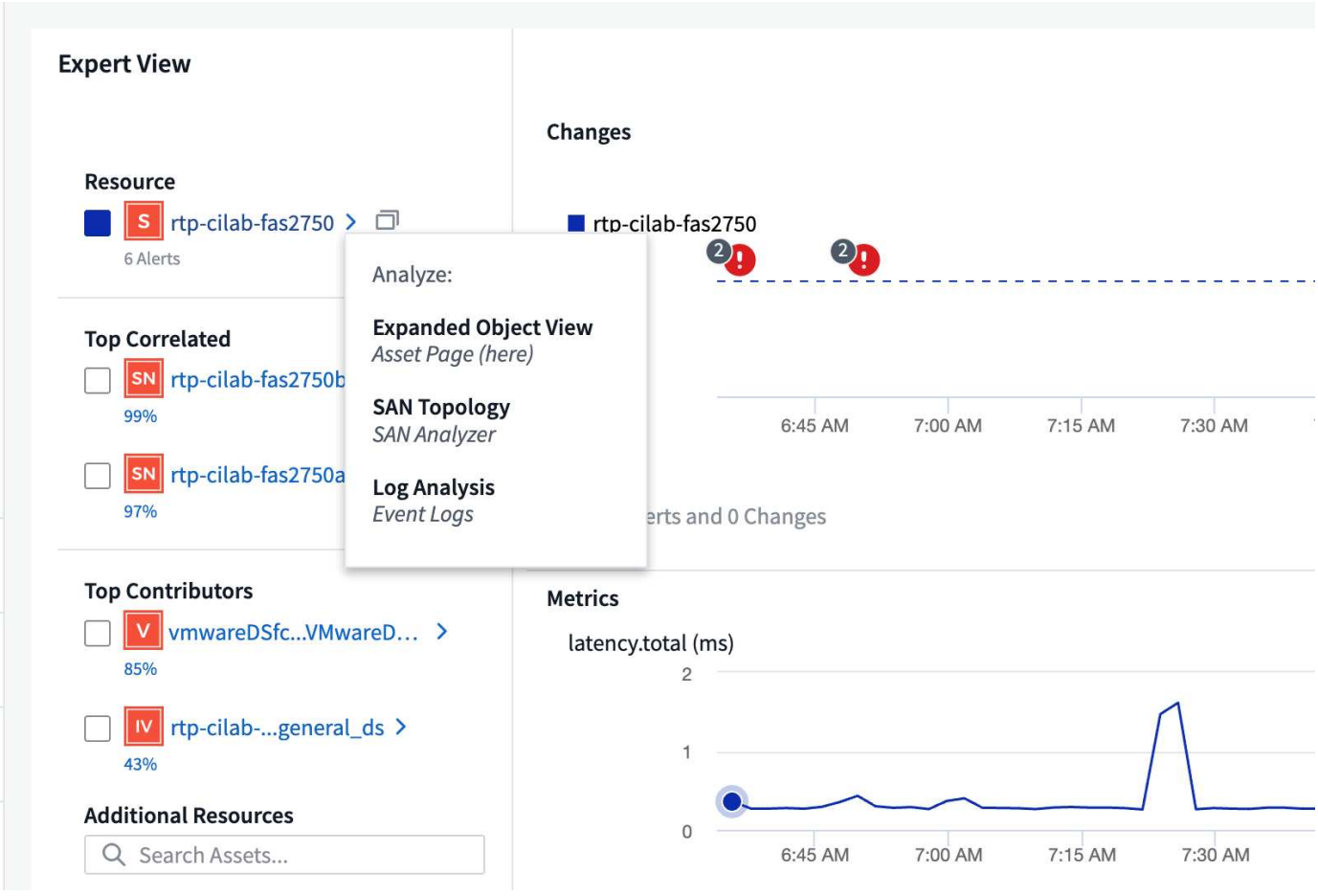
seront gérées dans les règles de notification, avec une règle unique pour les collecteurs ayant des destinataires identiques. Les collectionneurs ayant des destinataires différents auront des règles distinctes. Les notifications de collecteur existantes sont migrées vers les règles de notification.

Mars 2025

Navigation contextuelle améliorée pour une gestion efficace des infrastructures

Gagnez du temps en exploitant Data Infrastructure Insights pour l'excellence opérationnelle. Nous ajoutons désormais des liens de menu contextuel qui vous permettent de passer directement de n'importe quel objet à la page de destination des ressources pour obtenir des informations sur les performances des appareils, à SAN Analyzer pour la visualisation de la topologie du réseau, aux journaux pour la connaissance opérationnelle ou à Change Analyzer pour la gestion de la configuration.

Grâce à un accès instantané aux données clés sur plusieurs vues, vous obtenez une compréhension plus claire des relations entre les objets plus rapidement. Ce flux de travail rationalisé accélère la prise de décision et la résolution des problèmes, vous permettant ainsi de gagner du temps et d'améliorer vos capacités d'analyse globales.

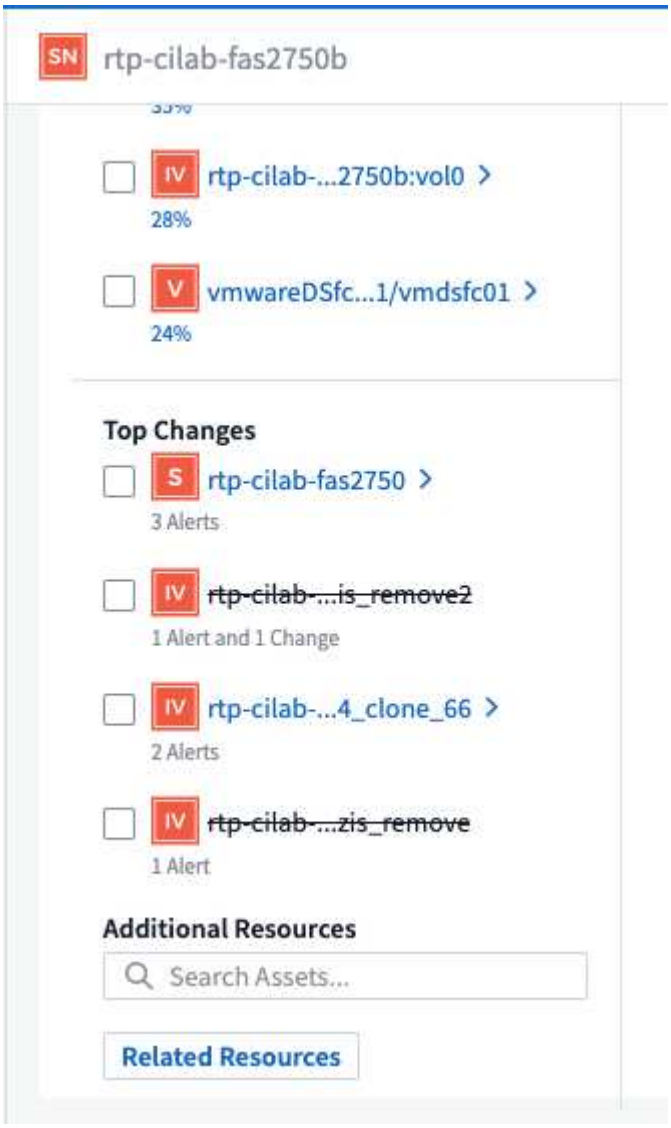


Préserver l'historique des ressources supprimées

Notre fonctionnalité améliorée de modification d'infrastructure préserve désormais l'historique des actifs supprimés tels que les qtrees et les volumes qui ont été déplacés et ne sont plus disponibles.

Il vous manque quelque chose dans votre puzzle de dépannage ? Pas plus! Vous verrez tout, y compris les objets supprimés marqués d'un barré, ce qui vous donne un contexte complet même après la suppression des ressources, vous assurant de ne jamais manquer d'éléments critiques des modifications passées ou des alertes sur l'ensemble du chemin.

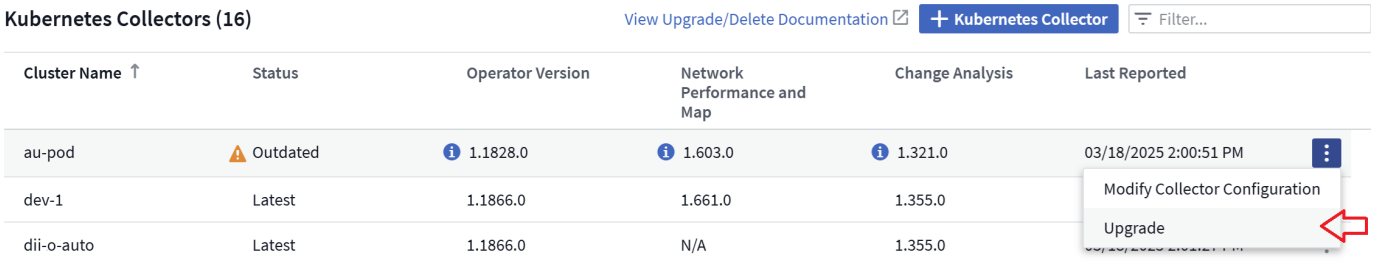
Le résultat ? Des délais de résolution plus rapides et des décisions d'infrastructure plus sûres, même lorsque les actifs en question n'existent plus.



Mise à niveau par simple pression sur un bouton de l'opérateur Kubernetes

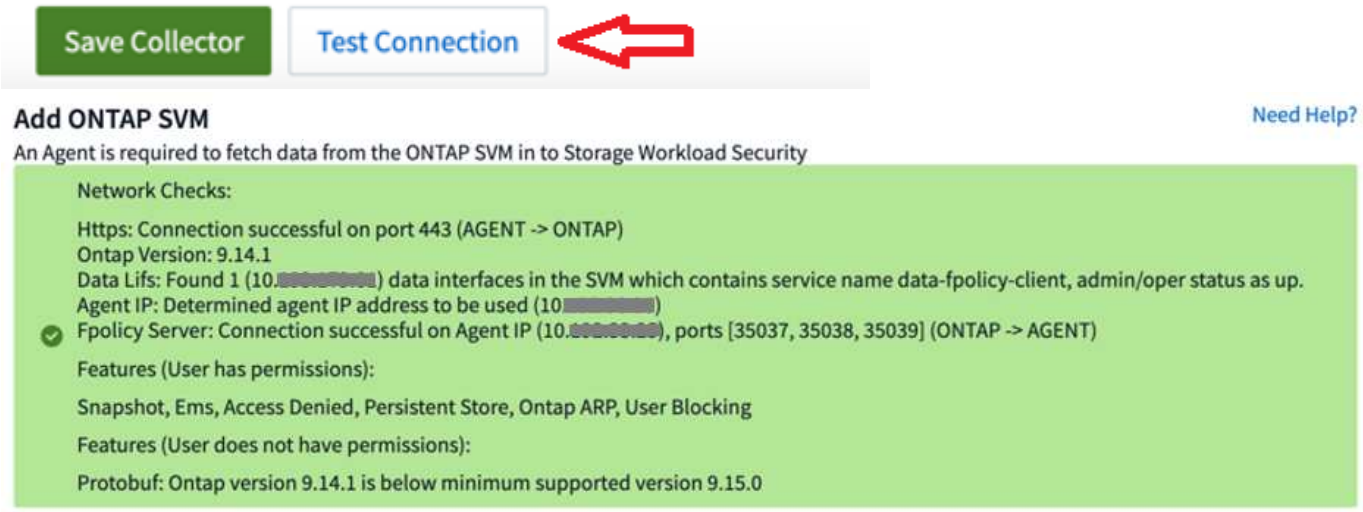
Vous voulez être sûr de disposer de la dernière version de Kubernetes Operator ? Mettez à niveau l'opérateur à la demande à partir du menu du cluster DII Kubernetes Collectors. Sélectionnez simplement Mettre à niveau dans le menu et l'opérateur vérifiera les signatures d'image, capturera un instantané de votre installation actuelle et effectuera la mise à niveau.

La mise à niveau par bouton-poussoir est une fonctionnalité facultative et son activation peut être gérée par cluster.



Tester la connectivité pour les collecteurs de données de sécurité des charges de travail de stockage

La fonctionnalité de connectivité de test vise à aider les utilisateurs finaux à identifier les causes spécifiques des échecs lors de la configuration des collecteurs de données dans Data Infrastructure Insights (DII) Workload Security. Cela permet aux utilisateurs de corriger eux-mêmes les problèmes liés à la communication réseau ou aux rôles manquants.



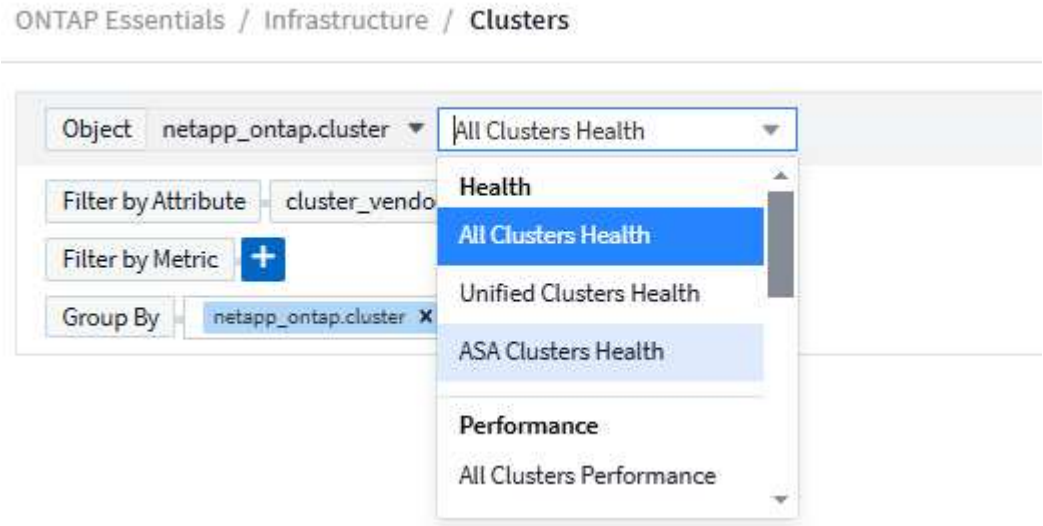
Prise en charge du système d'exploitation

Les systèmes d'exploitation suivants sont désormais pris en charge par les unités d'acquisition Data Infrastructure Insights , en plus de ceux"déjà pris en charge" :

- AlmaLinux 9.5
- Debian (64 bits) 11
- OpenSUSE Leap 15.6
- Oracle Enterprise Linux (64 bits) 8.9, 8.10, 9.5
- Red Hat (64 bits) 8.9, 8.10, 9.5
- Rocheux 9.5
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Server 24.04 LTS

Février 2025

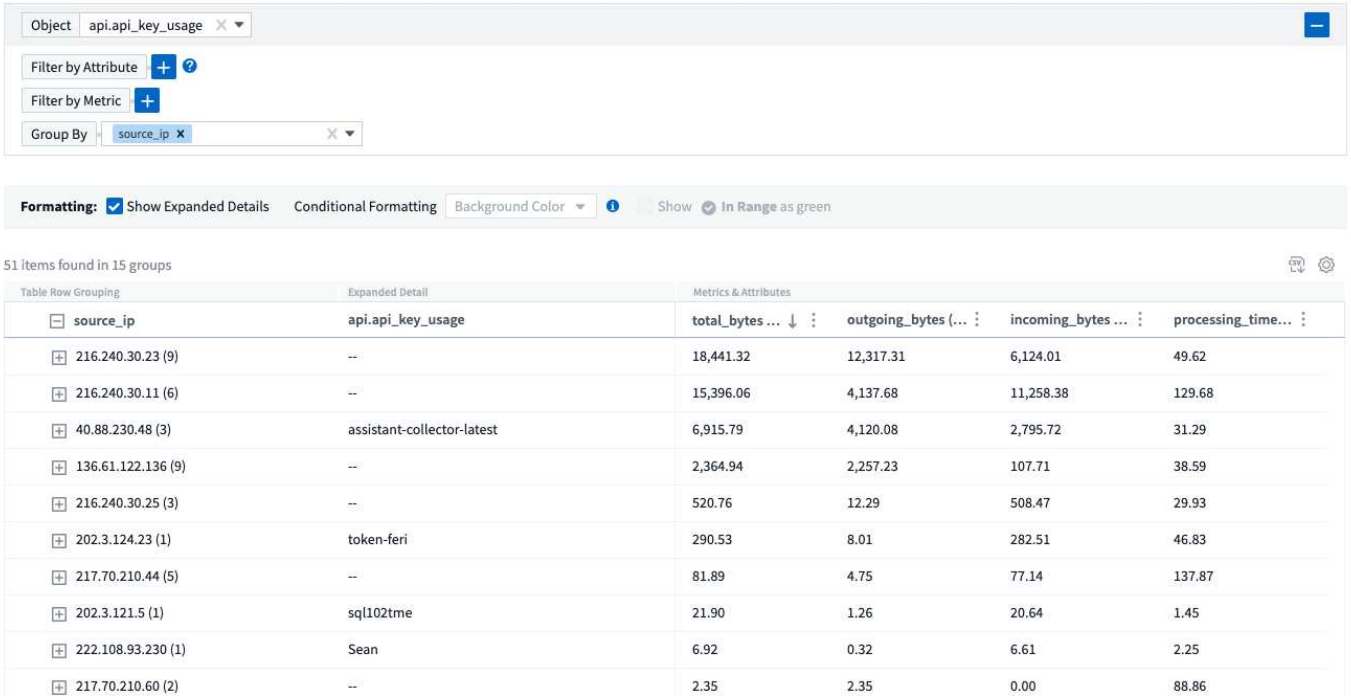
ONTAP Essentials inclut désormais une gestion prête à l'emploi pour la dernière génération de"ASA" appareils. Cela inclut SAN Analyzer pour les topologies VM vers LUN des charges de travail exécutées sur ONTAP, désormais également disponible avec la prise en charge NetApp dans le cadre de Data Infrastructure Insights Basic Edition.



Suivi de l'utilisation de l'API DII : améliorer la sécurité et l'efficacité

Renforcez votre posture de sécurité et rationalisez la gestion des ressources grâce au suivi amélioré de l'utilisation de l'API REST, disponible pour les utilisateurs administrateurs. Grâce au suivi de l'utilisation des API, vous pouvez voir quels jetons API sont utilisés, à partir de quelles adresses IP et le volume de trafic qu'ils génèrent. En associant des jetons à des adresses IP et des niveaux d'utilisation spécifiques, vous obtiendrez des informations précieuses sur les tendances d'accès et d'utilisation du système, vous donnant le contrôle dont vous avez besoin pour maintenir un environnement sûr et efficace et assurer le bon déroulement des opérations.

Pour afficher l'utilisation de l'API, accédez à **Observabilité > Admin > Accès API** et sélectionnez *Afficher l'utilisation de l'API*. Notez que cette API est disponible uniquement pour les API d'observabilité DII ; elle ne s'applique pas à la sécurité de la charge de travail.



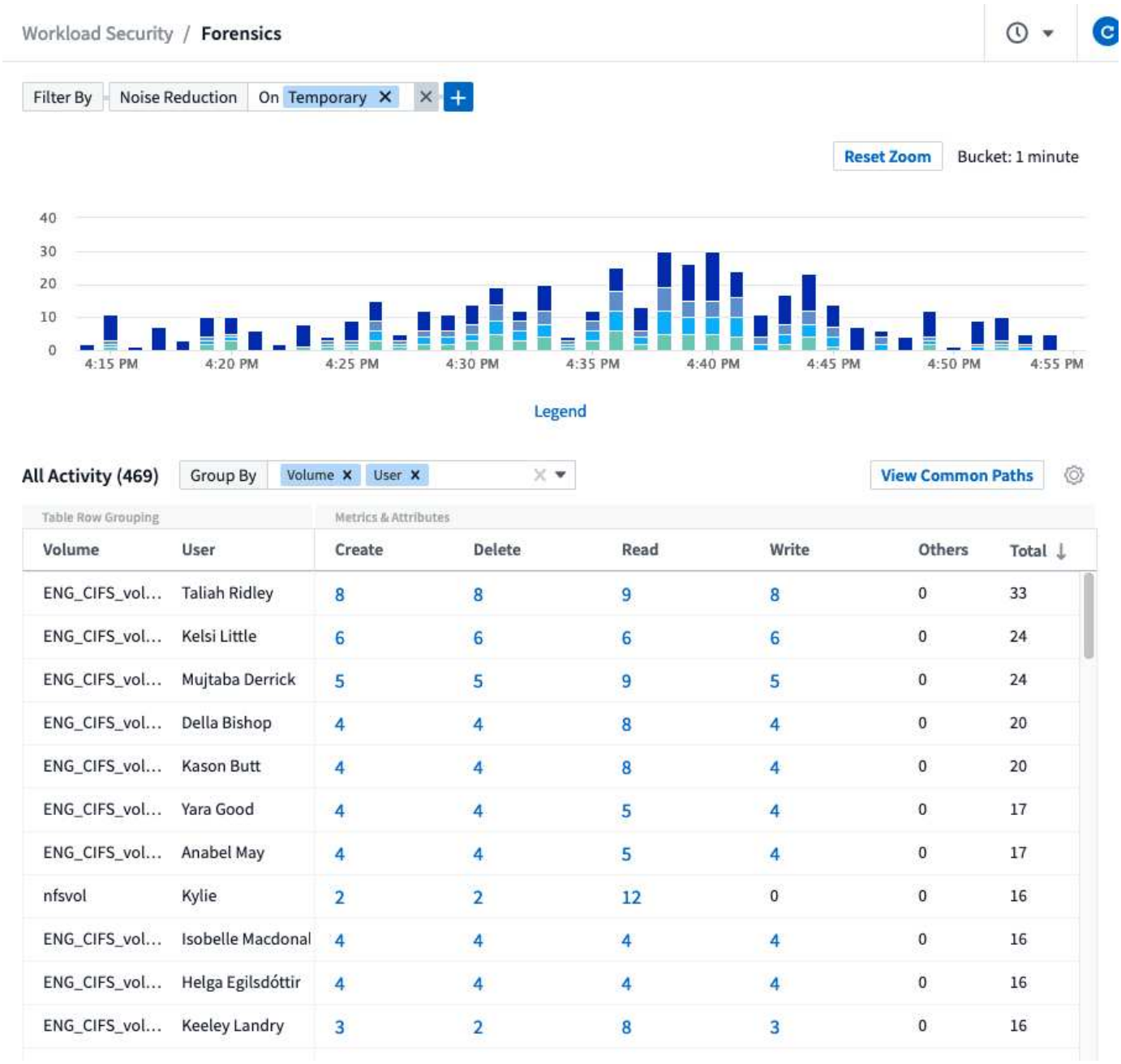
API de sécurité de la charge de travail pour restreindre les utilisateurs

Une nouvelle API a été ajoutée pour gérer les restrictions utilisateur dans Workload Security. Avec l'API, vous pouvez bloquer ou débloquer un utilisateur, ou modifier la durée de son accès restreint. Consultez la page Admin > Accès API > Documentation API pour l'API *cloudsecure_actions.block*.

Janvier 2025

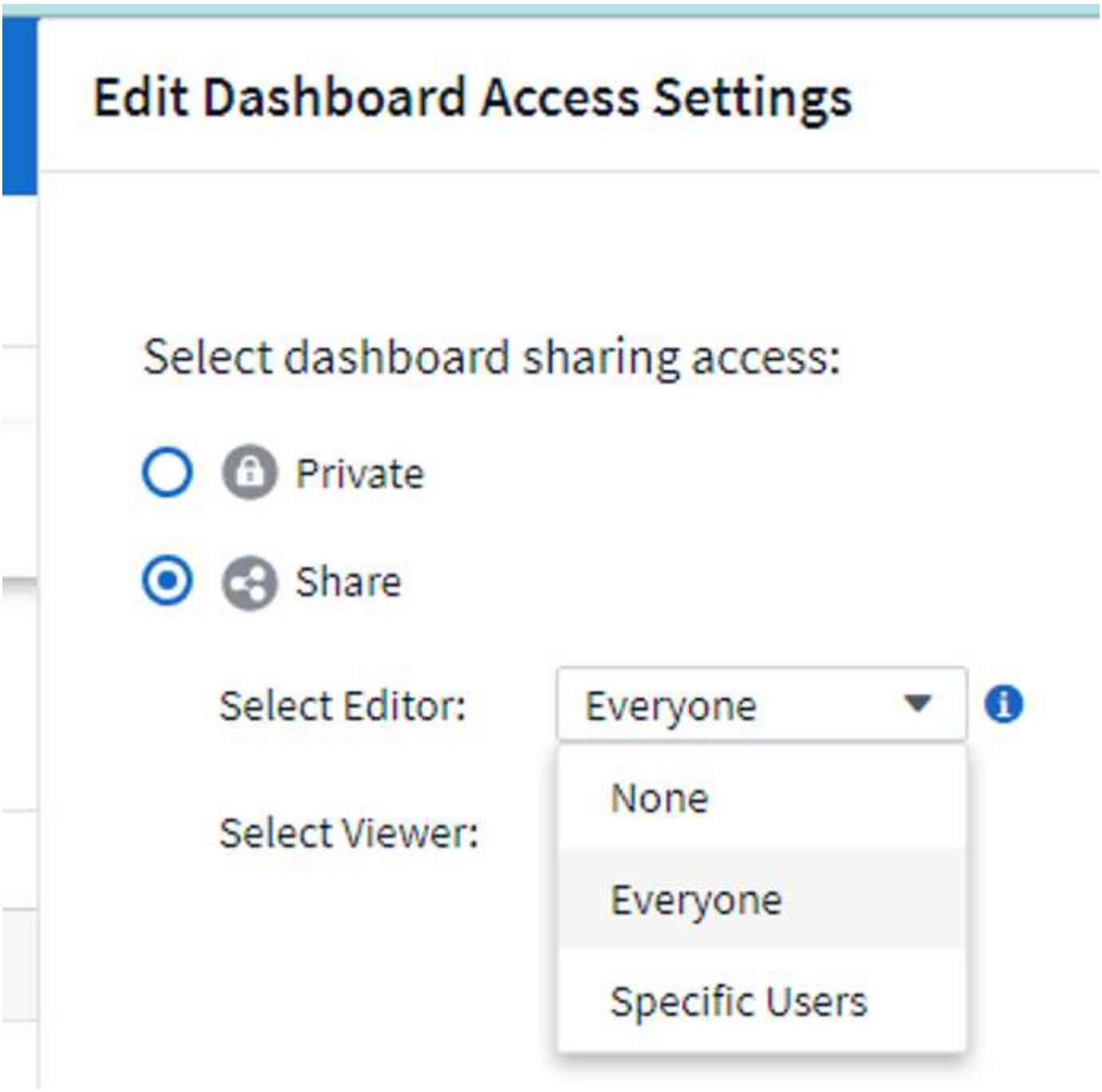
Gérez les risques de manière proactive avec Forensics Grouping

Présentation de notre dernière fonctionnalité conçue pour améliorer vos capacités de sécurité et de gestion des ressources ! Grâce à la fonctionnalité avancée de regroupement et à la prise en charge hiérarchique de plusieurs regroupements, vous pouvez désormais facilement identifier les utilisateurs qui ont accédé à des dossiers spécifiques, déterminer les utilisateurs et les partages les plus actifs et gérer de manière proactive les risques en suivant les adresses IP des clients actifs. Optimisez votre utilisation du stockage et de la bande passante en identifiant les fichiers et dossiers les plus consultés et obtenez un contrôle accru sur l'accès au système en identifiant les utilisateurs.



Contrôle d’accès au tableau de bord

Data Infrastructure Insights vous offre désormais un meilleur contrôle sur l’accès aux tableaux de bord que vous créez. Vous choisissez qui peut modifier vos graphiques. Vous contrôlez l’exposition aux informations potentiellement sensibles. Vous travaillez toujours sur un tableau de bord qui n’est pas prêt pour une visibilité générale ? Vous pouvez le garder privé jusqu’à ce que vous soyez prêt à le partager.

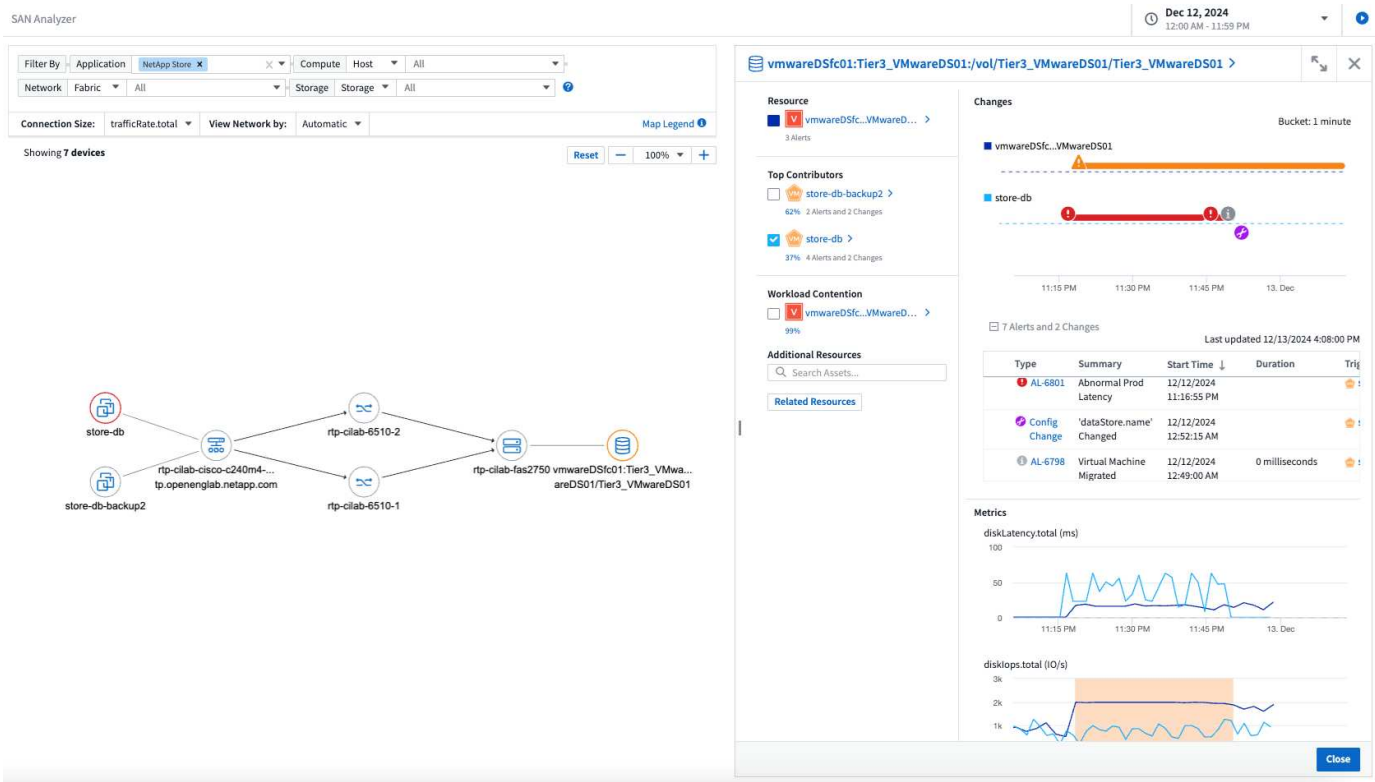


Décembre 2024

Présentation de SAN Analyzer : visibilité améliorée pour les charges de travail en mode bloc

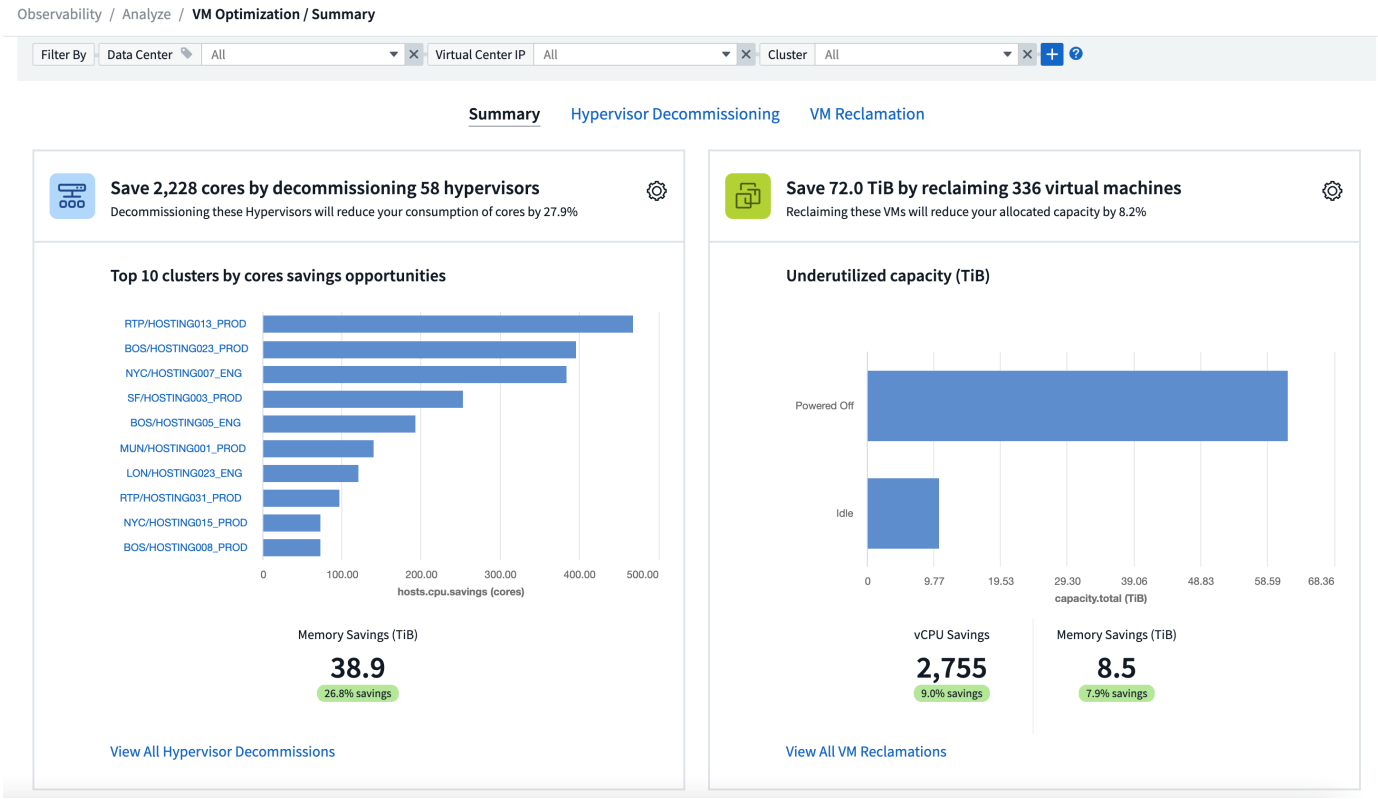
Le SAN joue un rôle crucial dans la gestion des charges de travail vitales, mais sa complexité peut entraîner des pannes importantes et des perturbations pour les clients. Avec **SAN Analyzer** de DII, la gestion du SAN devient plus simple et plus efficace. Cet outil puissant offre une visibilité de bout en bout, mappant les dépendances de la VM/hôte au réseau, au LUN et au stockage. En fournissant une carte topologique interactive, SAN Analyzer vous permet d'identifier les problèmes, de comprendre les changements et d'améliorer la compréhension du flux de données. Optimisez la gestion SAN dans les environnements

informatiques complexes avec SAN Analyzer et augmentez votre visibilité sur les charges de travail en bloc.



Optimisez les coûts des machines virtuelles grâce au déclassement intelligent des hôtes et à la récupération des machines virtuelles

Data Infrastructure Insights vous aide à gérer les coûts d'infrastructure et de licence en analysant le comportement historique de l'environnement et en établissant des prévisions à court et à long terme, en générant des recommandations détaillées pour la mise hors service de l'hôte et la récupération des machines virtuelles hors tension et inactives. Ces recommandations vous aident à garantir la stabilité des performances, à libérer la capacité inutilisée et à réduire l'allocation de mémoire et de processeur.



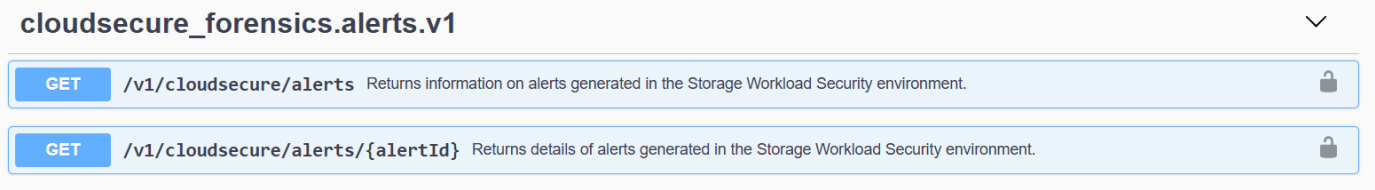
Découvrez les informations sur les journaux grâce aux graphiques temporels et à la prise en charge des widgets de tableau

Vous pouvez désormais exploiter des graphiques temporels (à barres, à lignes, à zones) pour identifier les tendances et les modèles dans les données de journal, tels que les erreurs récurrentes ou les pics d'activité, fournissant ainsi des informations précieuses sur le comportement du système au fil du temps. De plus, grâce aux tableaux, vous pouvez désormais inclure des messages de journal directement dans le tableau de bord, permettant une vue plus complète des détails du journal.

Novembre 2024

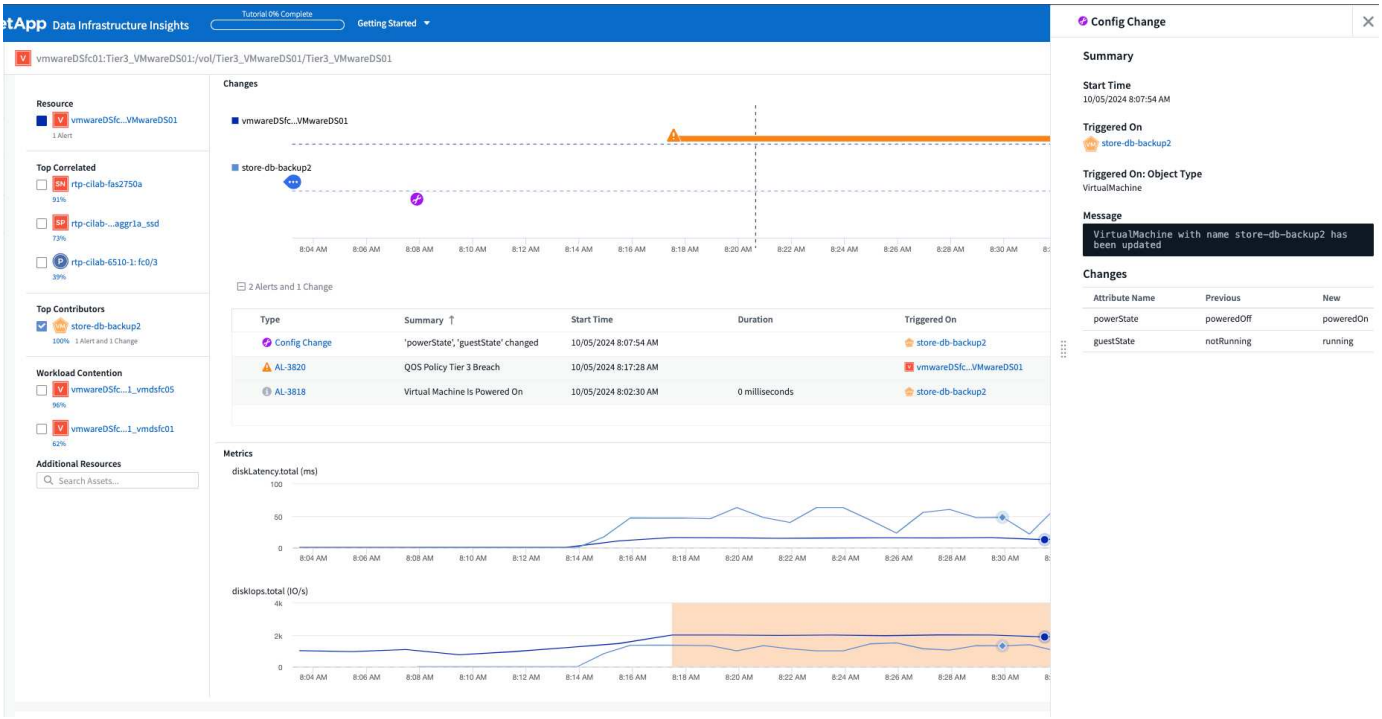
Nouvelle API d'alertes de sécurité de charge de travail

Récupérez les détails des alertes médico-légales avec la nouvelle sécurité de la charge de travail"API cloudsecure_forensics.alerts" .



Analyser les changements de configuration dans votre environnement

Les changements de configuration sont l'une des causes les plus courantes de problèmes dans l'informatique moderne. Les nouvelles informations de Data Infrastructure Insights(DII)"analyse des changements" Cette capacité vous permet de comprendre clairement les changements qui causent des problèmes dans votre environnement. Accélérez le temps de dépannage en affichant tous les changements dans les appareils et les composants d'infrastructure associés qui peuvent avoir conduit à un problème. De plus, lorsque vous ou votre équipe effectuez des modifications planifiées, vous pouvez valider ces modifications rapidement et garantir qu'il n'y a pas d'effets inattendus avant que les niveaux de service ne soient affectés.



Prise en charge de KubeVirt : surveiller les charges de travail des machines virtuelles exécutées dans votre cluster Kubernetes

DII prend désormais entièrement en charge KubeVirt, la solution de virtualisation native Kubernetes utilisée par des plateformes telles qu'OpenShift Virtualization et Harvester. Bénéficiez d'une visibilité complète sur les métriques, les événements, les modifications de configuration et le trafic réseau des machines virtuelles et des charges de travail des conteneurs au sein de vos clusters Kubernetes.

Octobre 2024

Débloquez de nouvelles perspectives grâce aux expressions personnalisées dans les moniteurs

Les expressions vous permettent d'effectuer des opérations arithmétiques dans les moniteurs de détection de métriques et d'anomalies. Voici quelques exemples :

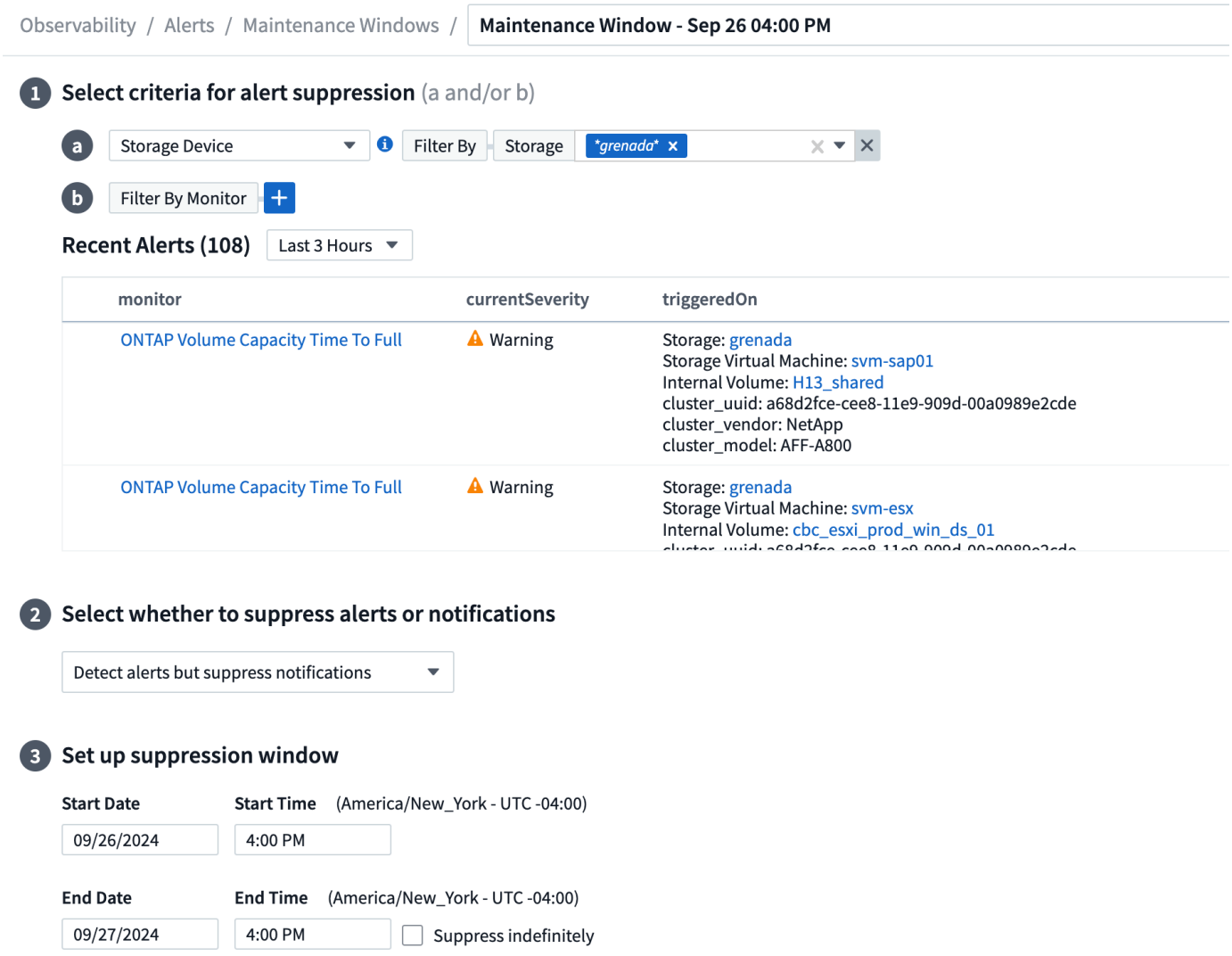
- Ratio : IOPS/To pour détecter où les limites de niveau de service sont atteintes sur les fournisseurs de stockage cloud.
- Pourcentage : utilisé/disponible pour calculer l'utilisation
- Agrégation : combinez plusieurs types d'erreurs de port physique dans un seul moniteur
- Comparaison : comparez l'utilisation actuelle de la marge de manœuvre des ressources avec le point de marge optimal pour identifier les ressources qui ne fonctionnent pas à pleine capacité.

Minimiser les interruptions d'alerte pendant la période de maintenance

Les fenêtres de maintenance vous permettent de supprimer les notifications d'alerte pendant les périodes de maintenance planifiées, vous aidant ainsi à éviter les interruptions inutiles.

Avec les fenêtres de maintenance, vous pouvez planifier des périodes de maintenance spécifiques pendant lesquelles les notifications d'alerte sont supprimées, pour les objets et les mesures que vous choisissez. Par exemple, vous pouvez supprimer les notifications d'alerte déclenchées par des systèmes de stockage spécifiques, lorsque ces systèmes de stockage sont dans une période de mise à niveau planifiée.

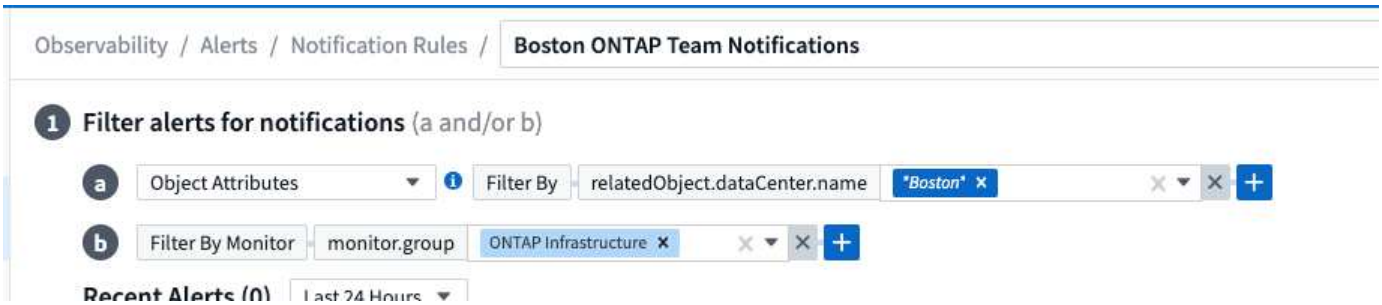
Notez que seules les notifications d'alerte sont supprimées (e-mail, webhook) ; les alertes elles-mêmes sont toujours affichées sur la page Observabilité > Alertes > Toutes les alertes.



Optimisez la gestion des alertes grâce à de nouvelles règles de notification d'alerte

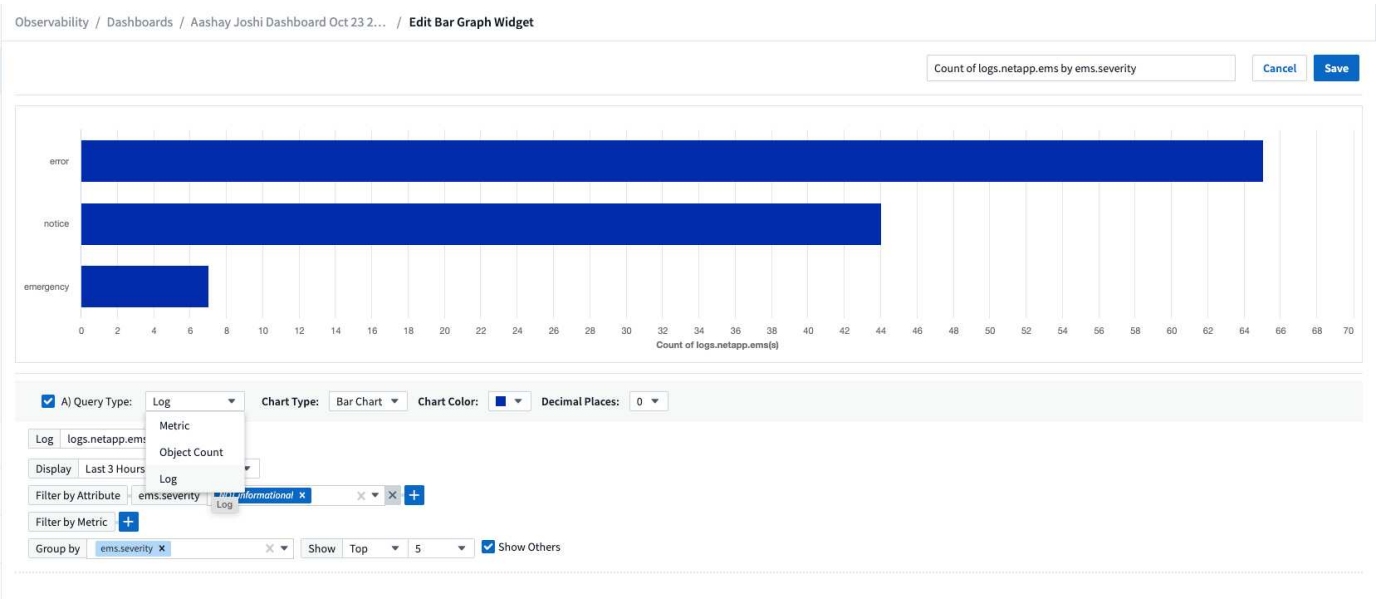
Les règles de notification d'alerte simplifient la gestion des notifications entre les moniteurs et les équipes.

Contrôlez la diffusion des alertes sur les canaux de votre organisation, en vous assurant que les bonnes informations parviennent à la bonne équipe. Pas besoin de gérer des moniteurs distincts pour différentes équipes ; acheminez les alertes en fonction des attributs d'objet associés (nom de stockage, centre de données, nom d'application) ou des attributs de surveillance (groupe, gravité).



Analyse des journaux dans les tableaux de bord

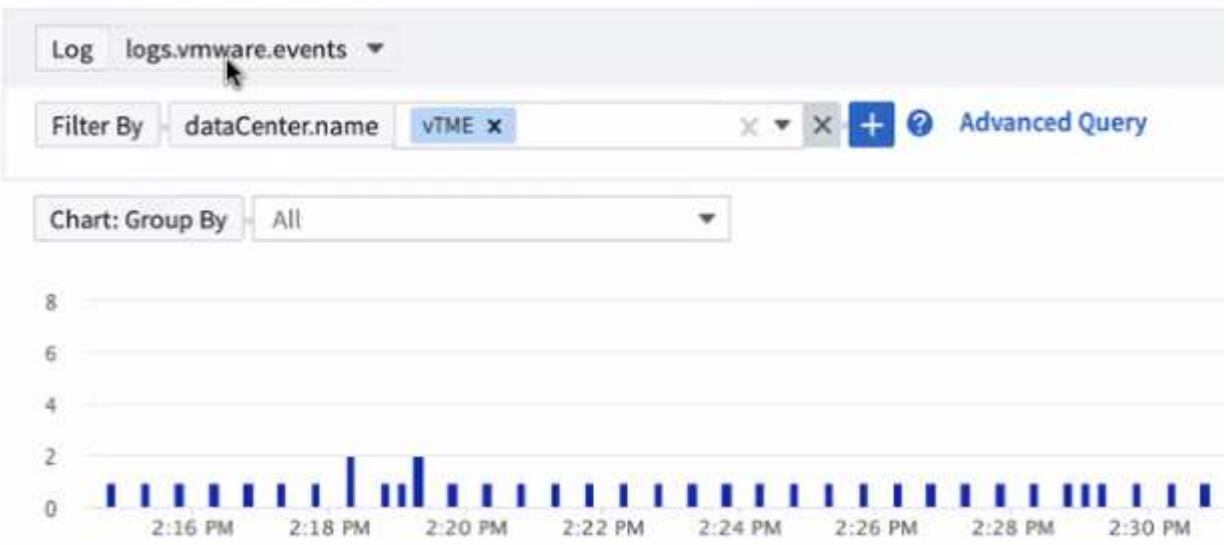
Vous pouvez désormais inclure des événements de journal dans vos tableaux de bord, pour visualiser les données d'événements et avoir une compréhension plus complète et contextuelle de votre environnement. Examinez les journaux et affichez les métriques associées sans quitter le tableau de bord !



Meilleure observabilité VMware avec VMware Events

Gérez et dépannez de manière proactive votre environnement VMware avec des événements en temps réel. Les événements VMware fournissent des informations sur les migrations de machines virtuelles, les allocations de ressources et l'état de l'hôte. Désormais disponible pour une utilisation dans les requêtes, les tableaux de bord et les moniteurs. Nécessite VMware version 8 ou supérieure. Sélectionnez simplement la source *logs.vmware.events*.

Les événements VMware sont également utilisés pour la nouvelle analyse des changements de configuration de DII mentionnée ci-dessus.



Mises à jour du collecteur de données :

- **Pure FlashBlade** : ce collecteur collecte les données d'inventaire et de performances des clusters FlashBlade qui exposent la version 2 de leur API REST.

Septembre 2024

Présentation de Data Infrastructure Insights, anciennement Cloud Insights

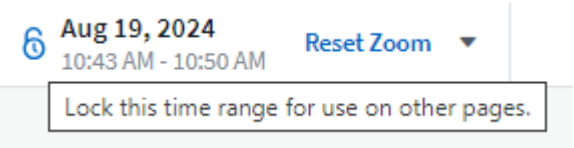
Le mardi 24 septembre 2024, NetApp a officiellement changé le nom de Cloud Insights en * Data Infrastructure Insights* (DII). Cela a été annoncé lors de la conférence des utilisateurs Insight par Haiyan Song dans son discours d'ouverture sur la scène principale et dans un communiqué de presse sur le produit de la conférence Insight.

Le service DII reste le même ; il n'y a aucun changement ou modification de fonctionnalités. Il s'agit d'un changement de nom visant à mieux aligner le nom du service avec ses capacités pour l'ensemble de l'infrastructure informatique.

Août 2024

Afficher les données spécifiques à votre plage horaire

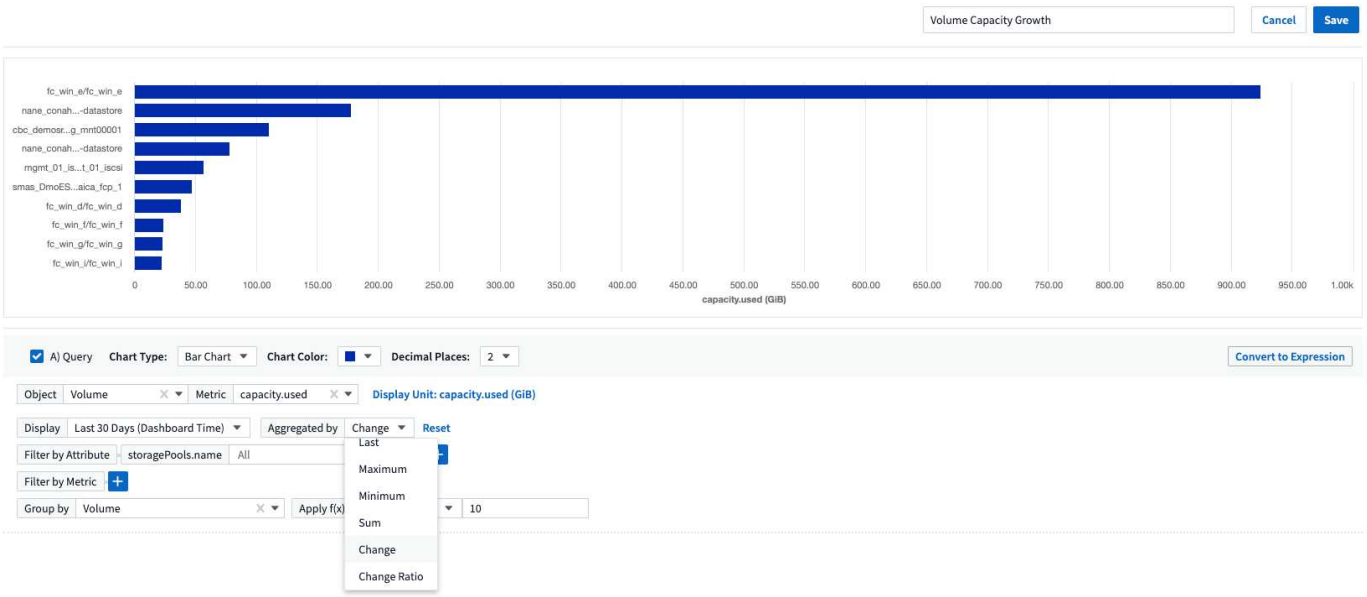
Vous enquêtez sur une alerte ? Vous avez zoomé sur un graphique ? Ces actions modifient la plage horaire de ces pages. Vous pouvez désormais verrouiller cette plage horaire, accéder à d'autres pages Cloud Insights et afficher les données spécifiques à cette plage horaire verrouillée. L'enquête et le dépannage sont désormais beaucoup plus faciles !



Analyse du changement et du taux de changement (%)

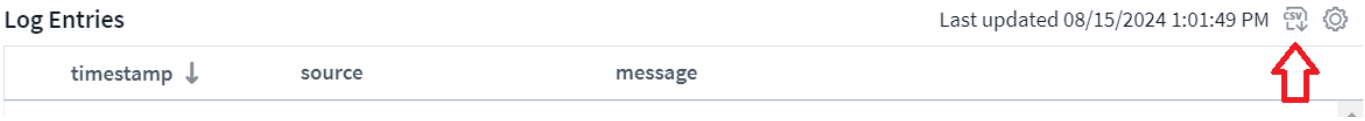
Les agrégations temporelles à ratio de changement vous aident à identifier les changements et les tendances significatifs dans les valeurs métriques au fil du temps. Ces informations sont essentielles pour comprendre ce qui a changé, comme une croissance considérable de la capacité pendant une période donnée ou un changement dans les performances d'un seul port.

- **Changement** - observer le changement d'une métrique entre deux points au cours d'une période sélectionnée.
- **Ratio de changement** - observer le changement proportionnel d'une métrique entre deux points, par rapport au point initial, au cours d'une période sélectionnée.



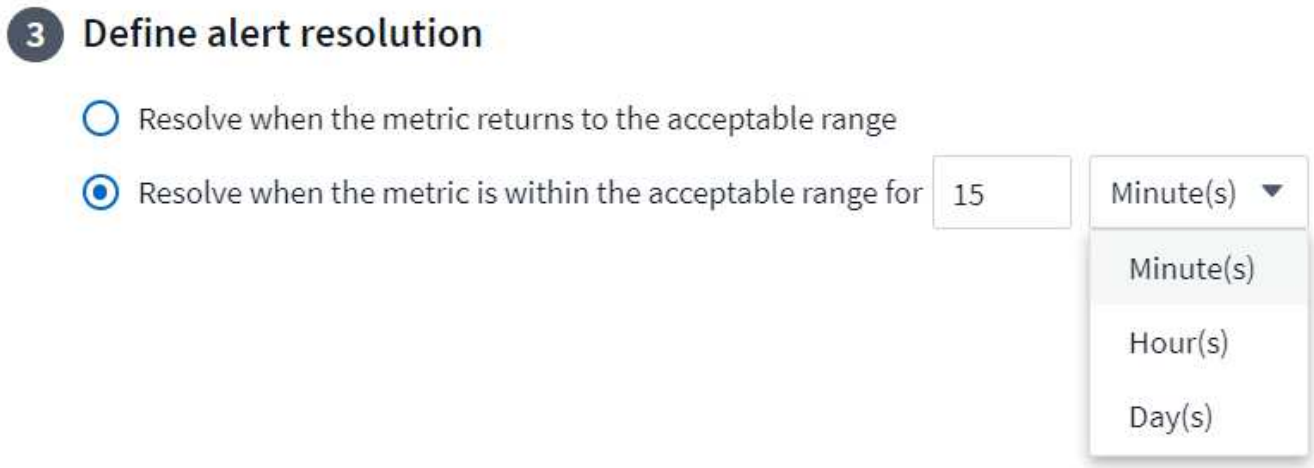
Exporter les résultats de la requête de journal au format .CSV

Lors de l'affichage des résultats de la requête de journal, exportez facilement jusqu'à 10 000 lignes au format .CSV en cliquant sur le nouveau bouton « Exporter ». Cela améliore l'accessibilité des données, facilite l'analyse et la création de rapports sur les données et facilite l'intégration transparente avec d'autres outils de traitement des données.



Résoudre les alertes par heure

Cloud Insights vous offre désormais la possibilité de résoudre une alerte lorsque la métrique surveillée reste dans la plage acceptable pendant une durée spécifiée. Cela vous permet de vous concentrer sur les problèmes réels, en réduisant le bruit associé aux mesures dépassant à plusieurs reprises les seuils définis en consolidant plusieurs alertes en une seule.



Juillet 2024

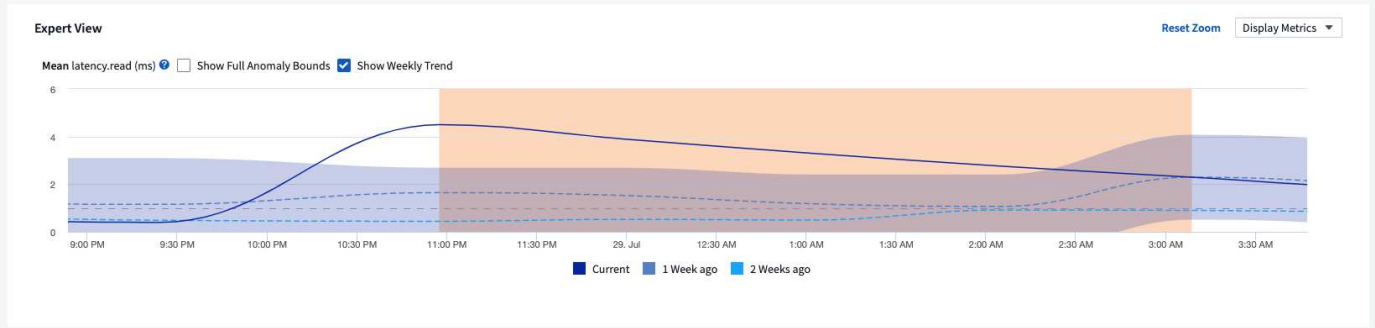
AIOps : détection d'anomalies

Cloud Insights utilise l'apprentissage automatique pour détecter les changements inattendus dans les modèles de données de votre environnement et fournir des alertes proactives pour vous aider à identifier les problèmes au plus tôt.

Un centre de données se comporte de différentes manières à différents moments de la journée et à différents jours de la semaine. Cloud Insights utilise la saisonnalité hebdomadaire pour comparer le comportement historique de chaque jour et de chaque heure.

La surveillance de détection d'anomalies peut fournir des alertes dans des situations telles que lorsque la définition de « normal » n'est pas claire, lorsque le comportement change au fil du temps ou lorsque vous travaillez avec de grandes quantités de données où la définition manuelle des seuils n'est pas pratique.

Nouveau"Moniteurs de détection d'anomalies" alerte lorsque des anomalies telles que celle-ci se produisent sur les métriques d'objet que vous choisissez.



Améliorations de la sécurité de la charge de travail

Prise en charge de NFS 4.1

Le collecteur de données SVM prend désormais en charge les versions NFS jusqu'à **NFS 4.1** inclus avec ONTAP 9.15.1 ou version ultérieure.

Nouvelle API d'activité médico-légale

L'activité médico-légale"API" a une nouvelle version. Lors de l'appel de l'API pour l'activité médico-légale, utilisez l'API **cloudsecure_forensics.activities.*v2***.

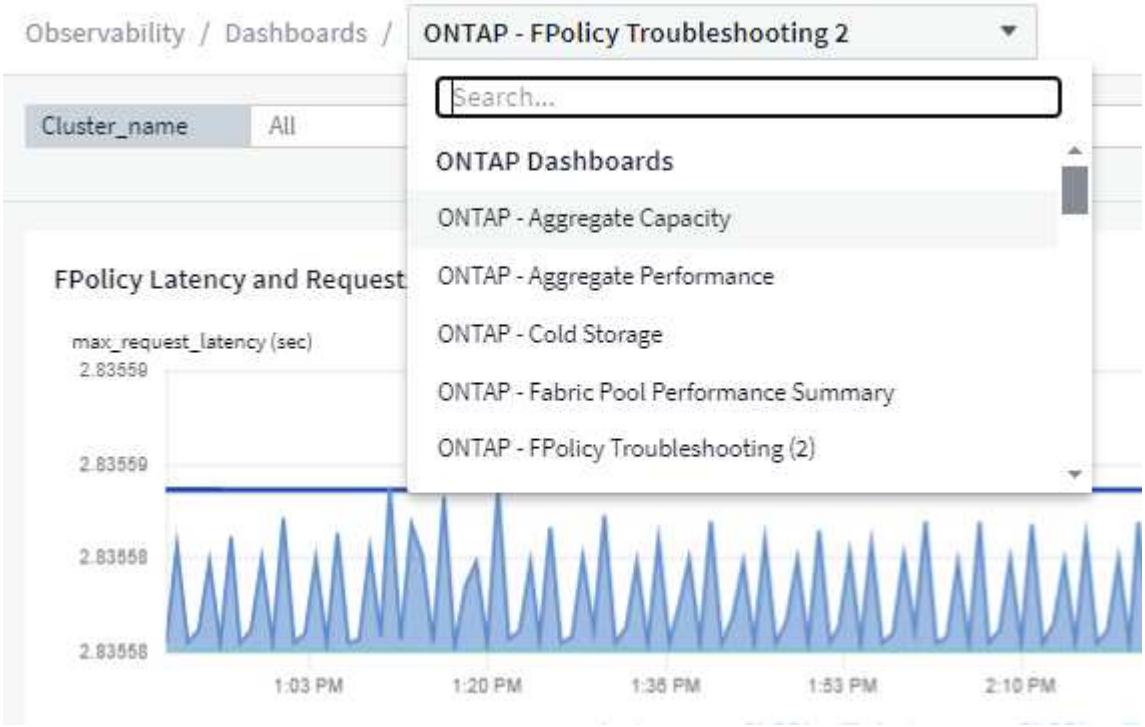
Notez que si vous effectuez plusieurs appels à cette API, pour de meilleurs résultats, assurez-vous que les appels se produisent de manière séquentielle, plutôt qu'en parallèle. Plusieurs appels parallèles peuvent entraîner l'expiration du délai d'attente de l'API.

Navigation simplifiée dans le tableau de bord

Cette fonctionnalité vise à rationaliser vos flux de travail opérationnels et à faciliter la collaboration entre les équipes.

Regrouper vos tableaux de bord vous permet d'obtenir plus rapidement la visibilité dont vous avez besoin, et désormais, grâce au nouveau menu de navigation, vous pouvez passer d'un tableau de bord à l'autre sans perdre votre place, ce qui facilite l'exploration et la gestion de votre infrastructure. Alignez les groupes de

tableaux de bord avec vos runbooks opérationnels pour améliorer encore votre expérience.



Juin 2024

Prise en charge du système d’exploitation

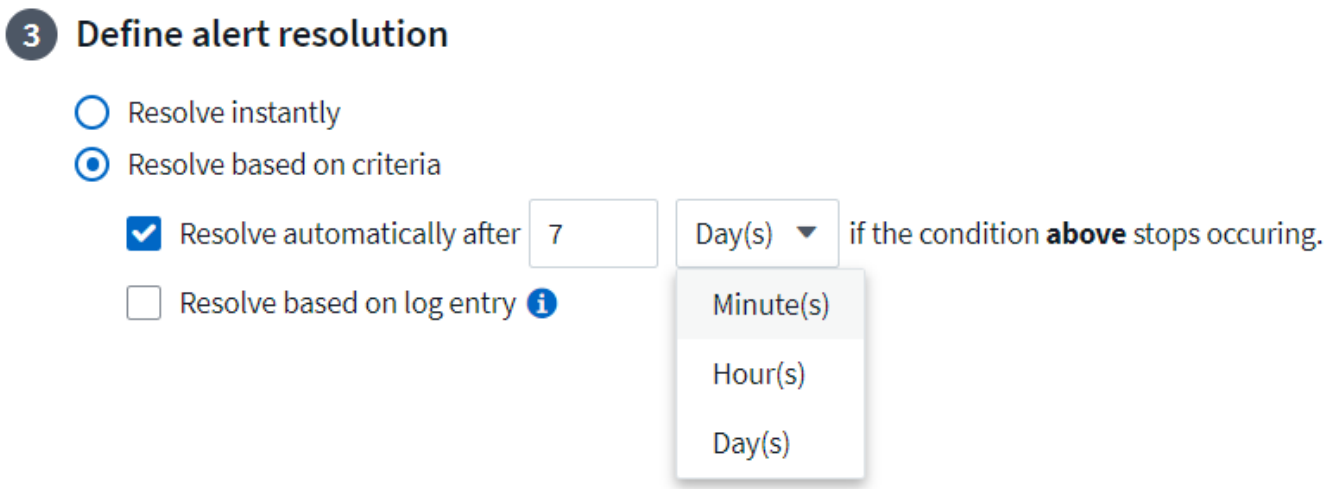
Les systèmes d’exploitation suivants sont pris en charge avec les unités d’acquisition Cloud Insights , en plus de ceux"déjà pris en charge" :

- Red Hat Enterprise Linux 8.9, 8.10, 9.4
- Rocky 9.4
- AlmaLinux 9.3 et 9.4

Mai 2024

Résoudre automatiquement les alertes en fonction du temps

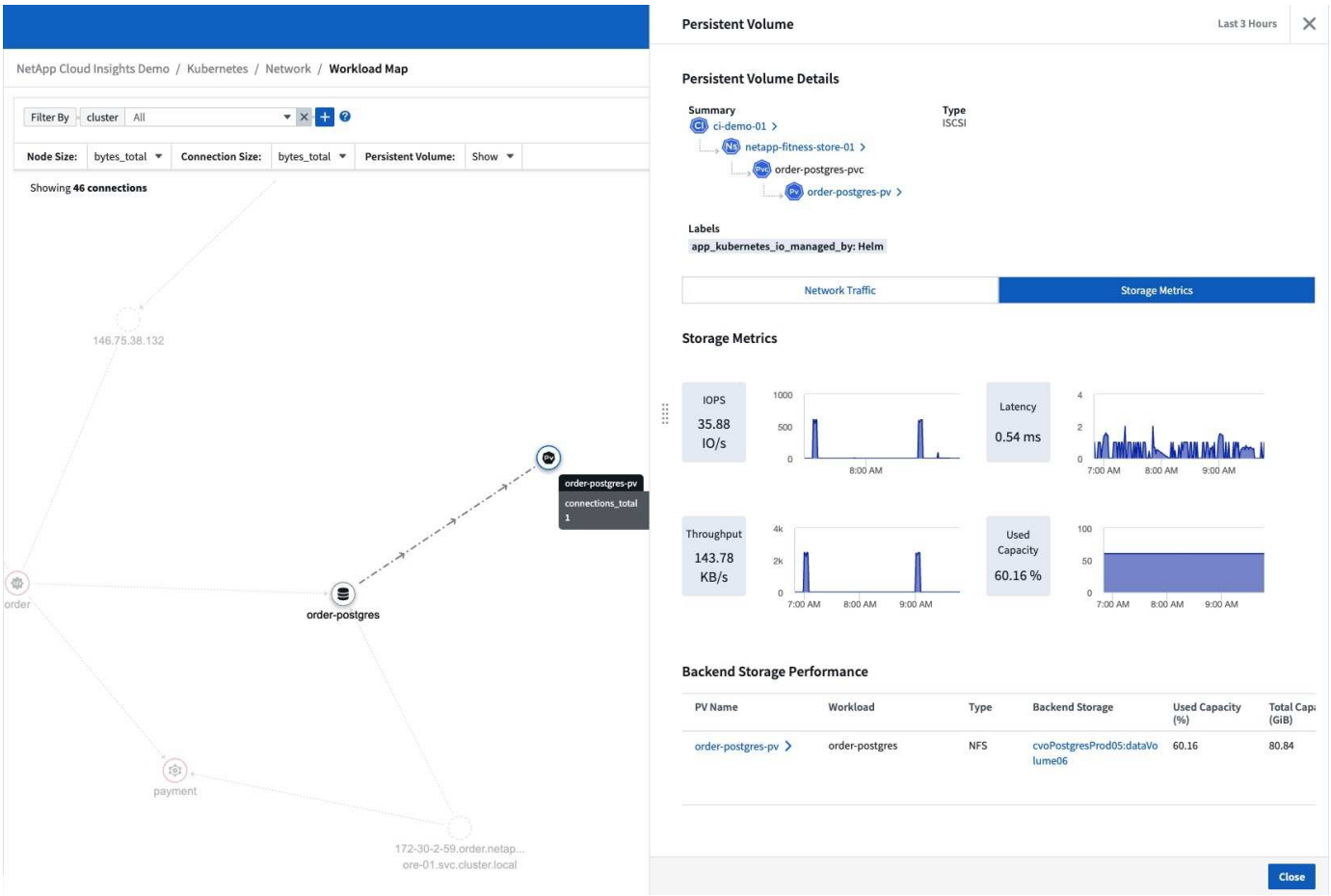
Les alertes de journal peuvent désormais être résolues en fonction du temps ; si la condition d’alerte cesse de se produire, Cloud Insights peut résoudre l’alerte automatiquement une fois le délai spécifié écoulé. Vous pouvez choisir de résoudre l’alerte en quelques minutes, heures ou jours.



Avril 2024

Prise en charge iSCSI pour Kubernetes

Cloud Insights prend désormais en charge la cartographie du stockage iSCSI associé à Kubernetes, permettant un dépannage plus rapide à l'aide de la carte réseau Kubernetes et la possibilité de fournir des rapports de rétrofacturation ou de rétrofacturation via Reporting.



Prise en charge du système d'exploitation

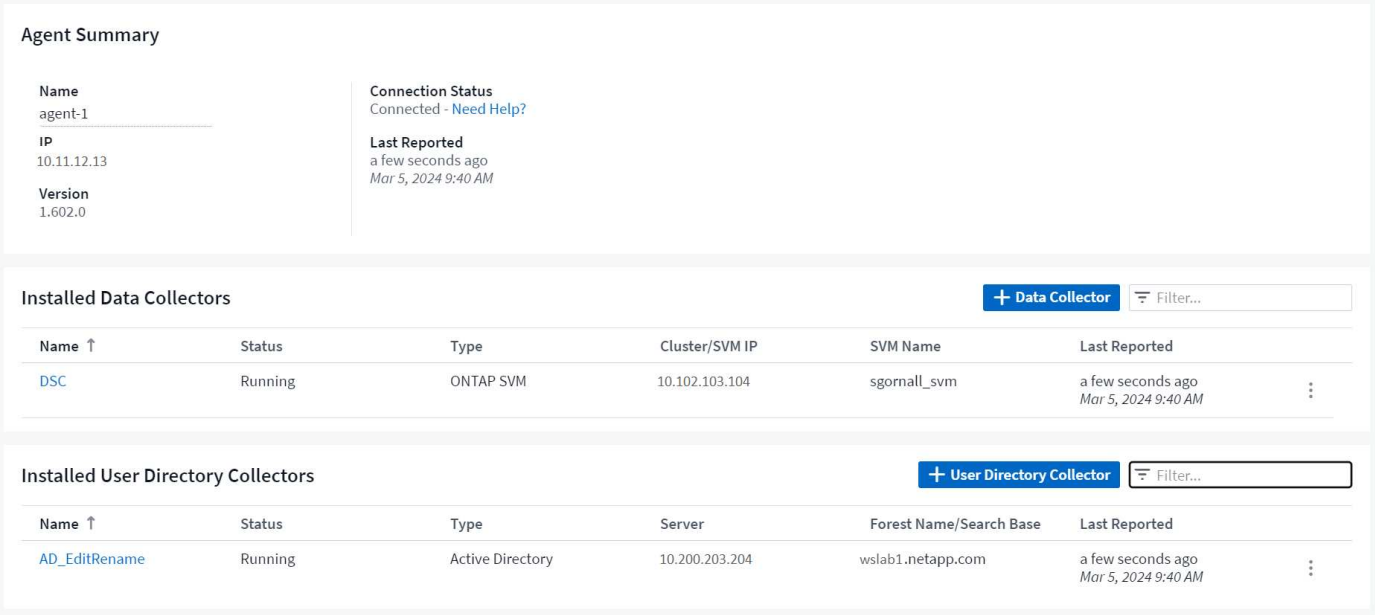
Les systèmes d'exploitation suivants sont pris en charge avec les unités d'acquisition Cloud Insights , en plus de ceux"déjà pris en charge" :

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- Rocky 9.3
- OpenSUSE Leap 15.1 à 15.5
- SUSE Enterprise Linux Server 15, 15 SP2 à 15 SP5

Mars 2024

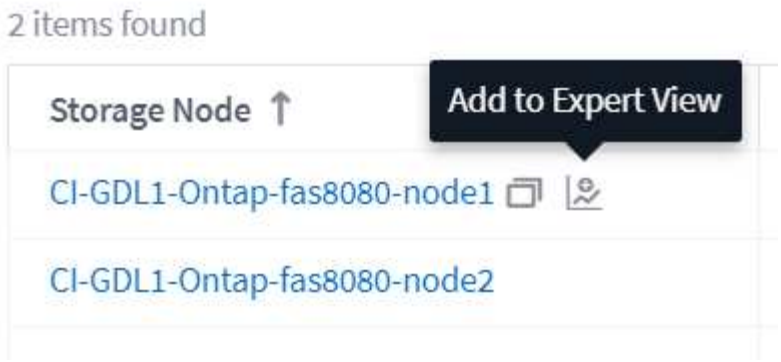
Détails de l'agent de sécurité de la charge de travail

Chacun de vos agents de sécurité de charge de travail dispose de sa propre page d'accueil, où vous pouvez facilement voir des informations récapitulatives sur l'agent ainsi que sur les collecteurs de données et d'annuaires utilisateurs installés associés à cet agent.

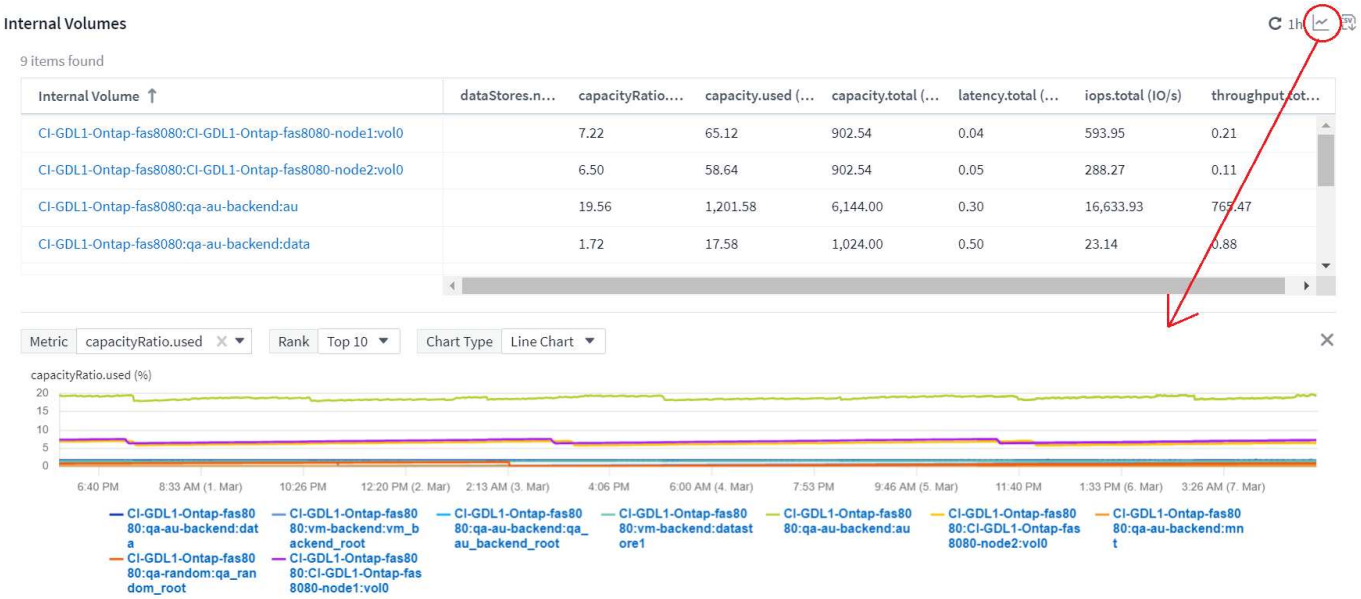


Créez des graphiques avec plus de données plus rapidement

Lors de l'analyse des données sur la page de destination d'un actif, l'ajout de données supplémentaires aux graphiques Expert View est un jeu d'enfant. Pour chaque tableau de la page de destination, si un type d'objet contient des données pertinentes, passez la souris sur cet objet pour afficher l'icône « Ajouter à la vue expert ». La sélection de cette icône ajoute cet objet aux ressources supplémentaires et l'affiche dans les graphiques de la vue Expert.



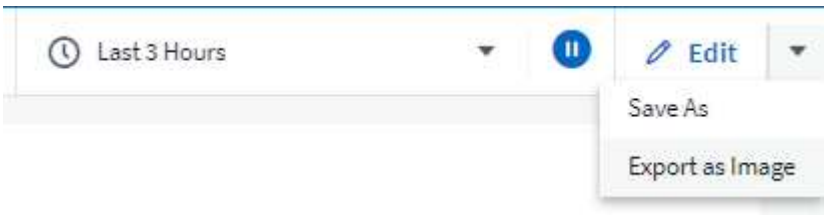
Ou peut-être souhaitez-vous voir les données d'un tableau de page de destination dans son propre graphique. Sélectionnez simplement l'icône *Afficher le graphique* pour ouvrir le graphique sous le tableau :



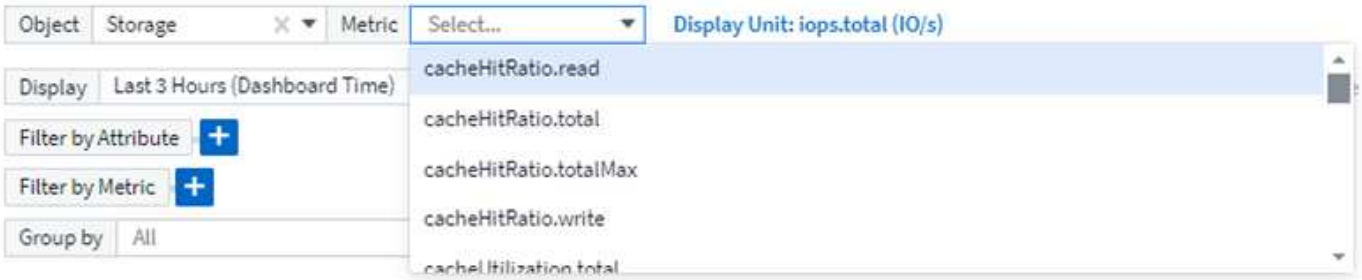
Février 2024

Améliorations de la convivialité

Enregistrez un **instantané** de votre tableau de bord actuel en sélectionnant *Exporter en tant qu'image* dans la liste déroulante du coin droit. Cloud Insights crée un fichier .PNG des états actuels du widget.

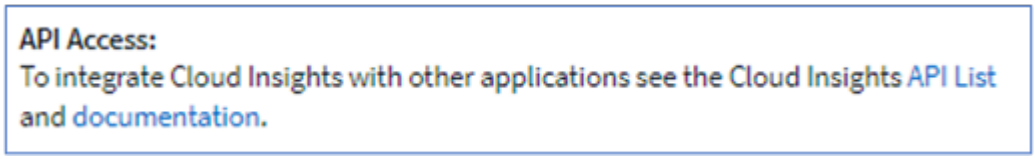


La sélection d'objets et de métriques est plus simple que jamais pour les widgets, les moniteurs, etc. Choisissez le type d'objet souhaité, puis sélectionnez une métrique pertinente pour cet objet dans la liste déroulante séparée.



Exportez les listes de collecteurs de données et d'unités d'acquisition au format .CSV en sélectionnant l'icône en haut de ces pages.

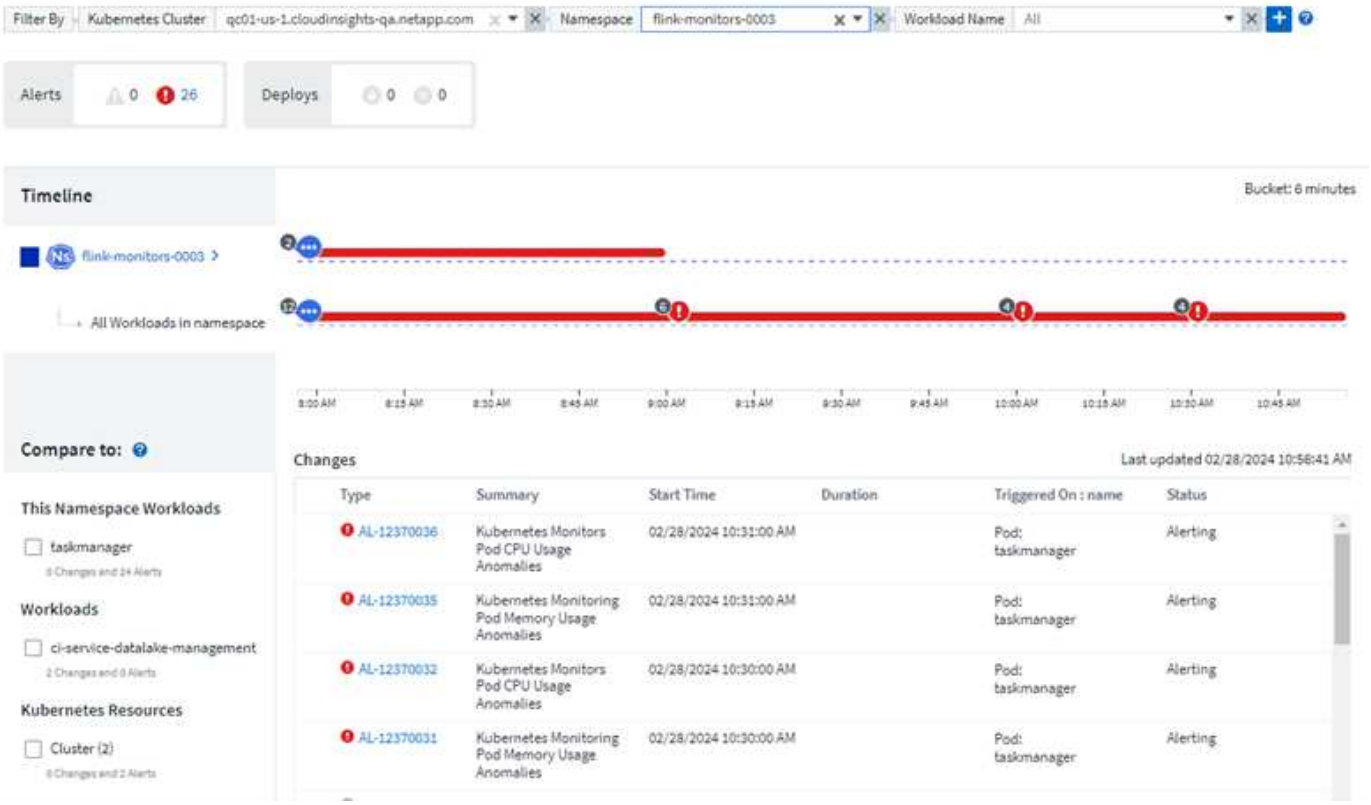
Nous avons **réorganisé la page Aide > Support** afin qu'il soit plus facile de trouver ce que vous cherchez, et parce que vous les avez demandés, nous avons ajouté des liens directs sur cette page vers **API Swagger** et la documentation utilisateur.



Les **liens** dans la colonne « triggeredOn » de la page de liste des alertes mèneront à la page de destination appropriée, si une page de destination est disponible pour cet objet.

Voir tous les changements dans votre espace de noms

Kubernetes Change Analysis vous permet désormais de voir une chronologie des modifications lors de la sélection du cluster et de l'espace de noms. Auparavant, la charge de travail devait également être sélectionnée. Lors du filtrage sur le cluster et l'espace de noms, la chronologie de toutes les modifications de charge de travail dans cet espace de noms est affichée sur une seule ligne.



Journaux associés aux alertes

Lors de l'affichage d'une alerte de journal, les entrées de journal associées sont affichées dans un nouveau tableau. Une entrée de journal est liée si elle se produit dans la même source et la même période que l'alerte et est soumise aux mêmes conditions. Sélectionnez « Analyser les journaux » pour explorer davantage.

Collecter les données du commutateur ONTAP

Cloud Insights peut collecter des données à partir des commutateurs back-end du système ONTAP ; activez simplement la collecte dans la section *Configuration avancée* du collecteur de données et assurez-vous que le système ONTAP est configuré pour fournir"informations sur le commutateur" et a le approprié"autorisations" ensemble.

API de collecte de données de sécurité de la charge de travail

Dans les environnements de grande taille, vous pouvez automatiser la création du collecteur Workload Security à l'aide de la nouvelle API Data Collectors. Accédez à **Admin > Accès API > Documentation API** et sélectionnez le type d'API *Sécurité de la charge de travail* pour en savoir plus.

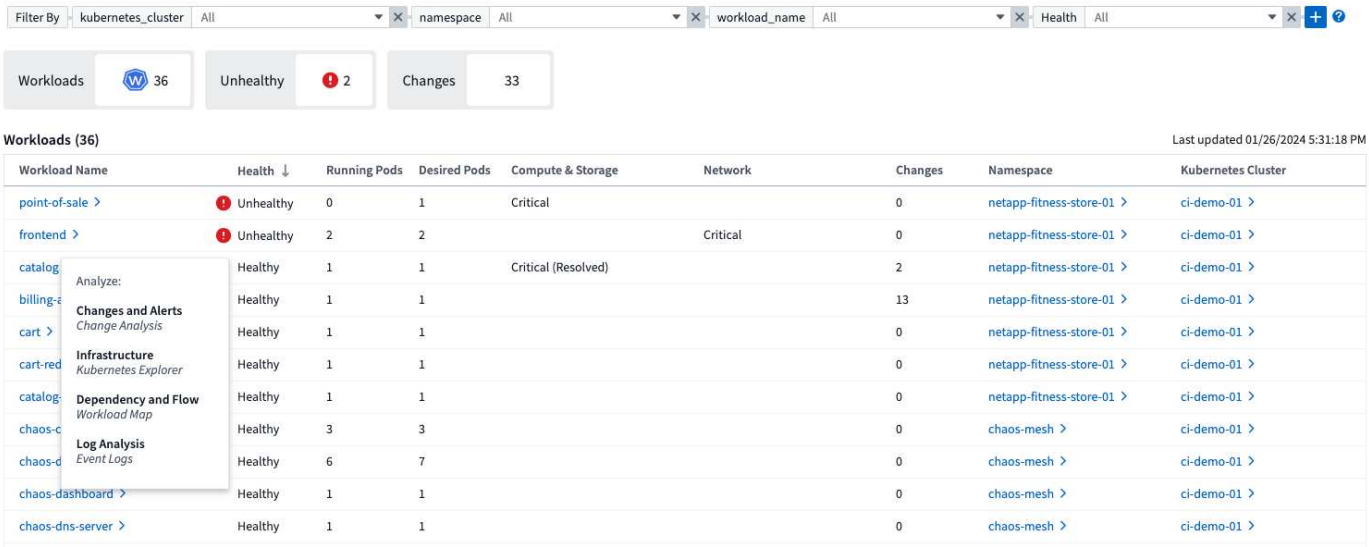
Janvier 2024

Essayez les fonctionnalités de Cloud Insights que vous n’avez pas encore utilisées

En plus de votre essai initial de Cloud Insights, vous pouvez également profiter de"Évaluations des modules" . Par exemple, si vous êtes abonné à Cloud Insights et que vous surveillez le stockage et les machines virtuelles, lorsque vous ajoutez Kubernetes à votre environnement, vous entrez automatiquement dans un essai de 30 jours de Kubernetes Observability. L’utilisation de l’unité gérée par Kubernetes Observability ne sera pas comptabilisée dans vos droits d’abonnement avant la fin de la période d’essai.

Dans quelle mesure mes charges de travail sont-elles saines ?

L’état de la charge de travail est disponible en un coup d’œil sur la page **Kubernetes > Explorer > Charges de travail**, ce qui vous permet de voir rapidement quelles charges de travail fonctionnent bien et lesquelles peuvent nécessiter de l’aide. Identifiez facilement si le problème de santé est lié à des changements d’infrastructure, de réseau ou de configuration, et analysez en profondeur la cause première.



Mises à jour du collecteur de données

Identification du domaine de données

Le collecteur Data Domain a été amélioré pour mieux identifier les systèmes HA afin d’assurer leur durabilité lors des événements de basculement. Ce changement entraînera une réidentification **unique** des appliances Data Domain dans les systèmes HA, ce qui entraînera ensuite la suppression de toutes les annotations sur ces ressources (car ces tableaux seront réidentifiés). Vous devrez rattacher les annotations à vos objets Data Domain.

Algorithme ML de détection de ransomware amélioré

Workload Security inclut un nouvel algorithme ML de détection de ransomware de 2e génération pour détecter les attaques les plus sophistiquées plus rapidement et avec plus de précision.

« Saisonnalité » des comportements : le comportement du week-end peut suivre des schémas différents de celui de la semaine, ou celui du matin de celui de l’après-midi. Les algorithmes de sécurité de la charge de travail prennent en compte cette saisonnalité.

Fonctionnalité obsolète

Parfois, certaines fonctionnalités sont obsolètes à mesure que les fonctionnalités évoluent. Voici quelques-unes des fonctionnalités qui ont été abandonnées dans Cloud Insights:

L'API REST Cloudsecure_forensics.activities.v1 de Workload Secure est obsolète

L'API *cloudsecure_forensics.activities.v1* est obsolète. Cette API renvoie des informations sur les activités associées aux entités dans l'environnement Storage Workload Security. Cette API a été remplacée par cloudsecure_forensics.activities.*v2*_.

GET pour cette API renvoyait précédemment ce qui suit :

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

Cette API renvoie désormais :

```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdnl9fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

Pour plus de détails, consultez la documentation Swagger dans « Admin > Accès API > Documentation API > Sécurité de la charge de travail ».

Décembre 2023

Change Analytics en un coup d'œil

Kubernetes"Analyse des changements" vous offre une vue tout-en-un des modifications récentes apportées à votre environnement Kubernetes. Les alertes et l'état du déploiement sont à portée de main. Avec Change

Analytics, vous pouvez suivre chaque changement de déploiement et de configuration et le corréler avec l'état et les performances des services, de l'infrastructure et des clusters K8.

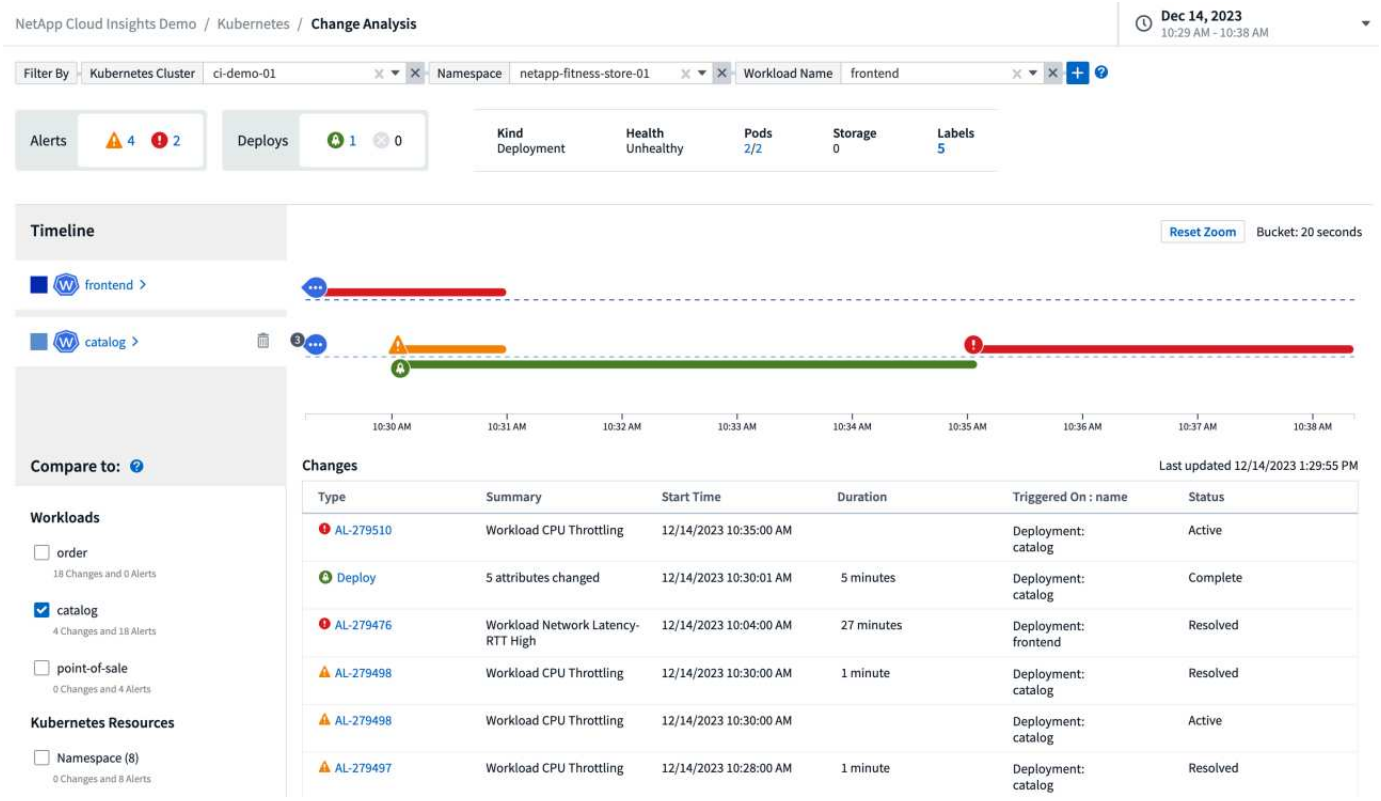
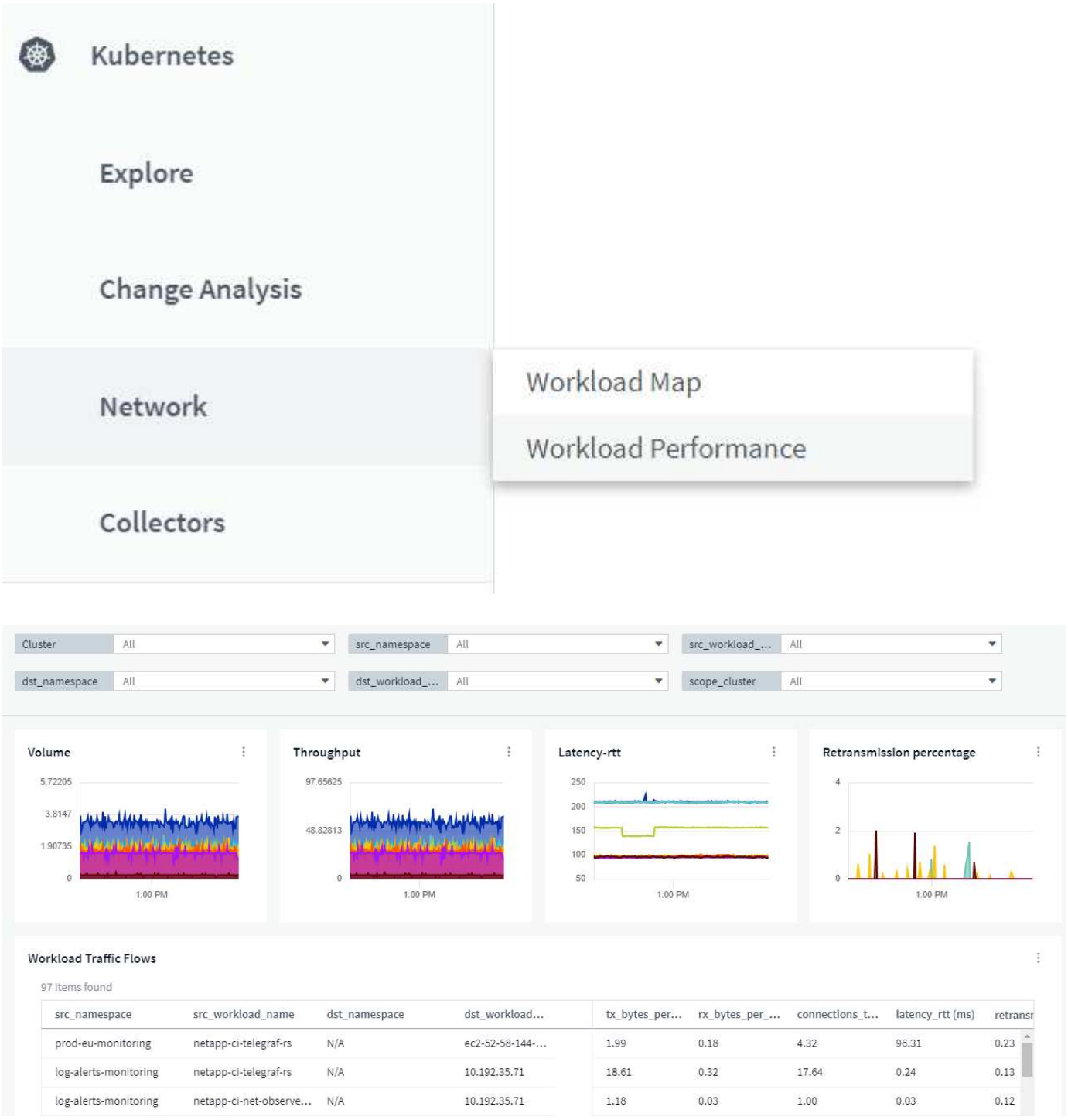


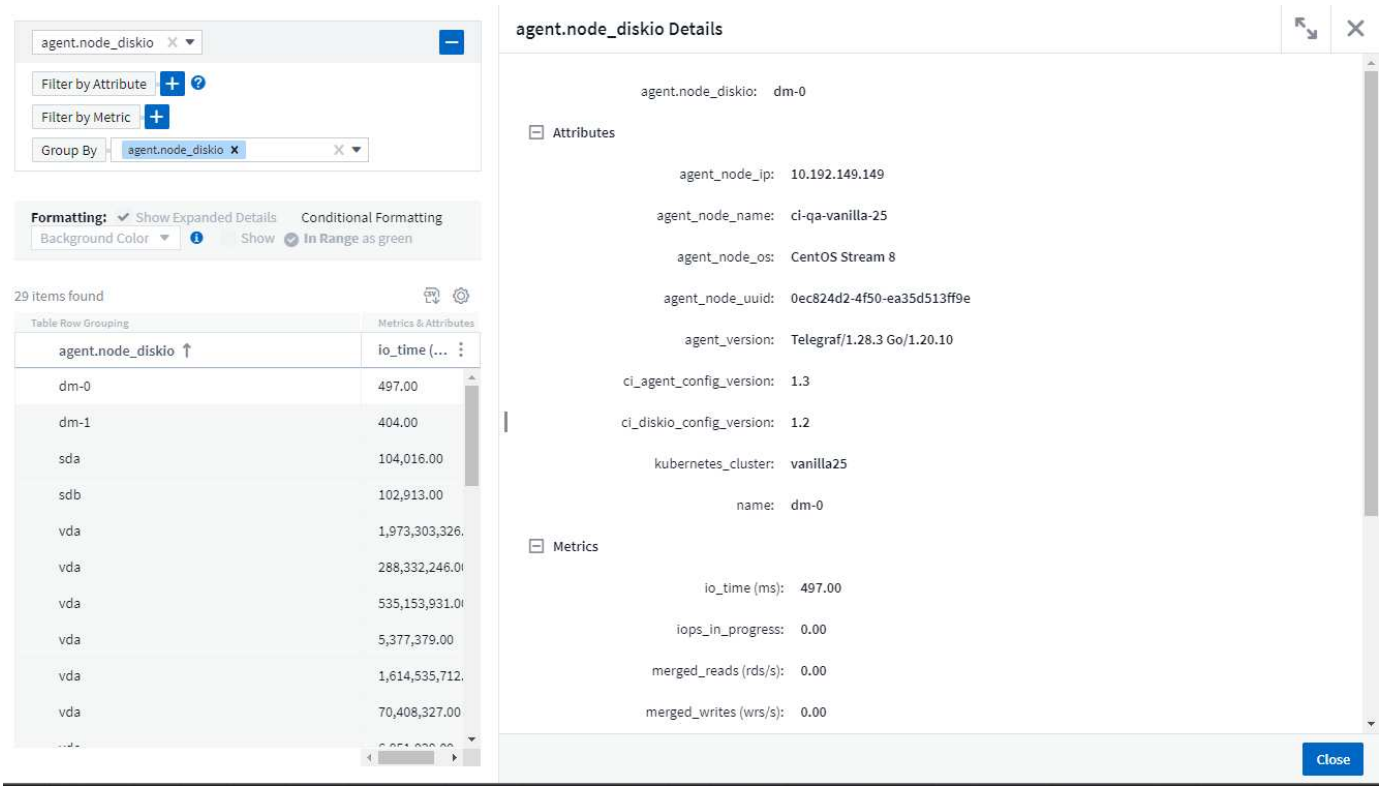
Tableau de bord des performances de la charge de travail Kubernetes

Les performances de la charge de travail sont disponibles en un coup d'œil dans le tableau de bord complet des performances de la charge de travail de Kubernetes. Affichez rapidement les graphiques des tendances de volume, de débit, de latence et de retransmission, ainsi qu'un tableau du trafic de charge de travail pour chaque espace de noms de votre environnement. Les filtres permettent de se concentrer facilement sur les zones d'intérêt.



Détails de la requête sur un seul écran

Dans une requête, la sélection d'une ligne ouvre un panneau latéral affichant les détails des attributs, des annotations et des métriques pour la ligne sélectionnée, fournissant des informations utiles sans avoir besoin d'explorer la page de destination de l'objet. Les liens dans la ligne ou le panneau latéral permettent une navigation facile.



Mises à jour du collecteur de données :

- * Brocade FOS REST* : Ce collecteur est déplacé hors de « Aperçu » et est désormais disponible en général. Quelques points à noter :
  - FOS a introduit son API REST avec FOS 8.2. Mais certaines fonctionnalités comme le routage n'ont reçu des capacités d'API REST qu'avec la version 9.0.
  - Si vous disposez d'une structure composée d'actifs FOS mixtes 8.2 supérieurs, ainsi que de certains < 8.2, le collecteur Cloud Insights FOS REST ne parviendra pas à détecter ces actifs plus anciens. Vous pouvez modifier le collecteur FOS REST et créer une liste délimitée par des virgules de l'adresse IPv4 de ces périphériques à exclure de ce collecteur.
- **SELinux** : Cloud Insights inclut des améliorations à l'installation initiale de l'unité d'acquisition Linux pour garantir la robustesse du fonctionnement dans les environnements Linux avec l'application SELinux activée. Ces améliorations n'impactent que les *nouveaux* déploiements AU ; si vous rencontrez des problèmes SELinux liés aux mises à niveau AU, contactez le support NetApp pour corriger votre configuration SELinux.

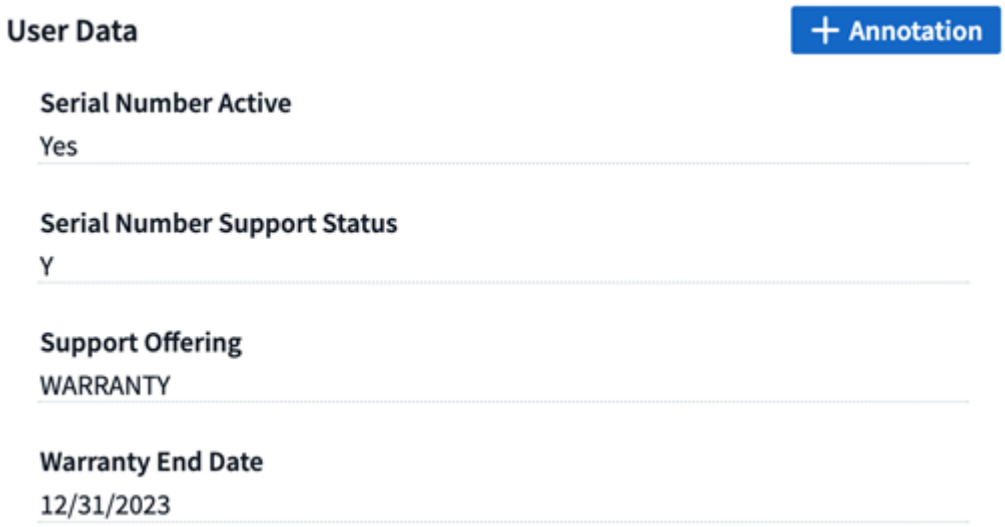
Novembre 2023

Sécurité de la charge de travail : suspendre/reprendre un collecteur

Dans Workload Security, vous pouvez suspendre un collecteur de données si le collecteur est à l'état *En cours d'exécution*. Ouvrez le menu « trois points » du collecteur et sélectionnez PAUSE. Pendant que le collecteur est en pause, aucune donnée n'est collectée à partir d' ONTAP et aucune donnée n'est envoyée du collecteur à ONTAP. Sélectionnez Reprendre pour recommencer la collecte.

Informations sur la prise en charge des nœuds de stockage

Sur la page de destination d'un nœud de stockage, la section *Données utilisateur* fournit des informations rapides sur votre offre d'assistance, l'état actuel, l'état de l'assistance et la date de fin de la garantie. Notez que Cloud Insights publie actuellement automatiquement ces informations uniquement pour les appareils NetApp . Notez également que ces champs de support sont des annotations, ils peuvent donc être utilisés dans des requêtes et des tableaux de bord.



Associer les balises VMware aux annotations Cloud Insights

Le"VMware" Le collecteur de données vous permet de renseigner les annotations de texte Cloud Insights avec des balises du même nom configurées sur VMWare.

Améliorations de la fiabilité du collecteur Brocade CLI pour le micrologiciel FOS 9.1.1c et supérieur

Sur certains commutateurs Brocade Fibre Channel exécutant le micrologiciel 9.1.1c, la sortie de certaines commandes CLI peut être précédée du texte de la bannière de connexion « motd » ou d'avertissements demandant aux utilisateurs de modifier les mots de passe par défaut. Le collecteur Brocade CLI a été amélioré pour ignorer ces deux types de texte superflu.

Avant cette amélioration, seuls les commutateurs FOS 9.1.1c sans Virtual Fabrics présents étaient susceptibles d'être détectables avec ce type de collecteur.

Octobre 2023

Sécurité renforcée de la charge de travail

La sécurité de la charge de travail a été améliorée avec les éléments suivants :

- **Accès refusé** : Workload Security s'intègre à ONTAP pour recevoir"Événements « Accès refusé »" et fournir une couche d'analyse supplémentaire et de réponses automatiques.
- **Types de fichiers autorisés** : Si une attaque de ransomware est détectée pour une extension de fichier

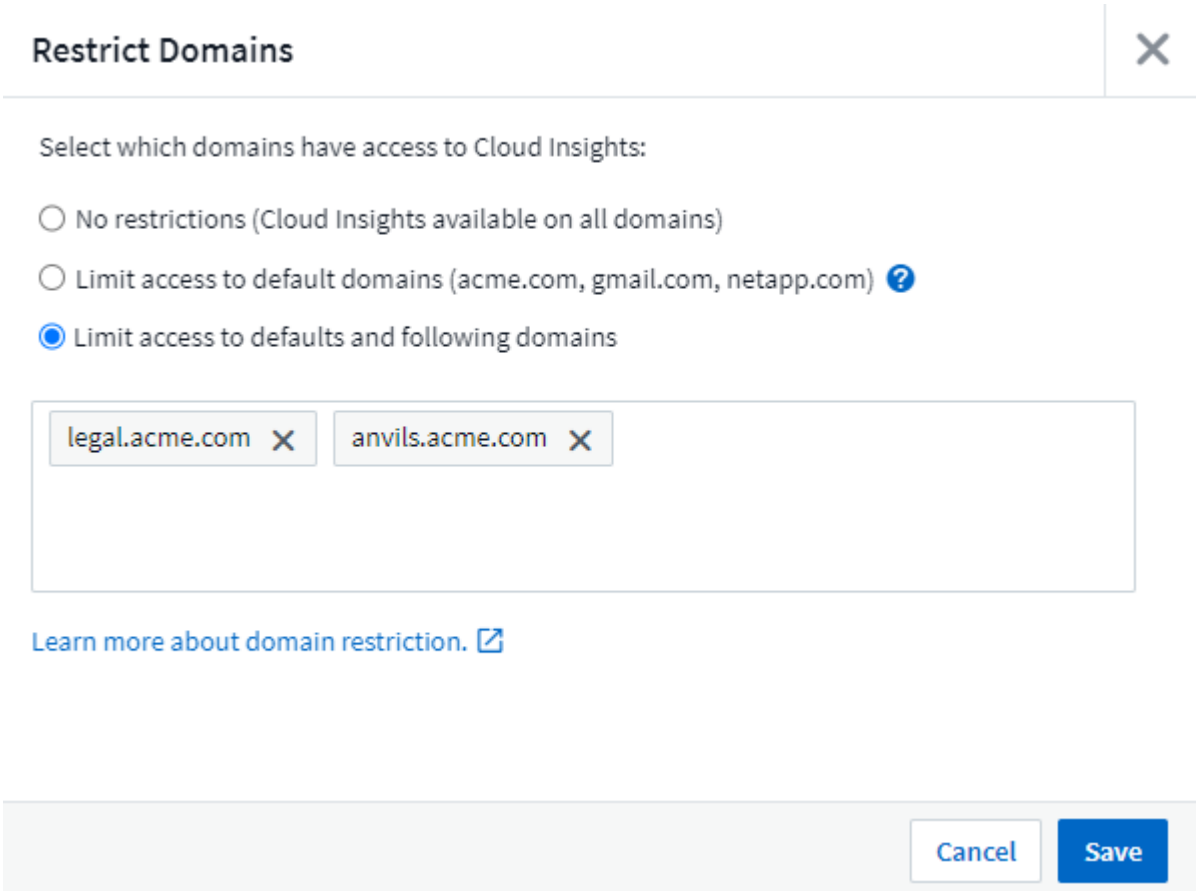
connue, cette extension de fichier peut être ajoutée à un"types de fichiers autorisés" liste pour éviter les alertes inutiles.

Essais de modules

En plus de votre essai initial de Cloud Insights, vous pouvez également profiter de"Évaluations des modules" . Par exemple, si vous êtes déjà abonné à Infrastructure Observability mais que vous ajoutez Kubernetes à votre environnement, vous entrerez automatiquement dans un essai de 30 jours de Kubernetes Observability. Vous ne serez facturé que pour votre utilisation de l'unité gérée par Kubernetes Observability à la fin de la période d'évaluation.

Restreindre l'accès à des domaines spécifiés

Les administrateurs et les propriétaires de compte ont désormais la possibilité de"restreindre l'accès à Cloud Insights" aux domaines de courrier électronique qu'ils spécifient. Accédez à **Admin > Gestion des utilisateurs** et sélectionnez le bouton *Restreindre les domaines*.



Mises à jour du collecteur de données

Les modifications suivantes ont été apportées à l'unité de collecte/d'acquisition de données :

- **Isilon / PowerScale REST** : divers nouveaux attributs et mesures ont été ajoutés aux capacités d'analyse améliorées de Cloud Insights sous le nom *emc_isilon.node_pool.**. Ces compteurs et attributs permettront aux utilisateurs de créer des tableaux de bord et de surveiller la consommation de capacité du pool de nœuds ; les utilisateurs avec des clusters Isilon construits à partir de modèles de nœuds matériels différents disposeront de plusieurs pools de nœuds, et la compréhension de votre consommation de disque dur/SSD/capacité totale au niveau du pool de nœuds est utile à la fois pour la surveillance et la

planification.

- **Rubrik** Prise en charge de l'authentification « Compte de service » : le collecteur Rubrik de Cloud Insights prend désormais en charge l'authentification de base HTTP traditionnelle (nom d'utilisateur et mot de passe) et l'approche Compte de service de Rubrik, qui nécessite un nom d'utilisateur + un secret + un ID d'organisation.

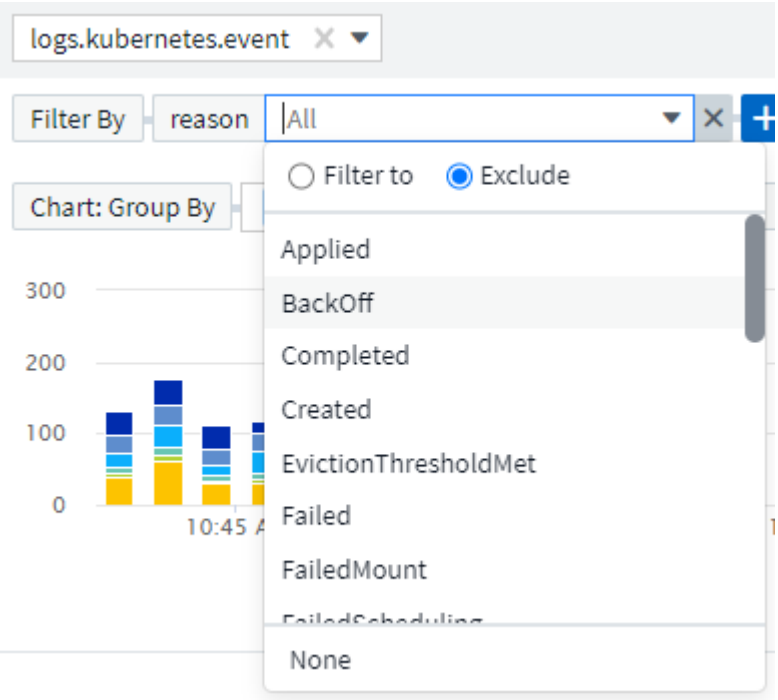
Septembre 2023

Trouvez facilement ce que vous voulez dans les journaux

La requête de journal (**Observabilité > Requêtes de journal > +Nouvelle requête de journal**) comprend un certain nombre de"améliorations" pour rendre l'exploration des journaux plus facile et plus informative.

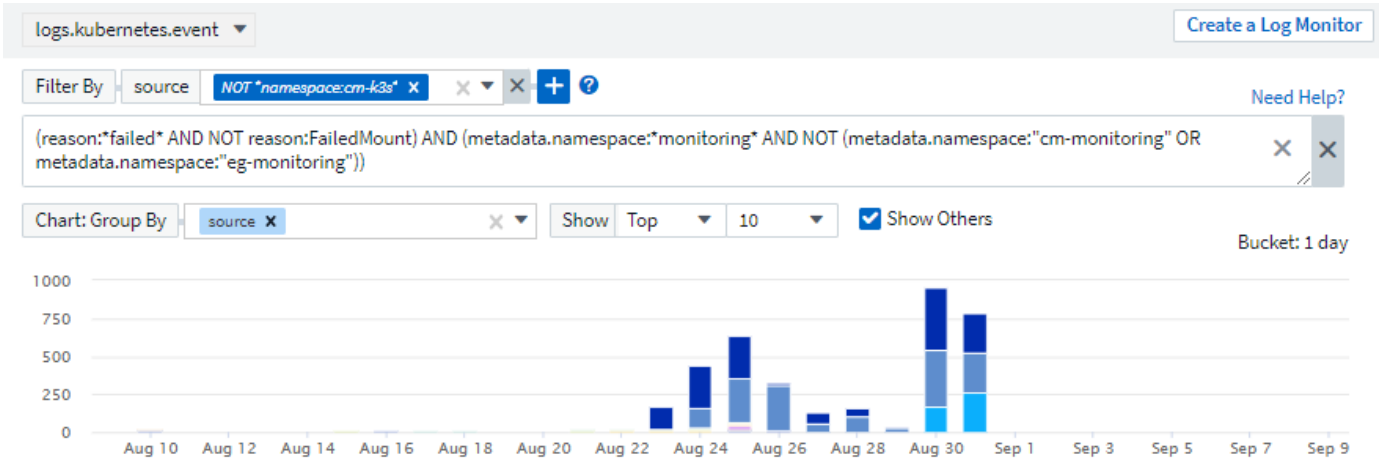
Inclure/Exclure

Lors du filtrage d'une valeur, vous pouvez facilement choisir d'**inclure** ou d'**exclure** les résultats correspondant au filtre. La sélection de « Exclure » crée un filtre « PAS <valeur> ». Vous pouvez combiner les valeurs Inclure et Exclure dans un seul filtre.



Requête avancée

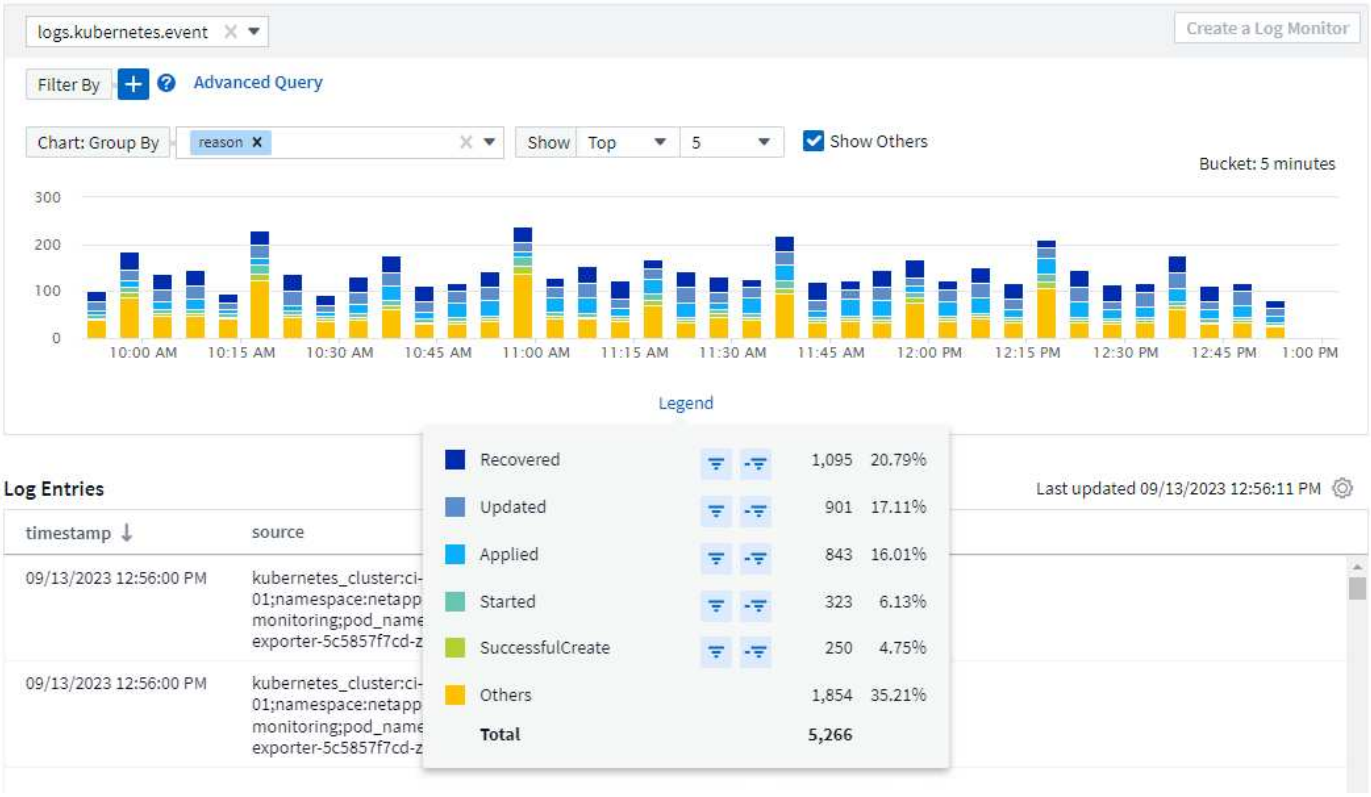
Advanced Querying vous donne la possibilité de créer des filtres « de forme libre », combinant ou excluant des valeurs à l'aide de AND, NOT, OR, de caractères génériques, etc.



Les fonctions « Filtrer par » et « Requête avancée » sont combinées par « ET » pour former une seule requête. Les résultats sont affichés dans la liste des résultats et le graphique.

Regroupement dans le graphique

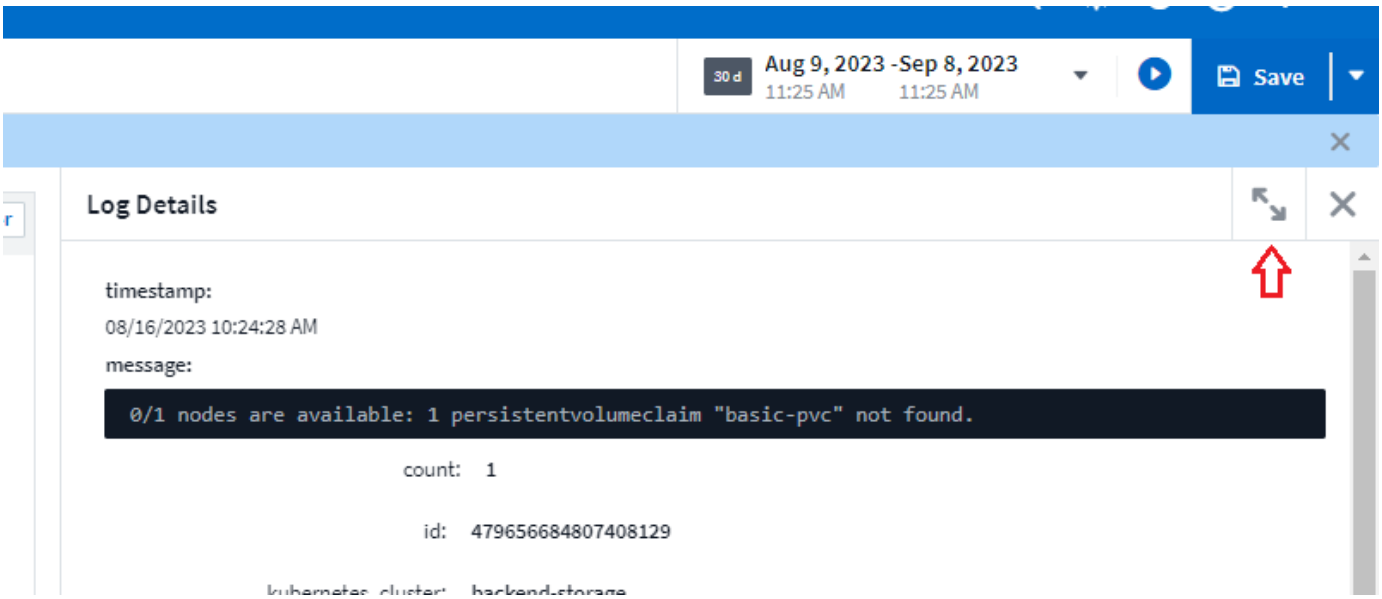
Lorsque vous sélectionnez un attribut de journal à **Grouper par**, la liste et le graphique affichent les résultats du filtre actuel. Dans le graphique, les colonnes sont regroupées par couleurs. Survoler une colonne du graphique affichera des détails sur les entrées spécifiques, similaires aux informations générales affichées lorsque vous développez la légende du graphique. Dans la légende, vous pouvez également choisir de définir un filtre d'inclusion ou d'exclusion pour un regroupement spécifique.



Panneau de détails du journal « flottant »

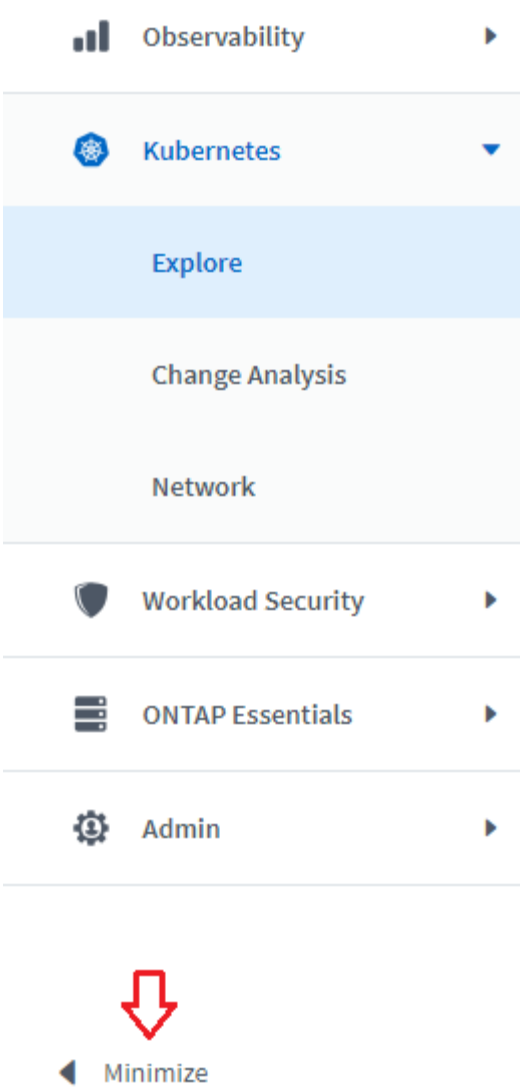
Lors de l'exploration des journaux à l'aide de la requête de journal, la sélection d'une entrée dans la liste ouvre un panneau de détails pour cette entrée. Vous pouvez désormais choisir d'afficher ce panneau coulissant

« flottant » (c'est-à-dire affiché sur le reste de l'écran) ou « dans la page » (c'est-à-dire affiché comme son propre cadre dans la page). Pour basculer entre ces vues, sélectionnez le bouton « Dans la page / Flottant » dans le coin supérieur droit du panneau.



Réduire le menu

Vous pouvez réduire le menu de navigation de Cloud Insights sur le côté gauche en sélectionnant le bouton « Réduire » sous le menu. Lorsque le menu est réduit, passez la souris sur une icône pour voir quelle section elle ouvre ; la sélection de l'icône ouvre le menu et vous amène directement à cette section.



Améliorations du collecteur de données

Cloud Insights a facilité l'affichage et la recherche d'informations sur les collecteurs de données :

- **Le traitement des listes de collecteurs de données** est plus efficace, ce qui signifie que le temps nécessaire pour afficher et parcourir ces listes est considérablement réduit. Si vous disposez d'un environnement de grande taille avec de nombreux collecteurs de données, vous constaterez une amélioration significative lors de la liste de vos collecteurs de données.
- La **matrice de support du collecteur de données** est passée d'un fichier .PDF à une page basée sur .HTML, plus rapide à parcourir et plus facile à maintenir. Découvrez la nouvelle Matrix ici : https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

Août 2023

Collecte des journaux Isilon/PowerScale et des données d'analyse avancées

Les collecteurs Isilon REST et PowerScale REST contiennent les améliorations suivantes :

- Les événements du journal Isilon sont disponibles pour une utilisation dans les requêtes et les alertes
- Les attributs d'analyse avancée d'Isilon peuvent être utilisés dans les requêtes, les tableaux de bord et les alertes :
  - emc_isilon.cluster
  - emc_isilon.node
  - emc_isilon.node_disk
  - emc_isilon.net_iface

Ceux-ci sont activés par défaut pour les utilisateurs des collecteurs Isilon REST et/ou PowerScale REST. NetApp encourage fortement les utilisateurs du collecteur basé sur l'interface de ligne de commande Isilon à migrer vers le nouveau collecteur basé sur l'API REST pour bénéficier d'améliorations telles que celles ci-dessus.

Carte de charge de travail améliorée

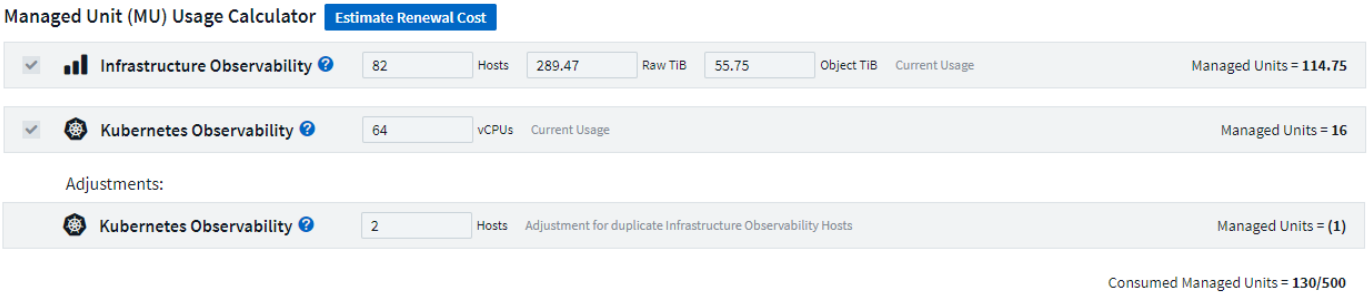
La carte de charge de travail est plus utilisable et moins bruyante ; elle regroupe tous les services externes similaires dans un seul nœud s'ils communiquent avec les mêmes charges de travail, réduisant ainsi la complexité du graphique et facilitant la compréhension de la manière dont les services sont interconnectés.

Le choix d'un nœud groupé affichera un tableau détaillé avec les mesures de trafic réseau pour chaque service externe pertinent pour ce nœud.

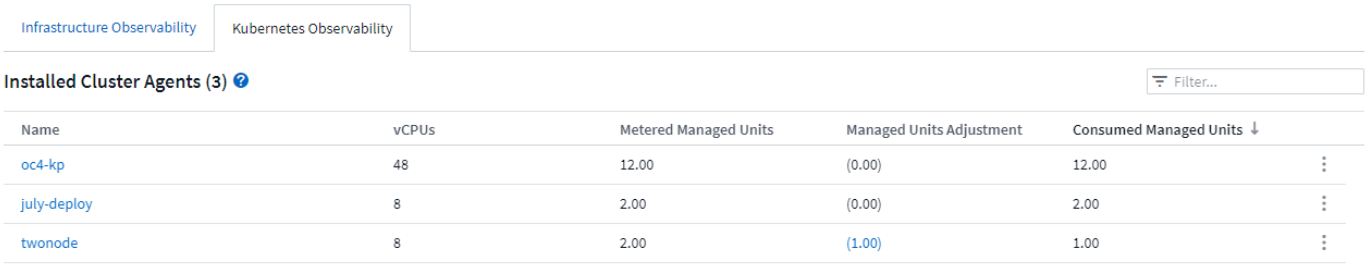
Ajustement de l'utilisation de l'unité gérée Kubernetes

Si une ressource de calcul dans votre environnement de cluster Kubernetes est comptée à la fois par l'opérateur de surveillance NetApp Kubernetes et par un collecteur de données d'infrastructure sous-jacent (par exemple, VMware), votre utilisation de ces ressources sera ajustée pour garantir le comptage le plus efficace des unités gérées. Vous pouvez afficher les ajustements de Kubernetes MU sur la page Admin > Abonnement, dans les onglets Résumé et Utilisation.

Onglet Résumé
:



Onglet
d'utilisation :



Modifications du collecteur/de l'acquisition :

Les modifications suivantes ont été apportées à l'unité de collecte/d'acquisition de données :

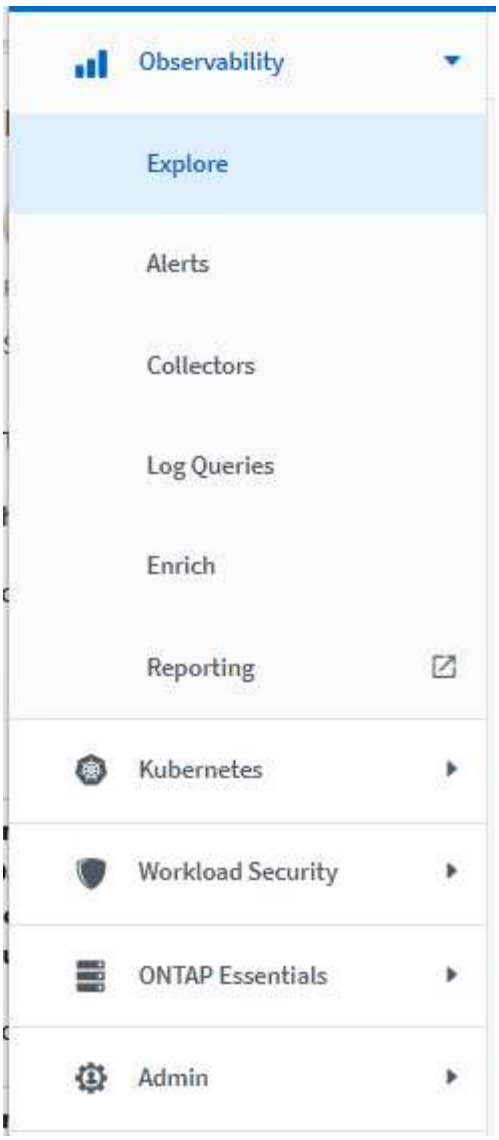
- Les unités d'acquisition prennent désormais en charge RHEL 8.7.

Menus améliorés

Nous avons mis à jour le menu de navigation de gauche pour mieux prendre en charge les flux de travail de nos clients. De nouveaux éléments de niveau supérieur tels que *Kubernetes* offrent un accès accéléré aux besoins du client, et une console d'administration consolidée prend en charge le rôle de propriétaire du locataire.

Voici quelques exemples supplémentaires de changements :

- Le menu de niveau supérieur *Observabilité* présente la découverte de données, les alertes et les requêtes de journaux
- Les fonctionnalités « Accès API » pour l'observabilité et la sécurité de la charge de travail sont regroupées dans un seul menu
- De même, pour la fonctionnalité « Notifications » d'observabilité et de sécurité de la charge de travail, désormais également sous un seul menu



Voici une brève liste des fonctionnalités que vous pouvez trouver sous chaque menu :

Observabilité :

- Explorer (tableaux de bord, requêtes de mesures, informations sur l'infrastructure)
- Alertes (moniteurs et alertes)
- Collecteurs (collecteurs de données et unités d'acquisition)
- Requêtes de journal
- Enrichir (Annotations et règles d'annotation, Applications, Résolution de périphérique)
- Rapports

Kubernetes :

- Exploration des clusters et carte du réseau

Sécurité de la charge de travail :

- Alertes

- criminalistique
- Collectionneurs
- Politiques

ONTAP Essentials :

- Protection des données
- Sécurité
- Alertes
- Infrastructure
- Réseautage
- Charges de travail *VMware

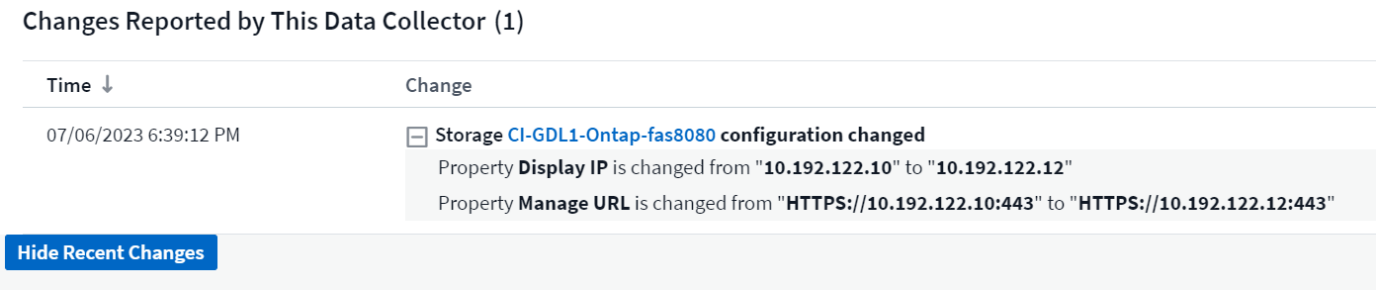
Administrateur:

- Accès API
- Audit
- Notifications
- Informations sur l'abonnement
- Gestion des utilisateurs

Juillet 2023

Afficher les modifications récentes

Les pages de destination du collecteur de données incluent désormais une liste des modifications récentes. Cliquez simplement sur le bouton « Modifications récentes » en bas de la page de destination de n'importe quel collecteur de données pour afficher les modifications récentes du collecteur de données.



Améliorations de l'opérateur

Les améliorations suivantes ont été apportées à"Opérateur Kubernetes" déploiement:

- Option pour contourner la collecte des métriques Docker
- Possibilité d'ajouter et de personnaliser les tolérances aux Daemonsets et Replicasets Telegraf

Aperçu : Récupérer les entrepôts frigorifiques

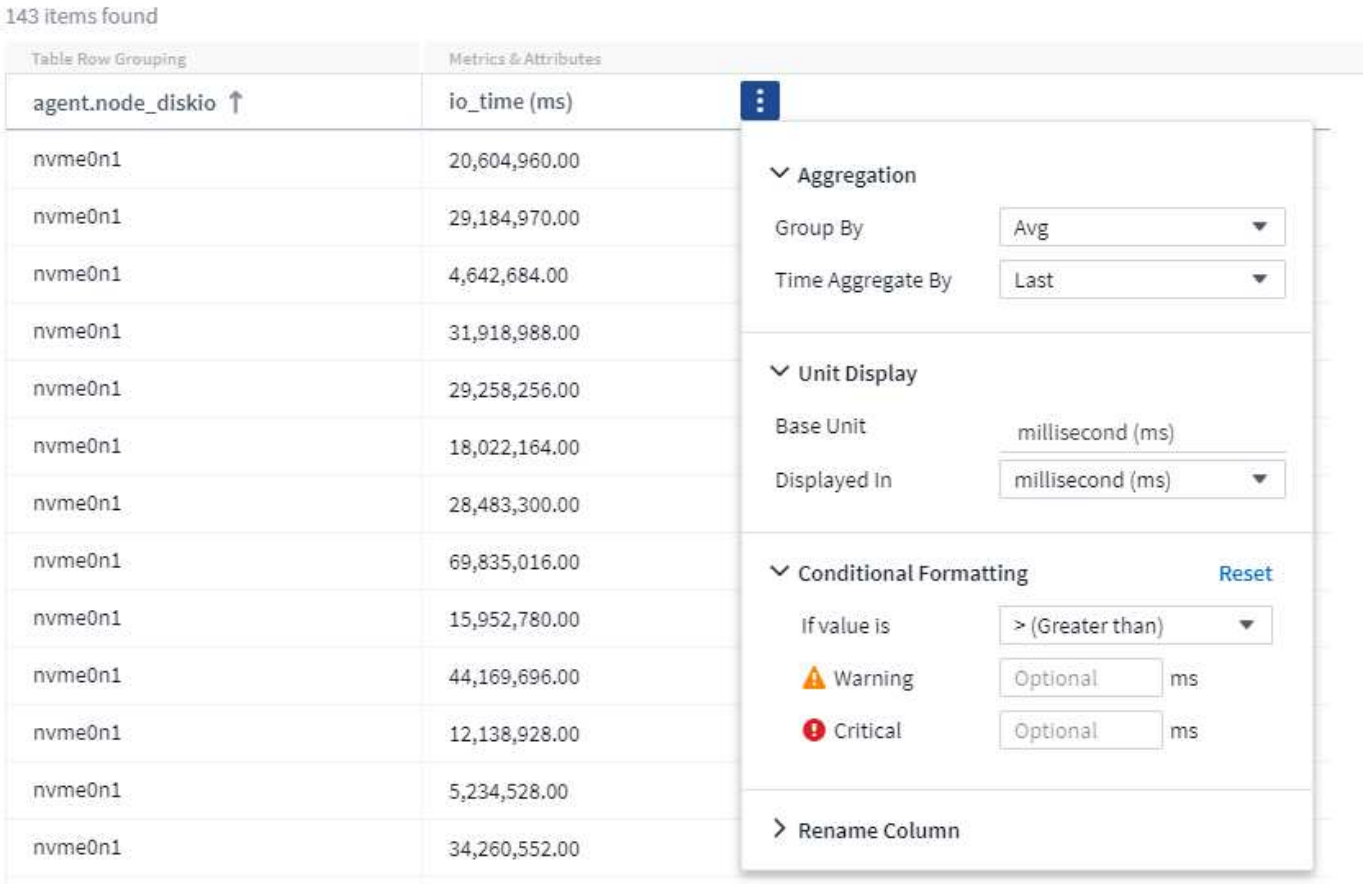
Le"Reclaim ONTAP Cold Storage Insight" prend désormais en charge FlexGroups et est désormais disponible pour tous les clients.

Signature de l'image de l'opérateur

Pour les clients qui utilisent un référentiel privé pour leur opérateur de surveillance NetApp Kubernetes, vous pouvez désormais copier la clé publique de signature d'image lors de l'installation de l'opérateur, ce qui vous permet de confirmer l'authenticité du logiciel téléchargé. Sélectionnez le bouton *Copier la clé publique de signature d'image* pendant l'étape facultative pour *Télécharger l'image de l'opérateur dans votre référentiel privé*.

Agrégation, mise en forme conditionnelle et plus pour les requêtes

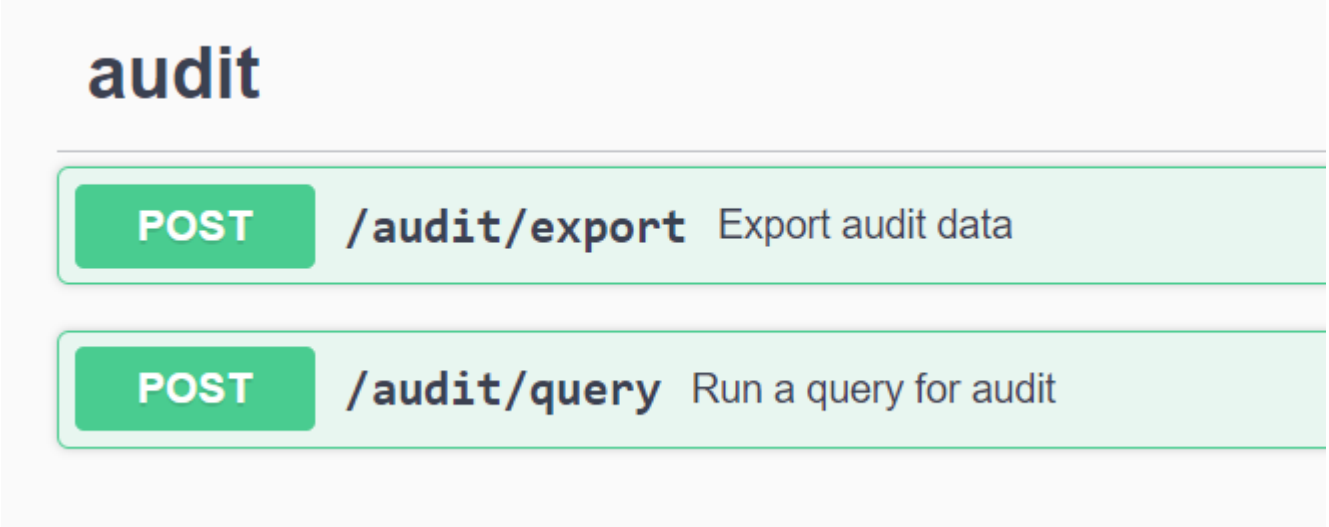
L'agrégation, la sélection d'unité, la mise en forme conditionnelle et le renommage des colonnes sont parmi les fonctionnalités les plus utiles d'un widget de tableau de bord, et ces mêmes fonctionnalités sont désormais disponibles pour"Requêtes" .



Ces fonctionnalités sont disponibles dès maintenant pour les données de type intégration (Kubernetes, ONTAP Advanced Metrics, etc.) et seront bientôt disponibles pour les objets d'infrastructure (stockage, volume, commutateur, etc.).

API pour l'audit

Vous pouvez désormais utiliser une API pour interroger ou exporter des événements audités. Accédez à Admin > Accès API et sélectionnez le lien *Documentation API* pour plus d'informations.



Collecteur de données : Trident Economy

Cloud Insights prend désormais en charge le pilote économique Trident , offrant ainsi les avantages suivants :

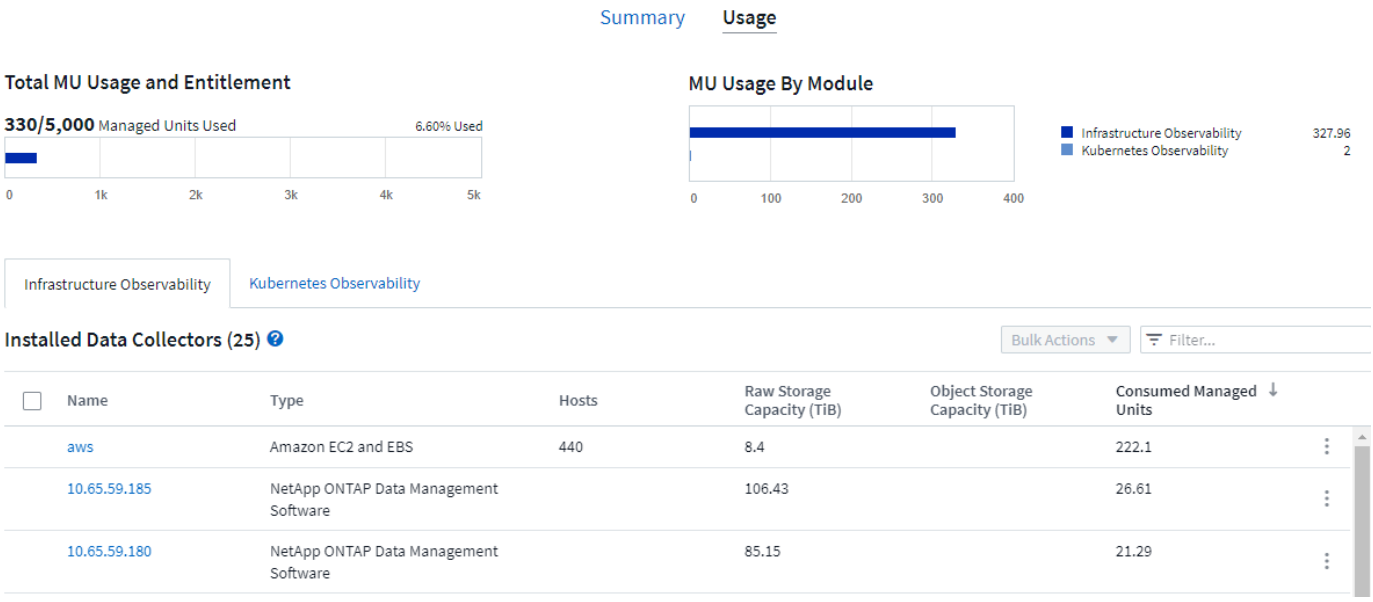
- Obtenez une visibilité sur le mappage et les mesures de performances du pod vers ONTAP Qtree.
- Offrez un dépannage transparent et une navigation facile depuis les pods Kubernetes vers le stockage backend
- Détecter de manière proactive les problèmes de performances du backend avec des moniteurs

---

Juin 2023

Vérifiez votre utilisation

À partir de juin 2023, Cloud Insights fournit une répartition de l'utilisation des unités gérées en fonction de l'ensemble de fonctionnalités. Vous pouvez désormais afficher et surveiller rapidement l'utilisation des unités gérées (MU) pour votre infrastructure ainsi que l'utilisation des MU liées à Kubernetes.



Kubernetes Network Monitoring and Map est disponible pour tous

Le"*Performances et cartographie du réseau Kubernetes*" simplifie le dépannage en mappant les dépendances entre les charges de travail Kubernetes, offrant une visibilité en temps réel sur les latences et les anomalies des performances du réseau Kubernetes pour identifier les problèmes de performances avant qu'ils n'affectent les utilisateurs. De nombreux clients l'ont trouvé utile lors de la phase d'aperçu, et il est désormais disponible pour que tout le monde puisse en profiter.

Modifications du collecteur/de l'acquisition :

Les modifications suivantes ont été apportées à l'unité de collecte/d'acquisition de données :

- Les MU Data Domain et Cohesity sont mesurés à 40 TiB : 1 MU.
- Les unités d'acquisition prennent désormais en charge RHEL et Rocky 9.0 et 9.1.

Nouveaux tableaux de bord ONTAP Essentials

Les tableaux de bord ONTAP Essentials suivants étaient disponibles dans les environnements Preview et sont désormais accessibles à tous :

- Tableau de bord de sécurité
- Tableau de bord de protection des données (comprend des aperçus de la protection locale et à distance)

Moniteurs système supplémentaires

Les moniteurs système suivants sont inclus avec Cloud Insights:

- Service FCP de la machine virtuelle de stockage indisponible
- Service iSCSI de la machine virtuelle de stockage indisponible

---

Mai 2023

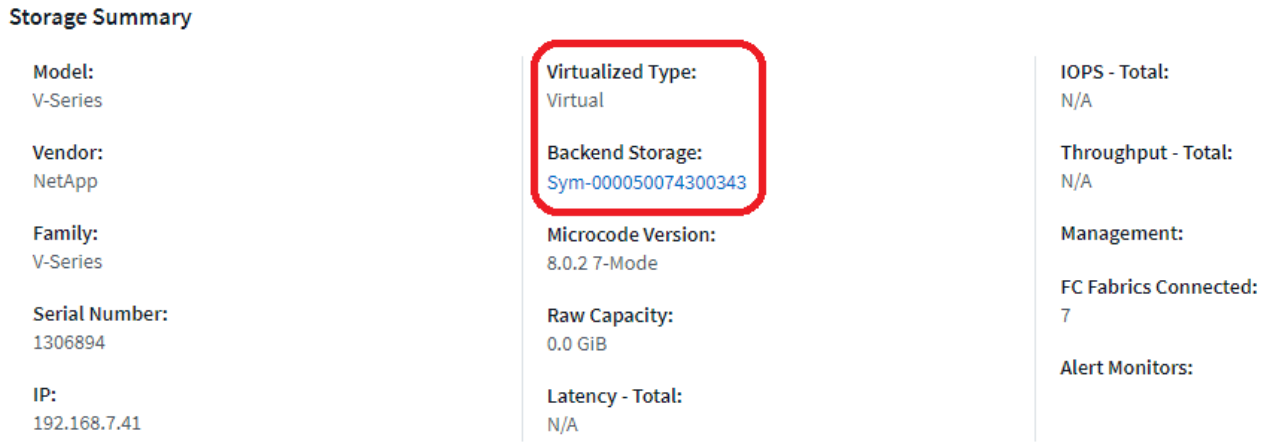
Installation améliorée de l'opérateur de surveillance Kubernetes

Installation et configuration du"Opérateur de surveillance NetApp Kubernetes" est plus facile que jamais grâce aux améliorations suivantes :

- Environnement"paramètres de configuration" sont conservés dans un fichier de configuration unique et auto-documenté.
- Instructions étape par étape pour télécharger des images de l'opérateur de surveillance Kubernetes vers votre référentiel privé.
- Simple à mettre à niveau avec une seule commande pour mettre à niveau votre surveillance Kubernetes tout en conservant les configurations personnalisées.
- Plus sécurisé : les clés API gèrent les secrets de manière sécurisée.
- Facile à intégrer et à déployer avec vos outils d'automatisation CI/CD.

Virtualisation du stockage

Cloud Insights peut faire la différence entre une baie de stockage disposant d'un stockage local ou d'une virtualisation d'autres baies de stockage. Cela vous donne la possibilité de relier les coûts et de distinguer les performances du front-end jusqu'au back-end de votre infrastructure.



Nouveaux paramètres de webhook

Lors de la création d'un"Webhook" notification, vous pouvez désormais inclure ces paramètres dans votre définition de webhook :

- %%TriggeredOnKeys%%
- %%TriggeredOnValues%%

Rapports sur les données Kubernetes

Les données Kubernetes collectées par Cloud Insights, notamment les volumes persistants (PV), les PVC, les charges de travail, les clusters et les espaces de noms, sont désormais disponibles pour une utilisation dans les rapports, permettant la rétrofacturation, les tendances, les prévisions, les calculs TTF et d'autres rapports commerciaux sur les métriques pour Kubernetes.

Moniteurs système ONTAP par défaut activés pour les nouveaux clients

De nombreux moniteurs système ONTAP sont activés (c'est-à-dire *Resumés*) par défaut dans les nouveaux environnements Cloud Insights . Auparavant, la plupart des moniteurs étaient par défaut en état *Paused*. Parce que les besoins des entreprises varient d'une entreprise à l'autre, nous vous recommandons toujours de jeter un œil à la"moniteurs système" dans votre environnement et en mettant en pause ou en reprenant chacun d'eux en fonction de vos besoins d'alerte.

Avril 2023

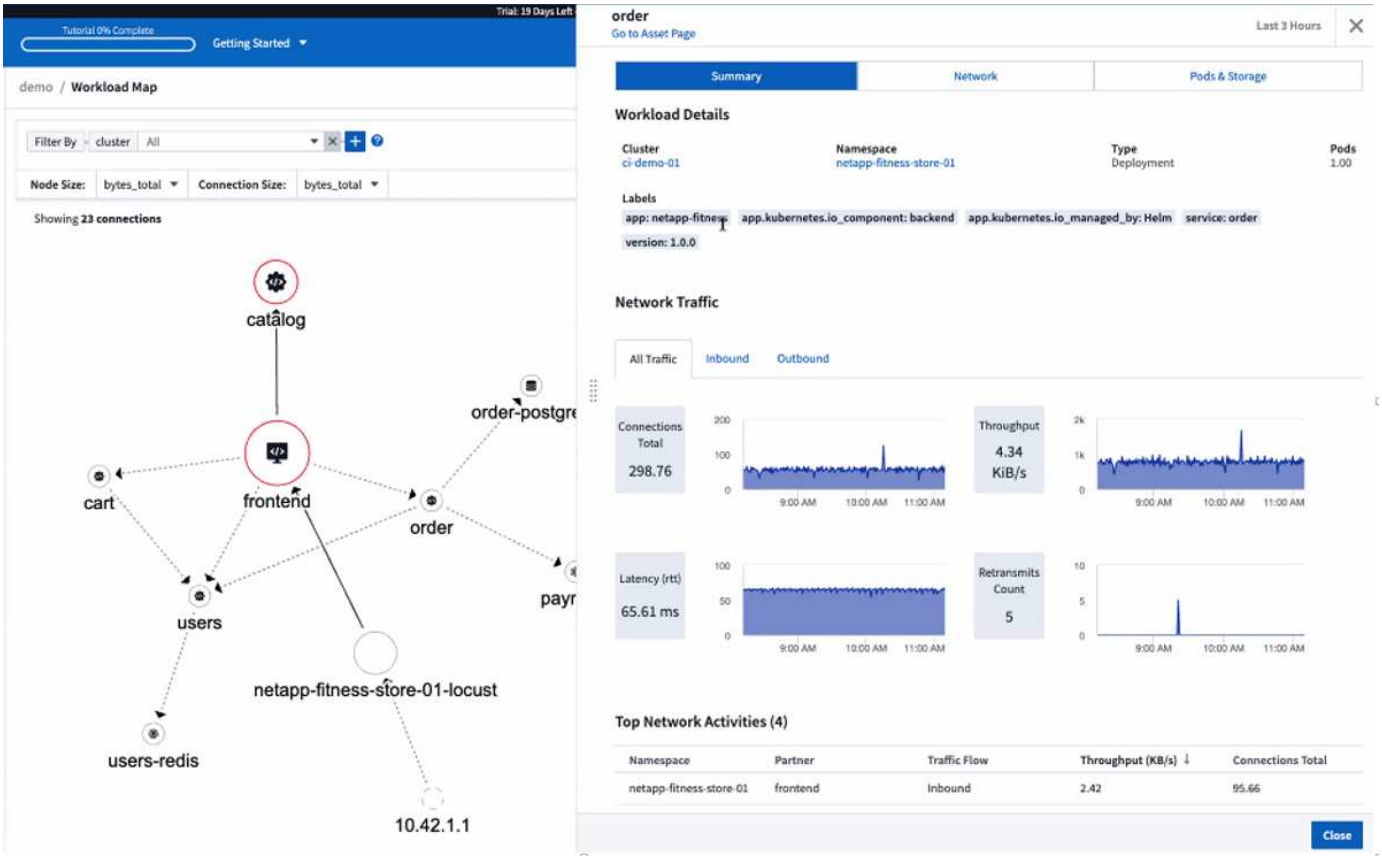
Surveillance et cartographie des performances de Kubernetes

Le"*Performances et cartographie du réseau Kubernetes*" La fonctionnalité simplifie le dépannage en mappant les dépendances entre les charges de travail Kubernetes. Il offre une visibilité en temps réel sur les latences et les anomalies des performances du réseau Kubernetes pour identifier les problèmes de performances avant qu'ils n'affectent les utilisateurs. Cette capacité aide les organisations à réduire les coûts globaux en analysant et en auditant les flux de trafic Kubernetes.

Principales fonctionnalités : • La carte de charge de travail présente les dépendances et les flux de charge de travail de Kubernetes et met en évidence les problèmes de réseau et de performances. • Surveillez le trafic

réseau entre les pods, les charges de travail et les nœuds Kubernetes ; identifiez la source des problèmes de trafic et de latence. • Réduisez les coûts globaux en analysant le trafic réseau entrant, sortant, interrégional et interzone.

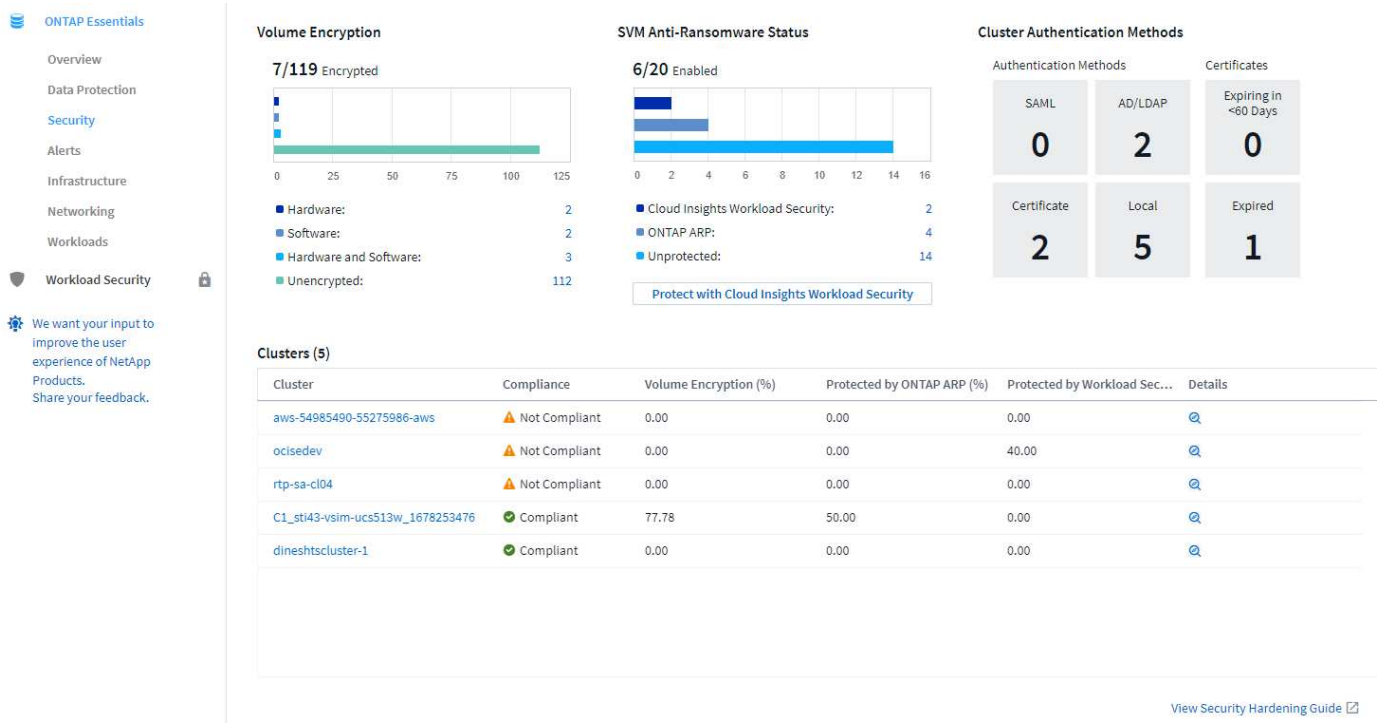
Carte de la charge de travail montrant les détails de « Slideout » :



Kubernetes Performance Monitoring and Map est disponible en tant que"Aperçu" fonctionnalité.

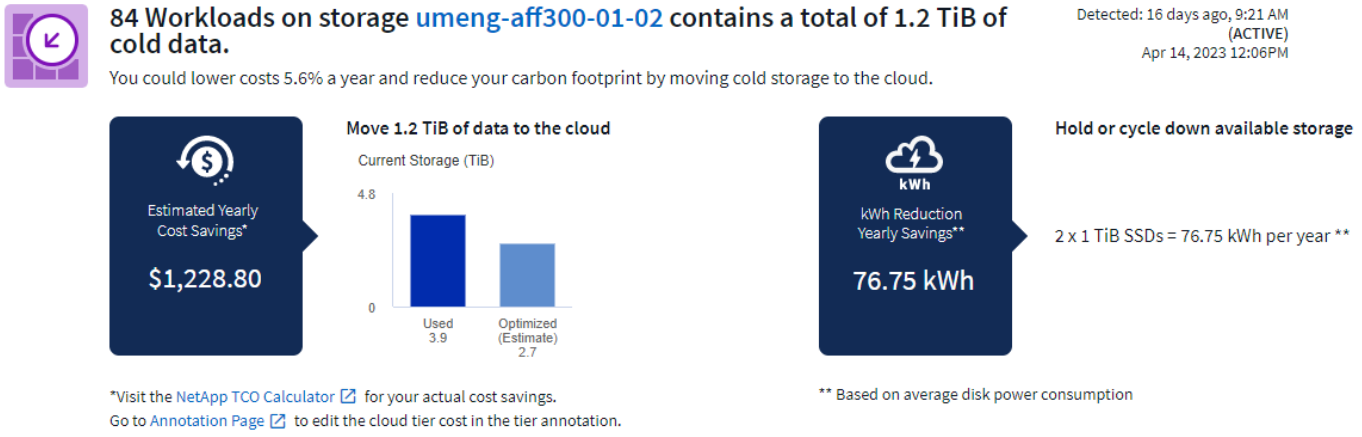
Tableau de bord de sécurité ONTAP Essentials

Le"Tableau de bord de sécurité" vous offre une vue instantanée de votre situation de sécurité actuelle, en affichant des graphiques pour le chiffrement du volume matériel et logiciel, l'état anti-ransomware et les méthodes d'authentification des clusters. Le tableau de bord de sécurité est disponible en tant que"Aperçu" fonctionnalité.



Récupérez le stockage à froid ONTAP

Reclaim ONTAP Cold Storage Insight fournit des données sur la capacité de réfrigération, les économies potentielles de coûts/d'énergie et les éléments d'action recommandés pour les volumes sur les systèmes ONTAP .



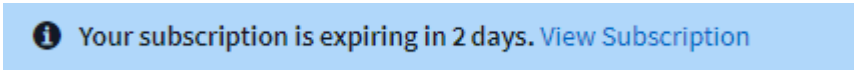
Grâce à cet aperçu, vous pouvez répondre à des questions telles que :

- Quelle quantité de données froides sur un cluster de stockage se trouve sur (a) des disques SSD coûteux, (b) des disques HDD et (c) des disques virtuels ?
- Quelles charges de travail contribuent le plus au stockage non optimisé ?
- Quelle est la durée (en jours) pendant laquelle les données sont restées froides sur une charge de travail donnée ?

Reclaim ONTAP Cold Storage est considéré comme un"*Aperçu*" fonctionnalité et est donc susceptible d'être modifiée.

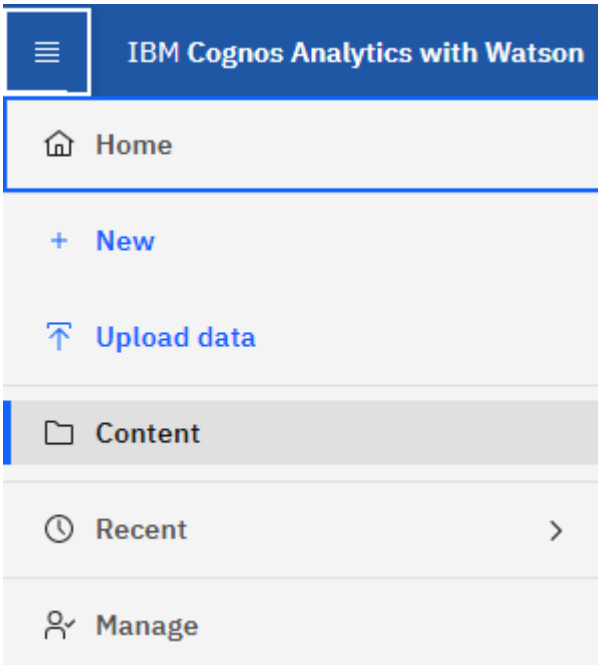
La notification d’abonnement contrôle également les messages de bannière

La définition des destinataires des notifications d’abonnement (Admin > Notifications) contrôle désormais également qui verra les notifications de bannière intégrées au produit liées à l’abonnement.



Le reporting a un nouveau look

Vous remarquerez que les écrans de rapports Cloud Insights ont une nouvelle apparence et que certaines options de navigation dans les menus ont changé. Ces écrans et modifications de navigation ont été mis à jour dans la version actuelle"Documentation de rapport" .



Moniteurs en pause par défaut

Pour les nouveaux environnements Cloud Insights , sachez que"moniteurs définis par le système" n’envoyez pas de notifications d’alerte par défaut. Vous devrez activer les notifications pour tout moniteur que vous souhaitez alerter, en ajoutant une ou plusieurs méthodes de livraison pour le moniteur. Pour les environnements Cloud Insights existants, la liste des destinataires de notification *globale* par défaut a été supprimée pour tous les moniteurs définis par le système actuellement dans l’état *En pause*. Les notifications définies par l’utilisateur restent inchangées, tout comme les paramètres de notification pour les moniteurs définis par le système actuellement actifs.

Vous recherchez l’onglet Mesure de l’API ?

Le comptage des API est passé de la page Abonnement à la page **Admin > Accès API**.

Mars 2023

Connexion Cloud pour ONTAP 9.9+ obsolète

Le collecteur de données Cloud Connection pour ONTAP 9.9+ est obsolète. À compter du 4 avril 2023, les collecteurs de données Cloud Connection de votre environnement ne collecteront plus de données et présenteront à la place une erreur lors de l'interrogation. Le collecteur de données Cloud Connection sera complètement supprimé de Cloud Insights dans une mise à jour ultérieure.

Avant le 4 avril 2023, il est obligatoire de configurer un nouveau collecteur de données du logiciel de gestion des données NetApp ONTAP pour tous les systèmes ONTAP actuellement collectés par Cloud Connection.

Janvier 2023

Nouveaux moniteurs de journaux

Nous avons ajouté près de deux douzaines"moniteurs système supplémentaires" pour alerter en cas de rupture de liens d'interconnexion, de problèmes de pulsation, etc. De plus, trois nouveaux moniteurs de journaux de protection des données ont été ajoutés pour alerter sur les modifications de SnapMirror Auto Resync, MetroCluster Mirroring et FabricPool Mirror Resync.

Notez que certains de ces moniteurs seront *activés* par défaut ; vous devez les *mettre en pause* si vous ne souhaitez pas être alerté à leur sujet. Notez également que ces moniteurs ne sont pas configurés pour envoyer des notifications ; vous devez configurer les destinataires des notifications sur ces moniteurs si vous souhaitez envoyer des alertes par e-mail ou webhook.

Exportation .CSV pour tous les widgets du tableau de bord

Garantir l'accessibilité à vos données est essentiel, c'est pourquoi nous avons rendu l'exportation .CSV disponible pour toutes les requêtes de métriques, les widgets de tableau de bord et les pages de destination d'objets, quel que soit le type de données (actif ou intégration) que vous interrogez.

Les personnalisations de données telles que la sélection de colonnes, le changement de nom des colonnes et les conversions d'unités sont désormais également incluses dans la nouvelle fonctionnalité d'exportation.

Décembre 2022

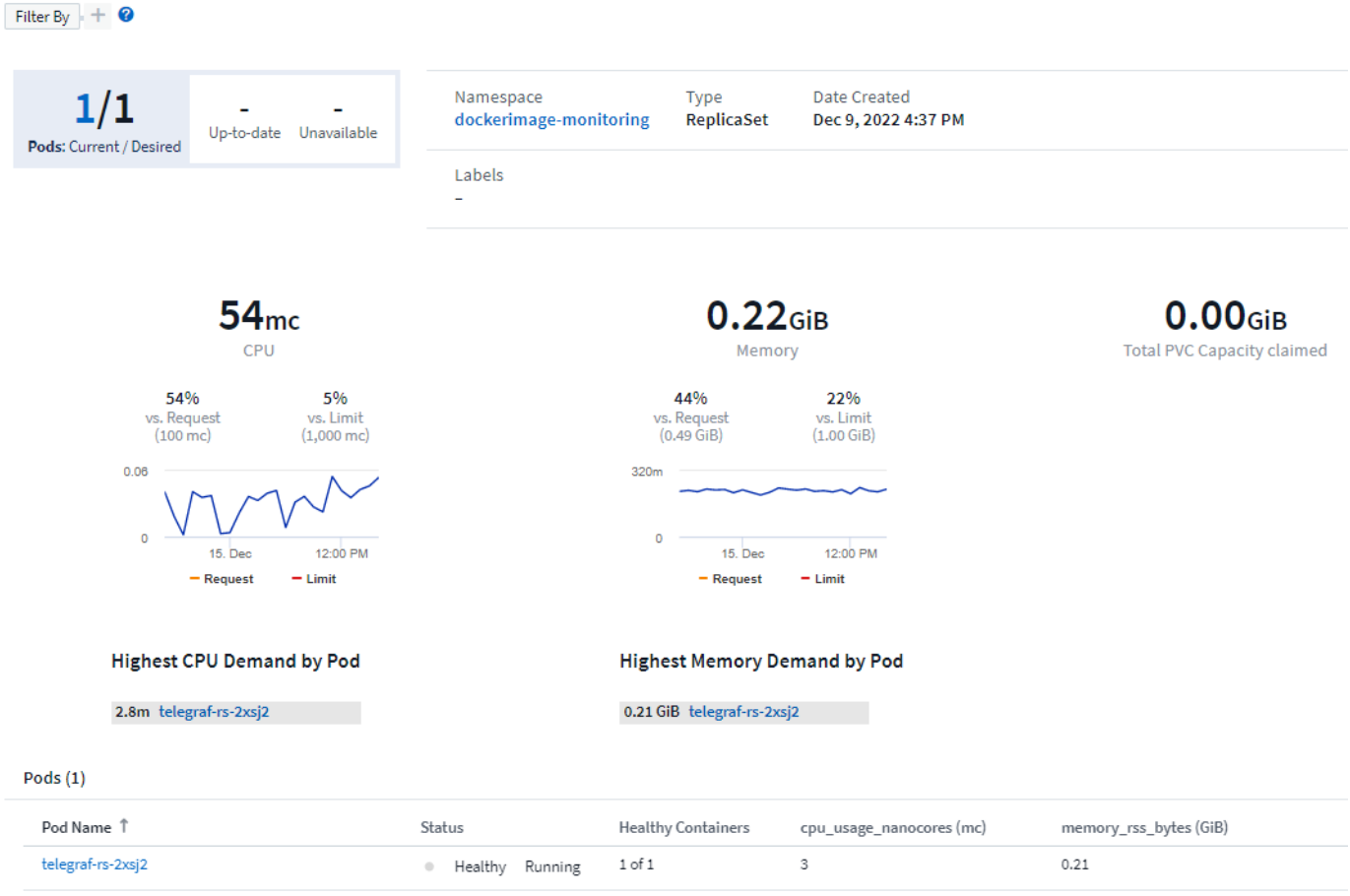
Découvrez la protection contre les ransomwares et d'autres fonctionnalités de sécurité pendant l'essai de Cloud Insights

À partir d'aujourd'hui, l'inscription à un nouvel essai de Cloud Insights vous permet d'explorer les fonctionnalités de sécurité telles que la détection des ransomwares et la politique de réponse automatisée au blocage des utilisateurs. Si vous n'êtes pas encore inscrit à votre essai, faites-le aujourd'hui !

Les charges de travail Kubernetes ont leur propre page de destination

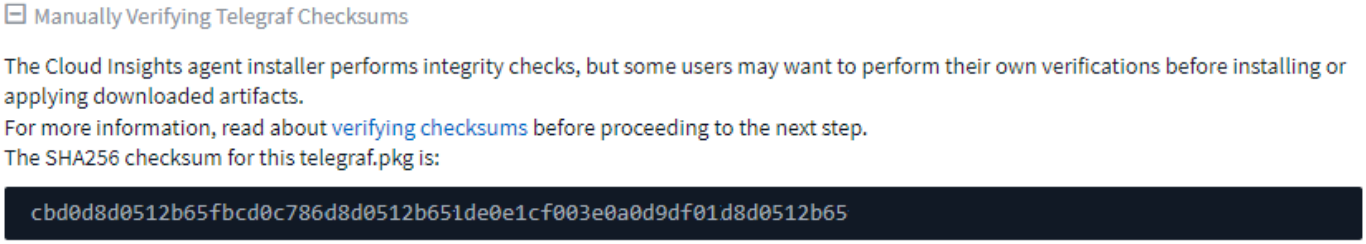
Les charges de travail sont un élément clé de votre environnement Kubernetes. Cloud Insights fournit donc désormais des pages de destination pour ces charges de travail. À partir de là, vous pouvez afficher, explorer

et résoudre les problèmes qui affectent vos charges de travail Kubernetes.



Vérifiez vos sommes de contrôle

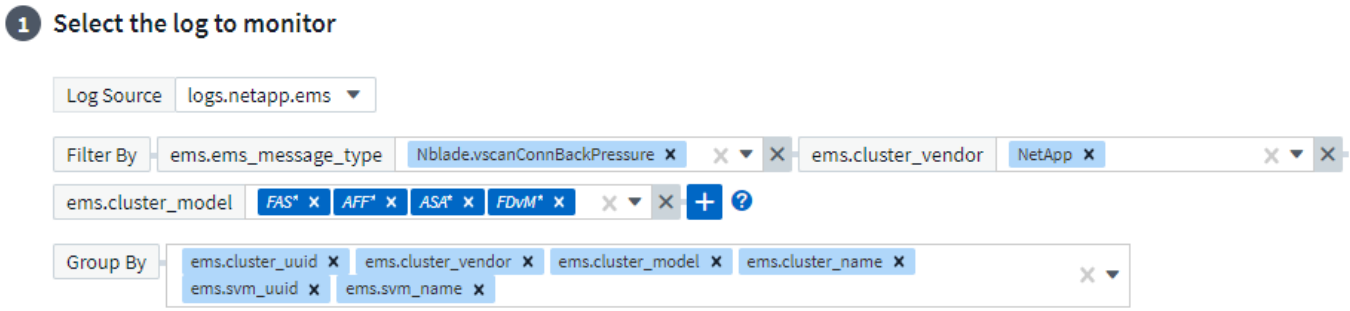
Vous nous avez demandé de vous fournir des valeurs de somme de contrôle lors de l'installation de l'agent pour Windows et Linux et nous pensons que c'est une excellente idée. Alors les voici :



Améliorations des alertes de journal

Grouper par

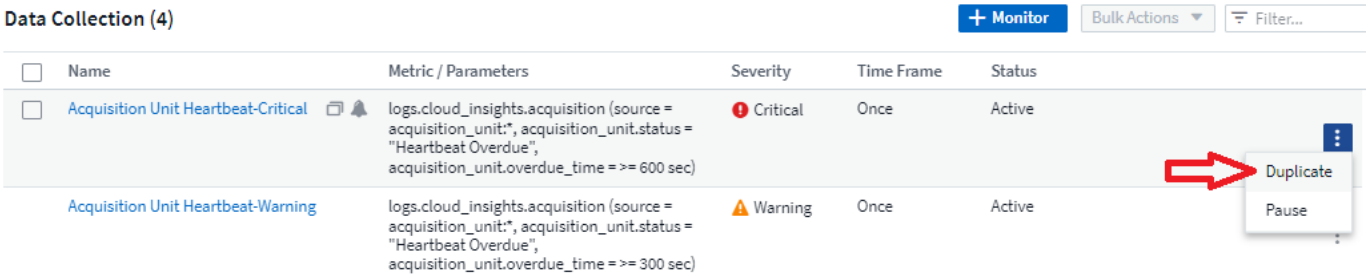
Lors de la création ou de la modification d'un moniteur de journal, vous pouvez désormais définir les attributs « Grouper par » pour permettre des alertes plus ciblées. Recherchez les attributs « Grouper par » sous les paramètres « filtre » dans la définition de votre moniteur.



Cette modification amène les moniteurs de métriques et les moniteurs de journaux à parité de fonctionnalités en normalisant l'aspect « Grouper par » des définitions de moniteur. Cette parité permettra aux clients de cloner/dupliquer **tous** les moniteurs par défaut définis par le système pour une personnalisation supplémentaire.

Duplication

Vous pouvez désormais cloner (dupliquer) les moniteurs du journal des modifications, du journal Kubernetes et du journal du collecteur de données. Cela crée un nouveau moniteur de journal personnalisé que vous pouvez modifier selon vos définitions spécifiques.



11 nouveaux moniteurs ONTAP par défaut couvrant SnapMirror pour la continuité des activités

Nous avons ajouté près d'une douzaine de nouveaux"moniteurs système" pour SnapMirror for Business Continuity (SMBC), qui alerte sur les modifications apportées aux certificats SMBC et aux médiateurs ONTAP .

Novembre 2022

Plus de 40 nouveaux moniteurs de sécurité, de collecte de données et de CVO !

Nous avons ajouté des dizaines de nouveaux moniteurs définis par le système pour vous alerter des problèmes potentiels liés aux volumes Cloud, à la sécurité et à la protection des données. En savoir plus sur ces moniteurs"ici" .

Octobre 2022

Détection de ransomwares meilleure et plus précise grâce à l'intégration d' ONTAP Autonomous Ransomware Protection

Cloud Secure améliore la détection des ransomwares grâce à l'intégration avec ONTAP"Protection autonome contre les ransomwares" (ARP).

Cloud Secure reçoit les événements ONTAP ARP sur l'activité potentielle de chiffrement de fichiers de volume, et

- Met en corrélation les événements de chiffrement de volume avec l'activité de l'utilisateur pour identifier qui cause les dommages,
- Met en œuvre des politiques de réponse automatique pour bloquer l'attaque,
- Identifie les fichiers affectés, contribuant ainsi à une récupération plus rapide et à la conduite d'enquêtes sur les violations de données.

Septembre 2022

Moniteurs disponibles en édition de base

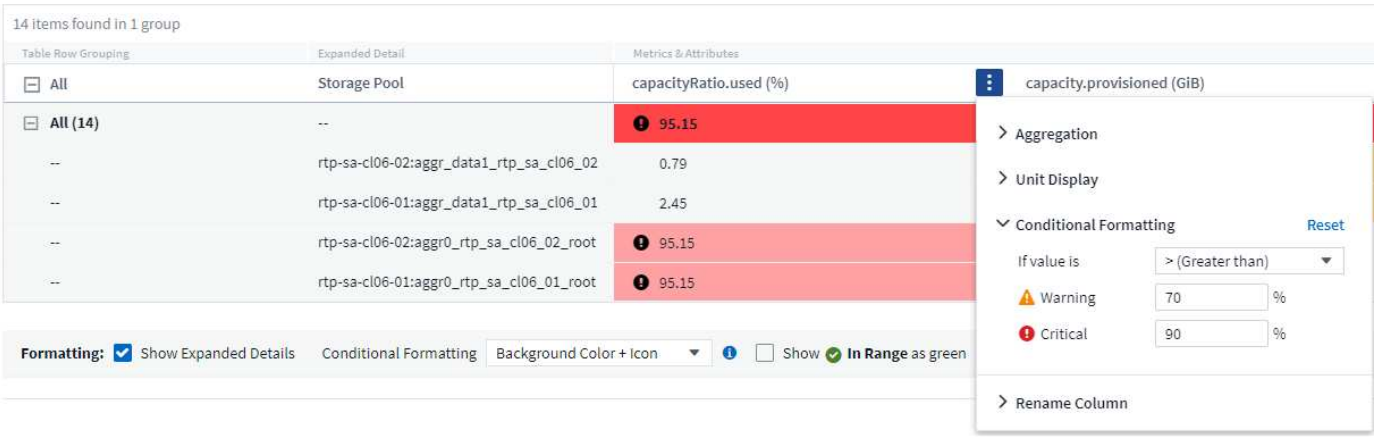
ONTAP"Moniteurs par défaut" désormais disponible pour une utilisation dans Cloud Insights Basic Edition. Cela comprend plus de 70 moniteurs d'infrastructure et 30 exemples de charge de travail.

Tableaux de bord ONTAP Power et StorageGRID

La galerie de tableaux de bord comprend un nouveau tableau de bord pour ONTAP Power et Temperature ainsi que quatre tableaux de bord pour StorageGRID. Si votre environnement collecte des mesures d'alimentation ONTAP et/ou des données StorageGRID , importez ces tableaux de bord en sélectionnant **+Depuis la galerie**.

Visibilité des seuils en un coup d'œil dans les tableaux

La mise en forme conditionnelle vous permet de définir et de mettre en évidence les seuils de niveau d'avertissement et de niveau critique dans les widgets de tableau, offrant une visibilité instantanée sur les valeurs aberrantes et les points de données exceptionnels.

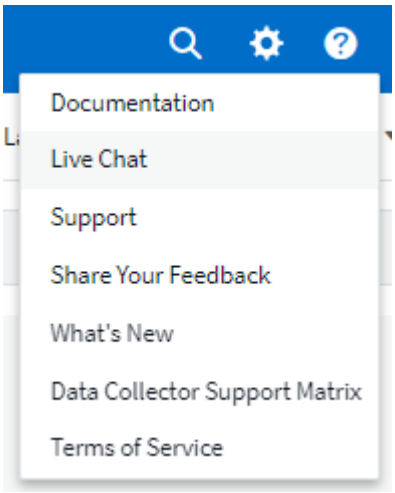


Moniteur de sécurité

Cloud Insights peut vous alerter lorsqu'il détecte que le mode FIPS est désactivé sur le système ONTAP . En savoir plus sur"Moniteurs système" , et surveillez cet espace pour plus de moniteurs de sécurité, à venir bientôt !

Discutez de n'importe où

Discutez avec un spécialiste du support NetApp depuis n'importe quel écran Cloud Insights en sélectionnant le nouveau lien **Aide > Chat en direct**. L'aide est disponible à partir de l'icône « ? » en haut à droite de l'écran.



Des informations plus visibles

Si votre environnement connaît une"Aperçu" comme *Ressources partagées sous stress* ou *Espaces de noms Kubernetes à court d'espace*, les pages de destination des ressources affectées incluent désormais des liens vers l'Insight lui-même, offrant une exploration et un dépannage plus rapides.

Nouveaux collecteurs de données

- Amazon S3 (disponible en version préliminaire)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Autres mises à jour du collecteur de données

Toutes les sources de données sont désormais optimisées pour reprendre l'interrogation des performances après les mises à jour et/ou les correctifs de l'unité d'acquisition.

Prise en charge du système d'exploitation

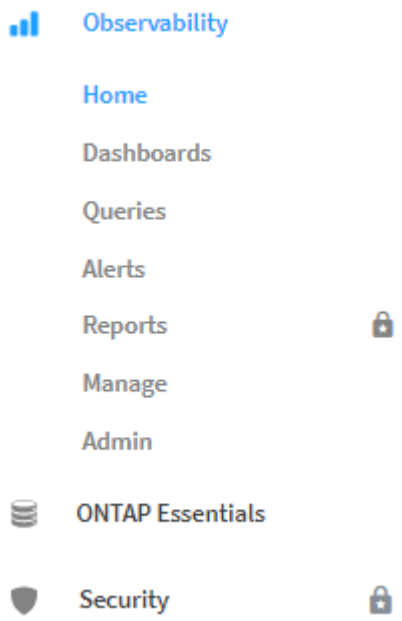
Les systèmes d'exploitation suivants sont pris en charge avec les unités d'acquisition Cloud Insights , en plus de ceux"déjà pris en charge" :

- Red Hat Enterprise Linux 8.5, 8.6

Août 2022

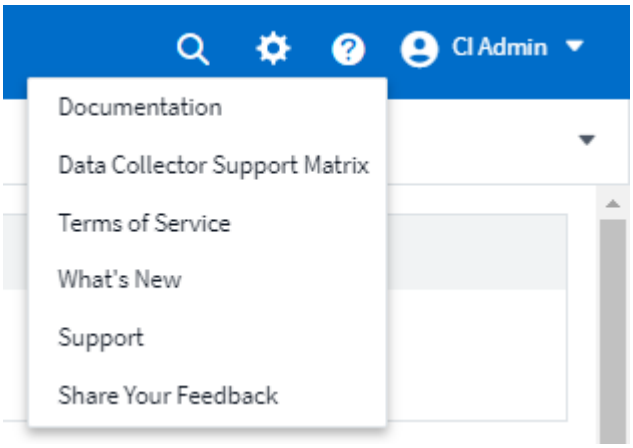
Cloud Insights a un nouveau look !

À partir de ce mois-ci, « Surveiller et optimiser » a été renommé **Observabilité**. Vous trouverez ici toutes vos fonctionnalités préférées telles que les tableaux de bord, les requêtes, les alertes et les rapports. De plus, recherchez Cloud Secure dans le nouveau menu **Sécurité**. Notez que seuls les menus ont changé ; les fonctionnalités restent les mêmes.



Vous recherchez le menu **Aide** ?

L'aide se trouve désormais dans le coin supérieur droit de l'écran.

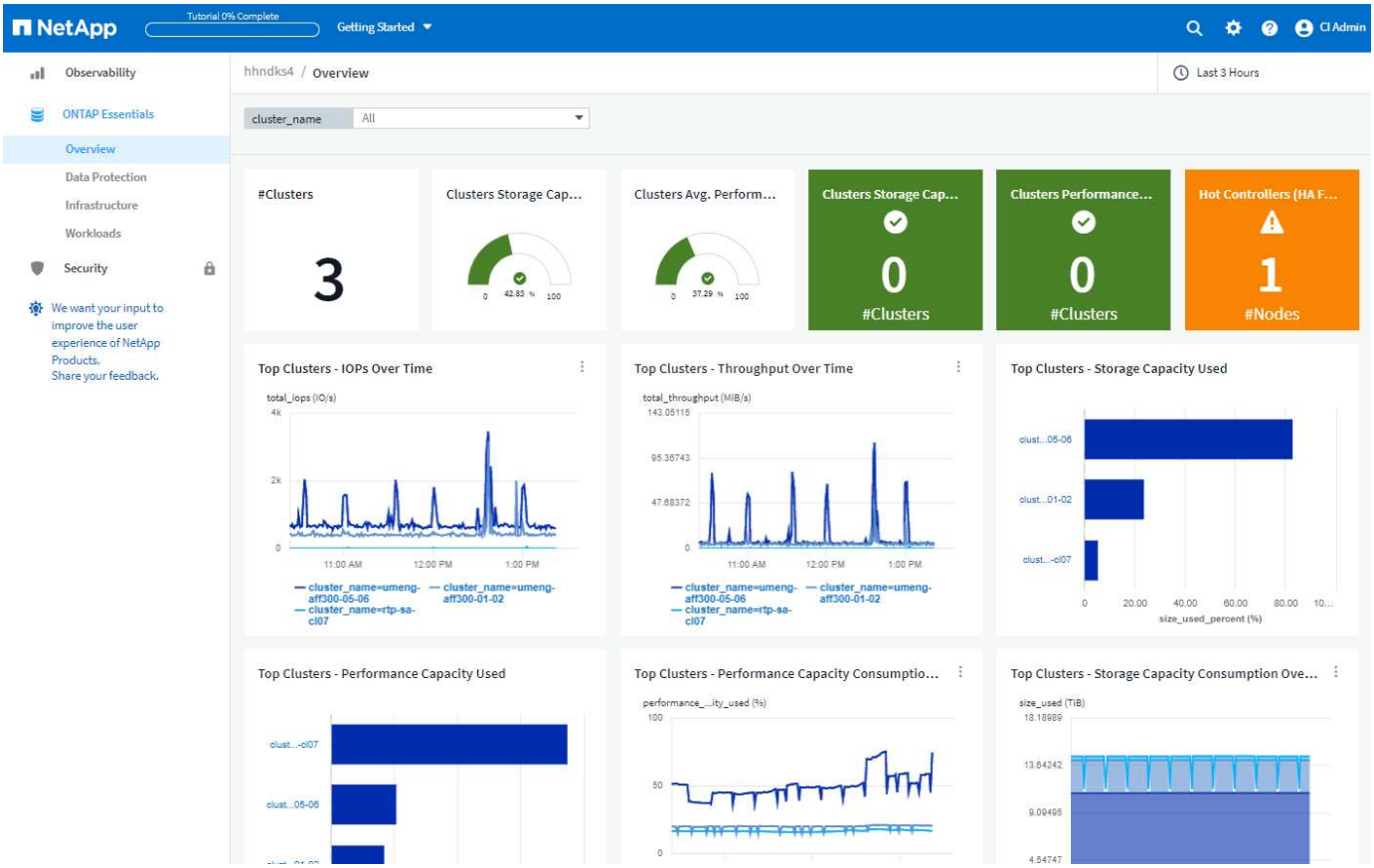


Vous ne savez pas par où commencer ? Découvrez ONTAP Essentials !

"* ONTAP Essentials *"est un ensemble de tableaux de bord et de flux de travail qui fournissent des vues détaillées sur vos inventaires, charges de travail et protection des données NetApp ONTAP , y compris des prévisions de jours à pleine capacité pour la capacité de stockage et les performances. Vous pouvez même voir si des contrôleurs fonctionnent à un niveau d'utilisation élevé. ONTAP Essentials est l'endroit idéal pour

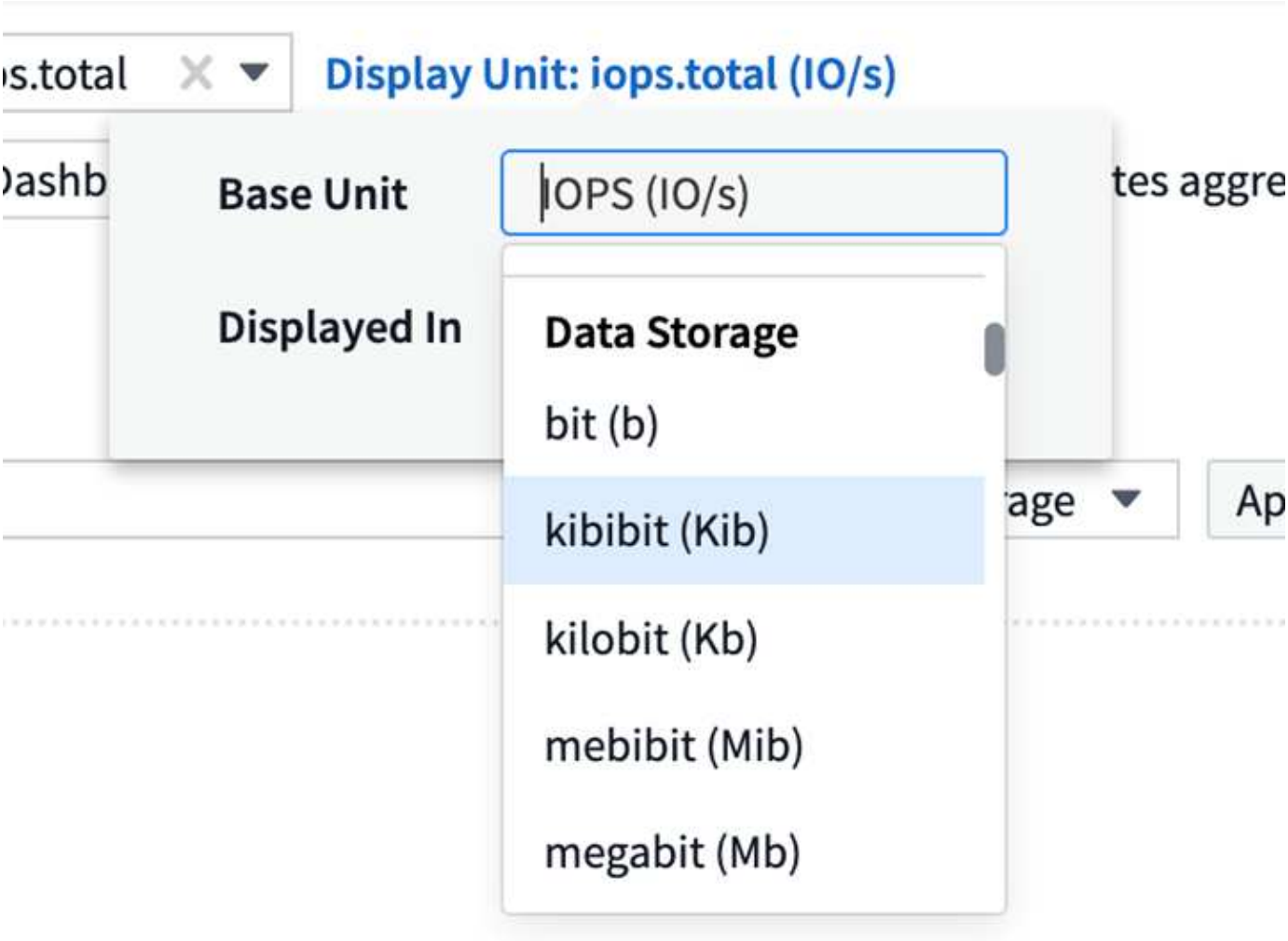
tous vos besoins de surveillance NetApp ONTAP !

ONTAP Essentials, disponible dans toutes les éditions, est conçu pour être intuitif pour les opérateurs et administrateurs ONTAP existants, facilitant la transition d'ActiveIQ Unified Manager vers des outils de gestion basés sur les services.



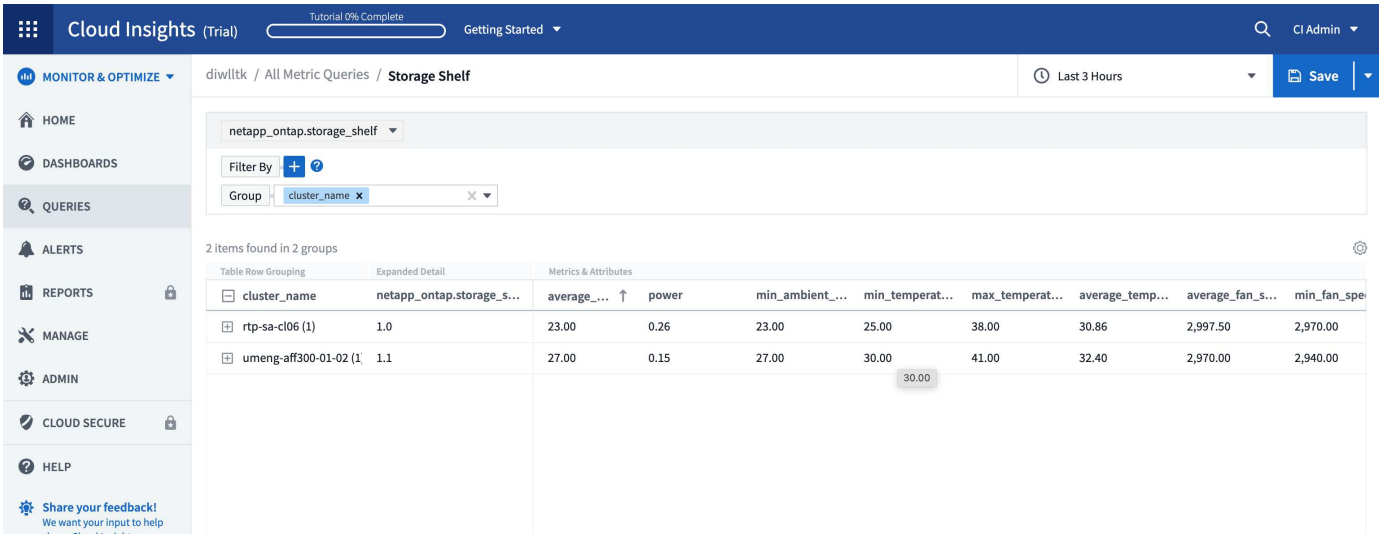
Les familles de données de stockage sont fusionnées

Vous l'avez demandé, et maintenant vous l'avez. Les unités de données de stockage de base 2 et de base 10 sont désormais combinées en une seule famille, des bits et octets aux tébibits et téraoctets, ce qui facilite l'affichage des données à votre façon sur vos tableaux de bord. Les débits de données constituent désormais également une grande famille à part entière.



Quelle est la quantité d'énergie utilisée par mon système de stockage ?

Affichez et surveillez la consommation électrique, la température et la vitesse du ventilateur de votre étagère de stockage et de votre nœud ONTAP , à l'aide des mesures netapp_ontap.storage_shelf, netapp_ontap.system_node et netapp_ontap.cluster (consommation électrique uniquement).



Fonctionnalités graduées à partir de l'aperçu

Les fonctionnalités suivantes ont été retirées de la version Preview et sont désormais disponibles pour tous les clients :

Fonctionnalité	Description
Les espaces de noms Kubernetes manquent d'espace	L'aperçu *Kubernetes Namespaces Running Out of Space* vous donne un aperçu des charges de travail sur vos espaces de noms Kubernetes qui risquent de manquer d'espace, avec une estimation du nombre de jours restants avant que chaque espace ne soit plein."En savoir plus"
Ressource partagée sous pression	L'analyse *Shared Resource Under Stress* utilise l'IA/ML pour identifier automatiquement où la contention des ressources entraîne une dégradation des performances dans votre environnement, met en évidence les charges de travail affectées par celle-ci et fournit des actions recommandées pour y remédier, vous permettant de résoudre les problèmes de performances plus rapidement."En savoir plus"
Cloud Secure – Bloquer l'accès des utilisateurs en cas d'attaque	Une meilleure protection pour vos données critiques pour votre entreprise avec la possibilité de bloquer l'accès des utilisateurs lorsqu'une attaque est détectée. L'accès peut être bloqué automatiquement, à l'aide de politiques de réponse automatisées, ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur."En savoir plus"

Comment se porte ma collecte de données ?

Cloud Insights fournit deux nouveaux moniteurs de pulsation pour vos unités d'acquisition, ainsi que deux moniteurs pour vous alerter des défaillances du collecteur de données. Ils peuvent être utilisés pour vous alerter rapidement des problèmes de collecte de données.

Les moniteurs suivants sont désormais disponibles dans le groupe de moniteurs *Data Collect* :

- Unité d'acquisition Heartbeat-Critical
- Avertissement de battement de cœur de l'unité d'acquisition
- Échec du collecteur
- Avertissement aux collectionneurs

Notez que ces moniteurs sont dans l'état *Paused* par défaut. Activez-les pour être alerté des problèmes de collecte de données.

Jetons API à renouvellement automatique

Les jetons d'accès API peuvent désormais être définis pour le renouvellement automatique. En activant cette fonctionnalité, de nouveaux jetons d'accès API/actualisés seront automatiquement générés pour les jetons expirant. Les agents Cloud Insights utilisant un jeton expirant seront automatiquement mis à jour pour utiliser le jeton d'accès API nouveau/actualisé correspondant, leur permettant de continuer à fonctionner de manière transparente. Cochez simplement la case « Renouveler le jeton automatiquement » lors de la création de votre

jeton. Cette fonctionnalité est actuellement prise en charge sur les agents Cloud Insights exécutés sur la plateforme Kubernetes avec le dernier opérateur de surveillance NetApp Kubernetes.

L'édition de base vous offre plus qu'avant

Votre essai se termine mais vous n'êtes pas encore sûr qu'un abonnement vous convienne ? L'édition de base vous a toujours donné la possibilité de continuer à utiliser Cloud Insights avec votre collecteur de données ONTAP actuel, mais vous pouvez désormais continuer à capturer également les données de version, de topologie et d'IOPS/débit/latence de VMWare. Les clients NetApp disposant d'un support premium sur leurs systèmes de stockage auront également droit au support pour Cloud Insights.

Prêt à en savoir plus ?

Consultez la section **Centre d'apprentissage** de la page Aide > Support pour obtenir des liens vers les offres de cours NetApp University Cloud Insights !

Prise en charge du système d'exploitation

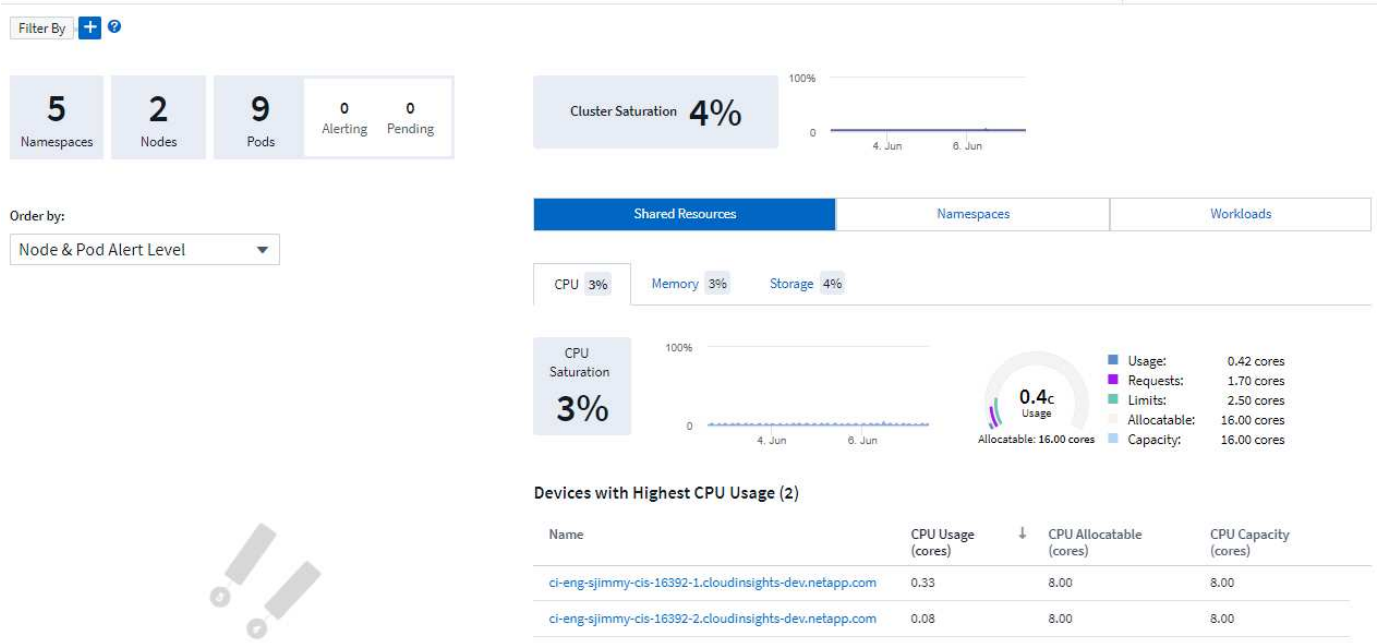
Le système d'exploitation suivant est pris en charge avec les unités d'acquisition Cloud Insights , en plus de ceux"déjà pris en charge" :

- Windows 11

Juin 2022

Saturation du cluster Kubernetes et autres détails

Cloud Insights facilite plus que jamais l'exploration de votre environnement Kubernetes, avec une page de détails de cluster améliorée qui fournit des détails de saturation ainsi qu'une vue plus claire des espaces de noms et des charges de travail.

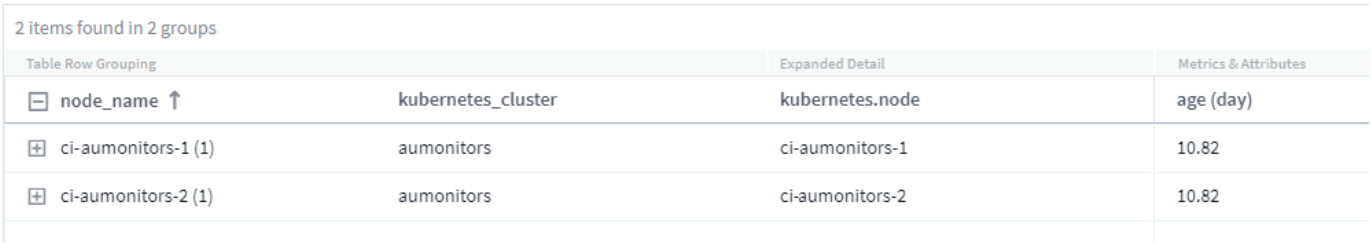


La page de liste des clusters vous donne également un aperçu rapide de la saturation, en plus des nombres de nœuds, de pods, d'espaces de noms et de charges de travail :

Name	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

Quel âge a votre cluster Kubernetes ?

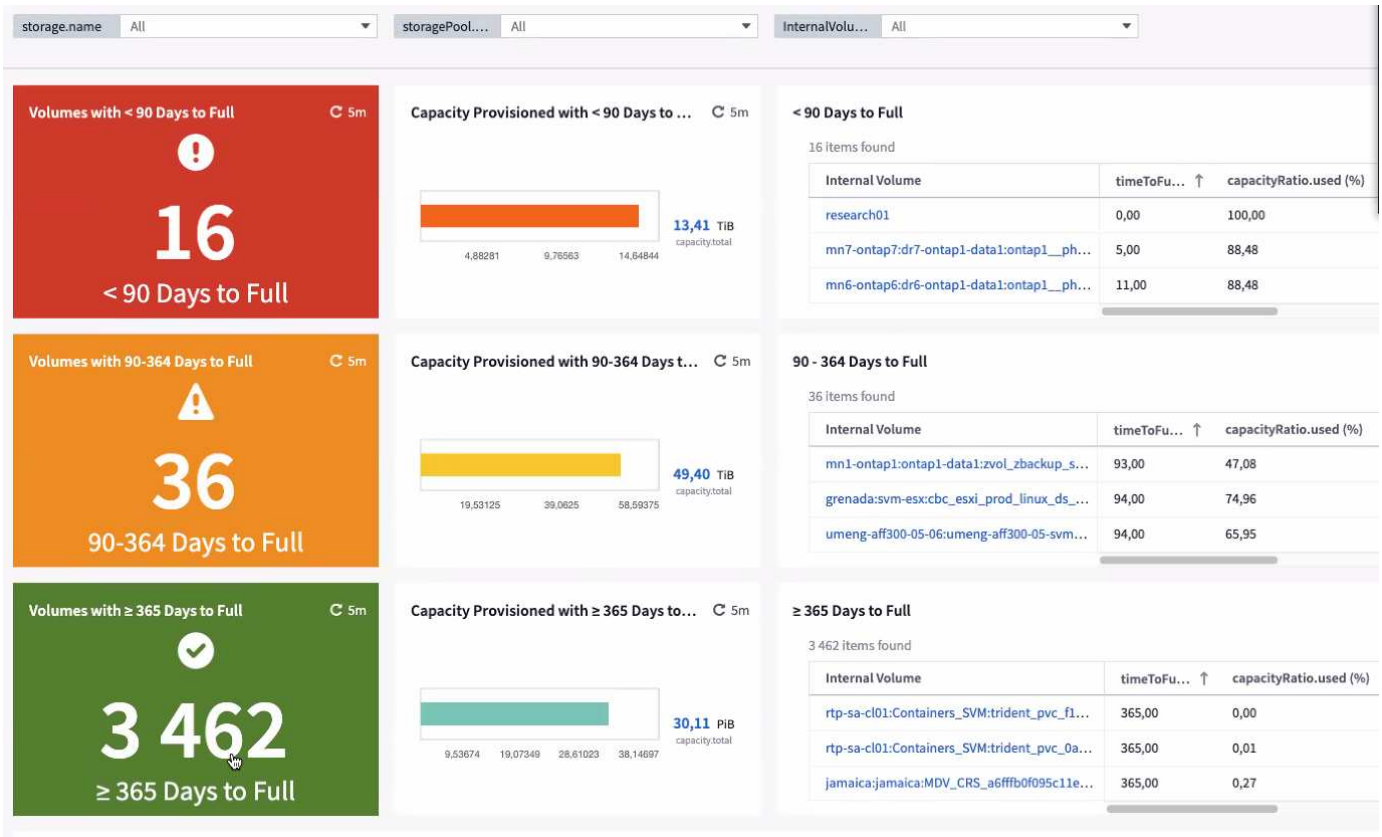
Votre cluster débute-t-il dans le monde ou a-t-il connu une longue vie numérique ? *Age* a été ajouté comme mesure de temps collectée pour les nœuds Kubernetes.



node_name	kubernetes_cluster	kubernetes.node	age (day)
ci-aumonitors-1 (1)	aumonitors	ci-aumonitors-1	10.82
ci-aumonitors-2 (1)	aumonitors	ci-aumonitors-2	10.82

Prévision du temps de remplissage de la capacité

Cloud Insights fournit un tableau de bord permettant de prévoir le nombre de jours jusqu'à ce que la capacité soit épuisée pour chaque volume interne surveillé. Ces valeurs peuvent contribuer à réduire considérablement le risque de panne.

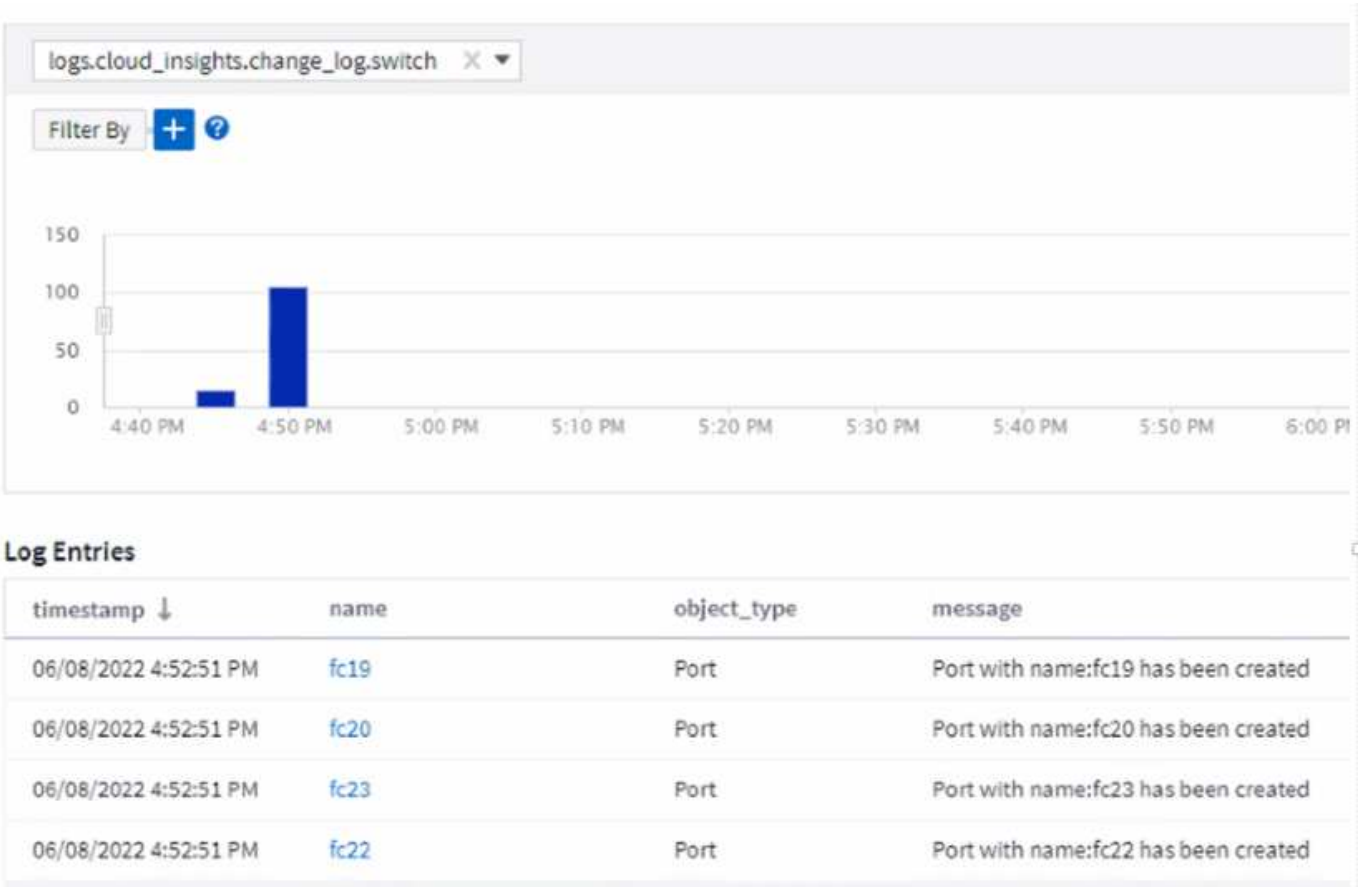


Les compteurs TTF sont également disponibles pour le stockage, le pool de stockage et le volume. Continuez à surveiller cet espace pour des tableaux de bord supplémentaires pour ces objets.

Notez que les prévisions de délai d'exécution ne sont plus disponibles dans *Preview* et seront déployées auprès de tous les clients.

Qu'est-ce qui a changé dans mon environnement ?

Les entrées du journal des modifications ONTAP peuvent être visualisées dans l'explorateur de journaux.



Prise en charge du système d'exploitation

Les systèmes d'exploitation suivants sont pris en charge avec les unités d'acquisition Cloud Insights , en plus de ceux"déjà pris en charge" :

- CentOS Stream 9
- Windows 2022

Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration Telegraf a été mis à jour vers la version **1.22.3**, avec des améliorations de performances et de sécurité. Les utilisateurs souhaitant effectuer une mise à jour peuvent se référer à la section de mise à niveau appropriée du"Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans aucune action de l'utilisateur requise.

Fonctionnalités d'aperçu

Cloud Insights met régulièrement en avant un certain nombre de nouvelles fonctionnalités d'aperçu intéressantes. Si vous souhaitez découvrir en avant-première une ou plusieurs de ces fonctionnalités, contactez votre"Équipe commerciale NetApp" pour plus d'informations.

Fonctionnalité	Description

Les espaces de noms Kubernetes manquent d'espace	L'aperçu *Kubernetes Namespaces Running Out of Space* vous donne un aperçu des charges de travail sur vos espaces de noms Kubernetes qui risquent de manquer d'espace, avec une estimation du nombre de jours restants avant que chaque espace ne soit plein."En savoir plus"
Cloud Secure – bloquer l'accès des utilisateurs en cas d'attaque	Une meilleure protection pour vos données critiques pour votre entreprise avec la possibilité de bloquer l'accès des utilisateurs lorsqu'une attaque est détectée. L'accès peut être bloqué automatiquement, à l'aide de politiques de réponse automatisées ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur."En savoir plus"
Ressource partagée sous pression	L'analyse *Shared Resource Under Stress* utilise l'IA/ML pour identifier automatiquement où la contention des ressources entraîne une dégradation des performances dans votre environnement, met en évidence les charges de travail affectées par celle-ci et fournit des actions recommandées pour y remédier, vous permettant de résoudre les problèmes de performances plus rapidement."En savoir plus"

Mai 2022

Discutez en direct avec le support NetApp

Vous pouvez désormais discuter en direct avec le personnel du support NetApp ! Sur la page Aide > Assistance, cliquez simplement sur l'icône Chat ou cliquez sur *Chat* dans la section « Contactez-nous » pour démarrer une session de chat. L'assistance par chat est disponible les jours ouvrables aux États-Unis pour les utilisateurs des éditions Standard et Premium.

Opérateur Kubernetes

Nous avons simplifié votre mise en service avec la surveillance avancée de Kubernetes et l'explorateur de clusters de Cloud Insights.

Le"Opérateur de surveillance Kubernetes" (NKMO) est la méthode préférée pour l'installation de Kubernetes pour Cloud Insights Insights, pour une configuration plus flexible de la surveillance en moins d'étapes, ainsi que des opportunités améliorées de surveillance d'autres logiciels exécutés dans le cluster K8s.

Cliquez sur le lien ci-dessus pour plus d'informations et les prérequis

Gérer les utilisateurs et les invitations avec l'API

Vous pouvez désormais gérer les utilisateurs et les invitations à l'aide de la puissante API de Cloud Insights. En savoir plus dans le"Documentation de l'API Swagger" .

Alertes de collecte de données

Ne manquez pas de mesures critiques en raison d'un collecteur défaillant !

Il est plus facile que jamais de suivre vos collecteurs de données grâce aux nouveaux"alertes" pour les pannes des collecteurs de données et des unités d'acquisition. Notez que ces moniteurs sont *en pause* par défaut. Pour l'activer, accédez à la page de vos moniteurs et recherchez et reprenez « Arrêt de l'unité d'acquisition » et « Échec du collecteur ».

Alerte sur les modifications du stockage ONTAP

Ne laissez pas des changements de stockage inattendus entraîner des pannes !

Vous pouvez désormais configurer Cloud Insights pour alerter lorsque la modification ou la suppression de FlexVols, de nœuds et de SVM est détectée sur les systèmes ONTAP .

Fonctionnalités d'aperçu

Cloud Insights met régulièrement en avant un certain nombre de nouvelles fonctionnalités d'aperçu intéressantes. Si vous souhaitez découvrir en avant-première une ou plusieurs de ces fonctionnalités, contactez votre"Équipe commerciale NetApp" pour plus d'informations.

Fonctionnalité	Description
Les espaces de noms Kubernetes manquent d'espace	L'aperçu *Kubernetes Namespaces Running Out of Space* vous donne un aperçu des charges de travail sur vos espaces de noms Kubernetes qui risquent de manquer d'espace, avec une estimation du nombre de jours restants avant que chaque espace ne soit plein."En savoir plus"
Prévisions du volume interne et du temps de remplissage de la capacité volumique	Cloud Insights est capable de prédire le nombre de jours jusqu'à ce que la capacité soit épuisée pour chaque volume interne et volume surveillé. Cette valeur peut contribuer à réduire considérablement le risque de panne.
Cloud Secure – bloquer l'accès des utilisateurs en cas d'attaque	Une meilleure protection pour vos données critiques pour votre entreprise avec la possibilité de bloquer l'accès des utilisateurs lorsqu'une attaque est détectée. L'accès peut être bloqué automatiquement, à l'aide de politiques de réponse automatisées ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur."En savoir plus"

Ressource partagée sous pression	L'analyse *Shared Resource Under Stress* utilise l'IA/ML pour identifier automatiquement où la contention des ressources entraîne une dégradation des performances dans votre environnement, met en évidence les charges de travail affectées par celle-ci et fournit des actions recommandées pour y remédier, vous permettant de résoudre les problèmes de performances plus rapidement."En savoir plus"

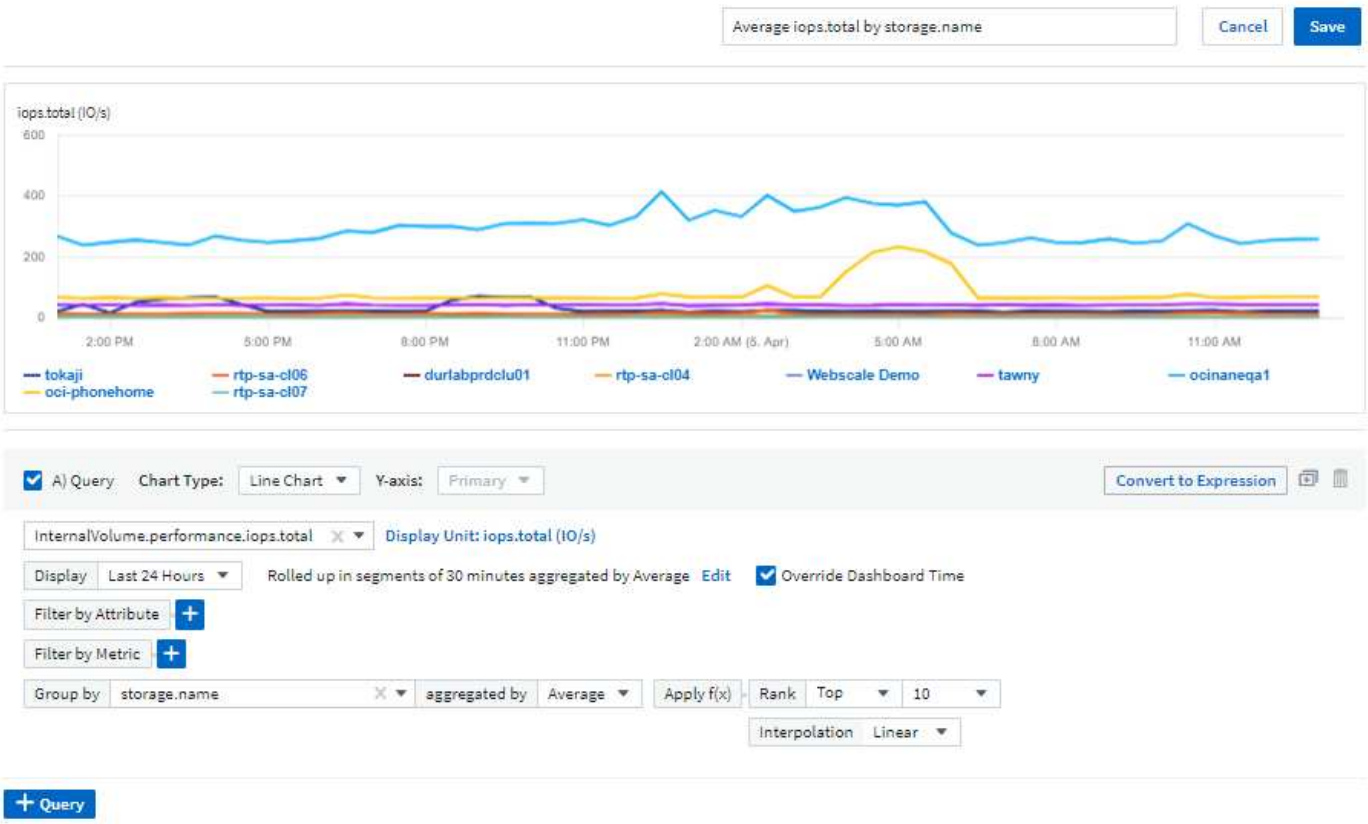
Avril 2022

Partagez vos commentaires!

Nous souhaitons votre contribution pour nous aider à façonner Cloud Insights. Gagnez des points et des prix en participant au programme **Insights to Action** de NetApp. **"Inscrivez-vous maintenant"** !

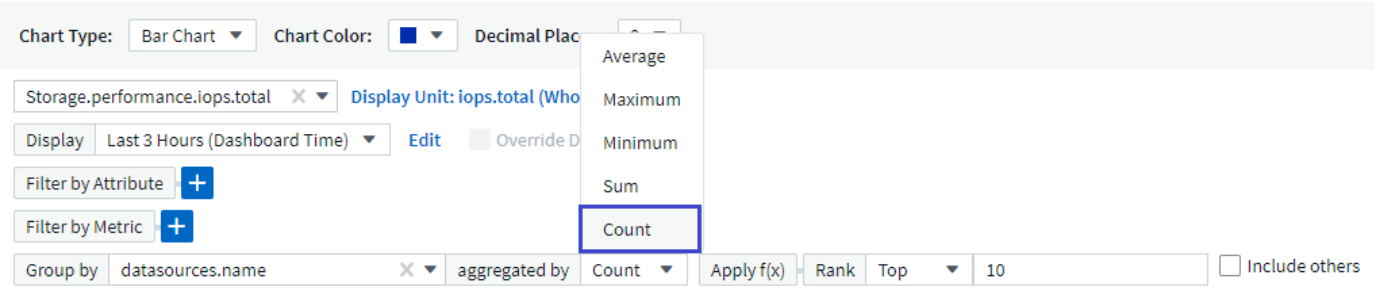
Éditeur de tableau de bord mis à jour

Nous avons remanié nos outils de création de tableaux de bord pour vous permettre de visualiser vos données encore plus rapidement. Accédez à la page « Tableaux de bord » de Cloud Insights pour modifier un tableau de bord existant, en ajouter un à partir de notre galerie de tableaux de bord ou créer votre propre tableau de bord pour le consulter.



Une nouvelle méthode d'agrégation de comptage a également été introduite. Lorsque vous regroupez des données dans des widgets de graphique à barres, de graphique à colonnes et de graphique à secteurs, vous

pouvez afficher rapidement et facilement le nombre d'objets pertinents pour la métrique sélectionnée.



De plus, les graphiques linéaires vous permettent désormais de sélectionner l'un des trois"interpolation" méthodes:

- Aucun - Aucune interpolation n'est effectuée
- Linéaire - Interpole un point de données entre les points existants
- Escalier - Utilise le point de données précédent comme point de données interpolé

Surveillance améliorée de votre infrastructure Kubernetes

Cloud Insights vous permet de rester informé des modifications apportées à votre environnement Kubernetes en vous alertant lorsque des pods, des daemonsets et des replicasets sont créés ou supprimés, ainsi que lorsque de nouveaux déploiements sont créés. Les moniteurs Kubernetes sont par défaut en état *en pause*, vous devez donc activer uniquement ceux dont vous avez besoin.

Fonctionnalités d'aperçu

Cloud Insights met régulièrement en avant un certain nombre de nouvelles fonctionnalités d'aperçu intéressantes. Si vous souhaitez découvrir en avant-première une ou plusieurs de ces fonctionnalités, contactez votre"Équipe commerciale NetApp" pour plus d'informations.

Fonctionnalité	Description
Prévisions du volume interne et du temps de remplissage de la capacité volumique	Cloud Insights est capable de prédire le nombre de jours jusqu'à ce que la capacité soit épuisée pour chaque volume interne et volume surveillé. Cette valeur peut contribuer à réduire considérablement le risque de panne.
Cloud Secure – bloquer l'accès des utilisateurs en cas d'attaque	Une meilleure protection pour vos données critiques pour votre entreprise avec la possibilité de bloquer l'accès des utilisateurs lorsqu'une attaque est détectée. L'accès peut être bloqué automatiquement, à l'aide de politiques de réponse automatisées ou manuellement à partir des pages d'alerte ou de détails de l'utilisateur."En savoir plus"

Ressource partagée sous pression	L'analyse des ressources partagées sous stress utilise l'IA/ML pour identifier automatiquement où la contention des ressources entraîne une dégradation des performances dans votre environnement, met en évidence les charges de travail affectées par celle-ci et fournit des actions recommandées pour y remédier, vous permettant de résoudre les problèmes de performances plus rapidement."En savoir plus"

Nouveau collecteur de données

- **Cohesity SmartFiles** - Ce collecteur basé sur l'API REST acquerra un cluster Cohesity, découvrira les « vues » (en tant que volumes internes CI), les différents nœuds, ainsi que collectera des mesures de performances.

Autres mises à jour du collecteur de données

La collecte et l'affichage des données de performance ont été améliorés sur les collecteurs de données suivants :

- Interface de ligne de commande Brocade
- Dell/EMC VPlex, PowerStore, Isilon/PowerScale, VNX Block/Clariion CLI, XtremIO, Unity/VNXe
- Tableau Flash pur

Ces améliorations de performances sont déjà disponibles dans tous les collecteurs de données NetApp ainsi que dans VMware et Cisco, et seront déployées sur tous les autres collecteurs de données au cours des prochains mois.

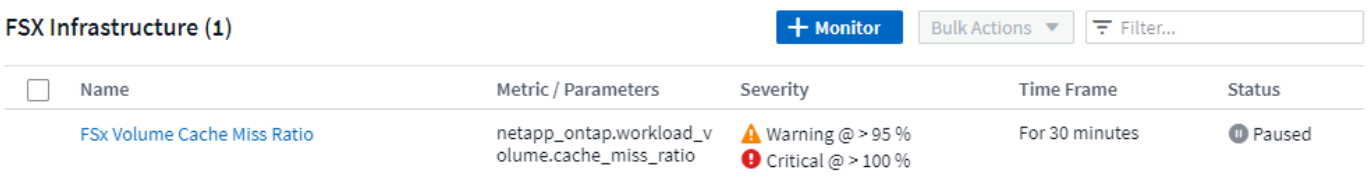
Mars 2022

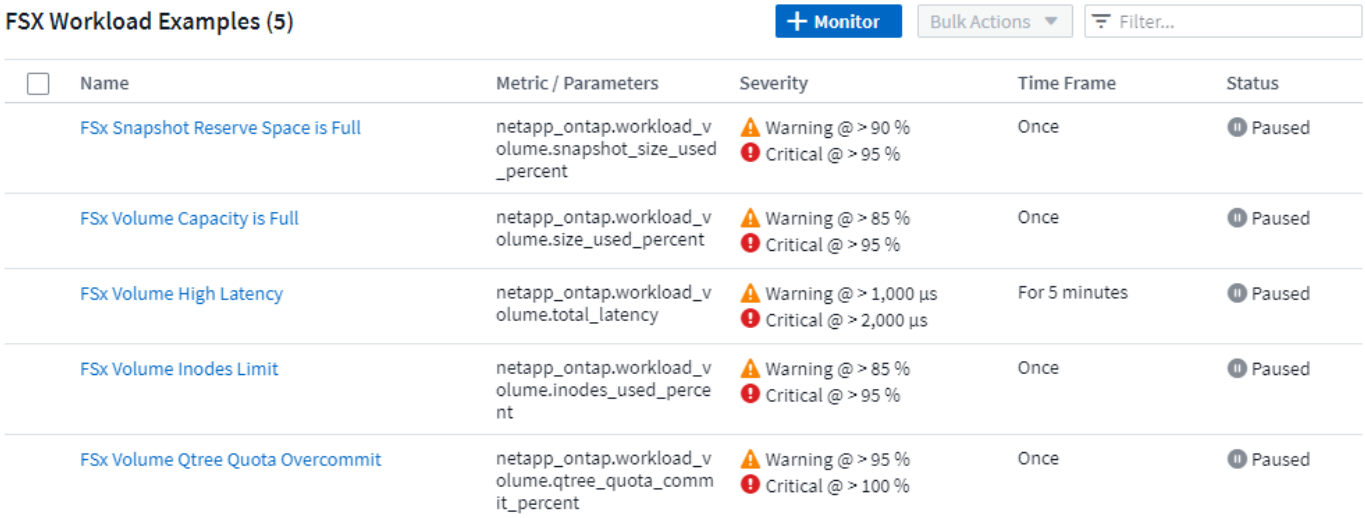
Connexion Cloud pour ONTAP 9.9+

Le"Connexion au cloud NetApp pour ONTAP 9.9+" Le collecteur de données élimine le besoin d'installer une unité d'acquisition externe, simplifiant ainsi le dépannage, la maintenance et le déploiement initial.

Nouveau FSx pour les moniteurs NetApp ONTAP

La surveillance de votre environnement FSx pour NetApp ONTAP est facile avec le nouveau"moniteurs définis par le système" pour l'infrastructure (métriques) et les charges de travail (journaux).





Nouvelles fonctionnalités Cloud Secure accessibles à tous

Votre environnement est plus sécurisé que jamais grâce aux fonctionnalités Cloud Secure suivantes désormais disponibles :

Fonctionnalité	Description
Destruction de données – Détection d'attaque par suppression de fichiers	Détectez les activités anormales de suppression de fichiers à grande échelle, bloquez l'accès aux fichiers malveillants par des utilisateurs malveillants et prenez des instantanés automatiques avec des politiques de réponse automatique.
Notifications distinctes pour les avertissements et les alertes	Les notifications d'avertissement et d'alerte peuvent être envoyées à des destinataires distincts, garantissant que la bonne équipe peut rester informée

Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration Telegraf a été mis à jour vers la version **1.21.2**, avec des améliorations de performances et de sécurité. Les utilisateurs souhaitant effectuer une mise à jour peuvent se référer à la section de mise à niveau appropriée du"Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans aucune action de l'utilisateur requise.

Mises à jour du collecteur de données

- Le collecteur de données des commutateurs Broadcom Fibre Channel a été optimisé pour réduire le nombre de commandes CLI émises à chaque interrogation d'inventaire.

Février 2022

Cloud Insights corrige les vulnérabilités d'Apache Log4j

La sécurité des clients est une priorité absolue chez NetApp. Cloud Insights inclut des mises à jour de ses bibliothèques logicielles pour résoudre les récentes vulnérabilités d'Apache Log4j.

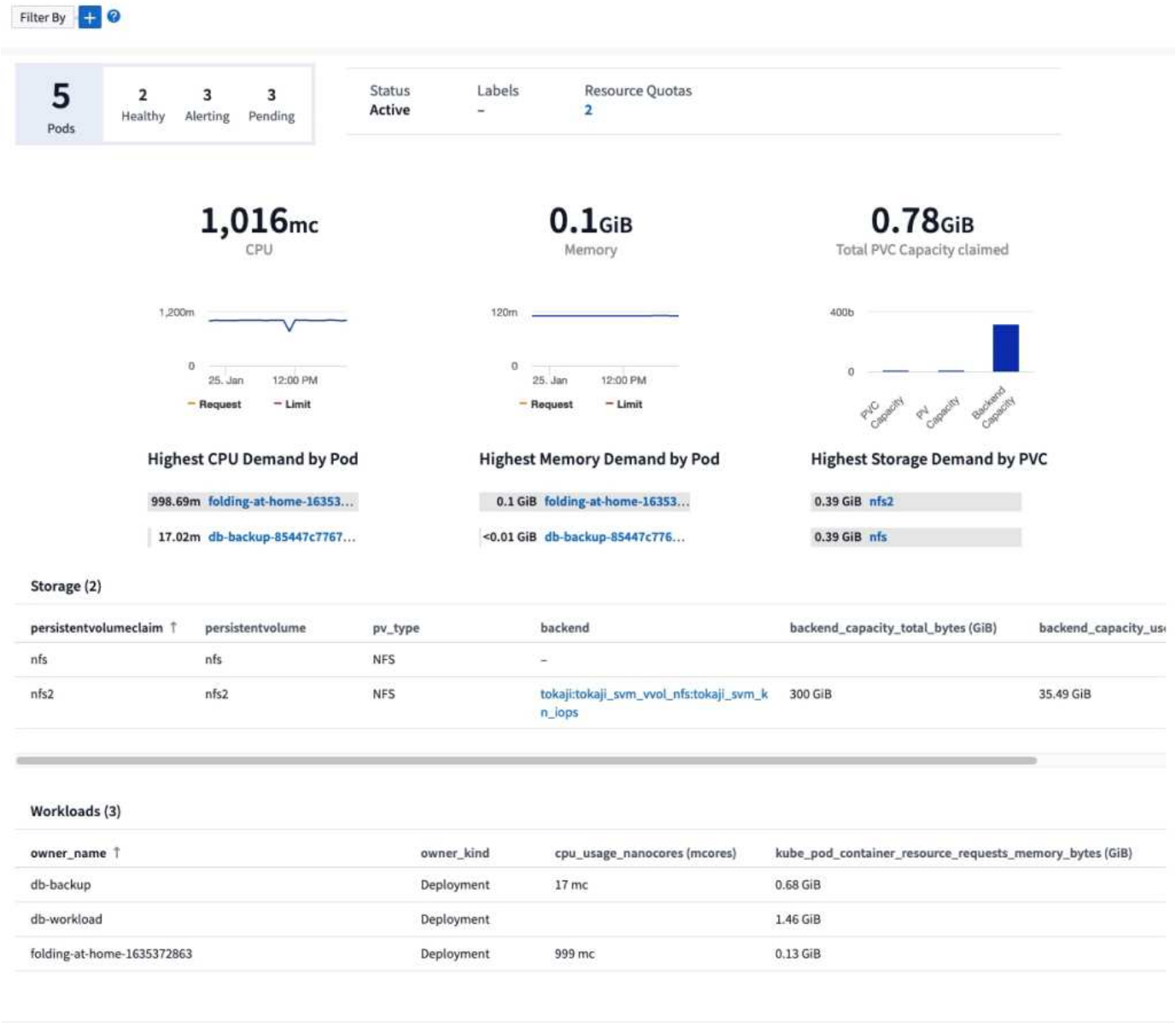
Veuillez vous référer aux informations suivantes sur le site Web des avis de sécurité des produits NetApp :

"CVE-2021-44228" "CVE-2021-45046" "CVE-2021-45105"

Vous pouvez en savoir plus sur ces vulnérabilités et la réponse de NetApp sur le"Salle de presse NetApp" .

Page de détails de l'espace de noms Kubernetes

L'exploration de votre environnement Kubernetes est désormais meilleure que jamais, avec des pages de détails informatives pour les espaces de noms de votre cluster. La page de détails de l'espace de noms fournit un résumé de toutes les ressources utilisées par un espace de noms, y compris toutes les ressources de stockage back-end et leurs utilisations de capacité.



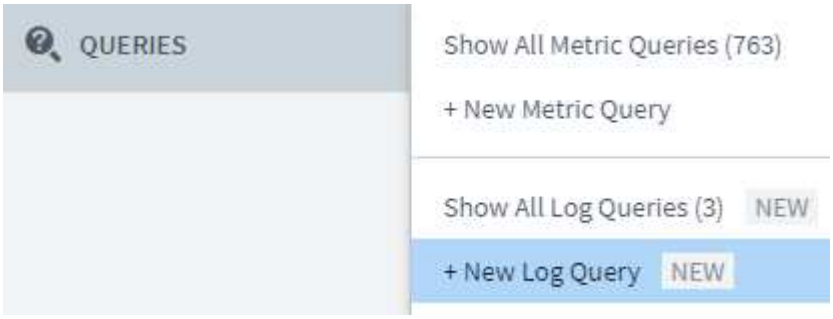
Décembre 2021

Intégration plus poussée pour les systèmes ONTAP

Simplifiez les alertes pour les pannes matérielles ONTAP et plus encore grâce à la nouvelle intégration avec NetApp Event Management System (EMS). "Explorer et alerter" sur les messages ONTAP de bas niveau dans Cloud Insights pour informer et améliorer les flux de travail de dépannage et réduire davantage la dépendance aux outils de gestion des éléments ONTAP .

Interrogation des journaux

Pour les systèmes ONTAP , les requêtes Cloud Insights incluent un puissant"Explorateur de journaux" , vous permettant d'enquêter et de dépanner facilement les entrées du journal EMS.



Notifications au niveau du collecteur de données.

Outre les moniteurs définis par le système et créés sur mesure pour les alertes, vous pouvez également définir des notifications d'alerte pour les collecteurs de données ONTAP , ce qui vous permet de spécifier les destinataires des alertes au niveau du collecteur, indépendamment des autres alertes de surveillance.

Une plus grande flexibilité des rôles Cloud Secure

Les utilisateurs peuvent se voir accorder l'accès aux fonctionnalités Cloud Secure en fonction de"rôles" défini par un administrateur :

Rôle	Accès Cloud Secure
Administrateur	Peut exécuter toutes les fonctions Cloud Secure , y compris celles pour les alertes, l'analyse médico-légale, les collecteurs de données, les politiques de réponse automatisées et les API pour Cloud Secure. Un administrateur peut également inviter d'autres utilisateurs, mais ne peut attribuer que des rôles Cloud Secure .
Utilisateur	Peut afficher et gérer les alertes et consulter les analyses médico-légales. Le rôle utilisateur peut modifier l'état de l'alerte, ajouter une note, prendre des instantanés manuellement et bloquer l'accès utilisateur.
Invité	Peut afficher les alertes et les analyses médico-légales. Le rôle d'invité ne peut pas modifier l'état de l'alerte, ajouter une note, prendre des instantanés manuellement ou bloquer l'accès des utilisateurs.

Prise en charge du système d’exploitation

La prise en charge de CentOS 8.x est remplacée par la prise en charge de **CentOS 8 Stream**. CentOS 8.x atteindra sa fin de vie le 31 décembre 2021.

Mises à jour du collecteur de données

Un certain nombre de noms de collecteurs de données Cloud Insights ont été ajoutés pour refléter les changements de fournisseur :

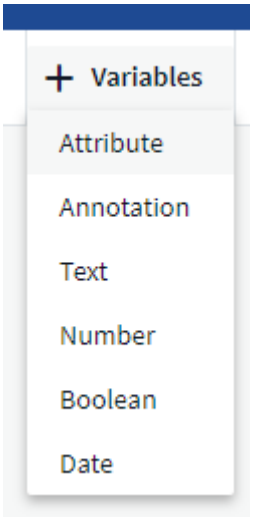
Fournisseur/Modèle	Nom précédent
Dell EMC PowerScale	Isilon
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Agile

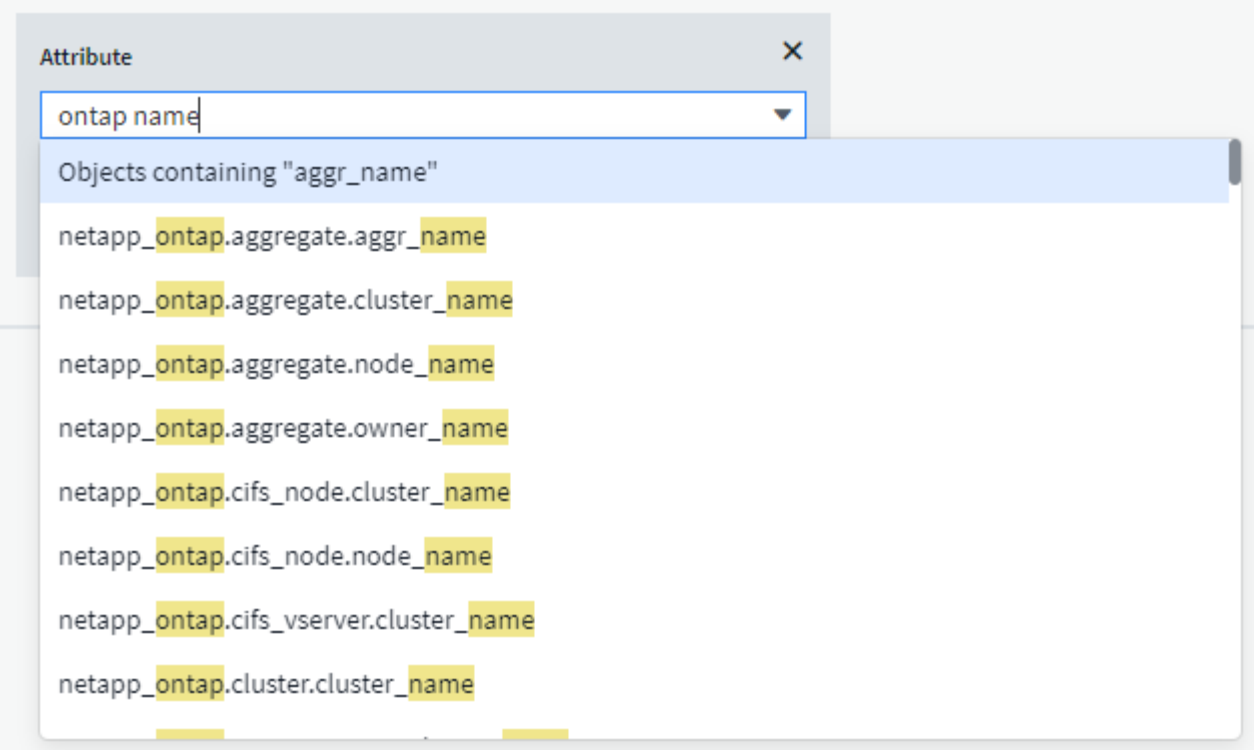
Novembre 2021

Tableaux de bord adaptatifs

Nouvelles variables pour les attributs et possibilité d’utiliser des variables dans les widgets.

Les tableaux de bord sont désormais plus puissants et flexibles que jamais. Créez des tableaux de bord adaptatifs avec des variables d’attribut pour filtrer rapidement les tableaux de bord à la volée. En utilisant ces éléments et d’autres préexistants"variables" vous pouvez désormais créer un tableau de bord de haut niveau pour afficher les métriques de l’ensemble de votre environnement et filtrer de manière transparente par nom de ressource, type, emplacement, etc. Utilisez des variables numériques dans les widgets pour associer des métriques brutes aux coûts, par exemple le coût par Go pour le stockage en tant que service.





Accéder à la base de données de rapports via l'API

Fonctionnalités améliorées d'intégration avec des outils de reporting tiers, ITSM et d'automatisation : la puissante solution Cloud Insights"API" permet aux utilisateurs d'interroger directement la base de données Cloud Insights Reporting, sans passer par l'environnement Cognos Reporting.

Tables de pods sur la page de destination de la machine virtuelle

Navigation transparente entre les machines virtuelles et les pods Kubernetes qui les utilisent : pour un dépannage amélioré et une meilleure gestion des performances, un tableau des pods Kubernetes associés apparaîtra désormais sur les pages de destination des machines virtuelles.

Mises à jour du collecteur de données

- ECS signale désormais le micrologiciel pour le stockage et le nœud
- Isilon a amélioré la détection rapide
- Azure NetApp Files collecte les données de performances plus rapidement
- StorageGRID prend désormais en charge l'authentification unique (SSO)
- Brocade CLI signale correctement le modèle pour X&-4

Systèmes d’exploitation supplémentaires pris en charge

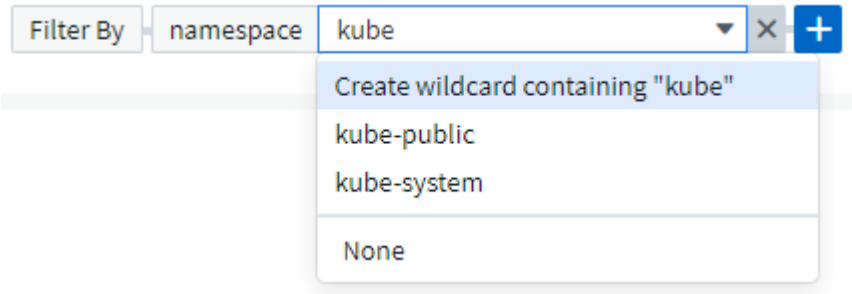
L’unité d’acquisition Cloud Insights prend en charge les systèmes d’exploitation suivants, en plus de ceux déjà pris en charge :

- Centos (64 bits) 8.4
- Oracle Enterprise Linux (64 bits) 8.4
- Red Hat Enterprise Linux (64 bits) 8.4

Octobre 2021

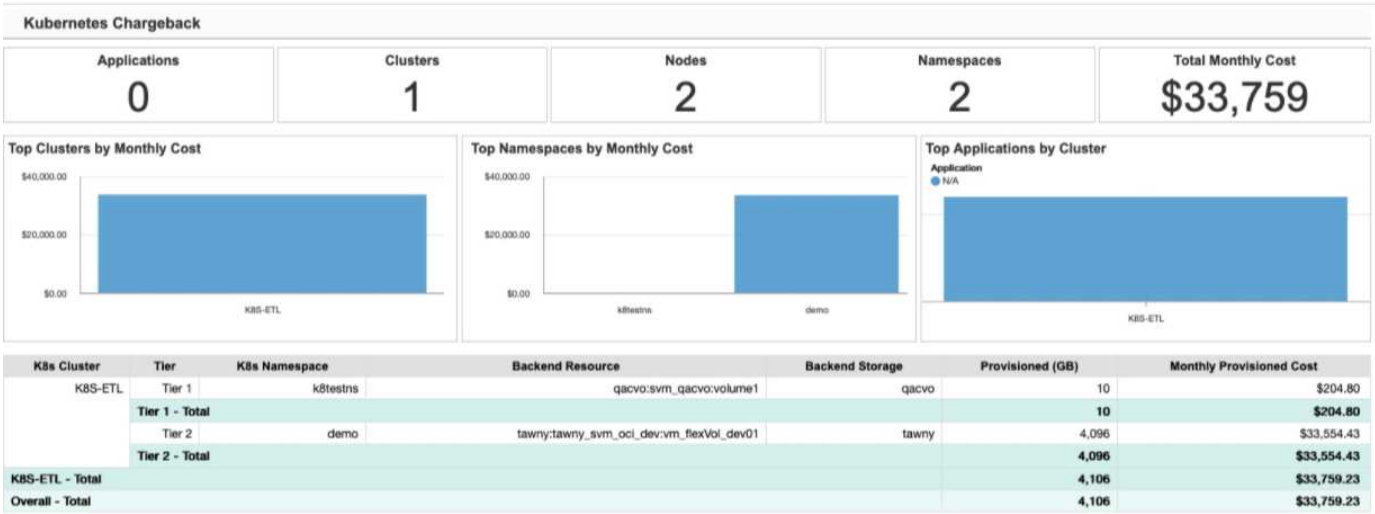
Filtres sur les pages de K8S Explorer

"Explorateur Kubernetes"les filtres de page vous offrent un contrôle ciblé des données affichées pour l’exploration de votre cluster, de votre nœud et de votre pod Kubernetes.



Données K8s pour les rapports

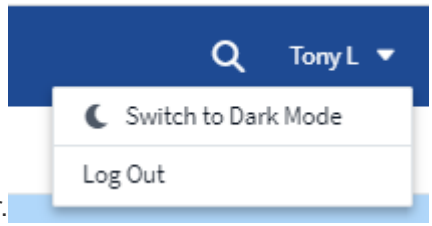
Les données Kubernetes sont désormais disponibles pour une utilisation dans les rapports, vous permettant de créer des rétrofacturations ou d’autres rapports. Pour que les données de rétrofacturation Kubernetes soient transmises à Reporting, vous devez disposer d’une connexion active à votre cluster Kubernetes ainsi qu’à son stockage back-end et Cloud Insights doit recevoir des données de celui-ci. S’il n’y a aucune donnée reçue du stockage back-end, Cloud Insights ne peut pas envoyer de données d’objet Kubernetes à Reporting.

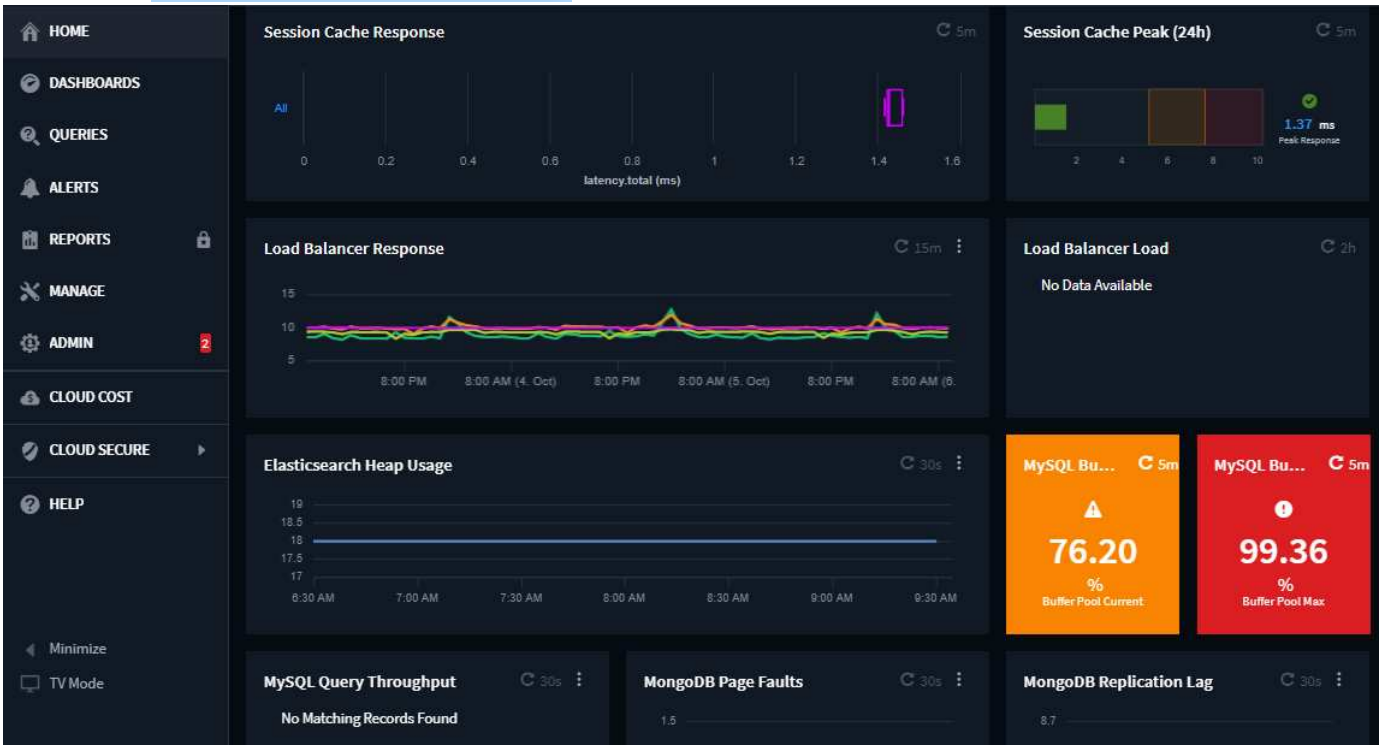


K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

Le thème sombre est arrivé

Beaucoup d'entre vous ont demandé un thème sombre, et Cloud Insights a répondu. Pour basculer entre le thème clair et le thème sombre, cliquez sur le menu déroulant à côté de votre nom d'utilisateur.





Assistance au collecteur de données

Nous avons apporté quelques améliorations aux collecteurs de données Cloud Insights . Voici quelques points saillants :

- Nouveau collecteur pour Amazon FSx pour ONTAP

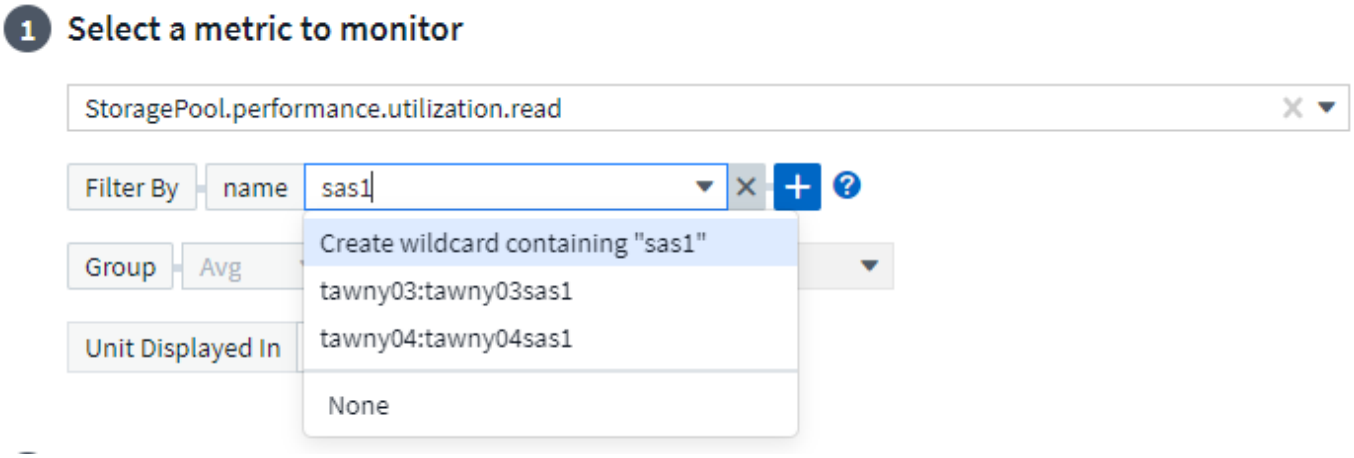
Septembre 2021

Les politiques de performance sont désormais des moniteurs

Les moniteurs et les alertes ont supplanté les politiques de performances et les violations dans Cloud Insights. "Alertes avec moniteurs" offre une plus grande flexibilité et un meilleur aperçu des problèmes ou tendances potentiels dans votre environnement.

Suggestions de saisie semi-automatique, caractères génériques et expressions dans les moniteurs

Lors de la création d'un moniteur d'alerte, la saisie d'un filtre est désormais prédictive, vous permettant de rechercher et de trouver facilement les métriques ou les attributs de votre moniteur. De plus, vous avez la possibilité de créer un filtre générique basé sur le texte que vous saisissez.



Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration Telegraf a été mis à jour vers la version **1.19.3**, avec des améliorations de performances et de sécurité. Les utilisateurs souhaitant effectuer une mise à jour peuvent se référer à la section de mise à niveau appropriée du"Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans aucune action de l'utilisateur requise.

Assistance au collecteur de données

Nous avons apporté quelques améliorations aux collecteurs de données Cloud Insights . Voici quelques points saillants :

- Le collecteur Microsoft Hyper-V utilise désormais PowerShell au lieu de WMI
- Le collecteur de machines virtuelles et de disques durs virtuels Azure est désormais jusqu'à 10 fois plus rapide grâce aux appels parallèles
- HPE Nimble prend désormais en charge les configurations fédérées et iSCSI

Et comme nous améliorons constamment la collecte de données, voici quelques autres changements récents à noter :

- Nouveau collecteur pour EMC Powerstore
- Nouveau collecteur pour Hitachi Ops Center
- Nouveau collecteur pour Hitachi Content Platform
- Collecteur ONTAP amélioré pour signaler les pools Fabric
- ANF amélioré avec performances de pool de stockage et de volume
- EMC ECS amélioré avec nœuds de stockage et performances de stockage ainsi que le nombre d'objets dans les buckets
- EMC Isilon amélioré avec nœud de stockage et métriques Qtree

- EMC Symetrix amélioré avec mesures de limite de qualité de service du volume
- Numéro de série parent amélioré d'IBM SVC et EMC PowerStore avec nœuds de stockage

Août 2021

Nouvelle interface utilisateur de la page d'audit

Le"Page d'audit" fournit une interface plus propre et permet désormais l'exportation des événements d'audit vers un fichier .CSV.

Gestion améliorée des rôles d'utilisateur

Cloud Insights offre désormais encore plus de liberté pour l'attribution des rôles d'utilisateur et des contrôles d'accès. Les utilisateurs peuvent désormais se voir attribuer des autorisations granulaires pour la surveillance, la création de rapports et Cloud Secure séparément.

Cela signifie que vous pouvez autoriser davantage d'utilisateurs à accéder aux fonctions de surveillance, d'optimisation et de création de rapports, tout en limitant l'accès à vos données d'audit et d'activité Cloud Secure sensibles uniquement à ceux qui en ont besoin.

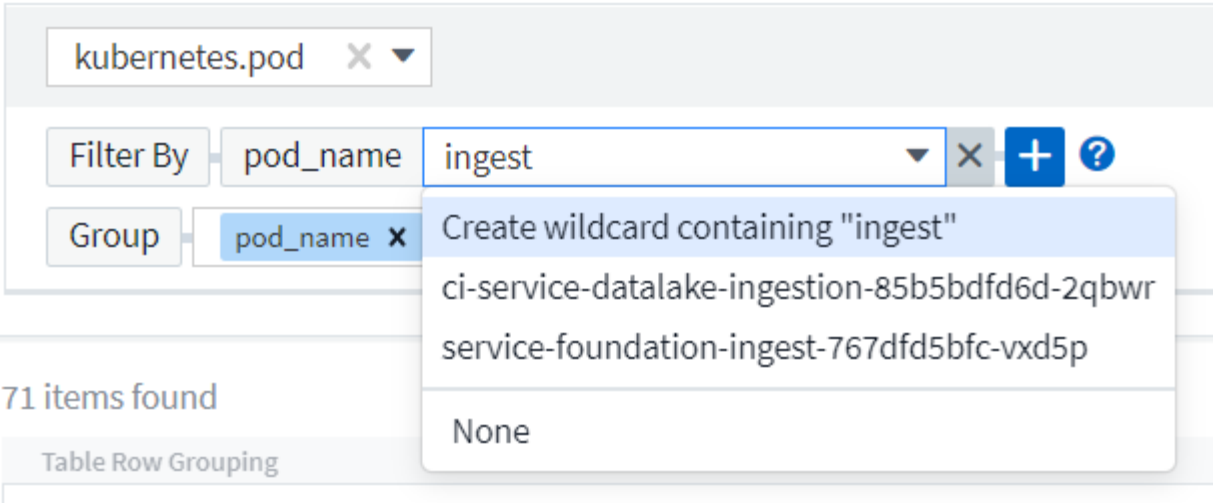
"En savoir plus"sur les différents niveaux d'accès dans la documentation Cloud Insights .

Juin 2021

Suggestions de saisie semi-automatique, caractères génériques et expressions dans les filtres

Avec cette version de Cloud Insights, vous n'avez plus besoin de connaître tous les noms et valeurs possibles sur lesquels filtrer dans une requête ou un widget. Lors du filtrage, vous pouvez simplement commencer à saisir et Cloud Insights suggérera des valeurs en fonction de votre texte. Plus besoin de rechercher à l'avance les noms des applications ou les attributs Kubernetes juste pour trouver ceux que vous souhaitez afficher dans votre widget.

Lorsque vous saisissez un filtre, celui-ci affiche une liste intelligente de résultats parmi lesquels vous pouvez choisir, ainsi que la possibilité de créer un **filtre générique** basé sur le texte actuel. La sélection de cette option renverra tous les résultats correspondant à l'expression générique. Vous pouvez bien sûr également sélectionner plusieurs valeurs individuelles que vous souhaitez ajouter au filtre.



De plus, vous pouvez créer des **expressions** dans un filtre en utilisant NOT ou OR, ou vous pouvez sélectionner l'option « Aucun » pour filtrer les valeurs nulles dans le champ.

En savoir plus sur"options de filtrage" dans les requêtes et les widgets.

API disponibles par édition

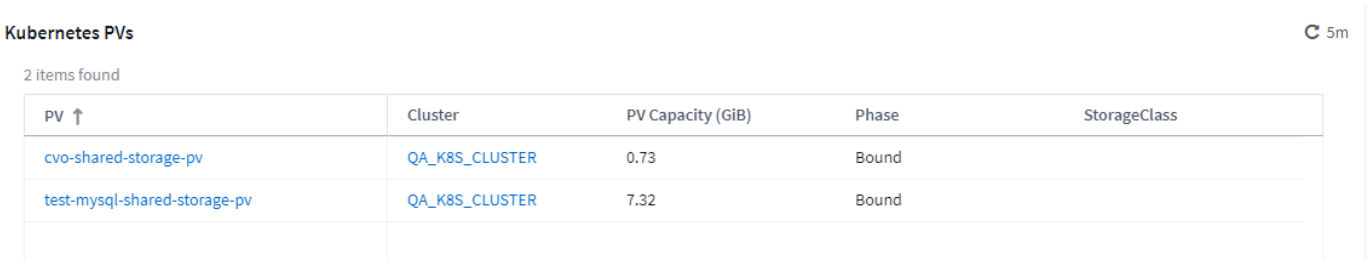
Les puissantes API de Cloud Insights sont plus accessibles que jamais, les API Alerts étant désormais disponibles dans les éditions Standard et Premium. Les API suivantes sont disponibles pour chaque édition :

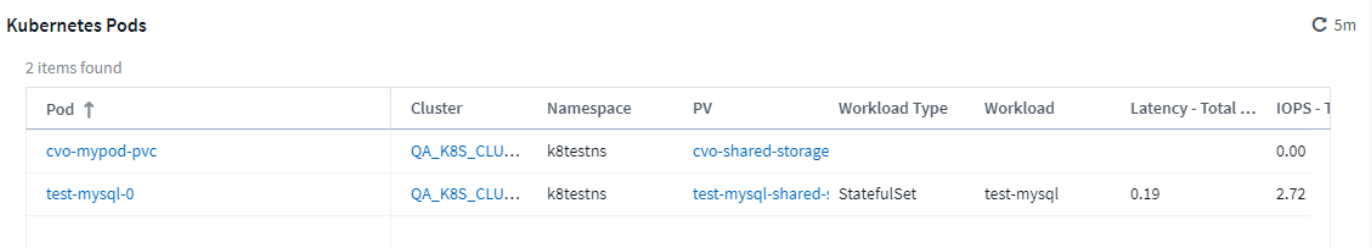
Catégorie d'API	Basique	Standard	Prime
Unité d'acquisition	✔	✔	✔
Collecte de données	✔	✔	✔
Alertes		✔	✔
Actifs		✔	✔
Ingestion de données		✔	✔

Visibilité des PV et des pods Kubernetes

Cloud Insights offre une visibilité sur le stockage back-end de vos environnements Kubernetes, vous donnant un aperçu de vos pods Kubernetes et de vos volumes persistants (PV). Vous pouvez désormais suivre les compteurs PV tels que les IOPS, la latence et le débit de l'utilisation d'un seul Pod via un compteur PV jusqu'à un PV et jusqu'au périphérique de stockage back-end.

Sur une page de destination Volume ou Volume interne, deux nouveaux tableaux s'affichent :

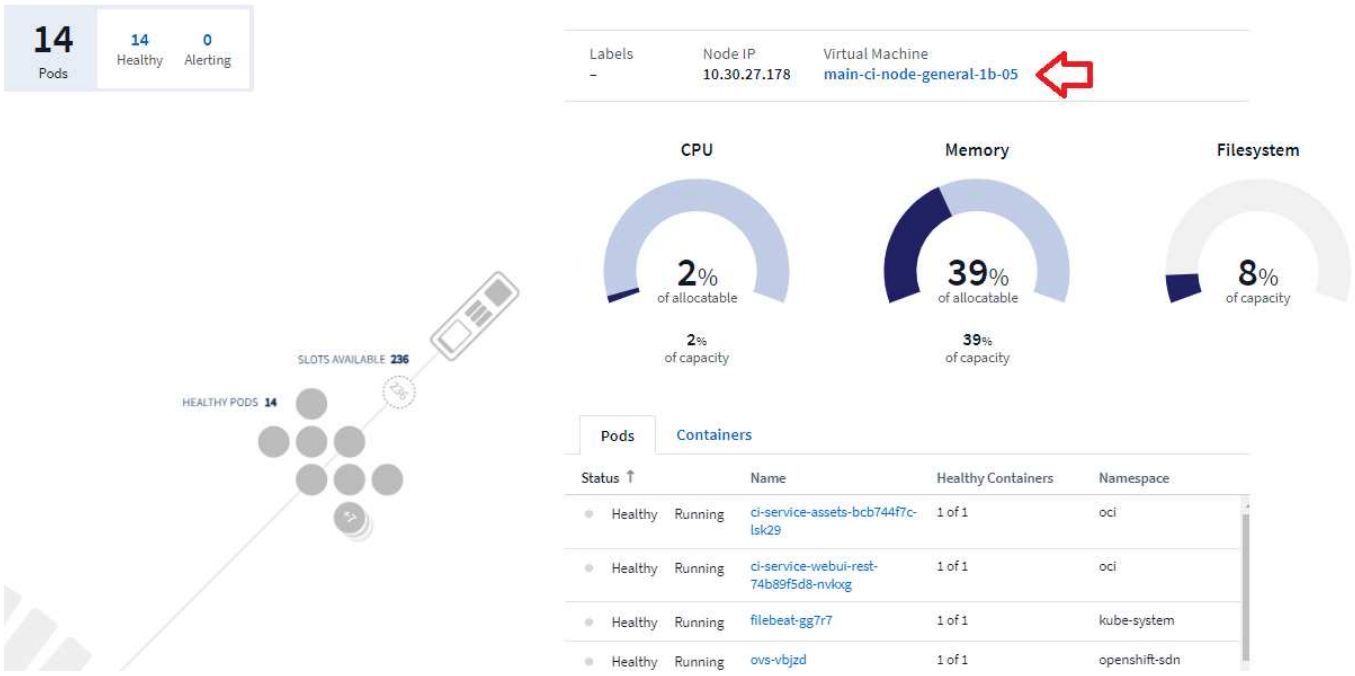


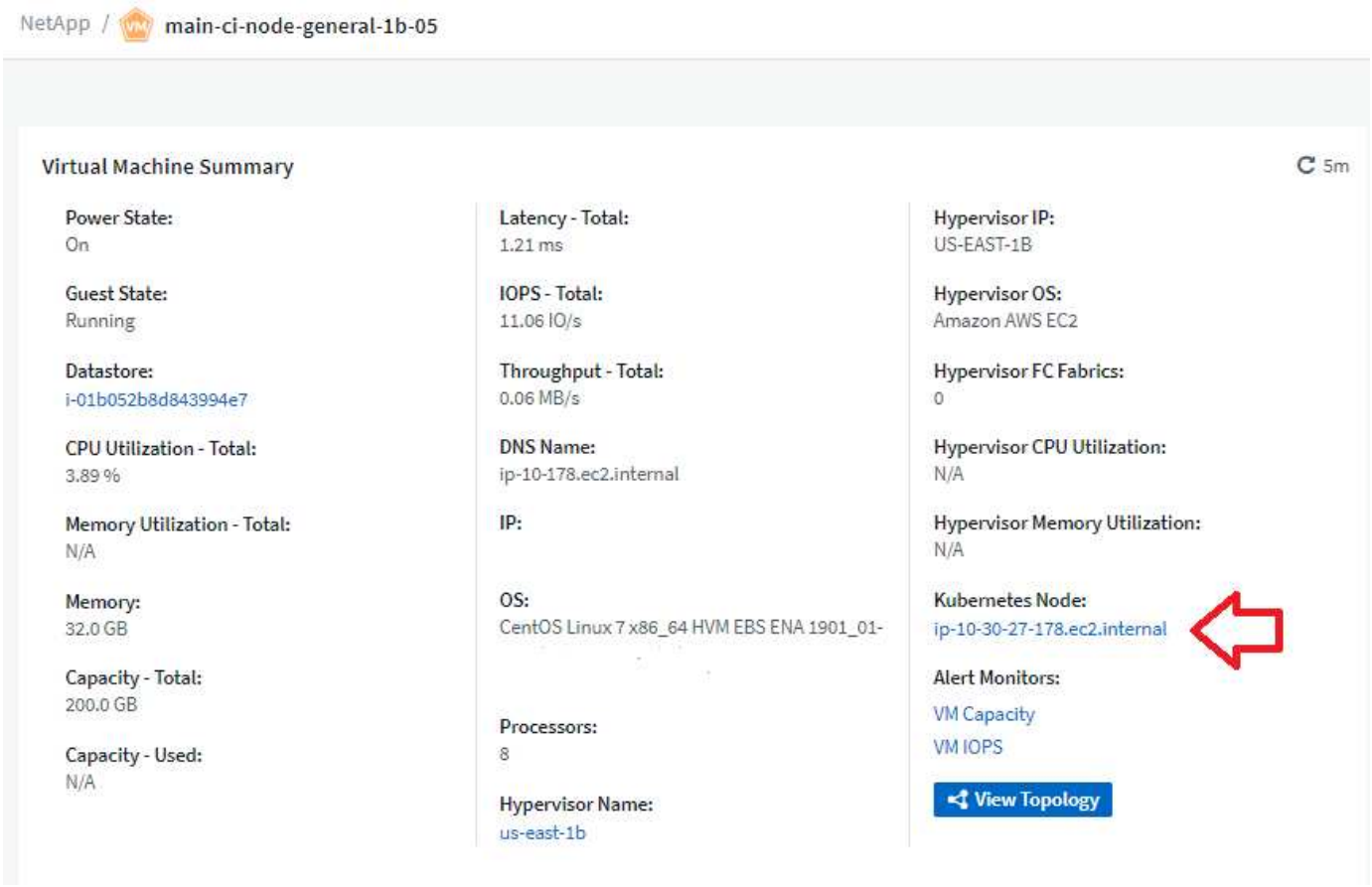


Notez que pour profiter de ces nouvelles tables, il est recommandé de désinstaller votre agent Kubernetes actuel et de l'installer à nouveau. Vous devez également installer Kube-State-Metrics version 2.1.0 ou ultérieure.

Liens entre le nœud Kubernetes et la VM

Sur une page de nœud Kubernetes, vous pouvez désormais cliquer pour ouvrir la page de la machine virtuelle du nœud. La page VM inclut également un lien vers le nœud lui-même.





Les moniteurs d’alerte remplacent les politiques de performance

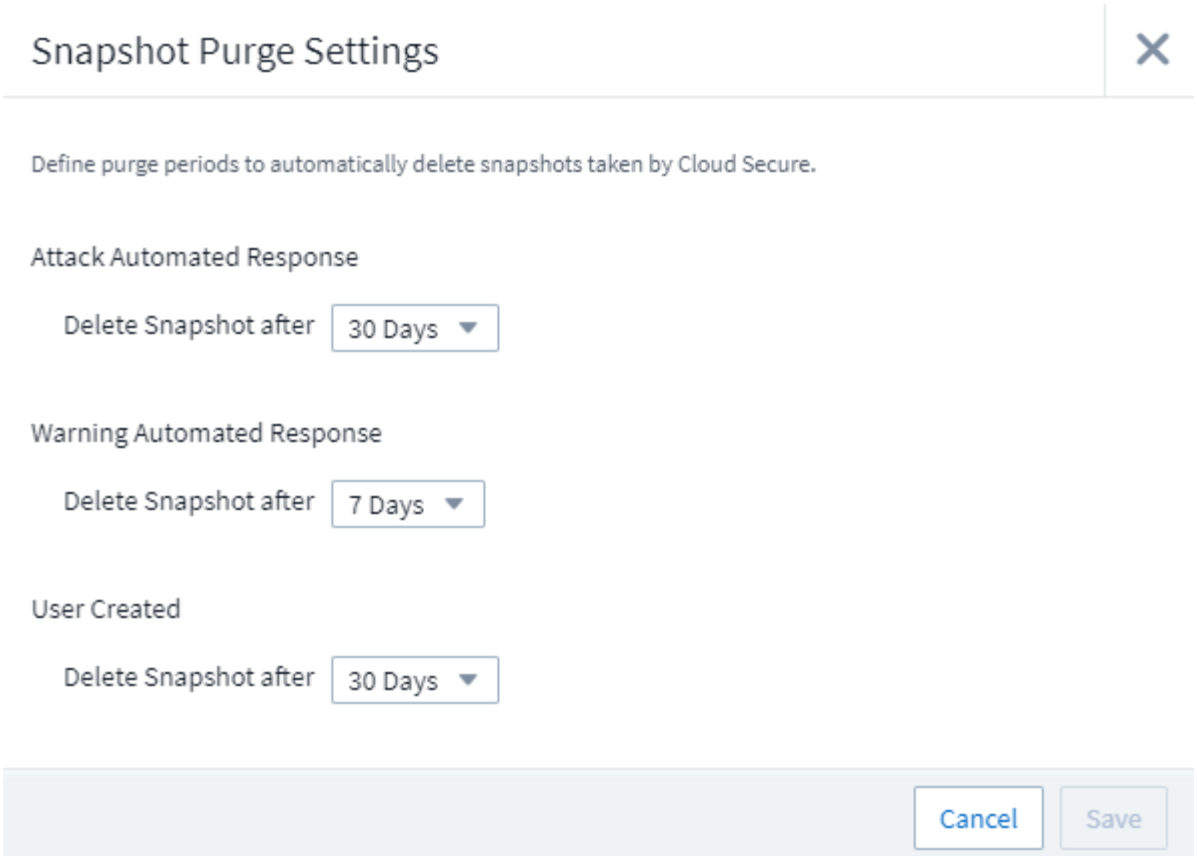
Pour permettre les avantages supplémentaires des seuils multiples, de la diffusion d’alertes par webhook et par e-mail, des alertes sur toutes les métriques à l’aide d’une interface unique, et bien plus encore, Cloud Insights convertira les clients Standard et Premium Edition de **Performance Policies** à **Monitors** au cours des mois de juillet et août 2021. En savoir plus sur"Alertes et moniteurs" , et restez à l’écoute de ce changement passionnant.

Cloud Secure prend en charge NFS

Cloud Secure prend désormais en charge NFS pour la collecte de données ONTAP . Surveillez l’accès des utilisateurs SMB et NFS pour protéger vos données contre les attaques de ransomware. De plus, Cloud Secure prend en charge les annuaires utilisateurs Active Directory et LDAP pour la collecte des attributs utilisateur NFS.

Purge des instantanés Cloud Secure

Cloud Secure supprime automatiquement les instantanés en fonction des paramètres de purge des instantanés, pour économiser de l’espace de stockage et réduire le besoin de suppression manuelle des instantanés.



Vitesse de collecte de données Cloud Secure

Un seul système d'agent de collecte de données peut désormais publier jusqu'à 20 000 événements par seconde sur Cloud Secure.

Mai 2021

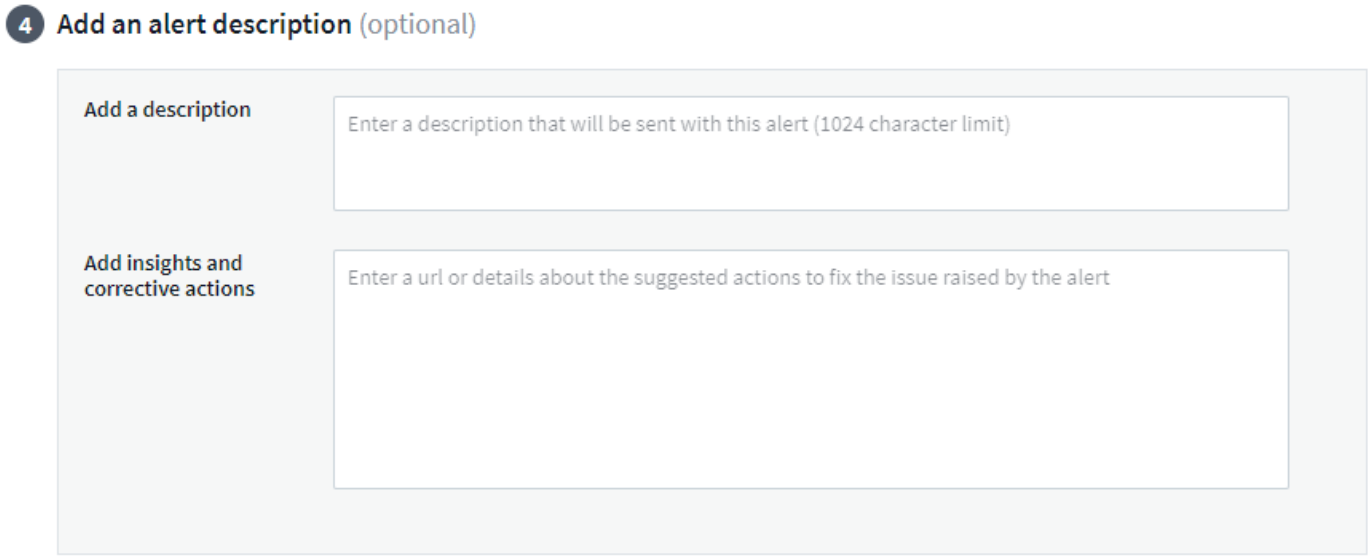
Voici quelques-uns des changements que nous avons apportés en avril :

Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration Telegraf a été mis à jour vers la version 1.17.3, avec des améliorations de performances et de sécurité. Les utilisateurs souhaitant effectuer une mise à jour peuvent se référer à la section de mise à niveau appropriée du"Installation de l'agent" documentation. Les versions précédentes de l'agent continueront de fonctionner sans aucune action de l'utilisateur requise.

Ajouter des actions correctives à une alerte

Vous pouvez désormais ajouter une description facultative ainsi que des informations supplémentaires et/ou des actions correctives lors de la création ou de la modification d'un moniteur en remplissant la section **Ajouter une description d'alerte**. La description sera envoyée avec l'alerte. Le champ *informations et actions correctives* peut fournir des étapes et des conseils détaillés pour gérer les alertes et sera affiché dans la section récapitulative de la page de destination des alertes.



API Cloud Insights pour toutes les éditions

L'accès API est désormais disponible dans toutes les éditions de Cloud Insights. Les utilisateurs de l'édition Basic peuvent désormais automatiser les actions pour les unités d'acquisition et les collecteurs de données, et les utilisateurs de l'édition Standard peuvent interroger des métriques et ingérer des métriques personnalisées. L'édition Premium continue de permettre l'utilisation complète de toutes les catégories d'API.

Catégorie d'API	Basique	Standard	Prime
Unité d'acquisition	✔	✔	✔
Collecte de données	✔	✔	✔
Actifs		✔	✔
Ingestion de données		✔	✔
Entrepôt de données			✔

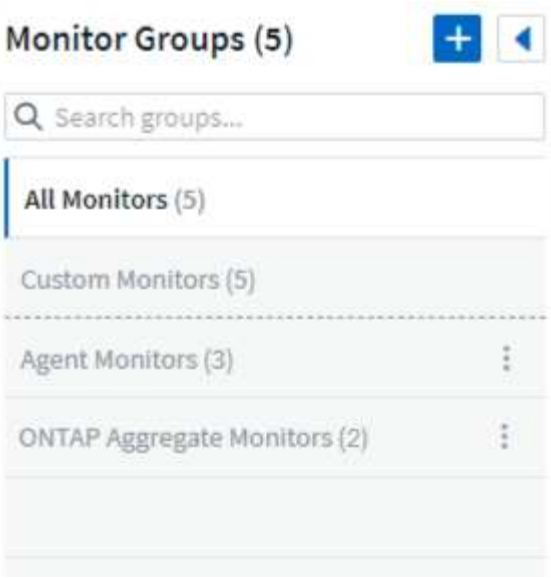
Pour plus de détails sur l'utilisation de l'API, veuillez vous référer au"Documentation API" .

Avril 2021

Gestion simplifiée des moniteurs

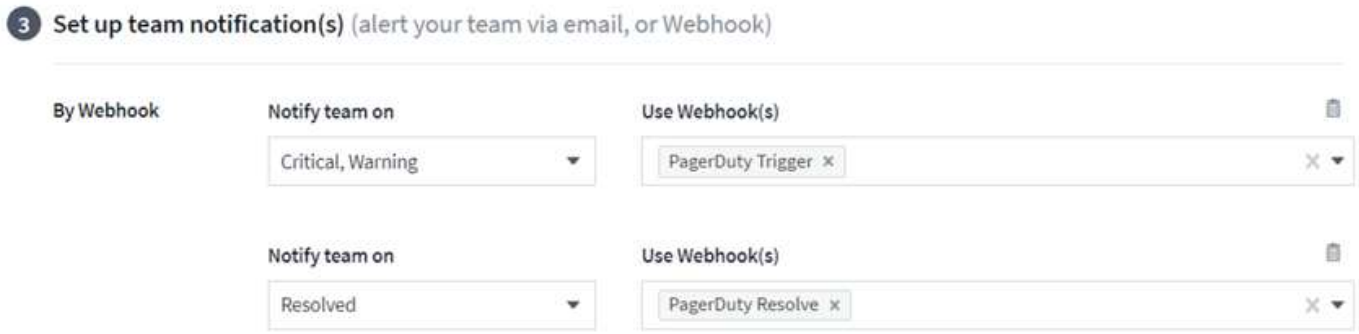
"Regroupement des moniteurs"simplifie la gestion des moniteurs dans votre environnement. Plusieurs moniteurs peuvent désormais être regroupés et mis en pause comme un seul. Par exemple, si une mise à jour est en cours sur une pile d'infrastructures, vous pouvez suspendre les alertes de tous ces appareils en un seul clic.

Les groupes de surveillance constituent la première partie d'une nouvelle fonctionnalité intéressante apportant une gestion améliorée des périphériques ONTAP à Cloud Insights.



Options d'alerte améliorées à l'aide de Webhooks

De nombreuses applications commerciales prennent en charge"Webhooks" comme interface d'entrée standard. Cloud Insights prend désormais en charge bon nombre de ces canaux de diffusion, en fournissant des modèles par défaut pour Slack, PagerDuty, Teams et Discord, en plus de fournir des webhooks génériques personnalisables pour prendre en charge de nombreuses autres applications.



Identification améliorée des appareils

Pour améliorer la surveillance et le dépannage ainsi que pour fournir des rapports précis, il est utile de comprendre les noms des appareils plutôt que leurs adresses IP ou autres identifiants. Cloud Insights intègre désormais un moyen automatique d'identifier les noms des périphériques de stockage et des hôtes physiques dans l'environnement, à l'aide d'une approche basée sur des règles appelée**"Résolution de l'appareil"** , disponible dans le menu **Gérer**.

Vous en avez demandé plus !

Une demande populaire des clients a été de disposer de davantage d'options par défaut pour visualiser la plage de données. Nous avons donc ajouté les cinq nouveaux choix suivants, désormais disponibles dans l'ensemble du service via le sélecteur de plage de temps :

- Les 30 dernières minutes
- Les 2 dernières heures

- Les 6 dernières heures
- Les 12 dernières heures
- Les 2 derniers jours

Plusieurs abonnements dans un seul environnement Cloud Insights

À partir du 2 avril, Cloud Insights prend en charge plusieurs abonnements du même type d'édition pour un client dans une seule instance Cloud Insights . Cela permet aux clients de combiner certaines parties de leur abonnement Cloud Insights avec des achats d'infrastructure. Contactez le service commercial NetApp pour obtenir de l'aide sur plusieurs abonnements.

Choisissez votre chemin

Lors de la configuration de Cloud Insights, vous pouvez désormais choisir de commencer par la surveillance et les alertes ou par la détection des ransomwares et des menaces internes. Cloud Insights configurera votre environnement de démarrage en fonction du chemin que vous choisissez. Vous pouvez configurer l'autre chemin à tout moment par la suite.

Intégration Cloud Secure

Et il est plus facile que jamais de commencer à utiliser Cloud Secure, avec une nouvelle liste de contrôle de configuration étape par étape.

Comme toujours, nous aimons entendre vos suggestions ! Envoyez-les à ng-cloudinsights-customerfeedback@netapp.com.

Février 2021

Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration Telegraf a été mis à jour vers la version 1.17.0, qui inclut des corrections de vulnérabilités et de bogues.

Analyseur de coûts du cloud

Découvrez la puissance de Spot by NetApp avec Cloud Cost, qui fournit une analyse détaillée des coûts des dépenses passées, présentes et estimées, offrant une visibilité sur l'utilisation du cloud dans votre environnement. Le tableau de bord des coûts du cloud offre une vue claire des dépenses du cloud et une analyse détaillée des charges de travail, des comptes et des services individuels.

Cloud Cost peut vous aider à relever ces défis majeurs :

- Suivi et surveillance de vos dépenses cloud
- Identifier les gaspillages et les domaines d'optimisation potentiels
- Fournir des éléments d'action exécutables

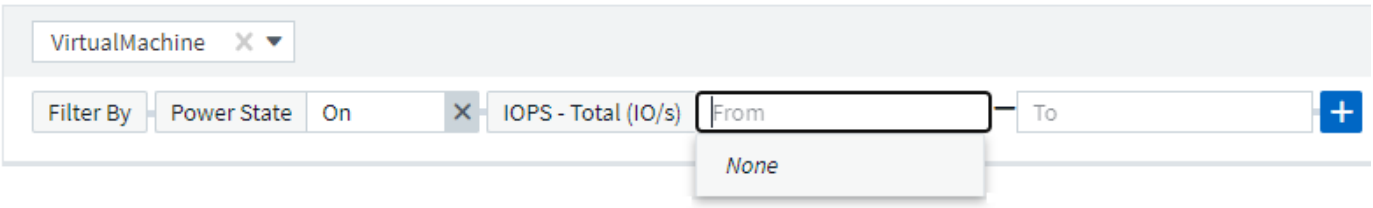
Cloud Cost est axé sur la surveillance. Passez au compte Spot by NetApp complet pour permettre des économies automatiques et une optimisation de l'environnement.

Interrogation d'objets ayant des valeurs nulles à l'aide de filtres

Cloud Insights permet désormais de rechercher des attributs et des métriques ayant des valeurs nulles/aucune grâce à l'utilisation de filtres. Vous pouvez effectuer ce filtrage sur tous les attributs/métriques aux endroits suivants :

- Sur la page de requête
- Dans les widgets du tableau de bord et les variables de page
- Sur la page de la liste des alertes
- Lors de la création de moniteurs

Pour filtrer les valeurs nulles/aucune, sélectionnez simplement l'option *Aucun* lorsqu'elle apparaît dans la liste déroulante de filtre appropriée.



Prise en charge multirégionale

À partir d'aujourd'hui, nous proposons le service Cloud Insights dans différentes régions du monde, ce qui facilite les performances et augmente la sécurité pour les clients basés en dehors des États-Unis. Cloud Insights/ Cloud Secure stocke les informations en fonction de la région dans laquelle votre environnement est créé.

Cliquez"ici" pour plus d'informations.

Janvier 2021

Mesures ONTAP supplémentaires renommées

Dans le cadre de nos efforts continus visant à améliorer l'efficacité de la collecte de données à partir des systèmes ONTAP , les mesures ONTAP suivantes ont été renommées.

Si vous disposez de widgets de tableau de bord ou de requêtes utilisant l'une de ces mesures, vous devrez les modifier ou les recréer pour utiliser les nouveaux noms de mesures.

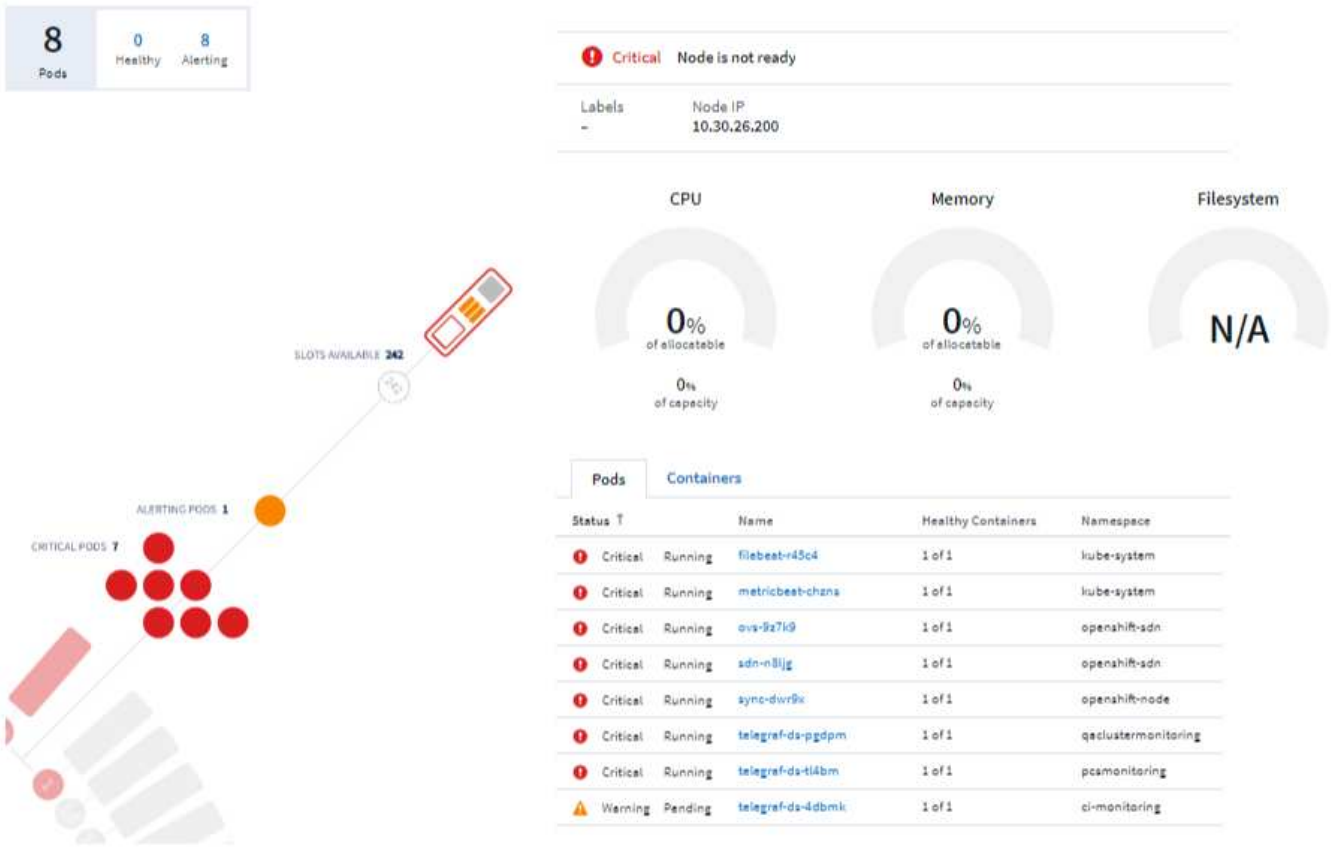
Nom métrique précédent	Nouveau nom de métrique
netapp_ontap.disk_constituent.total_transfers	netapp_ontap.disk_constituent.total_iops
netapp_ontap.disk.total_transfers	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.débit_de_lecture
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.débit_d'écriture
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.débit_de_lecture
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.débit_d'écriture
netapp_ontap.lif.recv_data	netapp_ontap.lif.recv_throughput
netapp_ontap.lif.données_envoyées	netapp_ontap.lif.débit_envoyé
netapp_ontap.lun.read_data	netapp_ontap.lun.read_throughput
netapp_ontap.lun.write_data	netapp_ontap.lun.write_throughput
netapp_ontap.nic_common.rx_bytes	netapp_ontap.nic_common.rx_throughput
netapp_ontap.nic_common.tx_bytes	netapp_ontap.nic_common.tx_throughput
netapp_ontap.path.read_data	netapp_ontap.path.read_throughput
netapp_ontap.path.write_data	netapp_ontap.path.write_throughput
netapp_ontap.path.total_data	netapp_ontap.path.débit_total
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.lecture_throughput
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.débit_d'écriture
netapp_ontap.policy_group.autres_données	netapp_ontap.policy_group.autre_débit
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.débit_total
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_throughput_read
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.débit_disque_écrit
netapp_ontap.system_node.hdd_data_read	netapp_ontap.system_node.hdd_throughput_read
netapp_ontap.system_node.hdd_data_written	netapp_ontap.system_node.hdd_throughput_written
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_throughput_read

Nom métrique précédent	Nouveau nom de métrique
netapp_ontap.system_node.ssd_data_written	netapp_ontap.system_node.ssd_throughput_written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.system_node.fcp_data_recv	netapp_ontap.system_node.fcp_throughput_recv
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_throughput_sent
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_throughput
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_write_throughput
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_throughput
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_throughput
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_throughput
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_throughput
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_throughput
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_throughput
netapp_ontap.volume.read_data	netapp_ontap.volume.read_throughput
netapp_ontap.volume.write_data	netapp_ontap.volume.write_throughput
netapp_ontap.workload.lire_données	netapp_ontap.workload.read_throughput
netapp_ontap.workload.write_data	netapp_ontap.workload.write_throughput
netapp_ontap.workload_volume.read_data	netapp_ontap.workload_volume.read_throughput
netapp_ontap.workload_volume.write_data	netapp_ontap.workload_volume.write_throughput

Nouvel explorateur Kubernetes

Le"Explorateur Kubernetes" fournit une vue topologique simple des clusters Kubernetes, permettant même aux non-experts d'identifier rapidement les problèmes et les dépendances, du niveau du cluster jusqu'au conteneur et au stockage.

Une grande variété d'informations peut être explorée à l'aide des détails détaillés de Kubernetes Explorer concernant l'état, l'utilisation et l'intégrité des clusters, des nœuds, des pods, des conteneurs et du stockage dans votre environnement Kubernetes.



Décembre 2020

Installation simplifiée de Kubernetes

L'installation de l'agent Kubernetes a été simplifiée pour nécessiter moins d'interactions utilisateur. "Installation de l'agent Kubernetes" inclut désormais la collecte de données Kubernetes.

Novembre 2020

Tableaux de bord supplémentaires

Les nouveaux tableaux de bord suivants axés sur ONTAP ont été ajoutés à la galerie et sont disponibles pour l'importation :

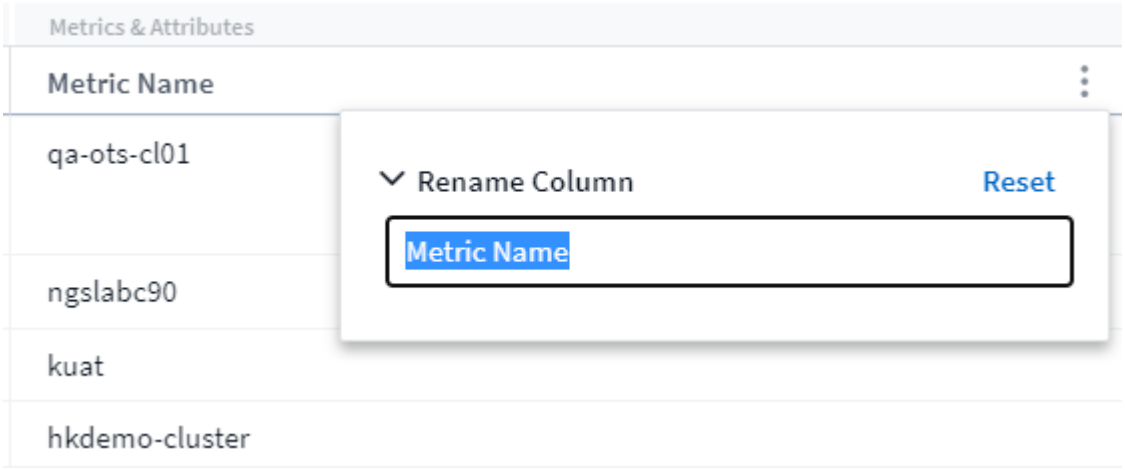
- ONTAP: Performances et capacités globales
- ONTAP FAS/ AFF - Utilisation des capacités
- ONTAP FAS/ AFF - Capacité du cluster
- ONTAP FAS/ AFF - Efficacité
- ONTAP FAS/ AFF - Performances FlexVol

- ONTAP FAS/ AFF - Points opérationnels/optimaux du nœud
- ONTAP FAS/ AFF - Efficacité des capacités pré-post
- ONTAP: Activité du port réseau
- ONTAP: Performances des protocoles de nœuds
- ONTAP: Performances de la charge de travail des nœuds (front-end)
- ONTAP: Processeur
- ONTAP: Performances de la charge de travail SVM (front-end)
- ONTAP: Performances de la charge de travail volumique (front-end)

Renommer les colonnes dans les widgets de tableau

Vous pouvez renommer les colonnes dans la section *Métriques et attributs* d'un widget de table en ouvrant le widget en mode Édition et en cliquant sur le menu en haut de la colonne. Saisissez le nouveau nom et cliquez sur *Enregistrer*, ou cliquez sur *Réinitialiser* pour rétablir le nom d'origine de la colonne.

Notez que cela affecte uniquement le nom d'affichage de la colonne dans le widget de tableau ; le nom de la métrique/attribut ne change pas dans les données sous-jacentes elles-mêmes.



Octobre 2020

Extension par défaut des données d'intégration

Le regroupement de widgets de tableau permet désormais des extensions par défaut des métriques Kubernetes, ONTAP Advanced Data et Agent Node. Par exemple, si vous regroupez les *Nœuds* Kubernetes par *Cluster*, vous verrez une ligne dans le tableau pour chaque cluster. Vous pouvez ensuite développer chaque ligne de cluster pour voir une liste des objets Node.

Support technique de l'édition de base

Le support technique est désormais disponible pour les abonnés à Cloud Insights Basic Edition en plus des éditions Standard et Premium. De plus, Cloud Insights a simplifié le flux de travail de création d'un ticket de support NetApp .

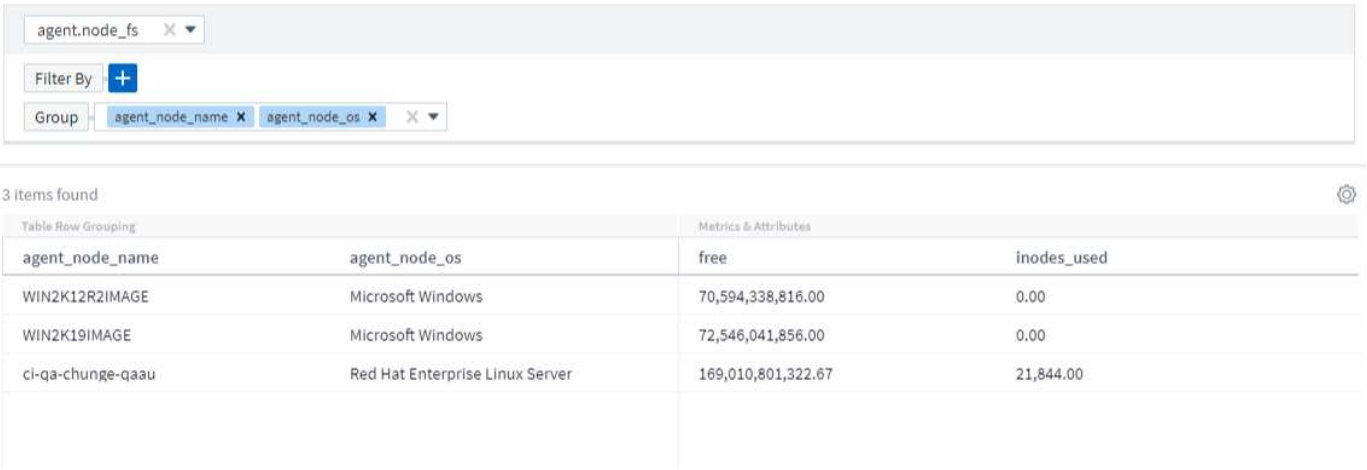
API publique Cloud Secure

Cloud Secure prend en charge"API REST" pour accéder aux informations sur les activités et les alertes. Cela est réalisé grâce à l'utilisation de jetons d'accès API, créés via l'interface utilisateur d'administration Cloud Secure , qui sont ensuite utilisés pour accéder aux API REST. La documentation Swagger pour ces API REST est intégrée à Cloud Secure.

Septembre 2020

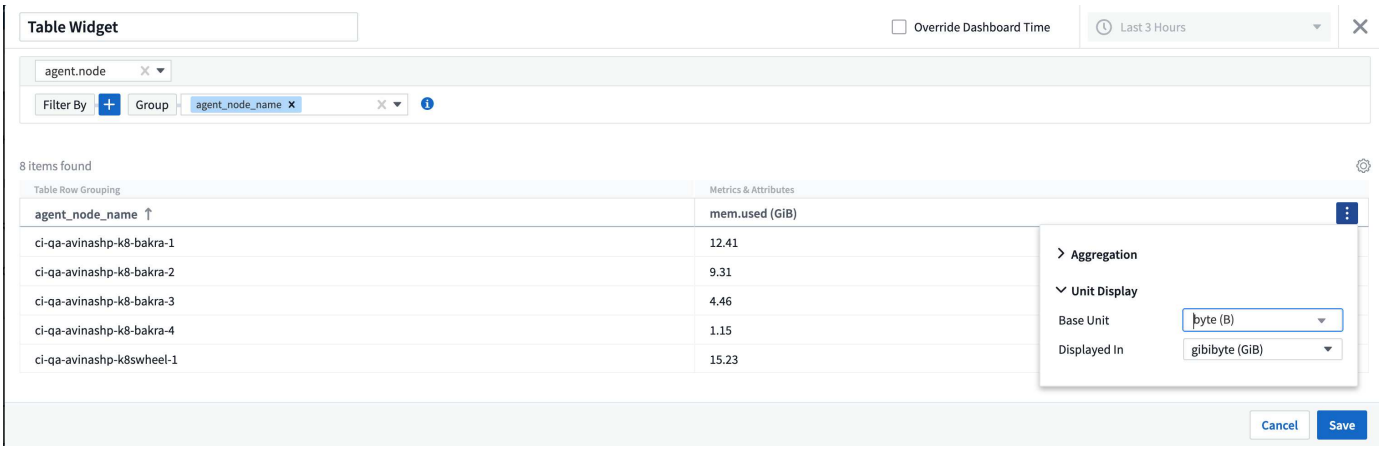
Page de requête avec données d'intégration

La page de requête Cloud Insights prend en charge les données d'intégration (c'est-à-dire de Kubernetes, ONTAP Advanced Metrics, etc.). Lorsque vous travaillez avec des données d'intégration, le tableau des résultats de la requête affiche une vue « Écran partagé », avec l'objet/le regroupement sur le côté gauche et les données d'objet (attributs/métriques) sur la droite. Vous pouvez également choisir plusieurs attributs pour regrouper les données d'intégration.



Formatage de l'affichage des unités dans le widget de tableau

La mise en forme de l'affichage des unités est désormais disponible dans les widgets de tableau pour les colonnes qui affichent des données métriques/compteurs (par exemple, gigaoctets, Mo/seconde, etc.). Pour modifier l'unité d'affichage d'une métrique, cliquez sur le menu « trois points » dans l'en-tête de la colonne et sélectionnez « Affichage de l'unité ». Vous pouvez choisir parmi l'une des unités disponibles. Les unités disponibles varient en fonction du type de données métriques dans la colonne d'affichage.



Page de détails de l'unité d'acquisition

Les unités d'acquisition disposent désormais de leur propre page de destination, fournissant des détails utiles pour chaque AU ainsi que des informations pour aider au dépannage. Le"Page de détails AU" fournit des liens vers les collecteurs de données de l'UA ainsi que des informations utiles sur l'état d'avancement.

Dépendance Docker Cloud Secure supprimée

La dépendance de Cloud Secure sur Docker a été supprimée. Docker n'est plus requis pour l'installation de l'agent Cloud Secure .

Rapports sur les rôles des utilisateurs

Si vous disposez de Cloud Insights Premium Edition avec Reporting, chaque utilisateur Cloud Insights de votre environnement dispose également d'une connexion Single Sign-On (SSO) à l'application Reporting (c'est-à-dire Cognos) ; en cliquant sur le lien **Rapports** dans le menu, ils seront automatiquement connectés à Reporting.

Leur rôle d'utilisateur dans Cloud Insights détermine leur"Rôle d'utilisateur de reporting" :

Rôle de Cloud Insights	Rôle de reporting	Autorisations de signalement
Invité	Consommateur	Peut afficher, planifier et exécuter des rapports et définir des préférences personnelles telles que celles concernant les langues et les fuseaux horaires. Les consommateurs ne peuvent pas créer de rapports ni effectuer de tâches administratives.
Utilisateur	Auteur	Peut exécuter toutes les fonctions du consommateur ainsi que créer et gérer des rapports et des tableaux de bord.

Administrateur	Administrateur	Peut exécuter toutes les fonctions d'auteur ainsi que toutes les tâches administratives telles que la configuration des rapports et l'arrêt et le redémarrage des tâches de reporting.

Cloud Insights Reporting est disponible pour les environnements de 500 MU ou plus.

Si vous êtes un client actuel de l'édition Premium et que vous souhaitez conserver vos rapports, lisez ceci"note importante pour les clients existants" .

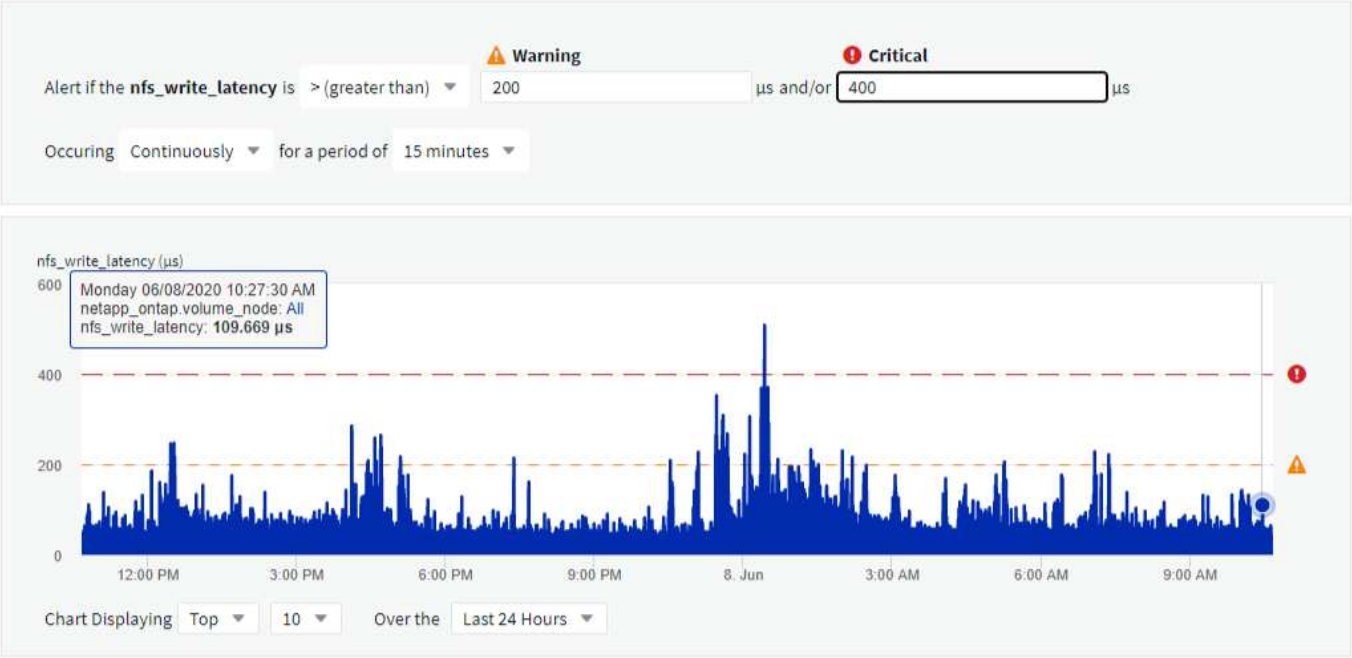
Nouvelle catégorie d'API pour l'ingestion de données

Cloud Insights a ajouté une catégorie d'API **Ingestion de données**, vous offrant un meilleur contrôle sur les données et les agents personnalisés. Une documentation détaillée pour cette catégorie d'API et d'autres est disponible dans Cloud Insights en accédant à **Admin > Accès API** et en cliquant sur le lien *Documentation API*. Vous pouvez également joindre un commentaire à l'AU dans le champ Note, qui s'affiche sur la page de détails de l'AU ainsi que sur la page de liste des AU.

Août 2020

Surveillance et alerte

Outre la possibilité actuelle de définir des politiques de performances pour les objets de stockage, les machines virtuelles, EC2 et les ports, Cloud Insights Standard Edition inclut désormais la possibilité de"configurer les moniteurs" pour les seuils sur les données d'intégration pour Kubernetes, les métriques avancées ONTAP et les plugins Telegraf. Il vous suffit de créer un moniteur pour chaque métrique d'objet pour laquelle vous souhaitez déclencher des alertes, de définir les conditions des seuils de niveau d'avertissement ou de niveau critique et de spécifier le(s) destinataire(s) de courrier électronique souhaité(s) pour chaque niveau. Vous pouvez alors"afficher et gérer les alertes" pour suivre les tendances ou résoudre des problèmes.



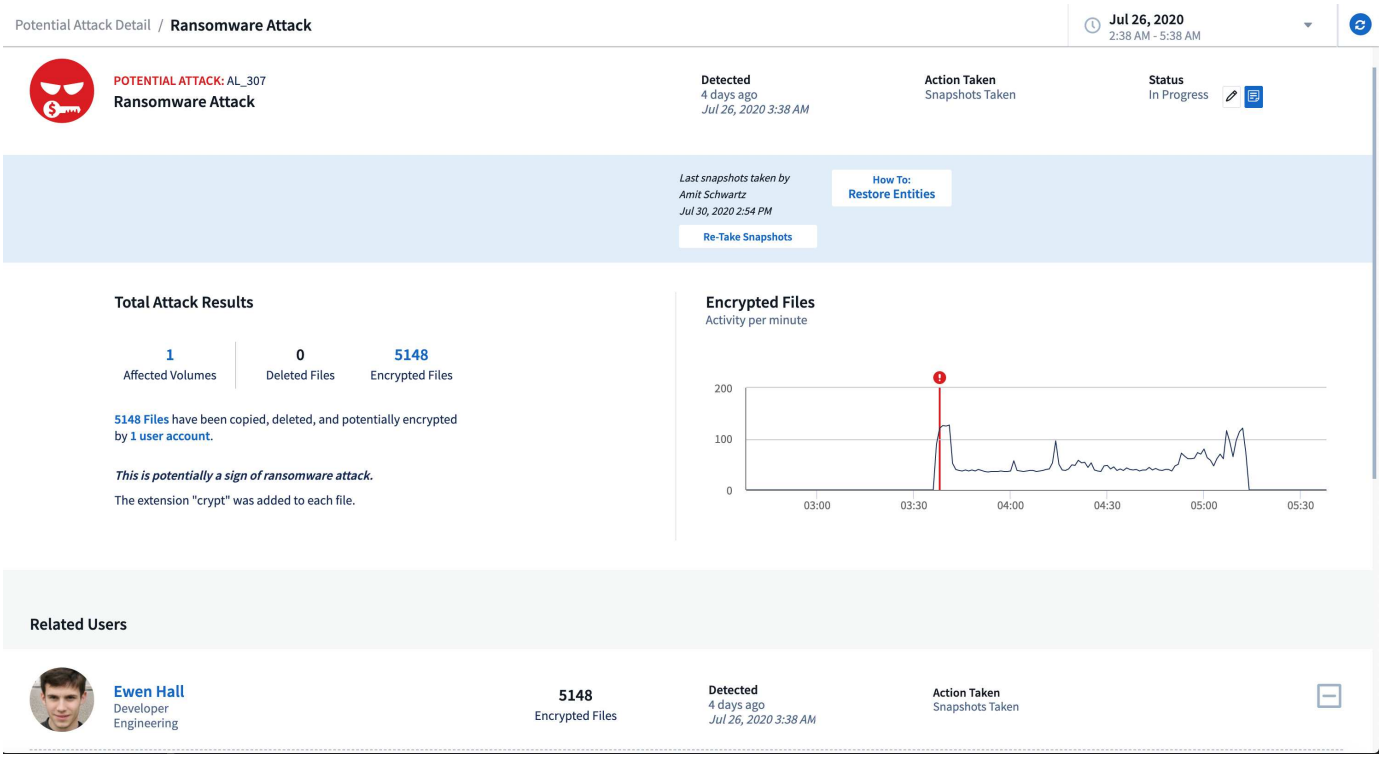
Juillet 2020

Cloud Secure *Prendre un instantané* Action

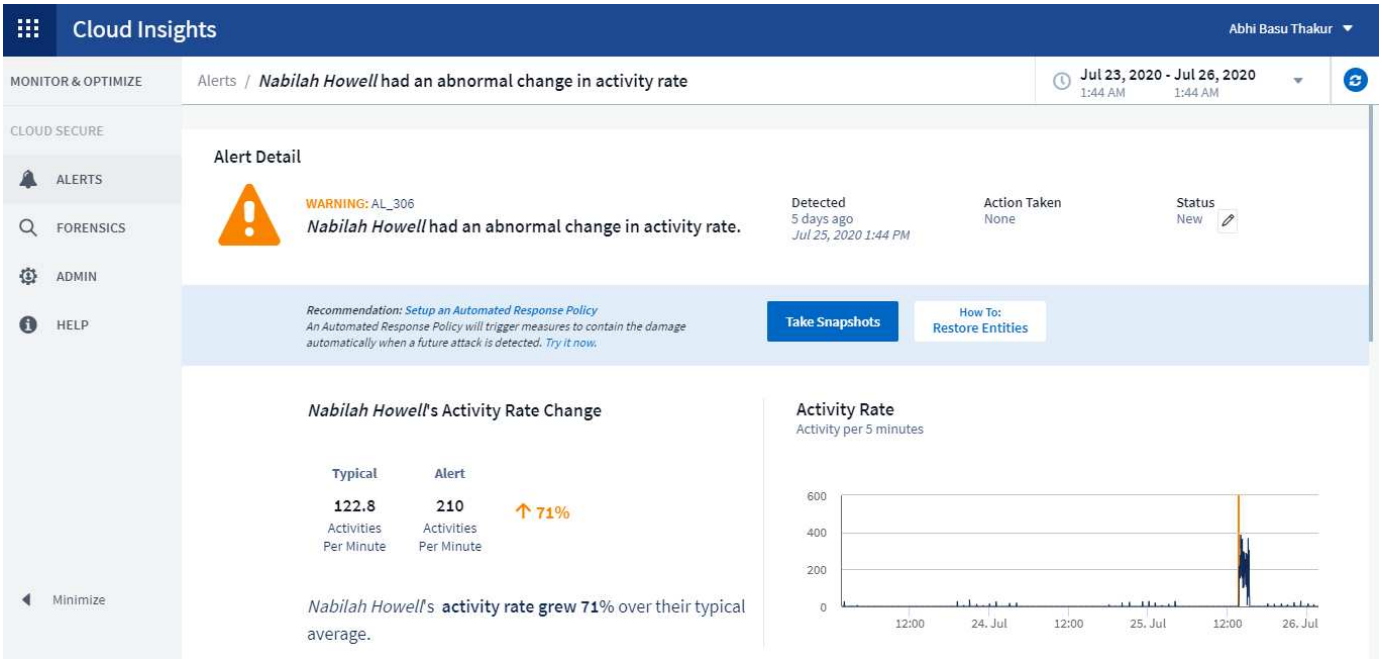
Cloud Secure protège vos données en prenant automatiquement un instantané lorsqu'une activité malveillante est détectée, garantissant ainsi que vos données sont sauvegardées en toute sécurité.

Vous pouvez définir des politiques de réponse automatisées qui prennent un instantané lorsqu'une attaque de ransomware ou une autre activité utilisateur anormale est détectée. Vous pouvez également prendre un instantané manuellement à partir de la page d'alerte.

Capture d'écran automatique
prise :



Instantané manuel :



Mises à jour des métriques/compteurs

Les compteurs de capacité suivants peuvent être utilisés dans l'interface utilisateur et l'API REST de Cloud Insights . Auparavant, ces compteurs n'étaient disponibles que pour l'entrepôt de données / le reporting.

Type d'objet	Comptoir
Stockage	Capacité - Capacité brute de réserve - Capacité brute défaillante

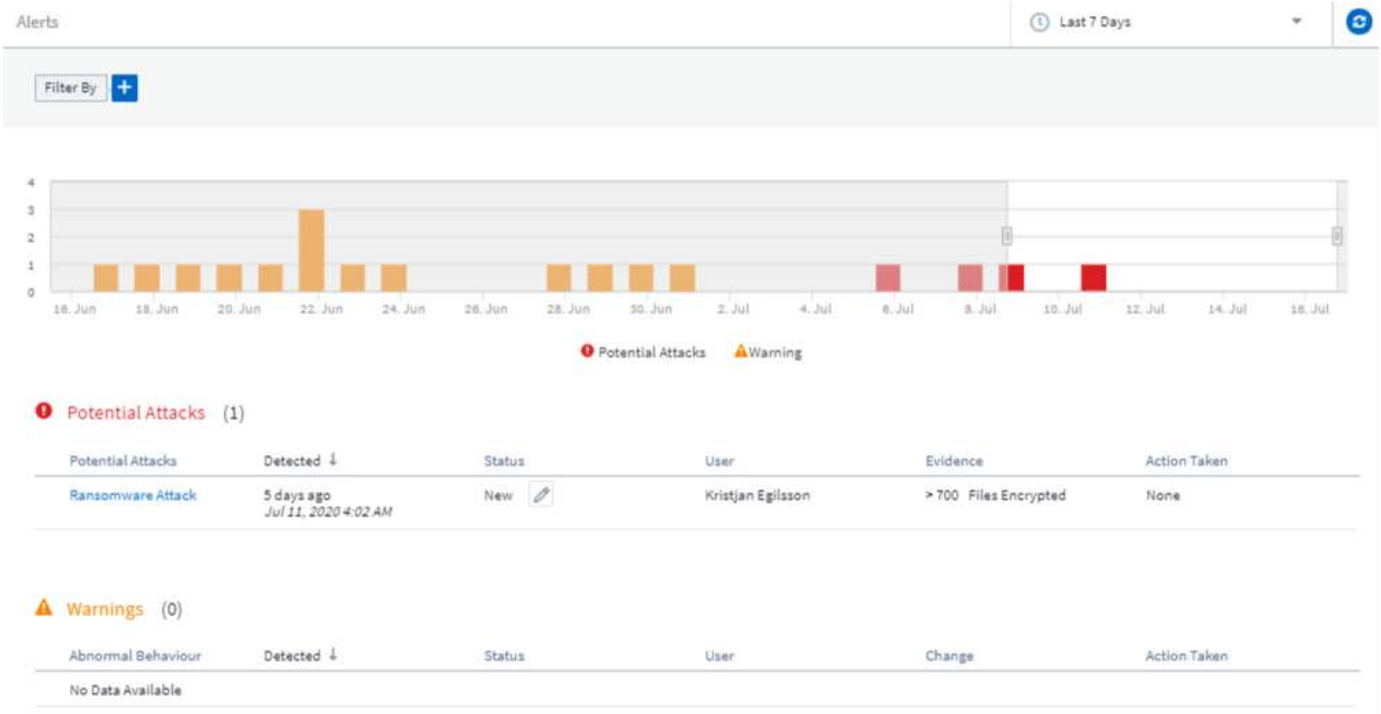
Type d'objet	Comptoir
Piscine de stockage	Capacité de données - Capacité de données utilisée - Total des autres capacités - Autre capacité utilisée - Capacité totale - Capacité brute - Limite souple
Volume interne	Capacité de données - Capacité de données utilisée - Total Autre capacité - Autre capacité utilisée - Total Capacité enregistrée du clone - Total

Détection d'attaques potentielles Cloud Secure

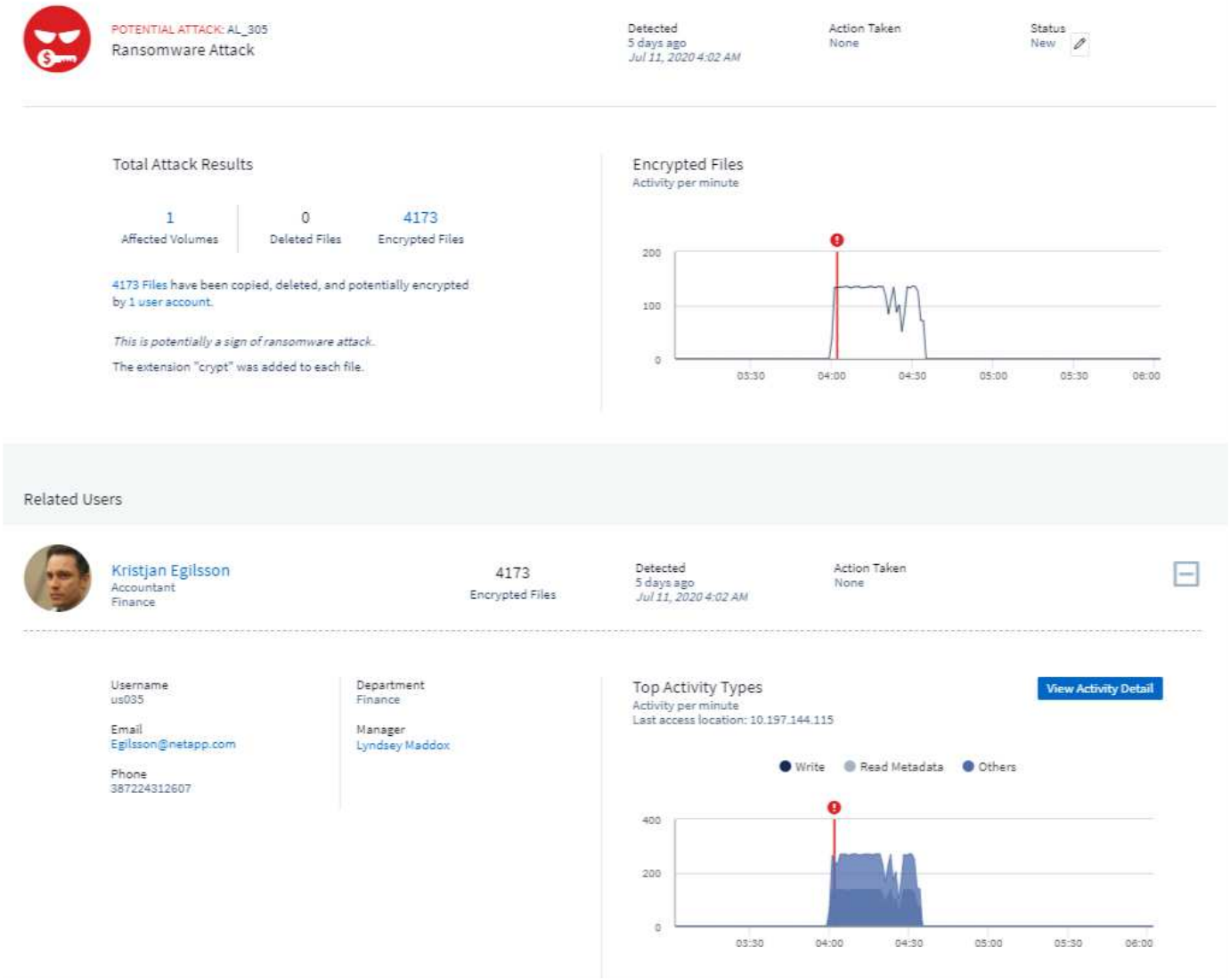
Cloud Secure détecte désormais les attaques potentielles telles que les ransomwares. Cliquez sur une alerte dans la page Liste des alertes pour ouvrir une page de détails affichant les éléments suivants :

- Heure de l'attaque
- Activité utilisateur et fichier associée
- Mesures prises
- Informations complémentaires pour aider à détecter d'éventuelles failles de sécurité

Page d'alertes indiquant une attaque potentielle par ransomware :



Page de détails sur une attaque potentielle par ransomware :



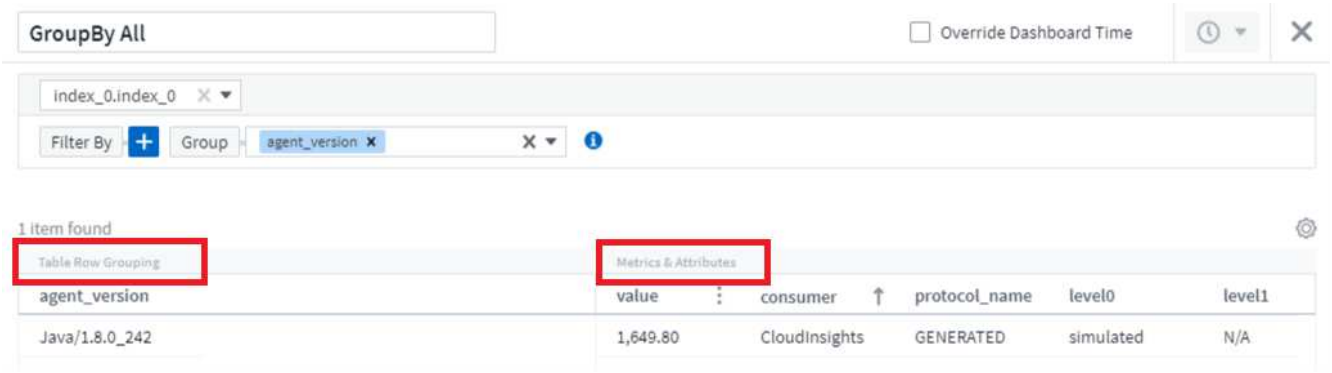
Abonnez-vous à l'édition Premium via AWS

Pendant votre essai de Cloud Insights, vous pouvez"auto-abonnement" via AWS Marketplace vers Cloud Insights Standard Edition ou Premium Edition. Auparavant, vous ne pouviez vous abonner que via AWS Marketplace à l'édition Standard.

Widget de tableau amélioré

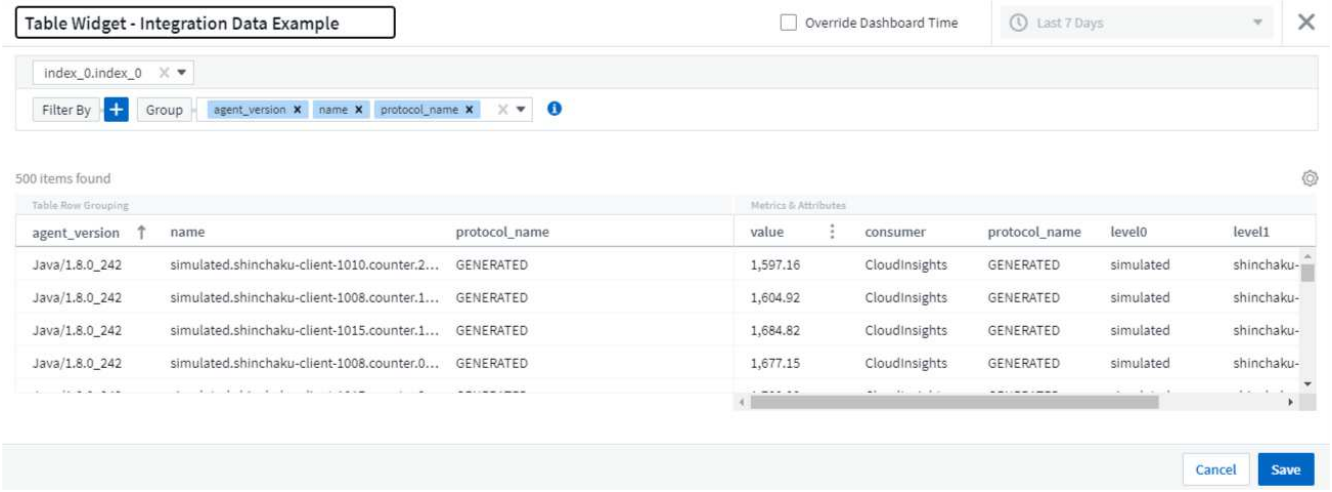
Le widget Tableau du tableau de bord/page d'actifs inclut les améliorations suivantes :

- Vue « Écran partagé » : les widgets de tableau affichent l'objet/le regroupement sur le côté gauche et les données de l'objet (attributs/métriques) sur le côté droit.



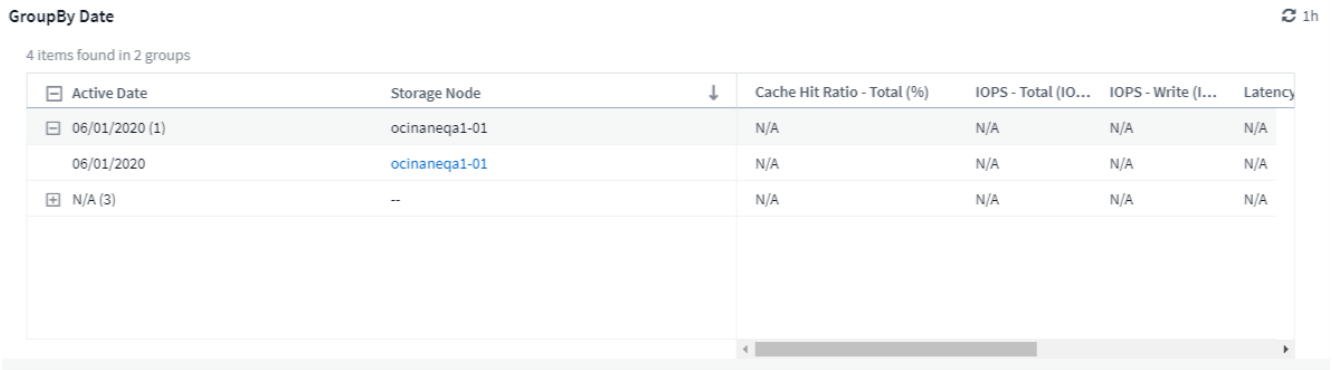
- Regroupement d'attributs multiples : pour les données d'intégration (Kubernetes, ONTAP Advanced Metrics, Docker, etc.), vous pouvez choisir plusieurs attributs pour le regroupement. Les données sont affichées en fonction des attributs de regroupement que vous choisissez.

  Regroupement avec données d'intégration (affiché en mode Édition) :



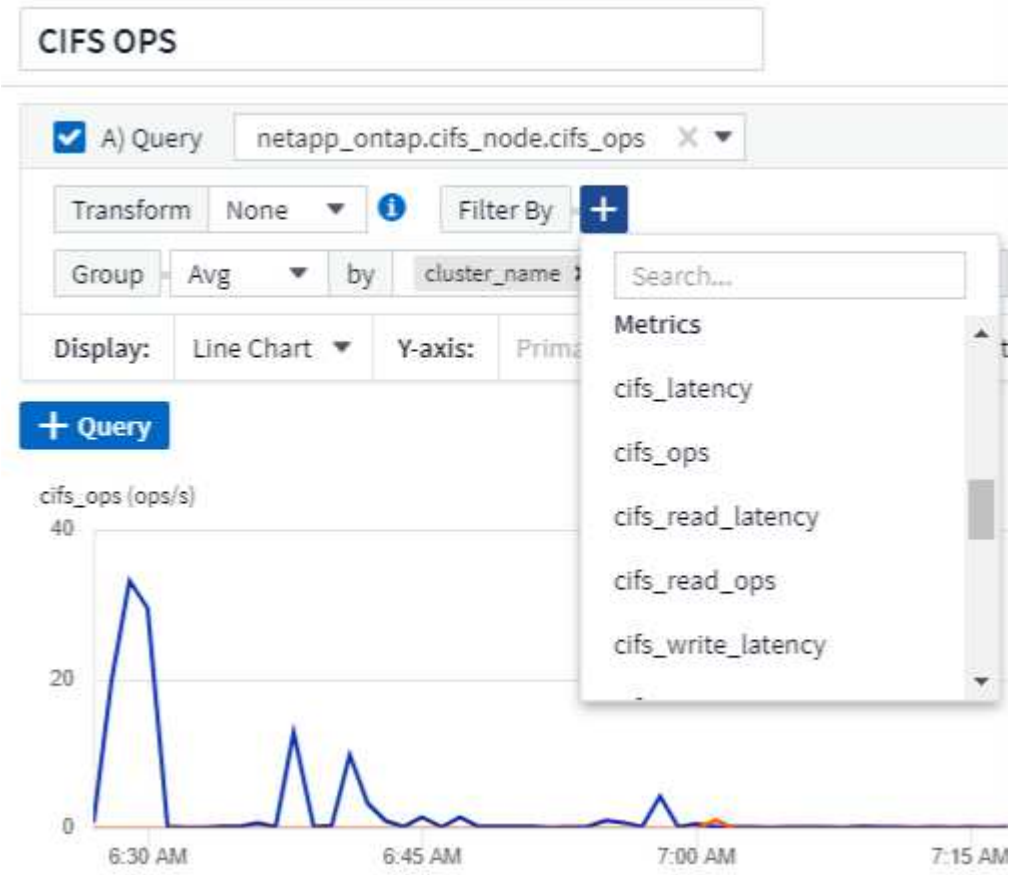
- Le regroupement des données d'infrastructure (stockage, EC2, VM, ports, etc.) s'effectue par un seul attribut comme auparavant. Lors du regroupement par un attribut qui n'est pas l'objet, le tableau vous permettra de développer la ligne du groupe pour voir tous les objets du groupe.

  Regroupement avec données d'infrastructure (affiché en mode d'affichage) :

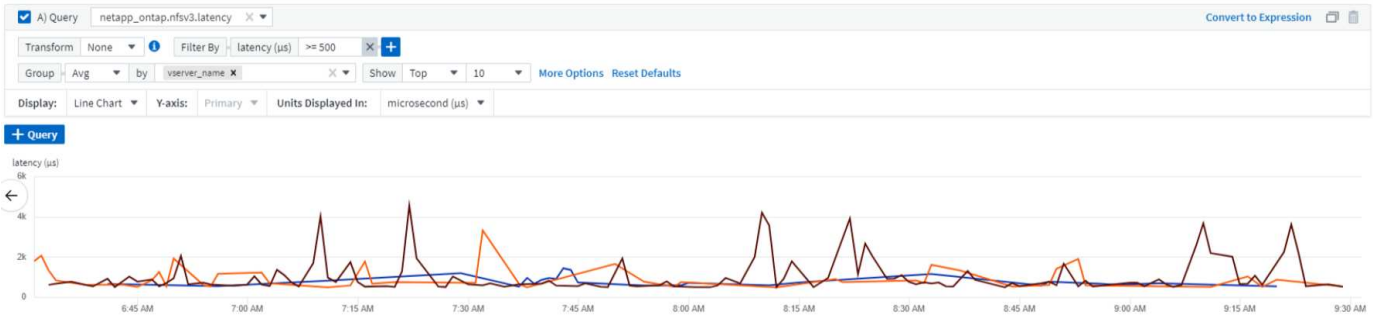


Filtrage des métriques

En plus de filtrer sur les attributs d'un objet dans un widget, vous pouvez désormais également filtrer sur les métriques.



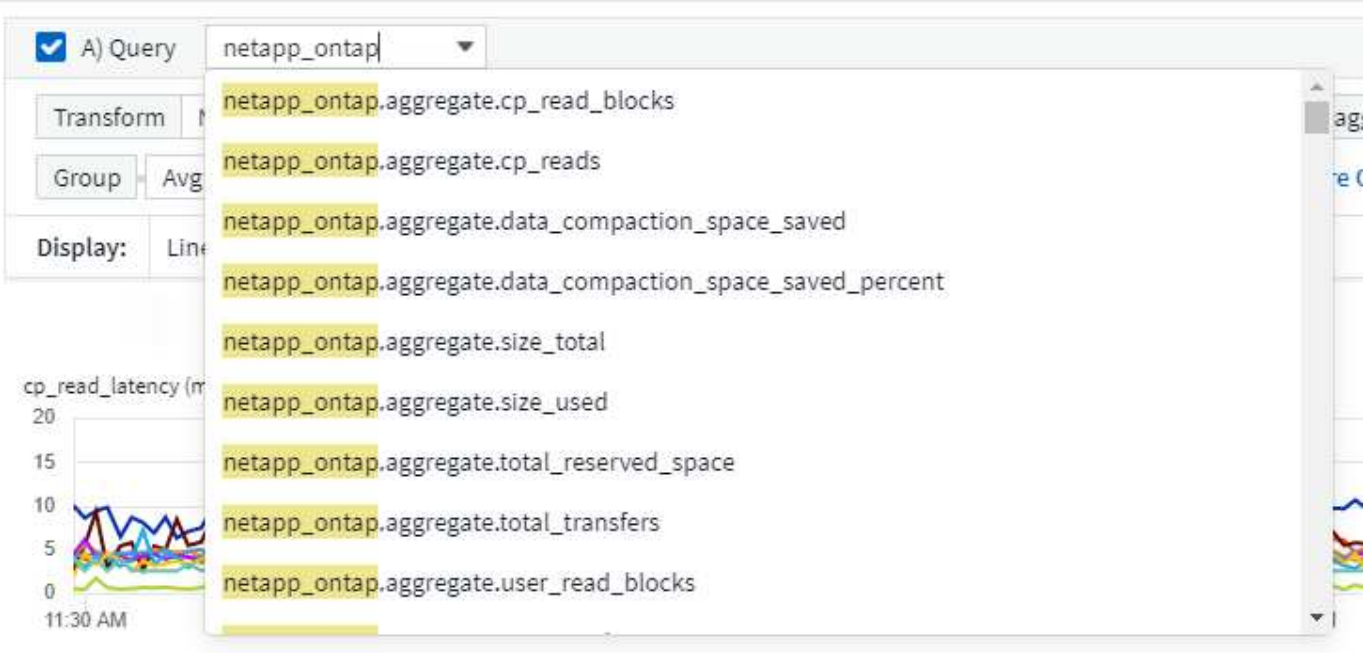
Lorsque vous travaillez avec des données d'intégration (Kubernetes, ONTAP Advanced Data, etc.), le filtrage des métriques supprime les points de données individuels/non appariés de la série de données tracées, contrairement aux données d'infrastructure (stockage, VM, ports, etc.) où les filtres fonctionnent sur la valeur agrégée de la série de données et suppriment potentiellement l'objet entier du graphique.



Données de compteur avancées ONTAP

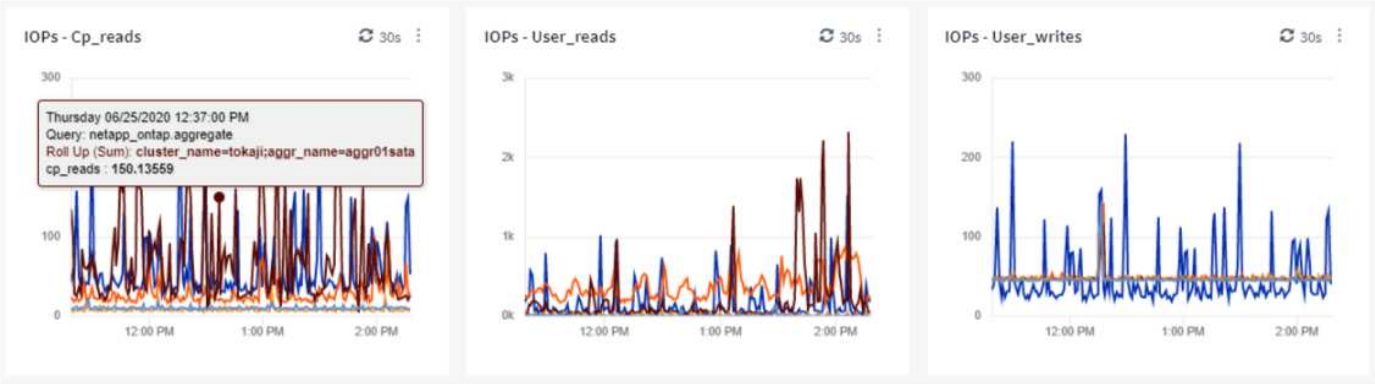
Cloud Insights tire parti des **données de compteur avancées** spécifiques à ONTAP de NetApp, qui fournissent une multitude de compteurs et de mesures collectés à partir des périphériques ONTAP . Les données de compteur avancées ONTAP sont disponibles pour tous les clients NetApp ONTAP . Ces mesures permettent une visualisation personnalisée et étendue dans les widgets et tableaux de bord Cloud Insights .

Les compteurs avancés ONTAP peuvent être trouvés en recherchant « netapp_ontap » dans la requête du widget et en sélectionnant parmi les compteurs.



Vous pouvez affiner votre recherche en saisissant des parties supplémentaires du nom du compteur. Par exemple:

- *vie*
- *agrégat*
- *offbox_vscan_server*
- et plus



Veuillez noter ce qui suit :

- La collecte de données avancées sera activée par défaut pour les nouveaux collecteurs de données ONTAP . Pour activer la collecte de données avancées pour vos collecteurs de données ONTAP existants, modifiez le collecteur de données et développez la section *Configuration avancée*.
- La collecte de données avancées n'est pas disponible pour ONTAP 7-mode.

Tableaux de bord de compteur avancés

Cloud Insights est fourni avec une variété de tableaux de bord prédéfinis pour vous aider à démarrer la visualisation des compteurs avancés ONTAP pour des sujets tels que *Performances globales*, *Charge de travail du volume*, *Activité du processeur*, et plus encore. Si vous avez au moins un collecteur de données ONTAP configuré, ceux-ci peuvent être importés à partir de la galerie de tableaux de bord sur n'importe quelle page de liste de tableaux de bord.

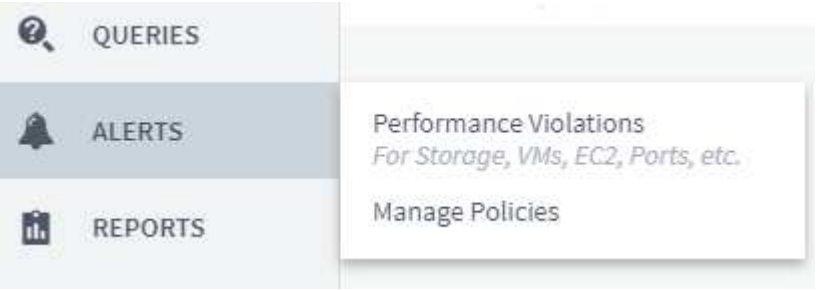
En savoir plus

Vous trouverez plus d'informations sur ONTAP Advanced Data via les liens suivants :

- https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest(Remarque : vous devrez vous connecter au support NetApp)
- https://nabox.org/faq/

Menu des politiques et des violations

Les politiques de performance et les violations se trouvent désormais dans le menu **Alertes**. Les fonctionnalités de politique et de violation restent inchangées.



Agent Telegraf mis à jour

L'agent d'ingestion des données d'intégration Telegraf a été mis à jour pour"version 1.14" , qui comprend des

corrections de bugs, des correctifs de sécurité et de nouveaux plugins.

Remarque : lors de la configuration d'un collecteur de données Kubernetes sur la plateforme Kubernetes, vous pouvez voir une erreur « Statut HTTP 403 Interdit » dans le journal, en raison d'autorisations insuffisantes dans l'attribut « clusterrole ».

Pour contourner ce problème, ajoutez les lignes en surbrillance suivantes à la section *rules:* du clusterrole d'accès au point de terminaison, puis redémarrez les pods Telegraf.

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

Juin 2020

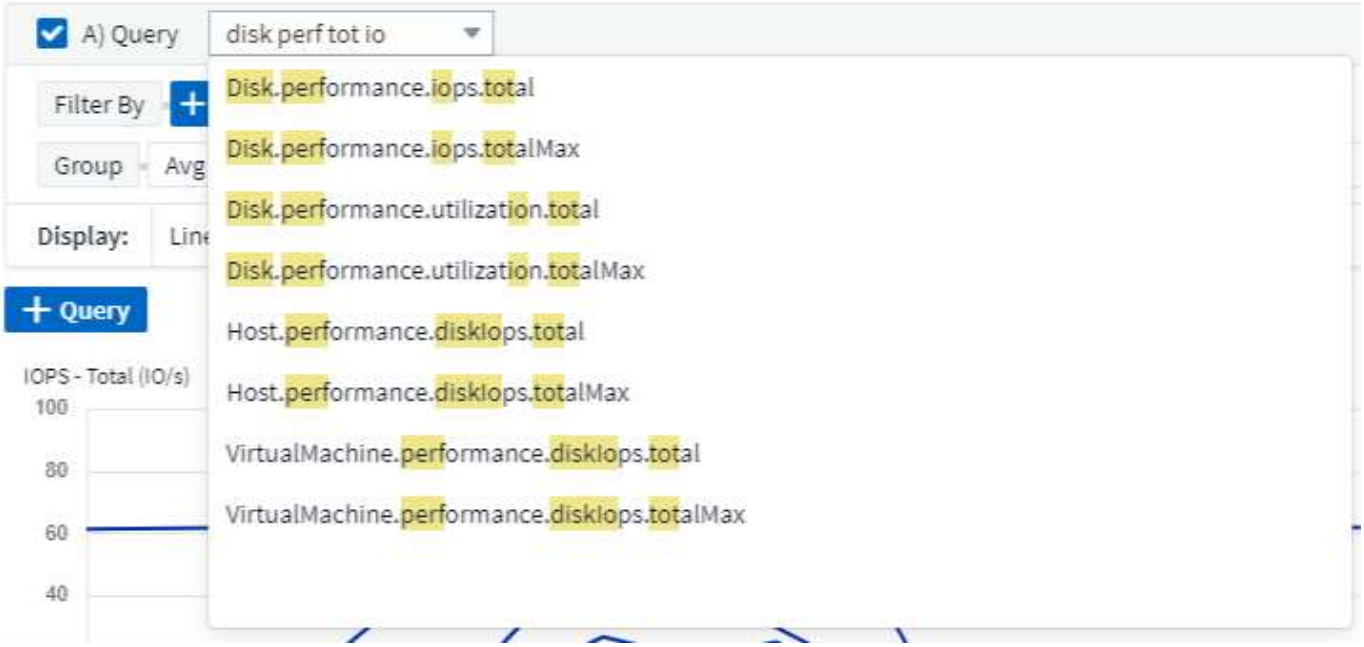
Rapport d'erreurs simplifié du collecteur de données

Signaler une erreur du collecteur de données est plus facile avec le bouton *Envoyer un rapport d'erreur* sur la page du collecteur de données. Cliquer sur le bouton envoie des informations de base sur l'erreur à NetApp et invite à enquêter sur le problème. Une fois appuyé, Cloud Insights reconnaît que NetApp a été notifié et le bouton Rapport d'erreur est désactivé pour indiquer qu'un rapport d'erreur pour ce collecteur de données a été envoyé. Le bouton reste désactivé jusqu'à ce que la page du navigateur soit actualisée.

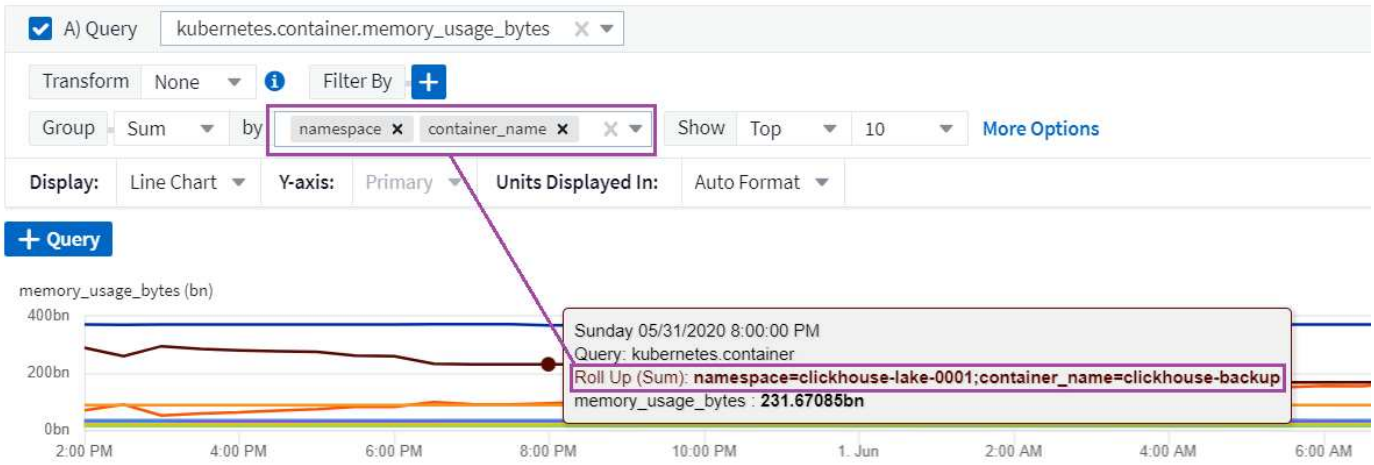
Améliorations des widgets

Les améliorations suivantes ont été apportées aux widgets du tableau de bord. Ces améliorations sont considérées comme des fonctionnalités d'aperçu et peuvent ne pas être disponibles pour tous les environnements Cloud Insights .

- Nouveau sélecteur d'objet/métrique : les objets (stockage, disque, ports, nœuds, etc.) et leurs métriques associées (IOPS, latence, nombre de CPU, etc.) sont désormais disponibles dans les widgets dans une seule liste déroulante inclusive avec une puissante capacité de recherche. Vous pouvez saisir plusieurs termes partiels dans la liste déroulante et Cloud Insights répertorie toutes les métriques d'objet répondant à ces termes.



- Regroupement de plusieurs balises : lorsque vous travaillez avec des données d'intégration (Kubernetes, etc.), vous pouvez regrouper les données par plusieurs balises/attributs. Par exemple, additionnez l'utilisation de la mémoire par espace de noms Kubernetes et nom de conteneur.



Mai 2020

Rapports sur les rôles des utilisateurs

Les rôles suivants ont été ajoutés pour le reporting :

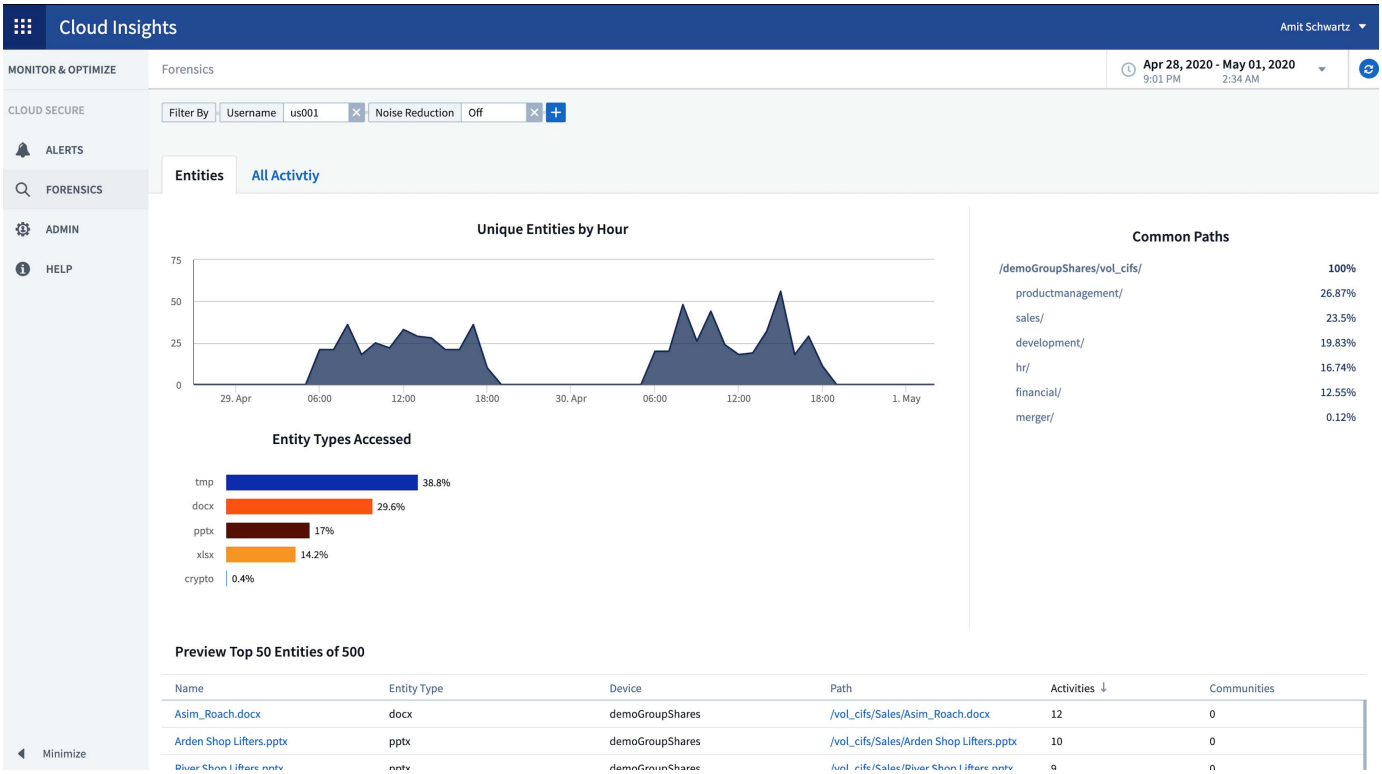
- Consommateurs Cloud Insights : peuvent exécuter et afficher des rapports
- Auteurs de Cloud Insights : peuvent exécuter les fonctions de consommateur ainsi que créer et gérer des rapports et des tableaux de bord
- Administrateurs Cloud Insights : peuvent exécuter les fonctions d'auteur ainsi que toutes les tâches administratives

Mises à jour Cloud Secure

Cloud Insights inclut les modifications récentes suivantes Cloud Secure .

Dans la page Forensics > Activity Forensics, nous proposons deux vues pour analyser et enquêter sur l'activité des utilisateurs :

- Vue d'activité, centrée sur l'activité de l'utilisateur (Quelle opération ? Où a-t-elle été réalisée ?)
- Vue des entités, centrée sur les fichiers auxquels l'utilisateur a accédé.

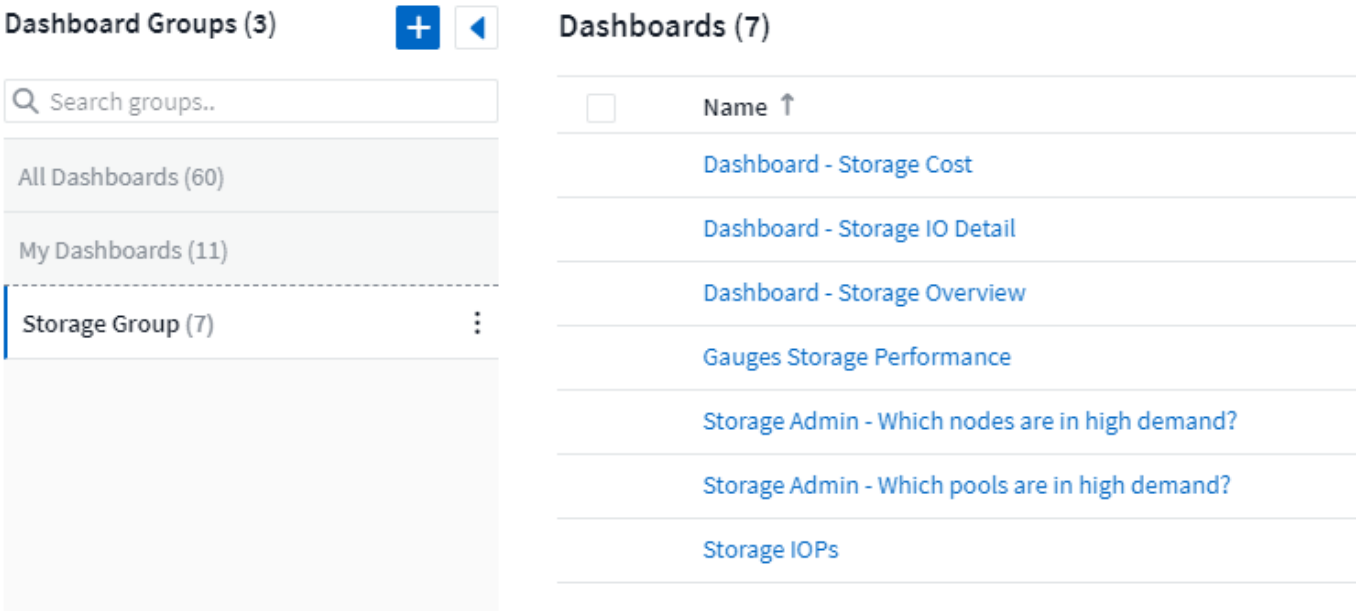


De plus, la notification par e-mail d'alerte contient désormais un lien direct vers la page d'alerte.

Regroupement du tableau de bord

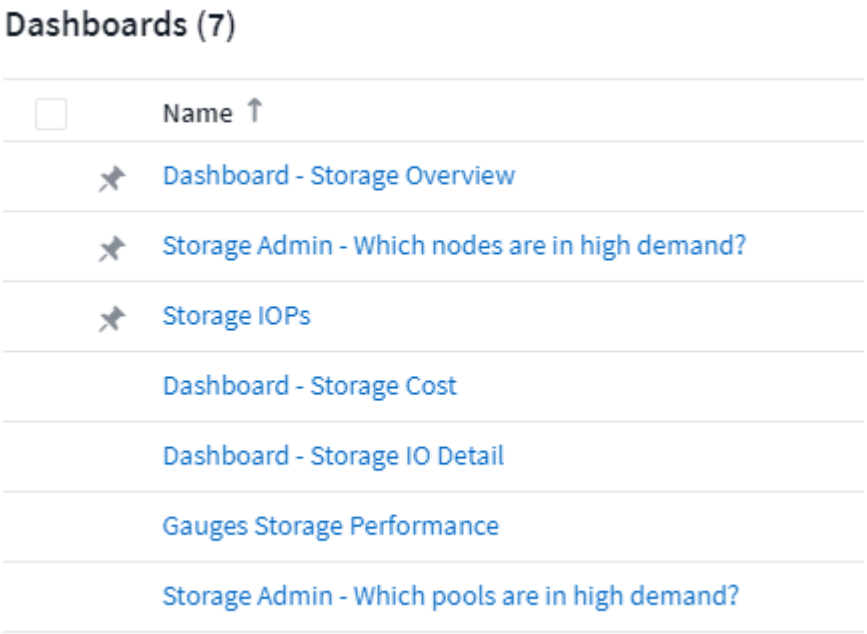
Le regroupement du tableau de bord permet une meilleure"gestion des tableaux de bord" qui vous concernent. Vous pouvez ajouter des tableaux de bord associés à un groupe pour une gestion « unique », par exemple, de votre stockage ou de vos machines virtuelles.

Les groupes sont personnalisés par utilisateur, donc les groupes d'une personne peuvent être différents de ceux d'une autre. Vous pouvez avoir autant de groupes que vous le souhaitez, avec aussi peu ou autant de tableaux de bord dans chaque groupe que vous le souhaitez.



Épinglage du tableau de bord

Vous pouvez épingler des tableaux de bord afin que les favoris apparaissent toujours en haut de la liste.



Mode TV et rafraîchissement automatique

"Mode TV et rafraîchissement automatique"permettre l'affichage en temps quasi réel des données sur un tableau de bord ou une page d'actif :

- **Le mode TV** offre un affichage épuré ; le menu de navigation est masqué, offrant plus d'espace à l'écran pour l'affichage de vos données.
- Données dans les widgets des tableaux de bord et des pages de destination des ressources **Actualisation automatique** selon un intervalle d'actualisation (aussi peu que toutes les 10 secondes) déterminé par la plage horaire du tableau de bord sélectionnée (ou la plage horaire du widget, si elle est définie pour remplacer l'heure du tableau de bord).

Combinés, le mode TV et l'actualisation automatique offrent une vue en direct de vos données Cloud Insights , parfaite pour des démonstrations transparentes ou une surveillance interne.

Avril 2020

Nouveaux choix de plages horaires du tableau de bord

Les choix de plage horaire pour les tableaux de bord et autres pages d'informations Cloud incluent désormais *Dernière heure* et *15 dernières minutes*.

Mises à jour Cloud Secure

Cloud Insights inclut les modifications récentes suivantes Cloud Secure .

- Meilleure reconnaissance des modifications des métadonnées des fichiers et des dossiers pour détecter si l'utilisateur a changé d'autorisation, de propriétaire ou de propriété de groupe.
- Exporter le rapport d'activité de l'utilisateur au format CSV.

Cloud Secure surveille et audite toutes les opérations d'accès des utilisateurs aux fichiers et aux dossiers. L'audit d'activité vous permet de vous conformer aux politiques de sécurité internes, de répondre aux exigences de conformité externes telles que PCI, GDPR et HIPAA, et de mener des enquêtes sur les violations de données et les incidents de sécurité.

Heure par défaut du tableau de bord

La plage horaire par défaut des tableaux de bord est désormais de 3 heures au lieu de 24 heures.

Temps d'agrégation optimisés

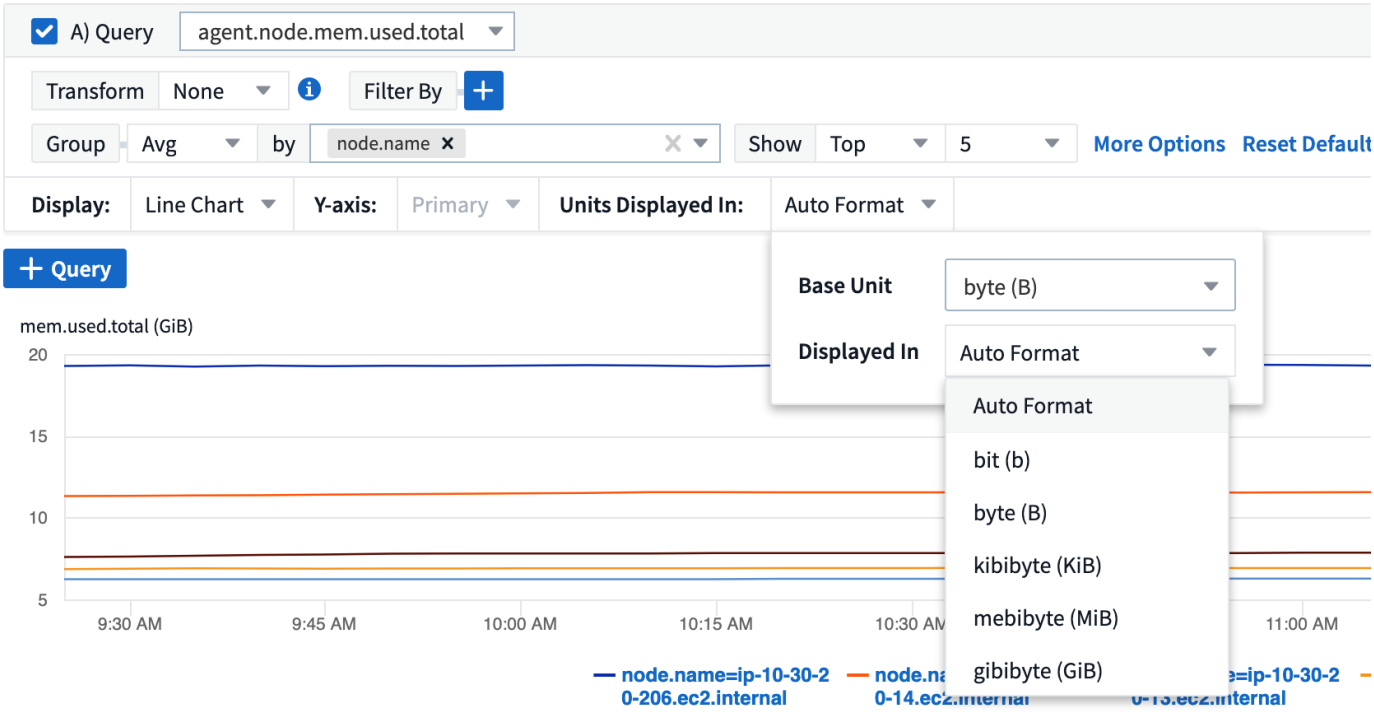
Optimisé"agrégation temporelle" Les intervalles dans les widgets de séries chronologiques (graphiques linéaires, splines, de surface et de surface empilée) sont plus fréquents pour les plages de temps de tableau de bord/widget de 3 heures et de 24 heures, ce qui permet une représentation graphique plus rapide des données.

- La plage horaire de 3 heures est optimisée sur un intervalle d'agrégation de 1 minute. Auparavant, c'était 5 minutes.
- La plage horaire de 24 heures est optimisée sur un intervalle d'agrégation de 30 minutes. Auparavant, c'était 1 heure.

Vous pouvez toujours remplacer l'agrégation optimisée en définissant un intervalle personnalisé.

Formatage automatique de l'unité d'affichage

Dans la plupart des widgets, Cloud Insights connaît l'unité de base dans laquelle afficher les valeurs, par exemple *Mégaoctets*, *Milliers*, *Pourcentage*, *Millisecondes (ms)*, etc., et maintenant"formate automatiquement" le widget à l'unité la plus lisible. Par exemple, une valeur de données de 1 234 567 890 octets serait automatiquement formatée à 1,23 gibioctet. Dans de nombreux cas, Cloud Insights connaît le meilleur format pour les données acquises. Dans les cas où le meilleur format n'est pas connu, ou dans les widgets où vous souhaitez remplacer le formatage automatique, vous pouvez choisir le format souhaité.



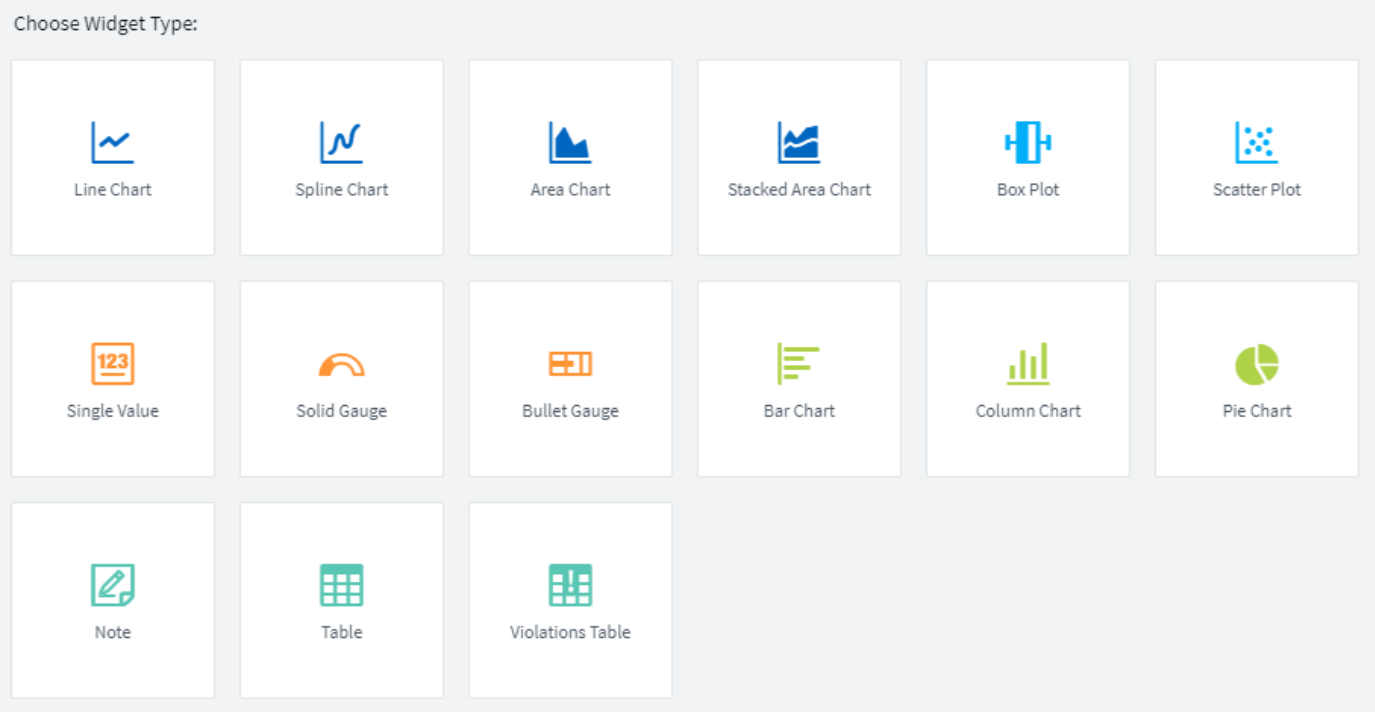
Importer des annotations à l'aide de l'API

Avec la puissante API de Cloud Insights Premium Edition, vous pouvez désormais"importer des annotations" et les affecter à des objets à l'aide d'un fichier .CSV. Vous pouvez également importer des applications et affecter des entités commerciales de la même manière.

Sélecteur de widgets plus simple

L'ajout de widgets aux tableaux de bord et aux pages de destination des ressources est simplifié grâce à un nouveau sélecteur de widgets qui affiche tous les types de widgets dans une vue unique et globale. L'utilisateur n'a donc plus besoin de parcourir une liste de types de widgets pour trouver celui qu'il souhaite ajouter. Les widgets associés sont coordonnés par couleur et regroupés par proximité dans le nouveau

sélecteur.



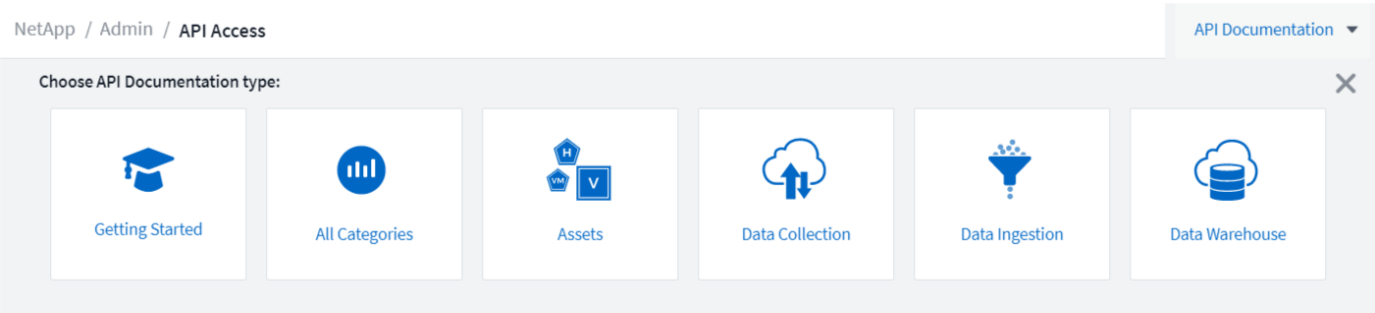
Février 2020

API avec édition Premium

Cloud Insights Premium Edition est livré avec un"API puissante" qui peut être utilisé pour intégrer Cloud Insights à d'autres applications, telles que CMDB ou d'autres systèmes de billetterie.

Des informations détaillées basées sur Swagger se trouvent dans **Admin > Accès API**, sous le lien **Documentation API**. Swagger fournit une brève description et des informations d'utilisation de l'API et vous permet d'essayer chaque API dans votre environnement.

L'API Cloud Insights utilise des jetons d'accès pour fournir un accès basé sur des autorisations aux catégories d'API, telles que les ACTIFS ou la COLLECTION.



Interrogation initiale après l'ajout d'un collecteur de données

Auparavant, après avoir configuré un nouveau collecteur de données, Cloud Insights interrogeait immédiatement le collecteur de données pour collecter les données d'inventaire, mais attendait l'intervalle

d'interrogation des performances configuré (généralement 15 minutes) pour collecter les données de performances initiales. Il attendrait ensuite un autre intervalle avant de lancer la deuxième enquête de performance, ce qui signifie qu'il faudrait jusqu'à *30 minutes* avant que des données significatives soient acquises à partir d'un nouveau collecteur de données.

Collecteur de données"vote" a été grandement amélioré, de sorte que l'enquête de performance initiale se produit immédiatement après l'enquête d'inventaire, la deuxième enquête de performance se produisant quelques secondes après la fin de la première enquête de performance. Cela permet à Cloud Insights de commencer à afficher des données utiles sur des tableaux de bord et des graphiques dans un délai très court.

Ce comportement de sondage se produit également après la modification de la configuration d'un collecteur de données existant.

Duplication de widgets plus facile

Il est plus facile que jamais de créer une copie d'un widget sur un tableau de bord ou une page de destination. En mode Édition du tableau de bord, cliquez sur le menu du widget et sélectionnez **Dupliquer**. L'éditeur de widgets est lancé, pré-rempli avec la configuration du widget d'origine et avec un suffixe « copie » dans le nom du widget. Vous pouvez facilement apporter les modifications nécessaires et enregistrer le nouveau widget. Le widget sera placé en bas de votre tableau de bord et vous pourrez le positionner selon vos besoins. N'oubliez pas de sauvegarder votre tableau de bord lorsque toutes les modifications sont terminées.

Authentification unique (SSO)

Avec Cloud Insights Premium Edition, les administrateurs peuvent activer *"Authentification unique" * Accès (SSO) à Cloud Insights pour tous les utilisateurs de leur domaine d'entreprise, sans avoir à les inviter individuellement. Avec SSO activé, tout utilisateur disposant de la même adresse e-mail de domaine peut se connecter à Cloud Insights à l'aide de ses informations d'identification d'entreprise.

SSO est uniquement disponible dans Cloud Insights Premium Edition et doit être configuré avant de pouvoir être activé pour Cloud Insights. La configuration SSO comprend"Fédération d'identité" via NetApp Cloud Central. La fédération permet aux utilisateurs à authentification unique d'accéder à vos comptes NetApp Cloud Central à l'aide des informations d'identification de votre annuaire d'entreprise.

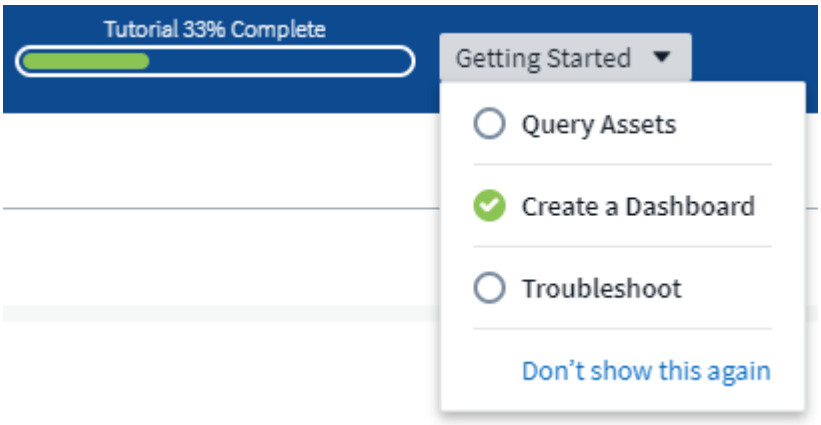
Janvier 2020

Documentation Swagger pour l'API REST

Swagger explique chaque API REST disponible dans Cloud Insights, ainsi que son utilisation et sa syntaxe. Des informations sur les API Cloud Insights sont disponibles dans"documentation" .

Barre de progression des didacticiels sur les fonctionnalités

La liste de contrôle des didacticiels de fonctionnalités a été déplacée vers la bannière supérieure et comporte désormais un indicateur de progression. Les tutoriels sont disponibles pour chaque utilisateur jusqu'à leur fermeture et sont toujours disponibles dans Cloud Insights"documentation" .



Modifications de l'unité d'acquisition

Lors de l'installation d'une unité d'acquisition (AU) sur un hôte ou une machine virtuelle portant le même nom qu'une AU déjà installée, Cloud Insights garantit un nom unique en ajoutant au nom de l'AU « _1 », « _2 », etc. C'est également le cas lors de la désinstallation et de la réinstallation d'une AU de la même machine virtuelle sans la supprimer au préalable de Cloud Insights. Vous voulez un nom d'UA complètement différent ? Aucun problème ; les AU peuvent être renommés après l'installation.

Agrégation temporelle optimisée dans les widgets

Dans les widgets, vous pouvez choisir entre un intervalle d'agrégation de temps *Optimisé* ou un intervalle *Personnalisé* que vous définissez. L'agrégation optimisée sélectionne automatiquement l'intervalle de temps approprié en fonction de la plage de temps du tableau de bord sélectionnée (ou de la plage de temps du widget, en cas de remplacement de l'heure du tableau de bord). L'intervalle change de manière dynamique à mesure que la plage de temps du tableau de bord ou du widget est modifiée.

Processus simplifié de « Mise en route avec Cloud Insights»

Le processus de démarrage de Cloud Insights a été simplifié pour rendre votre première configuration plus fluide et plus facile. Sélectionnez simplement un collecteur de données initial et suivez les instructions. Cloud Insights vous guidera dans la configuration du collecteur de données et de tout agent ou unité d'acquisition requis. Dans la plupart des cas, il importera même un ou plusieurs tableaux de bord initiaux afin que vous puissiez commencer à obtenir rapidement un aperçu de votre environnement (mais veuillez prévoir jusqu'à 30 minutes pour que Cloud Insights collecte des données significatives).

Améliorations supplémentaires :

- L’installation de l’unité d’acquisition est plus simple et plus rapide.
- Les choix de collecteurs de données alphabétiques facilitent la recherche de celui que vous recherchez.
- Les instructions de configuration du collecteur de données amélioré sont plus faciles à suivre.
- Les utilisateurs expérimentés peuvent ignorer le processus de démarrage en cliquant sur un bouton.
- Une nouvelle barre de progression vous indique où vous en êtes dans le processus.

Data Infrastructure Insights

Avant de pouvoir commencer à travailler avec Data Infrastructure Insights, vous devez vous inscrire sur le portail * NetApp Console*. Si vous disposez déjà d’une connexion à la NetApp Console , vous pouvez démarrer un essai gratuit de Data Infrastructure Insights en quelques étapes rapides.

Ces instructions sont en cours de mise à jour. Veuillez consulter cette page ultérieurement.

Sécurité

Data Infrastructure Insights et sécurité

La sécurité des données des produits et des clients est de la plus haute importance chez NetApp. Data Infrastructure Insights suit les meilleures pratiques de sécurité tout au long du cycle de vie de la version pour garantir que les informations et les données des clients sont sécurisées de la meilleure façon possible.

Aperçu de la sécurité

Sécurité physique

L'infrastructure de production de Data Infrastructure Insights est hébergée dans Amazon Web Services (AWS). Les contrôles liés à la sécurité physique et environnementale pour les serveurs de production Data Infrastructure Insights , qui incluent les bâtiments ainsi que les serrures ou les clés utilisées sur les portes, sont gérés par AWS. Selon AWS : « L'accès physique est contrôlé à la fois au niveau du périmètre et aux points d'entrée du bâtiment par un personnel de sécurité professionnel utilisant la vidéosurveillance, des systèmes de détection d'intrusion et d'autres moyens électroniques. Le personnel autorisé utilise des mécanismes d'authentification multifactorielle pour accéder aux étages du centre de données.

Data Infrastructure Insights suit les meilleures pratiques de la"Modèle de responsabilité partagée" décrit par AWS.

Sécurité des produits

Data Infrastructure Insights suit un cycle de développement conforme aux principes Agile, nous permettant ainsi de traiter plus rapidement les défauts logiciels liés à la sécurité, par rapport aux méthodologies de développement à cycle de publication plus long. Grâce à des méthodologies d'intégration continue, nous sommes en mesure de répondre rapidement aux changements fonctionnels et de sécurité. Les procédures et politiques de gestion des changements définissent quand et comment les changements se produisent et contribuent à maintenir la stabilité de l'environnement de production. Tous les changements importants sont formellement communiqués, coordonnés, correctement examinés et approuvés avant leur publication dans l'environnement de production.

Sécurité du réseau

L'accès réseau aux ressources de l'environnement Data Infrastructure Insights est contrôlé par des pare-feu basés sur l'hôte. Chaque ressource (comme un équilibreur de charge ou une instance de machine virtuelle) dispose d'un pare-feu basé sur l'hôte qui limite le trafic entrant aux seuls ports nécessaires à cette ressource pour exécuter sa fonction.

Data Infrastructure Insights utilise divers mécanismes, notamment des services de détection d'intrusion, pour surveiller l'environnement de production afin de détecter les anomalies de sécurité.

L'évaluation des risques

L'équipe Data Infrastructure Insights suit un processus d'évaluation des risques formalisé pour fournir un moyen systématique et reproductible d'identifier et d'évaluer les risques afin qu'ils puissent être gérés de manière appropriée grâce à un plan de traitement des risques.

Protection des données

L'environnement de production Data Infrastructure Insights est configuré dans une infrastructure hautement redondante utilisant plusieurs zones de disponibilité pour tous les services et composants. Outre l'utilisation d'une infrastructure informatique hautement disponible et redondante, les données critiques sont sauvegardées à intervalles réguliers et les restaurations sont testées périodiquement. Les politiques et procédures de sauvegarde formelles minimisent l'impact des interruptions des activités commerciales et protègent les processus commerciaux contre les effets des pannes des systèmes d'information ou des catastrophes et garantissent leur reprise rapide et adéquate.

Authentification et gestion des accès

Tous les accès clients à Data Infrastructure Insights se font via des interactions avec l'interface utilisateur du navigateur via https. L'authentification est réalisée via le service tiers, Auth0. NetApp a centralisé cette couche d'authentification pour tous les services de données cloud.

Data Infrastructure Insights suit les meilleures pratiques du secteur, notamment le « moindre privilège » et le « contrôle d'accès basé sur les rôles » autour de l'accès logique à l'environnement de production Data Infrastructure Insights . L'accès est contrôlé en fonction des besoins et n'est accordé qu'à un personnel autorisé sélectionné à l'aide de mécanismes d'authentification multifacteur.

Collecte et protection des données clients

Toutes les données client sont cryptées lors du transit sur les réseaux publics et cryptées au repos. Data Infrastructure Insights utilise le cryptage à différents points du système pour protéger les données des clients à l'aide de technologies telles que Transport Layer Security (TLS) et l'algorithme standard du secteur AES-256.

Déprovisionnement du client

Des notifications par courrier électronique sont envoyées à différents intervalles pour informer le client que son abonnement expire. Une fois l'abonnement expiré, l'interface utilisateur est restreinte et une période de grâce commence pour la collecte de données. Le client est ensuite averti par email. Les abonnements d'essai bénéficient d'une période de grâce de 14 jours et les comptes d'abonnement payants bénéficient d'une période de grâce de 28 jours. Une fois le délai de grâce expiré, le client est informé par e-mail que le compte sera supprimé dans 2 jours. Un client payant peut également demander directement à se déconnecter du service.

Les locataires expirés et toutes les données client associées sont supprimés par l'équipe Data Infrastructure Insights Operations (SRE) à la fin de la période de grâce ou dès confirmation de la demande d'un client de résilier son compte. Dans les deux cas, l'équipe SRE exécute un appel API pour supprimer le compte. L'appel API supprime l'instance du locataire et toutes les données client. La suppression du client est vérifiée en appelant la même API et en vérifiant que le statut du locataire client est « SUPPRIMÉ ».

Gestion des incidents de sécurité

Data Infrastructure Insights est intégré au processus de l'équipe de réponse aux incidents de sécurité des produits (PSIRT) de NetApp pour rechercher, évaluer et résoudre les vulnérabilités connues. Le PSIRT recueille des informations sur les vulnérabilités provenant de plusieurs canaux, notamment des rapports clients, de l'ingénierie interne et de sources largement reconnues telles que la base de données CVE.

Si un problème est détecté par l'équipe d'ingénierie de Data Infrastructure Insights , l'équipe lancera le processus PSIRT, évaluera et corrigera potentiellement le problème.

Il est également possible qu'un client ou un chercheur de Data Infrastructure Insights identifie un problème de sécurité avec le produit Data Infrastructure Insights et signale le problème au support technique ou

directement à l'équipe de réponse aux incidents de NetApp. Dans ces cas, l'équipe Data Infrastructure Insights lancera le processus PSIRT, évaluera et corrigera potentiellement le problème.

Tests de vulnérabilité et de pénétration

Data Infrastructure Insights suit les meilleures pratiques du secteur et effectue régulièrement des tests de vulnérabilité et de pénétration en faisant appel à des professionnels et des entreprises de sécurité internes et externes.

Formation de sensibilisation à la sécurité

L'ensemble du personnel de Data Infrastructure Insights suit une formation en sécurité, développée pour des rôles individuels, afin de garantir que chaque employé est équipé pour gérer les défis spécifiques liés à la sécurité de ses rôles.

Conformité

Data Infrastructure Insights effectue des audits indépendants par des tiers et des validations auprès d'un cabinet d'expertise comptable agréé externe de sa sécurité, de ses processus et de ses services, y compris la réalisation de l'audit SOC 2.

Avis de sécurité NetApp

Vous pouvez consulter les avis de sécurité disponibles de NetApp"ici" .

Informations et région

NetApp prend très au sérieux la sécurité des informations clients. Voici comment et où Data Infrastructure Insights stocke vos informations.

Quelles informations Data Infrastructure Insights stocke-t-il ?

Data Infrastructure Insights stocke les informations suivantes :

- Données de performance

  Les données de performances sont des données chronologiques fournissant des informations sur les performances du périphérique/de la source surveillée. Cela inclut, par exemple, le nombre d'E/S fournies par un système de stockage, le débit d'un port FibreChannel, le nombre de pages fournies par un serveur Web, le temps de réponse d'une base de données, etc.

- Données d'inventaire

  Les données d'inventaire se composent de métadonnées décrivant le périphérique/la source surveillée et la manière dont il est configuré. Cela inclut, par exemple, les versions matérielles et logicielles installées, les disques et les LUN d'un système de stockage, les cœurs de processeur, la RAM et les disques d'une machine virtuelle, les espaces table d'une base de données, le nombre et le type de ports sur un commutateur SAN, les noms de répertoire/fichier (si Storage Workload Security est activé), etc.

- Données de configuration

  Ceci résume les données de configuration fournies par le client utilisées pour gérer l'inventaire et les opérations du client, par exemple les noms d'hôte ou les adresses IP des périphériques surveillés, les intervalles d'interrogation, les valeurs de délai d'expiration, etc.

- Secrets

  Les secrets sont constitués des informations d'identification utilisées par l'unité d'acquisition Data Infrastructure Insights pour accéder aux appareils et services des clients. Ces informations d'identification sont cryptées à l'aide d'un cryptage asymétrique puissant et les clés privées sont stockées uniquement sur les unités d'acquisition et ne quittent jamais l'environnement client. Même les SRE privilégiés de Data Infrastructure Insights ne peuvent pas accéder aux secrets des clients en texte clair en raison de cette conception.

- Données fonctionnelles

  Il s'agit de données générées suite à la fourniture du service de données cloud par NetApp , qui informe NetApp dans le développement, le déploiement, les opérations, la maintenance et la sécurisation du service de données cloud. Les données fonctionnelles ne contiennent pas d'informations client ni d'informations personnelles.

- Données d'accès utilisateur

  Informations d'authentification et d'accès qui permettent à NetApp Console de communiquer avec les sites régionaux Data Infrastructure Insights , y compris les données liées à l'autorisation de l'utilisateur.

- Données de l'annuaire utilisateur de la sécurité de la charge de travail de stockage

  Dans les cas où la fonctionnalité de sécurité de la charge de travail est activée ET que le client choisit d'activer le collecteur d'annuaires utilisateurs, le système stockera les noms d'affichage des utilisateurs, les adresses e-mail d'entreprise et d'autres informations collectées à partir d'Active Directory.

Les données de l'annuaire utilisateur font référence aux informations de l'annuaire utilisateur collectées par le collecteur de données de l'annuaire utilisateur Workload Security, et non aux données sur les utilisateurs de Data Infrastructure Insights/Workload Security eux-mêmes.

Aucune donnée personnelle explicite n'est collectée à partir des ressources d'infrastructure et de services. Les informations collectées se composent uniquement de mesures de performances, d'informations de configuration et de métadonnées d'infrastructure, à l'instar de nombreuses informations téléphoniques des fournisseurs, notamment le support automatique NetApp et ActiveIQ. Cependant, en fonction des conventions de dénomination d'un client, les données relatives aux partages, aux volumes, aux machines virtuelles, aux qtrees, aux applications, etc. peuvent contenir des informations personnellement identifiables.

Si la sécurité de la charge de travail est activée, le système examine également les noms de fichiers et de répertoires sur SMB ou d'autres partages, qui peuvent contenir des informations personnellement identifiables. Lorsque les clients activent le collecteur d'annuaires utilisateurs Workload Security (qui mappe essentiellement les SID Windows aux noms d'utilisateur via Active Directory), le nom d'affichage, l'adresse e-mail de l'entreprise et tous les attributs supplémentaires sélectionnés seront collectés et stockés par Data Infrastructure Insights.

De plus, les journaux d'accès à Data Infrastructure Insights sont conservés et contiennent les adresses IP et e-mail des utilisateurs utilisées pour se connecter au service.

Où sont stockées mes informations ?

Data Infrastructure Insights stocke les informations en fonction de la région dans laquelle votre environnement est créé.

Les informations suivantes sont stockées dans la région hôte :

- Télémétrie et informations sur les actifs/objets, y compris les compteurs et les mesures de performance
- Informations sur l'unité d'acquisition
- Données fonctionnelles
- Informations d'audit sur les activités des utilisateurs dans Data Infrastructure Insights
- Informations sur la sécurité de la charge de travail Active Directory
- Informations sur l'audit de sécurité de la charge de travail

Les informations suivantes résident aux États-Unis, quelle que soit la région hébergeant votre environnement Data Infrastructure Insights :

- Informations sur le site environnemental (parfois appelé « locataire ») telles que le propriétaire du site/compte.
- Informations permettant à NetApp Console de communiquer avec les sites régionaux Data Infrastructure Insights , y compris tout ce qui concerne l'autorisation de l'utilisateur.
- Informations relatives à la relation entre l'utilisateur Data Infrastructure Insights et le locataire.

Régions d'accueil

Les régions hôtes comprennent :

- États-Unis : us-east-1
- EMEA : eu-central-1
- APAC : ap-sud-est-2

Plus d'informations

Vous pouvez en savoir plus sur la confidentialité et la sécurité de NetApp en suivant les liens suivants :

- "Centre de confiance"
- "Transferts de données transfrontaliers"
- "Règles d'entreprise contraignantes"
- "Répondre aux demandes de données de tiers"
- "Principes de confidentialité de NetApp"

Outil d'administration de sécurité

Data Infrastructure Insights inclut des fonctionnalités de sécurité qui permettent à votre environnement de fonctionner avec une sécurité renforcée. Les fonctionnalités incluent des améliorations du cryptage, du hachage de mot de passe et la possibilité de modifier les mots de passe des utilisateurs internes ainsi que les paires de clés qui cryptent et décryptent les mots de passe.

Pour protéger les données sensibles, NetApp vous recommande de modifier les clés par défaut et le mot de passe utilisateur *Acquisition* après une installation ou une mise à niveau.

Les mots de passe chiffrés de la source de données sont stockés dans Data Infrastructure Insights, qui utilise une clé publique pour crypter les mots de passe lorsqu'un utilisateur les saisit dans une page de configuration

du collecteur de données. Data Infrastructure Insights ne dispose pas des clés privées requises pour déchiffrer les mots de passe des collecteurs de données ; seules les unités d'acquisition (AU) disposent de la clé privée du collecteur de données requise pour déchiffrer les mots de passe des collecteurs de données.

Considérations relatives à la mise à niveau et à l'installation

Lorsque votre système Insight contient des configurations de sécurité non par défaut (c'est-à-dire que vous avez réinitialisé les mots de passe), vous devez sauvegarder vos configurations de sécurité. L'installation d'un nouveau logiciel, ou dans certains cas la mise à niveau d'un logiciel, rétablit votre système à une configuration de sécurité par défaut. Lorsque votre système revient à la configuration par défaut, vous devez restaurer la configuration non par défaut pour que le système fonctionne correctement.

Gestion de la sécurité sur l'unité d'acquisition

L'outil SecurityAdmin vous permet de gérer les options de sécurité pour Data Infrastructure Insights et est exécuté sur le système de l'unité d'acquisition. La gestion de la sécurité comprend la gestion des clés et des mots de passe, l'enregistrement et la restauration des configurations de sécurité que vous créez ou la restauration des configurations aux paramètres par défaut.

Avant de commencer

- Vous devez disposer de privilèges d'administrateur sur le système AU pour installer le logiciel Acquisition Unit (qui inclut l'outil SecurityAdmin).
- Si vous avez des utilisateurs non administrateurs qui devront ultérieurement accéder à l'outil SecurityAdmin, ils doivent être ajoutés au groupe *cisys*. Le groupe *cisys* est créé lors de l'installation d'AU.

Après l'installation d'AU, l'outil SecurityAdmin se trouve sur le système de l'unité d'acquisition à l'un de ces emplacements :

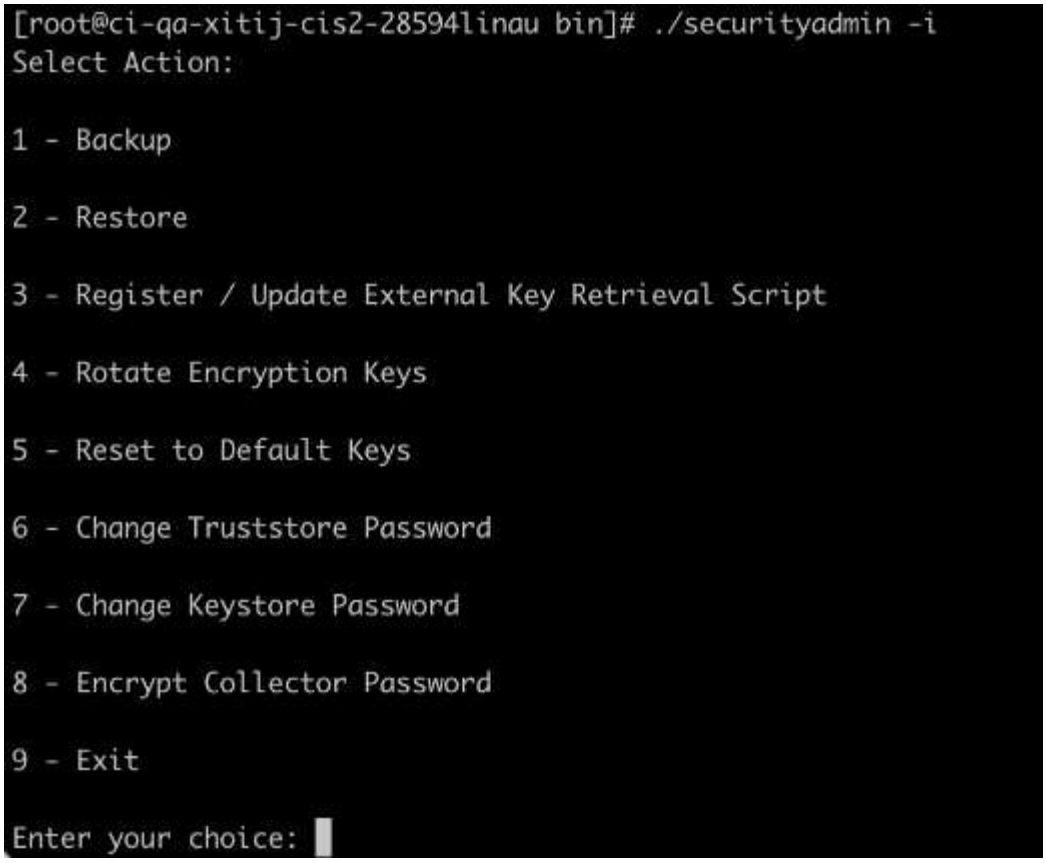
```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Utilisation de l'outil SecurityAdmin

Démarrez l'outil SecurityAdmin en mode interactif (-i).

> Il est recommandé d'utiliser l'outil SecurityAdmin en mode interactif, pour éviter de transmettre des secrets sur la ligne de commande, qui peuvent être capturés dans les journaux.

Les options suivantes s'affichent :



1. **Sauvegarde**

   Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier dans un emplacement spécifié par l'utilisateur, ou dans les emplacements par défaut suivants :

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Il est recommandé de conserver les sauvegardes du coffre-fort en toute sécurité, car elles contiennent des informations sensibles.

2. **Restaurer**

   Restaure la sauvegarde zip du coffre-fort qui a été créé. Une fois restaurés, tous les mots de passe et clés sont rétablis aux valeurs existantes au moment de la création de la sauvegarde.

   La restauration peut être utilisée pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple en suivant ces étapes : 1) Modifier les clés de chiffrement sur l'AU. 2) Créez une sauvegarde du coffre-fort. 3) Restaurez la sauvegarde du coffre-fort sur chacune des AU.

3. **Enregistrer / Mettre à jour le script de récupération de clé externe**

   Utilisez un script externe pour enregistrer ou modifier les clés de chiffrement AU utilisées pour chiffrer ou déchiffrer les mots de passe des appareils.

   Lorsque vous modifiez les clés de chiffrement, vous devez sauvegarder votre nouvelle configuration de

sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

Notez que cette option n'est disponible que sous Linux.

Lorsque vous utilisez votre propre script de récupération de clé avec l'outil SecurityAdmin, gardez à l'esprit les points suivants :

- L'algorithme actuellement pris en charge est RSA avec un minimum de 2048 bits.
- Le script doit renvoyer les clés privées et publiques en texte brut. Le script ne doit pas renvoyer de clés privées et publiques chiffrées.
- Le script doit renvoyer un contenu brut et codé (format PEM uniquement).
- Le script externe doit avoir des autorisations *execute*.

4. **Rotation des clés de chiffrement**

   Faites pivoter vos clés de chiffrement (annulez l'enregistrement des clés actuelles et enregistrez de nouvelles clés). Pour utiliser une clé provenant d'un système de gestion de clés externe, vous devez spécifier l'ID de clé publique et l'ID de clé privée.

5. **Réinitialiser les touches par défaut**

   Réinitialise le mot de passe de l'utilisateur d'acquisition et les clés de chiffrement de l'utilisateur d'acquisition aux valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

6. **Modifier le mot de passe du Truststore**

   Modifiez le mot de passe du truststore.

7. **Modifier le mot de passe du magasin de clés**

   Modifiez le mot de passe du keystore.

8. **Crypter le mot de passe du collecteur**

   Crypter le mot de passe du collecteur de données.

9. **Sortie**

   Quittez l'outil SecurityAdmin.

Choisissez l'option que vous souhaitez configurer et suivez les instructions.

Spécifier un utilisateur pour exécuter l'outil

Si vous êtes dans un environnement contrôlé et soucieux de la sécurité, vous n'avez peut-être pas le groupe *cisys*, mais vous souhaiterez peut-être néanmoins que des utilisateurs spécifiques exécutent l'outil SecurityAdmin.

Vous pouvez y parvenir en installant manuellement le logiciel AU et en spécifiant l'utilisateur/groupe pour lequel vous souhaitez l'accès.

- À l'aide de l'API, téléchargez le programme d'installation CI sur le système AU et décompressez-le.
  - Vous aurez besoin d'un jeton d'autorisation unique. Consultez la documentation API Swagger (*Admin* > *Accès API* et sélectionnez le lien *Documentation API*) et recherchez la section API *GET*

/au/oneTimeToken.

- Une fois que vous avez le jeton, utilisez l'API *GET /au/installers/{platform}/{version}* pour télécharger le fichier d'installation. Vous devrez fournir la plate-forme (Linux ou Windows) ainsi que la version du programme d'installation.

- Copiez le fichier d'installation téléchargé sur le système AU et décompressez-le.
- Accédez au dossier contenant les fichiers et exécutez le programme d'installation en tant que root, en spécifiant l'utilisateur et le groupe :

```
./cloudinsights-install.sh <User> <Group>
```

Si l'utilisateur et/ou le groupe spécifié n'existent pas, ils seront créés. L'utilisateur aura accès à l'outil SecurityAdmin.

Mise à jour ou suppression du proxy

L'outil SecurityAdmin peut être utilisé pour définir ou supprimer les informations de proxy pour l'unité d'acquisition en exécutant l'outil avec le paramètre *-pr* :

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Par exemple, pour supprimer le proxy, exécutez cette commande :

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Vous devez redémarrer l'unité d'acquisition après avoir exécuté la
commande.
```

Pour mettre à jour un proxy, la commande est

```
./securityadmin -pr -upr <arg>
```

Récupération de clés externes

Si vous fournissez un script shell UNIX, il peut être exécuté par l'unité d'acquisition pour récupérer la **clé privée** et la **clé publique** de votre système de gestion de clés.

Pour récupérer la clé, Data Infrastructure Insights exécutera le script en transmettant deux paramètres : *key id* et *key type*. *Key id* peut être utilisé pour identifier la clé dans votre système de gestion de clés. *Le type de clé* est soit « public » soit « privé ». Lorsque le type de clé est « public », le script doit renvoyer la clé publique. Lorsque le type de clé est « privé », la clé privée doit être renvoyée.

Pour renvoyer la clé à l'unité d'acquisition, le script doit imprimer la clé sur la sortie standard. Le script doit imprimer *uniquement* la clé sur la sortie standard ; aucun autre texte ne doit être imprimé sur la sortie standard. Une fois la clé demandée imprimée sur la sortie standard, le script doit quitter avec un code de sortie de 0 ; tout autre code de retour est considéré comme une erreur.

Le script doit être enregistré auprès de l'unité d'acquisition à l'aide de l'outil SecurityAdmin, qui exécutera le script avec l'unité d'acquisition. Le script doit avoir les autorisations *read* et *execute* pour l'utilisateur root et "cisys". Si le script shell est modifié après l'enregistrement, le script shell modifié doit être réenregistré auprès de l'unité d'acquisition.

paramètre d'entrée : identifiant de clé	Identificateur de clé utilisé pour identifier la clé dans le système de gestion des clés des clients.
paramètre d'entrée : type de clé	public ou privé.
sortir	La clé demandée doit être imprimée sur la sortie standard. La clé RSA 2048 bits est actuellement prise en charge. Les clés doivent être codées et imprimées au format suivant : format de clé privée - PEM, codé DER PKCS8 PrivateKeyInfo RFC 5958 format de clé publique - PEM, codé DER X.509 SubjectPublicKeyInfo RFC 5280
code de sortie	Code de sortie zéro en cas de réussite. Toutes les autres valeurs de sortie sont considérées comme un échec.
autorisations de script	Le script doit avoir l'autorisation de lecture et d'exécution pour l'utilisateur root et « cisys ».
journaux	Les exécutions de scripts sont enregistrées. Les journaux peuvent être trouvés dans - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Crypter un mot de passe à utiliser dans l'API

L'option 8 vous permet de crypter un mot de passe, que vous pouvez ensuite transmettre à un collecteur de données via l'API.

Démarrez l'outil SecurityAdmin en mode interactif et sélectionnez l'option 8 : *Crypter le mot de passe*.

```
 securityadmin.sh -i
Vous êtes invité à saisir le mot de passe que vous souhaitez crypter.
Notez que les caractères que vous tapez ne sont pas affichés à l'écran.
Saisissez à nouveau le mot de passe lorsque vous y êtes invité.
```

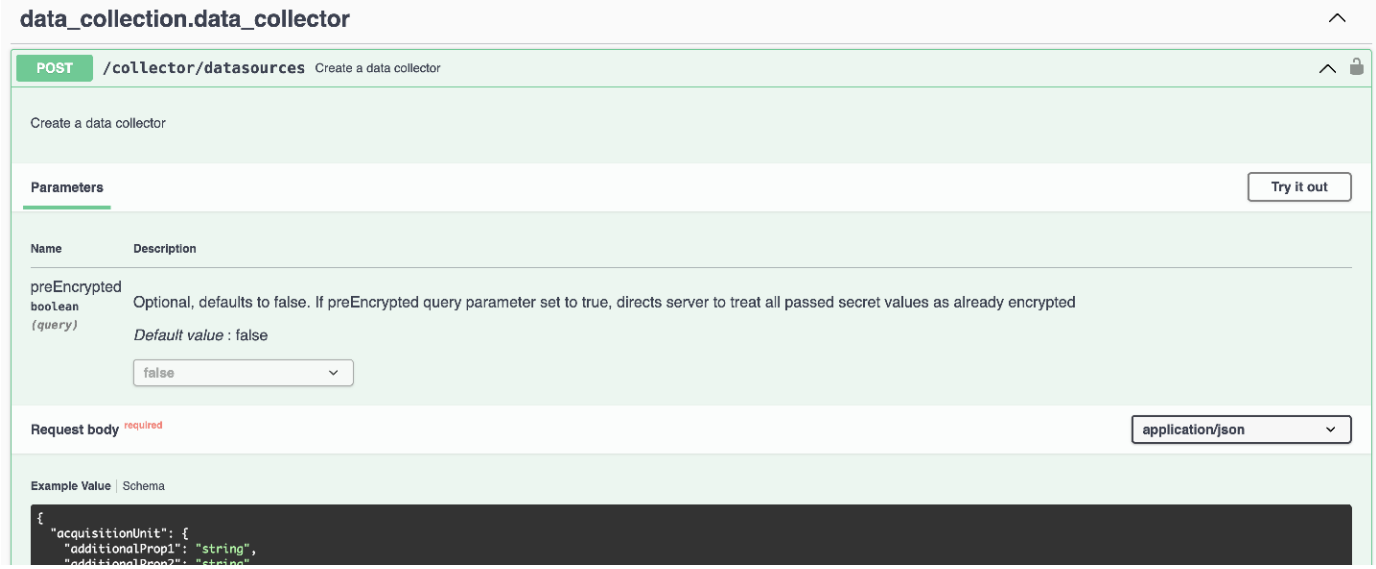
Alternativement, si vous utilisez la commande dans un script, sur une ligne de commande, utilisez *securityadmin.sh* avec le paramètre « -enc », en passant votre mot de passe non chiffré :

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Exemple de CLI"]
```

Le mot de passe crypté s'affiche à l'écran. Copiez la chaîne entière, y compris tous les symboles de début et de fin.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

Pour envoyer le mot de passe chiffré à un collecteur de données, vous pouvez utiliser l'API de collecte de données. Le swagger de cette API peut être trouvé dans **Admin > Accès API** et cliquez sur le lien « Documentation API ». Sélectionnez le type d'API « Collecte de données ». Sous l'en-tête *data_collection.data_collector*, choisissez l'API POST */collector/datasources* pour cet exemple.



Si vous définissez l'option *preEncrypted* sur *True*, tout mot de passe que vous transmettez via la commande API sera traité comme **déjà chiffré** ; l'API ne rechiffrera pas le(s) mot(s) de passe. Lors de la création de votre API, collez simplement le mot de passe précédemment crypté à l'emplacement approprié.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

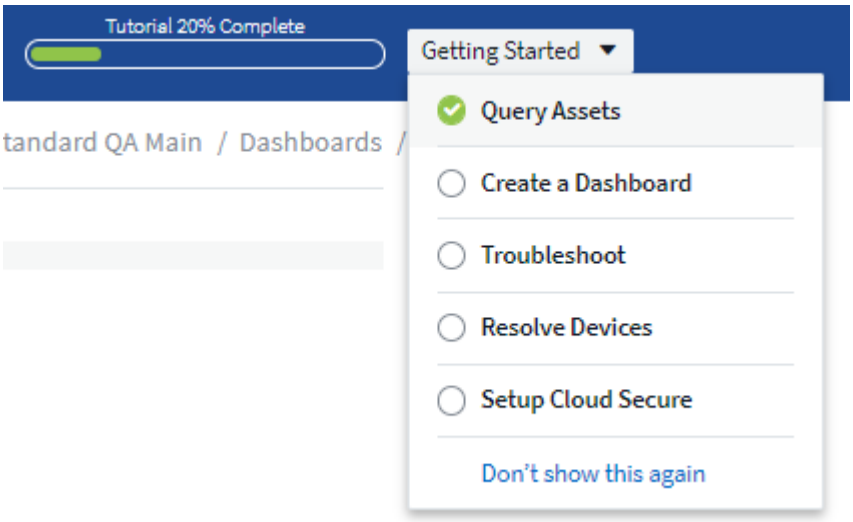
Commencer

Premiers pas avec les tutoriels vidéo

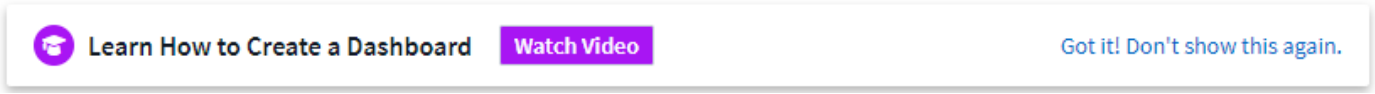
Apprenez efficacement les Data Infrastructure Insights grâce à nos tutoriels fonctionnels comprenant des guides vidéo étape par étape et une liste de contrôle de progression. Maîtrisez des compétences essentielles telles que la création de tableaux de bord, la construction de requêtes, la mise en place de la surveillance et le dépannage grâce à des tutoriels pratiques conçus pour vous rendre rapidement productif.

Liste de contrôle et didacticiels vidéo

La **liste de contrôle de démarrage** affichée sur votre locataire Data Infrastructure Insights contient une liste de plusieurs tâches et concepts utiles. La sélection d'un élément dans la liste de contrôle vous amène à la page Data Infrastructure Insights appropriée pour ce concept. Par exemple, cliquer sur l'élément *Créer un tableau de bord* ouvre la page **Tableaux de bord** de Data Infrastructure Insights .



En haut de la page se trouve un lien vers un didacticiel vidéo montrant comment créer un tableau de bord. Vous pouvez visionner la vidéo autant de fois que vous le souhaitez jusqu'à ce que vous cliquiez sur *Compris ! Ne plus afficher ceci* lien pour cette vidéo. La vidéo est disponible à chaque fois que vous accédez à la page Tableaux de bord, jusqu'à ce que vous la fermiez.



Après avoir regardé la vidéo au moins une fois, l'élément *Créer un tableau de bord* de la liste de contrôle est coché, indiquant que vous avez terminé le didacticiel. Vous pouvez ensuite passer au tutoriel suivant.

Vous pouvez consulter les tutoriels dans l'ordre de votre choix, autant de fois que vous le souhaitez jusqu'à leur fermeture.

Rejeter la liste de contrôle

La liste de contrôle de démarrage s'affiche jusqu'à ce que vous cliquiez sur le lien *Ne plus afficher* en bas de la liste de contrôle. Même après avoir ignoré la liste de contrôle, les didacticiels sont toujours disponibles sur chaque page Data Infrastructure Insights appropriée jusqu'à ce que vous les ignoriez tous à partir de la barre d'en-tête du message.

Tutoriels vidéo

Visionnez les vidéos suivantes pour en savoir plus.

"Transformer les données brutes en informations exploitables"

"Créez des tableaux de bord performants avec NetApp"

"Dépannage simplifié avec VM Analyzer"

"Explorez et analysez les données à l'aide de requêtes dans Data Infrastructure Insights"

"Surveillance proactive de l'infrastructure avec alertes et moniteurs"

Collecte de données

Commencer à collecter des données

Après vous être inscrit à Data Infrastructure Insights et connecté à votre environnement pour la première fois, vous serez guidé à travers les étapes suivantes afin de commencer à collecter et à gérer les données.

Les collecteurs de données découvrent des informations à partir de vos sources de données, telles que les périphériques de stockage, les commutateurs réseau et les machines virtuelles. Les informations recueillies sont utilisées à des fins d'analyse, de validation, de surveillance et de dépannage.

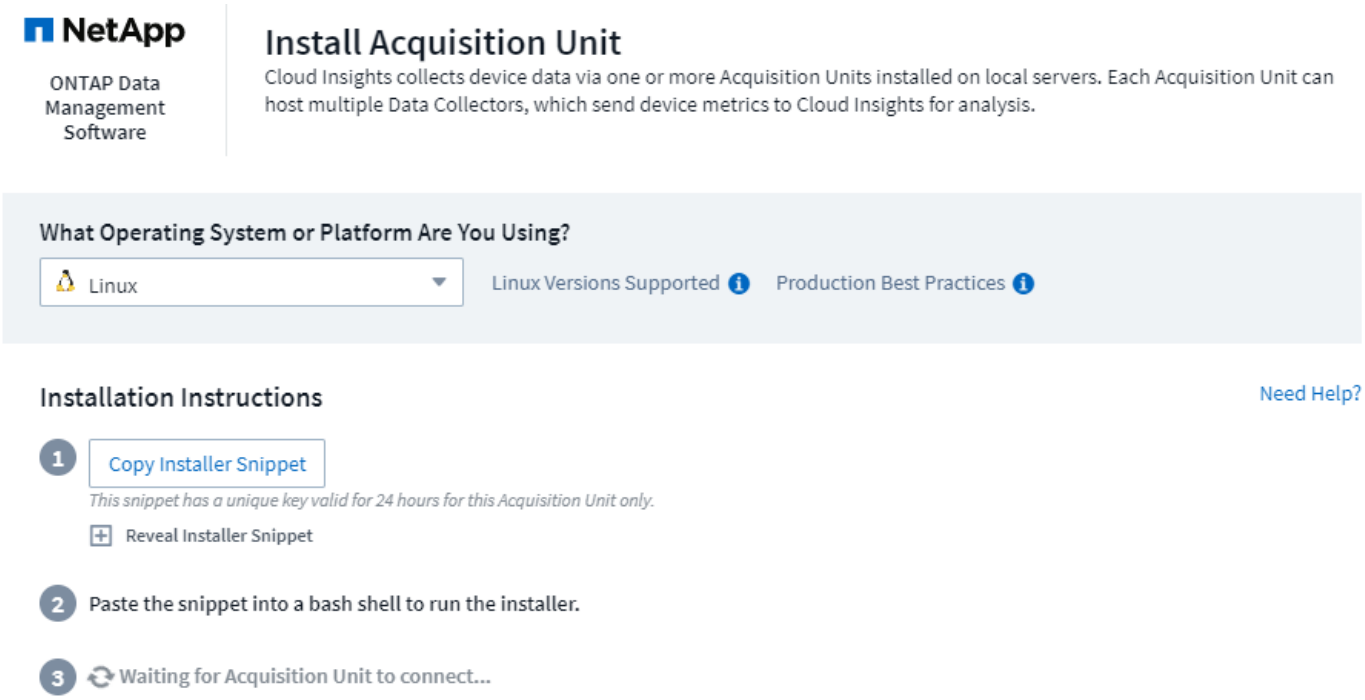
Data Infrastructure Insights propose trois types de collecteurs de données :

- Infrastructure (périphériques de stockage, commutateurs réseau, infrastructure de calcul)
- Systèmes d'exploitation (tels que VMware ou Windows)
- Services (tels que Kafka)

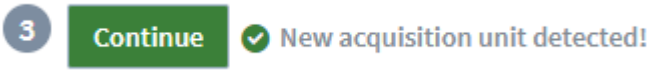
Sélectionnez votre premier collecteur de données parmi les fournisseurs et modèles pris en charge disponibles. Vous pouvez facilement ajouter des collecteurs de données supplémentaires ultérieurement.

Installer une unité d'acquisition

Si vous avez sélectionné un collecteur de données *Infrastructure*, une unité d'acquisition est requise pour injecter des données dans Data Infrastructure Insights. Vous devrez télécharger et installer le logiciel de l'unité d'acquisition sur un serveur ou une machine virtuelle du centre de données à partir duquel vous effectuerez la collecte. Une seule unité d'acquisition peut être utilisée pour plusieurs collecteurs de données.



- Suivez le"instructions" affiché pour installer votre unité d'acquisition. Une fois le logiciel de l'unité d'acquisition installé, le bouton Continuer s'affiche et vous pouvez passer à l'étape suivante.



Vous pouvez configurer des unités d'acquisition supplémentaires ultérieurement si nécessaire. Par exemple, vous souhaiterez peut-être que différentes unités d'acquisition collectent des informations à partir de centres de données situés dans différentes régions.

Configurer le collecteur de données - Infrastructure

Pour les collecteurs de données *Infrastructure*, il vous sera demandé de remplir les champs du collecteur de données présentés :

- Donnez au collecteur de données un nom unique et significatif.
- Saisissez les informations d'identification (nom d'utilisateur et mot de passe) pour vous connecter à l'appareil, le cas échéant.
- Remplissez tous les autres champs obligatoires dans les sections *Configuration* et *Configuration avancée*.
- Cliquez sur **Ajouter un collecteur** pour enregistrer le collecteur de données.

Vous pourrez configurer des collecteurs de données supplémentaires ultérieurement.

Configurer le collecteur de données – Systèmes d'exploitation et services

Système opérateur:

Pour les collecteurs de données *Système d'exploitation*, choisissez une plate-forme (Linux, Windows) pour installer un agent Data Infrastructure Insights . Vous devez disposer d'au moins un agent pour collecter les données des Services. L'agent collecte également des données de l'hôte lui-même, pour les utiliser dans Data Infrastructure Insights. Ces données sont classées comme données « Nœud » dans les widgets, etc.

- Ouvrez un terminal ou une fenêtre de commande sur l'hôte de l'agent ou la machine virtuelle et collez la commande affichée pour installer l'agent.
- Une fois l'installation terminée, cliquez sur **Terminer l'installation**.

Services:

Pour les collecteurs de données *Service*, cliquez sur une tuile pour ouvrir la page d'instructions pour ce service.

- Choisissez une plateforme et une clé d'accès d'agent.
- Si vous n'avez pas d'agent installé sur cette plateforme, suivez les instructions pour installer l'agent.
- Cliquez sur **Continuer** pour ouvrir la page d'instructions du collecteur de données.
- Suivez les instructions pour configurer le collecteur de données.
- Une fois la configuration terminée, cliquez sur **Terminer la configuration**.

Ajouter des tableaux de bord

Selon le type de collecteur de données initial que vous avez sélectionné pour configurer (stockage, commutateur, etc.), un ou plusieurs tableaux de bord pertinents seront importés. Par exemple, si vous avez configuré un collecteur de données de stockage, un ensemble de tableaux de bord liés au stockage sera importé et l'un d'eux sera défini comme page d'accueil de Data Infrastructure Insights . Vous pouvez modifier la page d'accueil à partir de la liste **Tableaux de bord > Afficher tous les tableaux de bord**.

Vous pouvez importer des tableaux de bord supplémentaires ultérieurement, ou"créez le vôtre" .

C'est tout ce qu'il y a à dire.

Une fois le processus de configuration initiale terminé, votre environnement commencera à collecter des données.

Si votre processus de configuration initiale est interrompu (par exemple, si vous fermez la fenêtre du navigateur), vous devrez suivre les étapes manuellement :

- Choisissez un collecteur de données
- Installez un agent ou une unité d'acquisition si vous y êtes invité
- Configurer le collecteur de données

Définitions utiles

Les définitions suivantes peuvent être utiles lorsque l'on parle des collecteurs de données ou des fonctionnalités de Data Infrastructure Insights :

- Cycle de vie du collecteur : Un collecteur appartiendra à l'un des états suivants dans son cycle de vie :
  - **Aperçu** : Disponible dans une capacité limitée ou pour un public limité. "Fonctionnalités d'aperçu" et les collecteurs de données devraient devenir GA après la période de prévisualisation. Les périodes d'aperçu varient en fonction du public ou des fonctionnalités.
  - **GA** : une fonctionnalité ou un collecteur de données généralement disponible pour tous les clients, en fonction de l'édition ou de l'ensemble de fonctionnalités.
  - **Obsolète** : s'applique aux collecteurs de données qui ne sont plus, ou ne devraient plus devenir, fonctionnellement viables. Les collecteurs de données obsolètes sont souvent remplacés par des

collecteurs de données plus récents et fonctionnellement mis à jour.

- **Supprimé** : un collecteur de données qui a été supprimé et n'est plus disponible.

- Unité d'acquisition : un ordinateur dédié à l'hébergement des collecteurs de données, généralement une machine virtuelle. Cet ordinateur est généralement situé dans le même centre de données / VPC que les éléments surveillés.
- Source de données : un module permettant de communiquer avec une pile matérielle ou logicielle. Il s'agit d'une configuration et d'un code qui s'exécutent sur l'ordinateur AU pour communiquer avec l'appareil.

Exigences relatives à l'unité d'acquisition

Vous devez installer une unité d'acquisition (AU) afin d'acquérir des informations à partir des collecteurs de données de votre infrastructure (stockage, VM, port, EC2, etc.). Avant d'installer l'unité d'acquisition, vous devez vous assurer que votre locataire répond aux exigences du système d'exploitation, du processeur, de la mémoire et de l'espace disque.

Exigences

Composant	Exigences Linux	Configuration requise pour Windows
Système opérateur	Un ordinateur exécutant une version sous licence de l'un des systèmes d'exploitation suivants : * AlmaLinux 9.5, 10 * Centos (64-bit) : Stream 9 * Debian (64-bit) : 11 à 13 * OpenSUSE Leap 15.2 à 15.6, 16 * Oracle Enterprise Linux (64-bit) : 8.10, 9.2, 9.4, 9.6, 10 * Red Hat (64-bit) : 8.10, 9.2, 9.4, 9.6, 10 * Rocky 9.2 à 9.6 * SUSE Linux Enterprise Server 15 SP4 à 15 SP7, 16 * Ubuntu Server : 20.04, 22.04, 24.04 LTS * SELinux sur les plateformes ci-dessus Cet ordinateur ne doit exécuter aucun autre logiciel applicatif. Un serveur dédié est recommandé. Si vous utilisez SELinux, il est recommandé d'exécuter les commandes suivantes sur le système de l'unité d'acquisition : sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/.*)?" sudo restorecon -R /opt/netapp/cloudinsights	Un ordinateur exécutant une version sous licence de l'un des systèmes d'exploitation suivants : * Microsoft Windows 11 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025. Cet ordinateur ne doit exécuter aucun autre logiciel applicatif. Un serveur dédié est recommandé.
processeur	2 cœurs de processeur	Même
Mémoire	8 Go de RAM	Même

Espace disque disponible	50 Go (100 Go recommandés) Pour Linux, l'espace disque doit être alloué de cette manière : /opt/netapp 10 Go (20 Go pour les grands environnements) /var/log/netapp 40 Go (80 Go pour les grands environnements) /tmp au moins 1 Go disponible pendant l'installation	50 Go
Réseau	Une connexion Ethernet de 100 Mbps/1 Gbps, une adresse IP statique et une connectivité de port 80 ou 443 (sortante) de l'unité d'acquisition vers *.cloudinsights.netapp.com ou votre locataire Data Infrastructure Insights (c.-à-d. https://<tenant_id>.c01.cloudinsights.netapp.com) sont requises. Pour connaître les exigences entre l'unité d'acquisition et chaque collecteur de données, veuillez vous référer aux instructions du"Collecteur de données" . Si votre organisation nécessite l'utilisation d'un proxy pour l'accès à Internet, vous devrez peut-être comprendre le comportement du proxy de votre organisation et rechercher certaines exceptions pour que Data Infrastructure Insights fonctionne. Par exemple, votre organisation bloque-t-elle l'accès par défaut et autorise-t-elle uniquement l'accès à des sites Web/domaines spécifiques par exception ? Si tel est le cas, vous devrez ajouter le domaine suivant à la liste des exceptions : *.cloudinsights.netapp.com. Pour plus d'informations, consultez la documentation sur les proxys."ici (Linux)" ou"ici (Windows)" .	Même
Autorisations	Autorisations Sudo sur le serveur de l'unité d'acquisition. /tmp doit être monté avec des capacités exécutives.	Autorisations d'administrateur sur le serveur de l'unité d'acquisition

Analyse antivirus		Lors de l'installation, vous devez désactiver complètement tous les antivirus. Après l'installation, les chemins utilisés par le logiciel de l'unité d'acquisition doivent être exclus de l'analyse antivirus.

Recommandations supplémentaires

- Pour un audit et des rapports de données précis, il est fortement recommandé de synchroniser l'heure sur la machine de l'unité d'acquisition à l'aide du **Network Time Protocol (NTP)** ou du **Simple Network Time Protocol (SNTP)**.

Concernant le dimensionnement

Vous pouvez démarrer avec une unité d'acquisition Data Infrastructure Insights avec seulement 8 Go de mémoire et 50 Go d'espace disque. Cependant, pour les environnements plus grands, vous devez vous poser les questions suivantes :

Vous attendez-vous à :

- Découvrez plus de 2500 machines virtuelles ou 10 grands clusters ONTAP (> 2 nœuds), Symmetrix ou baies HDS/HPE VSP/XP sur cette unité d'acquisition ?
- Déployer 75 collecteurs de données ou plus au total sur cette unité d'acquisition ?

Pour chaque réponse « Oui » ci-dessus, il est recommandé d'ajouter 8 Go de mémoire et 50 Go d'espace disque à l'AU. Ainsi, par exemple, si vous avez répondu « Oui » aux deux questions, vous devez déployer un système de mémoire de 24 Go avec 150 Go ou plus d'espace disque. Sous Linux, l'espace disque à ajouter à l'emplacement du journal.

Pour des questions supplémentaires sur le dimensionnement, contactez le support NetApp .

Configuration des unités d'acquisition

Data Infrastructure Insights collecte les données des appareils à l'aide d'une ou plusieurs unités d'acquisition installées sur des serveurs locaux. Chaque unité d'acquisition peut héberger plusieurs collecteurs de données, qui envoient des mesures d'appareil à Data Infrastructure Insights pour analyse.

Cette rubrique décrit comment ajouter des unités d'acquisition et décrit les étapes supplémentaires requises lorsque votre environnement utilise un proxy.

Pour un audit et des rapports de données précis, il est fortement recommandé de synchroniser l'heure sur la machine de l'unité d'acquisition à l'aide du **Network Time Protocol (NTP)** ou du **Simple Network Time Protocol (SNTP)**.

En savoir plus sur la sécurité de Data Infrastructure Insights"ici" .

Ajout d'une unité d'acquisition Linux

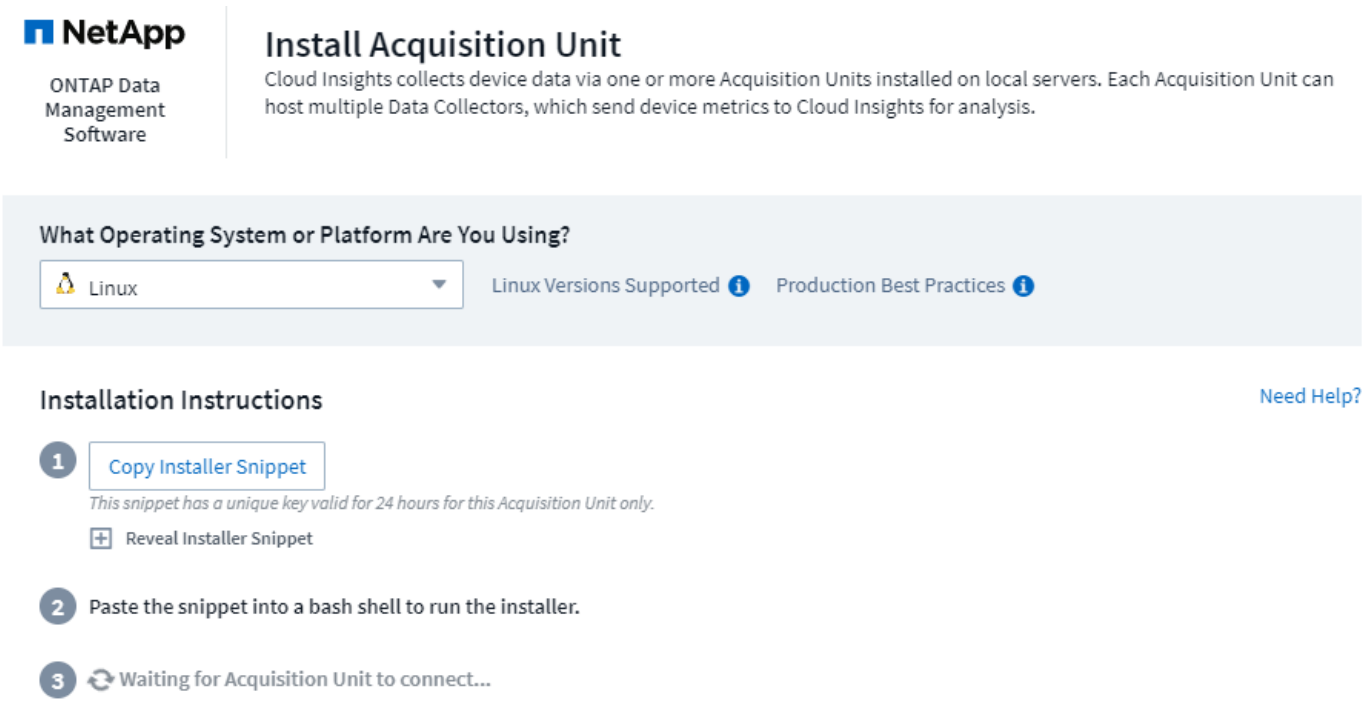
Avant de commencer

- Si votre système utilise un proxy, vous devez définir les variables d'environnement du proxy avant l'installation de l'unité d'acquisition. Pour plus d'informations, consultez la section Définition des variables d'environnement proxy .

Étapes d'installation de l'unité d'acquisition Linux

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Data Infrastructure Insights .
2. Cliquez sur **Observabilité > Collecteurs > Unités d'acquisition > +Unité d'acquisition**

   Le système affiche la boîte de dialogue *Installer l'unité d'acquisition*. Choisissez Linux.



1. Vérifiez que le serveur ou la machine virtuelle hébergeant l'unité d'acquisition répond à la configuration système requise recommandée.
2. Vérifiez que le serveur exécute une version prise en charge de Linux. Cliquez sur *Versions du système d'exploitation prises en charge (i)* pour obtenir la liste des versions prises en charge.
3. Copiez l'extrait de commande d'installation de la boîte de dialogue dans une fenêtre de terminal sur le serveur ou la machine virtuelle qui hébergera l'unité d'acquisition.
4. Collez et exécutez la commande dans le shell Bash.

Après avoir terminé

- Cliquez sur **Observabilité > Collecteurs > Unités d'acquisition** pour vérifier l'état des unités d'acquisition.
- Vous pouvez accéder aux journaux de l'unité d'acquisition à l'adresse /var/log/netapp/cloudinsights/acq/acq.log
- Utilisez le script suivant pour contrôler l'unité d'acquisition :
  - cloudinsights-service.sh (arrêter, démarrer, redémarrer, vérifier l'état)
- Utilisez le script suivant pour désinstaller l'unité d'acquisition :

- cloudinsights-uninstall.sh

Définition des variables d'environnement proxy

Pour les environnements qui utilisent un proxy, vous devez définir les variables d'environnement du proxy avant d'ajouter l'unité d'acquisition. Les instructions de configuration du proxy sont fournies dans la boîte de dialogue *Ajouter une unité d'acquisition*.

1. Cliquez sur + dans *Vous avez un serveur proxy ?*
2. Copiez les commandes dans un éditeur de texte et définissez vos variables proxy selon vos besoins.

   Remarque : tenez compte des restrictions sur les caractères spéciaux dans les champs de nom d'utilisateur et de mot de passe du proxy : « % » et « ! » sont autorisés dans le champ de nom d'utilisateur. ':', '%' et '!' sont autorisés dans le champ du mot de passe.

3. Exécutez la commande modifiée dans un terminal à l'aide du shell Bash.
4. Installez le logiciel de l'unité d'acquisition.

Configuration du proxy

L'unité d'acquisition utilise l'authentification bidirectionnelle/mutuelle pour se connecter au serveur Data Infrastructure Insights . Le certificat client doit être transmis au serveur Data Infrastructure Insights pour être authentifié. Pour ce faire, le proxy doit être configuré pour transmettre la requête https au serveur Data Infrastructure Insights sans déchiffrer les données.

La manière la plus simple de procéder consiste à spécifier une configuration générique dans votre proxy/pare-feu pour communiquer avec Data Infrastructure Insights, par exemple :

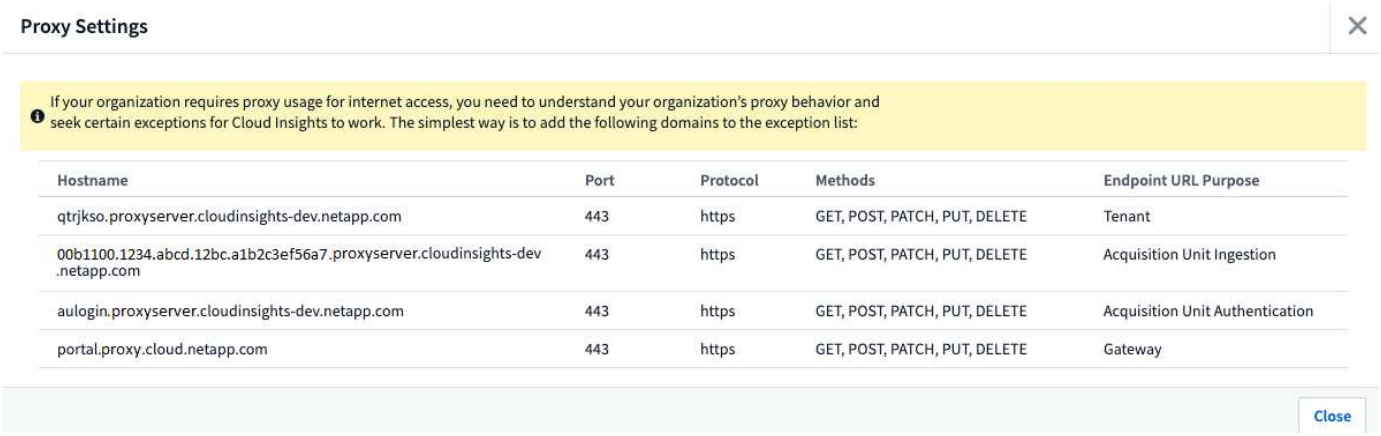
```
*.cloudinsights.netapp.com
```

L'utilisation d'un astérisque (*) comme caractère générique est courante, mais votre configuration proxy/pare-feu peut utiliser un format différent. Consultez la documentation de votre proxy pour garantir la spécification correcte des caractères génériques dans votre environnement.

Vous trouverez plus d'informations sur la configuration du proxy dans le NetApp"Base de connaissances" .

Affichage des URL proxy

Vous pouvez afficher les URL de vos points de terminaison proxy en cliquant sur le lien **Paramètres proxy** lors du choix d'un collecteur de données lors de l'intégration, ou sur le lien sous *Paramètres proxy* sur la page **Aide > Assistance**. Un tableau comme celui-ci s'affiche.



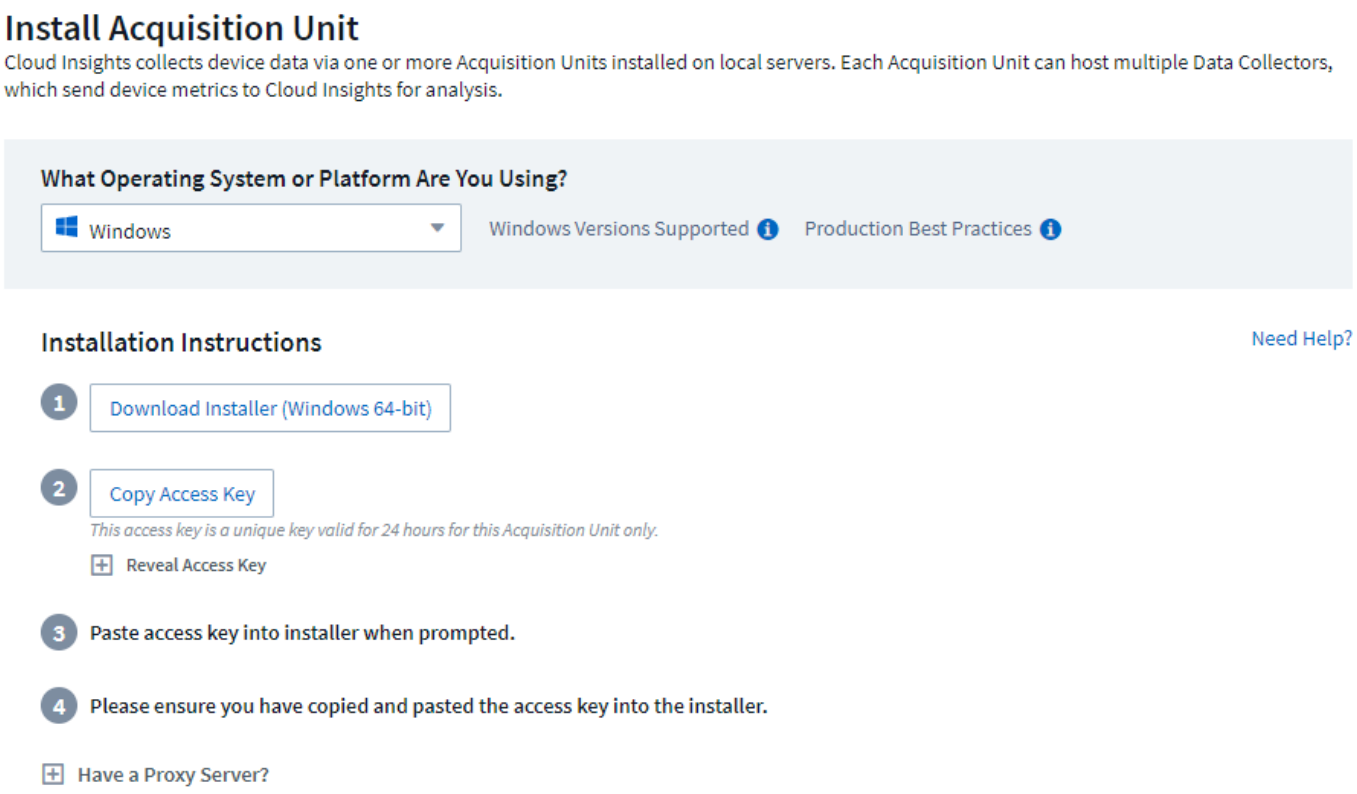
Si vous disposez de Workload Security sur votre locataire, les URL de point de terminaison configurées seront également affichées dans cette liste.

Ajout d'une unité d'acquisition Windows

Étapes d'installation de l'unité d'acquisition Windows

1. Connectez-vous au serveur/VM de l'unité d'acquisition en tant qu'utilisateur disposant d'autorisations d'administrateur.
2. Sur ce serveur, ouvrez une fenêtre de navigateur et connectez-vous à votre environnement Data Infrastructure Insights en tant qu'administrateur ou propriétaire de compte.
3. Cliquez sur **Observabilité > Collecteurs > Unités d'acquisition > +Unité d'acquisition** .

   Le système affiche la boîte de dialogue *Installer l'unité d'acquisition*. Choisissez Windows.



1. Vérifiez que le serveur ou la machine virtuelle hébergeant l'unité d'acquisition répond à la configuration

système requise recommandée.

2. Vérifiez que le serveur exécute une version prise en charge de Windows. Cliquez sur *Versions du système d'exploitation prises en charge (i)* pour obtenir la liste des versions prises en charge.
3. Cliquez sur le bouton **Télécharger le programme d'installation (Windows 64 bits)**.
4. Copiez la clé d'accès. Vous en aurez besoin lors de l'installation.
5. Sur le serveur/la machine virtuelle de l'unité d'acquisition, exécutez le programme d'installation téléchargé.
6. Collez la clé d'accès dans l'assistant d'installation lorsque vous y êtes invité.
7. Lors de l'installation, vous aurez la possibilité de fournir les paramètres de votre serveur proxy.

Après avoir terminé

- Cliquez sur * > Observabilité > Collecteurs > Unités d'acquisition* pour vérifier l'état des unités d'acquisition.
- Vous pouvez accéder au journal de l'unité d'acquisition dans <répertoire d'installation>\ Cloud Insights\Acquisition Unit\log\acq.log
- Utilisez le script suivant pour arrêter, démarrer, redémarrer ou vérifier l'état de l'unité d'acquisition :

```
cloudinsights-service.sh
```

Configuration du proxy

L'unité d'acquisition utilise l'authentification bidirectionnelle/mutuelle pour se connecter au serveur Data Infrastructure Insights . Le certificat client doit être transmis au serveur Data Infrastructure Insights pour être authentifié. Pour ce faire, le proxy doit être configuré pour transmettre la requête https au serveur Data Infrastructure Insights sans déchiffrer les données.

La manière la plus simple de procéder consiste à spécifier une configuration générique dans votre proxy/pare-feu pour communiquer avec Data Infrastructure Insights, par exemple :

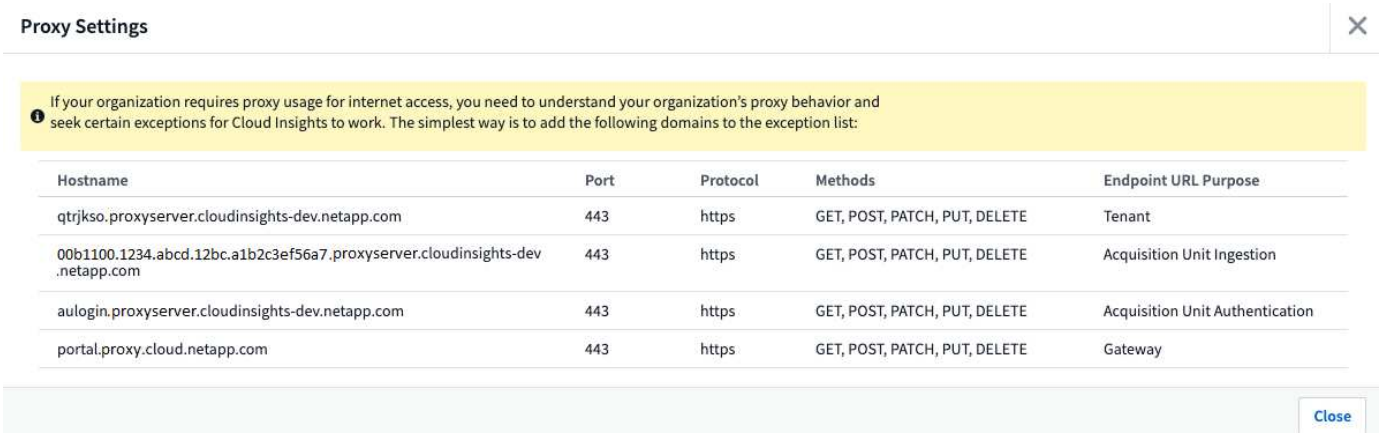
```
*.cloudinsights.netapp.com
```

> L'utilisation d'un astérisque (*) comme caractère générique est courante, mais votre configuration proxy/pare-feu peut utiliser un format différent. Consultez la documentation de votre proxy pour garantir la spécification correcte des caractères génériques dans votre environnement.

Vous trouverez plus d'informations sur la configuration du proxy dans le NetApp"Base de connaissances" .

Affichage des URL proxy

Vous pouvez afficher les URL de vos points de terminaison proxy en cliquant sur le lien **Paramètres proxy** lors du choix d'un collecteur de données lors de l'intégration, ou sur le lien sous *Paramètres proxy* sur la page **Aide > Assistance**. Un tableau comme celui-ci s'affiche.



Si vous disposez de Workload Security sur votre locataire, les URL de point de terminaison configurées seront également affichées dans cette liste.

Désinstallation d'une unité d'acquisition

Pour désinstaller le logiciel de l'unité d'acquisition, procédez comme suit :

Fenêtres :

Si vous désinstallez une unité d'acquisition **Windows** :

1. Sur le serveur/la machine virtuelle de l'unité d'acquisition, ouvrez le Panneau de configuration et choisissez **Désinstaller un programme**. Sélectionnez le programme Unité d'acquisition d' Data Infrastructure Insights pour la suppression.
2. Cliquez sur Désinstaller et suivez les instructions.

Linux:

Si vous désinstallez une unité d'acquisition **Linux** :

1. Sur le serveur/la machine virtuelle de l'unité d'acquisition, exécutez la commande suivante :

```
 sudo cloudinsights-uninstall.sh -p
. Pour obtenir de l'aide sur la désinstallation, exécutez :
```

```
sudo cloudinsights-uninstall.sh --help
```

Windows et Linux :

Après la désinstallation de l'AU :

1. Dans Data Infrastructure Insights, accédez à **Observabilité > Collecteurs et sélectionnez l'onglet *Unités d'acquisition**.
2. Cliquez sur le bouton Options à droite de l'unité d'acquisition que vous souhaitez désinstaller et sélectionnez *Supprimer*. Vous ne pouvez supprimer une unité d'acquisition que s'il n'y a aucun collecteur de données qui lui est attribué.

> ⓘ Vous ne pouvez pas supprimer une unité d'acquisition (AU) à laquelle des collecteurs de données sont connectés. Déplacez tous les collecteurs de données de l'AU vers une autre AU (modifiez le collecteur et sélectionnez simplement une autre AU) avant de supprimer l'AU d'origine.

Une unité d'acquisition avec une étoile à côté est utilisée pour la résolution de l'appareil. Avant de supprimer cette AU, vous devez sélectionner une autre AU à utiliser pour la résolution de l'appareil. Passez la souris sur une autre AU et ouvrez le menu « trois points » pour sélectionner « Utiliser pour la résolution de l'appareil ».

Réinstallation d'une unité d'acquisition

Pour réinstaller une unité d'acquisition sur le même serveur/VM, vous devez suivre ces étapes :

Avant de commencer

Vous devez disposer d'une unité d'acquisition temporaire configurée sur un serveur/une machine virtuelle distinct avant de réinstaller une unité d'acquisition.

Étapes

1. Connectez-vous au serveur/VM de l'unité d'acquisition et désinstallez le logiciel AU.
2. Connectez-vous à votre environnement Data Infrastructure Insights et accédez à **Observabilité > Collecteurs**.
3. Pour chaque collecteur de données, cliquez sur le menu Options à droite et sélectionnez *Modifier*. Affectez le collecteur de données à l'unité d'acquisition temporaire et cliquez sur **Enregistrer**.

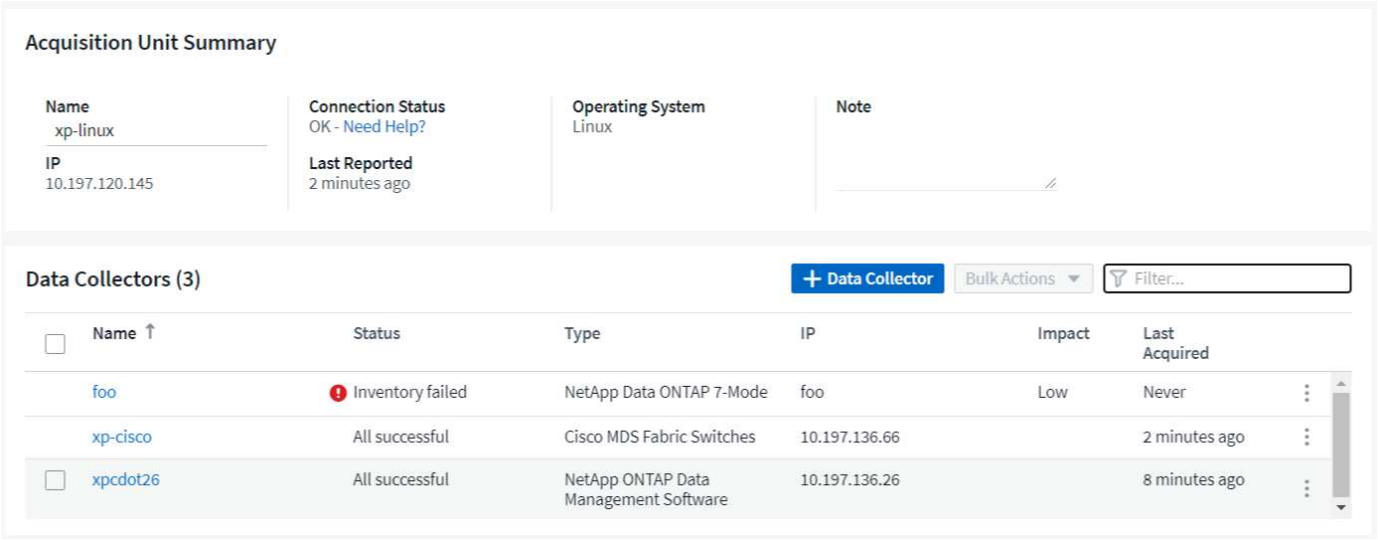
   Vous pouvez également sélectionner plusieurs collecteurs de données du même type et cliquer sur le bouton **Actions en masse**. Choisissez *Modifier* et attribuez les collecteurs de données à l'unité d'acquisition temporaire.

4. Une fois tous les collecteurs de données déplacés vers l'unité d'acquisition temporaire, accédez à **Observabilité > Collecteurs** et sélectionnez l'onglet **Unités d'acquisition**.
5. Cliquez sur le bouton Options à droite de l'unité d'acquisition que vous souhaitez réinstaller et sélectionnez *Supprimer*. Vous ne pouvez supprimer une unité d'acquisition que s'il n'y a aucun collecteur de données qui lui est attribué.
6. Vous pouvez maintenant réinstaller le logiciel de l'unité d'acquisition sur le serveur/VM d'origine. Cliquez sur **+Unité d'acquisition** et suivez les instructions ci-dessus pour installer l'unité d'acquisition.
7. Une fois l'unité d'acquisition réinstallée, réaffectez vos collecteurs de données à l'unité d'acquisition.

Affichage des détails de l'UA

La page de détails de l'unité d'acquisition (AU) fournit des détails utiles sur une AU ainsi que des informations pour aider au dépannage. La page de détails de l'AU contient les sections suivantes :

- Une section **résumée** montrant les éléments suivants :
  - **Nom** et **IP** de l'unité d'acquisition
  - Connexion actuelle **Statut** de l'UA
  - **Dernière heure de sondage réussie du collecteur de données signalée**
  - Le **système d'exploitation** de la machine AU
  - Une **Note** actuelle pour l'UA. Utilisez ce champ pour saisir un commentaire pour l'AU. Le champ affiche la note la plus récemment ajoutée.
- Un tableau des **Collecteurs de données** de l'UA indiquant, pour chaque collecteur de données :
  - **Nom** - Cliquez sur ce lien pour accéder à la page de détails du collecteur de données avec des informations supplémentaires
  - **Statut** - Informations sur la réussite ou l'erreur
  - **Type** - Fournisseur/modèle
  - Adresse **IP** du collecteur de données
  - Niveau d'**Impact** actuel
  - **Dernière acquisition** - quand le collecteur de données a été interrogé avec succès pour la dernière fois



Pour chaque collecteur de données, vous pouvez cliquer sur le menu « trois points » pour cloner, modifier, interroger ou supprimer le collecteur de données. Vous pouvez également sélectionner plusieurs collecteurs de données dans cette liste pour effectuer des actions groupées sur eux.

Pour redémarrer l'unité d'acquisition, cliquez sur le bouton **Redémarrer** en haut de la page. Déroulez ce bouton pour tenter de **Restaurer la connexion** à l'AU en cas de problème de connexion.

Configuration d'un agent pour collecter des données (Windows/Linux)

Utilisations de Data Infrastructure Insights"Télégraphe" en tant qu'agent de collecte des

données d'intégration. Telegraf est un agent serveur piloté par plugin qui peut être utilisé pour collecter et signaler des métriques, des événements et des journaux. Les plugins d'entrée sont utilisés pour collecter les informations souhaitées dans l'agent en accédant directement au système/OS, en appelant des API tierces ou en écoutant des flux configurés (c'est-à-dire Kafka, statsD, etc.). Les plugins de sortie sont utilisés pour envoyer les métriques, les événements et les journaux collectés de l'agent à Data Infrastructure Insights.

Pour plus d'informations sur l'installation sur Kubernetes, consultez le"Opérateur de surveillance NetApp Kubernetes" page.

Pour un audit et des rapports de données précis, il est fortement recommandé de synchroniser l'heure sur la machine Agent à l'aide du **Network Time Protocol (NTP)** ou du **Simple Network Time Protocol (SNTP)**.

Si vous souhaitez vérifier les fichiers d'installation avant d'installer l'agent, consultez la section ci-dessous surVérification des sommes de contrôle des packages Telegraf .

Installation d'un agent

Si vous installez un collecteur de données de service et que vous n'avez pas encore configuré d'agent, vous êtes invité à installer d'abord un agent pour le système d'exploitation approprié. Cette rubrique fournit des instructions pour l'installation de l'agent Telegraf sur les systèmes d'exploitation suivants :

- Windows
- RHEL et CentOS
- Ubuntu et Debian

Pour installer un agent, quelle que soit la plateforme que vous utilisez, vous devez d'abord effectuer les opérations suivantes :

1. Connectez-vous à l'hôte que vous utiliserez pour votre agent.
2. Connectez-vous à votre environnement Data Infrastructure Insights et accédez à **Observabilité > Collecteurs**.
3. Cliquez sur **+Collecteur de données** et choisissez un collecteur de données à installer.
4. Choisissez la plateforme appropriée pour votre hébergeur (Windows, Linux)
5. Suivez les étapes restantes pour chaque plateforme.

Une fois que vous avez installé un agent sur un hôte, vous n'avez pas besoin d'installer à nouveau un agent sur cet hôte.

Une fois que vous avez installé un agent sur un serveur/une machine virtuelle, Data Infrastructure Insights collecte des métriques à partir de ce système en plus de celles collectées à partir de tous les collecteurs de données que vous configurez. Ces mesures sont collectées comme"Métriques « Node »" .

Si vous utilisez un proxy, lisez les instructions du proxy pour votre plateforme avant d'installer l'agent Telegraf.

Emplacements des journaux

Les messages journaux Telegraf sont redirigés de stdout vers les fichiers journaux suivants par défaut :

- RHEL/CentOS : /var/log/telegraf/telegraf.log
- Ubuntu/Debian : /var/log/telegraf/telegraf.log
- Windows : C:\Program Files\telegraf\telegraf.log

Windows

Prérequis :

- PowerShell doit être installé
- Si vous êtes derrière un proxy, vous devez suivre les instructions de la section **Configuration de la prise en charge du proxy pour Windows**.

Configuration de la prise en charge du proxy pour Windows

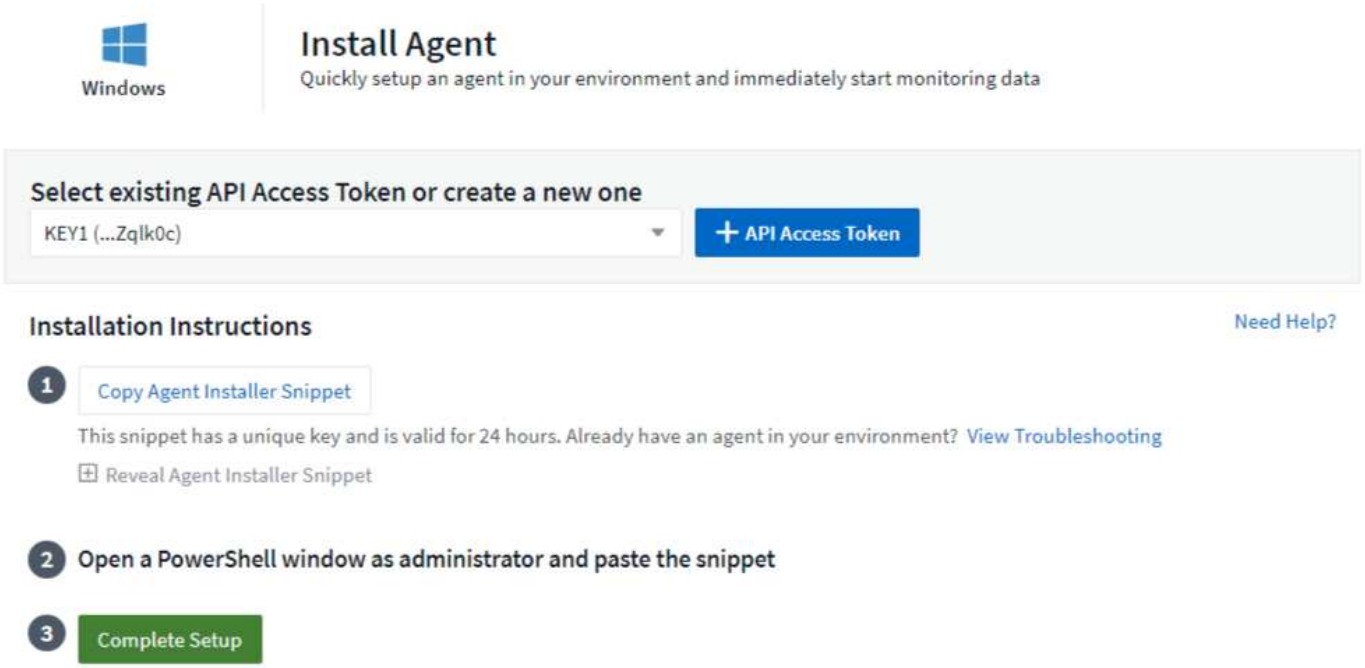
Si votre environnement utilise un proxy, lisez cette section avant de procéder à l'installation.

Les étapes ci-dessous décrivent les actions nécessaires pour définir les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, les utilisateurs peuvent également avoir besoin de définir la variable d'environnement *no_proxy*.

Pour les systèmes résidant derrière un proxy, procédez comme suit pour définir les variables d'environnement *https_proxy* et/ou *http_proxy* **AVANT** d'installer l'agent Telegraf :

```
[System.Environment]:SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>", [System.EnvironmentVariableTarget]:Machine)
```

Installation de l'agent



Étapes pour installer l'agent sur Windows :

1. Choisissez une clé d'accès d'agent.
2. Copiez le bloc de commande à partir de la boîte de dialogue d'installation de l'agent. Vous pouvez cliquer sur l'icône du presse-papiers pour copier rapidement la commande dans le presse-papiers.
3. Ouvrir une fenêtre PowerShell
4. Collez la commande dans la fenêtre PowerShell et appuyez sur Entrée.
5. La commande téléchargera le programme d'installation de l'agent approprié, l'installera et définira une configuration par défaut. Une fois terminé, le service de l'agent redémarrera. La commande possède une clé unique et est valable 24 heures.
6. Cliquez sur **Terminer** ou **Continuer**

Une fois l'agent installé, vous pouvez utiliser les commandes suivantes pour démarrer/arrêter le service :

```
Start-Service telegraf
Stop-Service telegraf
```

Désinstallation de l'agent

Pour désinstaller l'agent sous Windows, procédez comme suit dans une fenêtre PowerShell :

1. Arrêter et supprimer le service Telegraf :

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Supprimer le certificat du trustore :

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Supprimez le dossier *C:\Program Files\telegraf* pour supprimer les fichiers binaires, les journaux et les fichiers de configuration
4. Supprimez la clé *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* du registre

Mise à niveau de l'agent

Pour mettre à niveau l'agent Telegraf, procédez comme suit :

1. Arrêtez et supprimez le service Telegraf :

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Supprimez la clé *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* du registre
3. Supprimer *C:\Program Files\telegraf\telegraf.conf*
4. Supprimer *C:\Program Files\telegraf\telegraf.exe*
5. "Installer le nouvel agent" .

RHEL et CentOS

Prérequis :

- Les commandes suivantes doivent être disponibles : curl, sudo, ping, sha256sum, openssl et dmidecode
- Si vous êtes derrière un proxy, vous devez suivre les instructions de la section **Configuration de la prise en charge du proxy pour RHEL/CentOS**.

Configuration de la prise en charge du proxy pour RHEL/CentOS

Si votre environnement utilise un proxy, lisez cette section avant de procéder à l'installation.

Les étapes ci-dessous décrivent les actions nécessaires pour définir les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, les utilisateurs peuvent également avoir besoin de définir la variable d'environnement *no_proxy*.

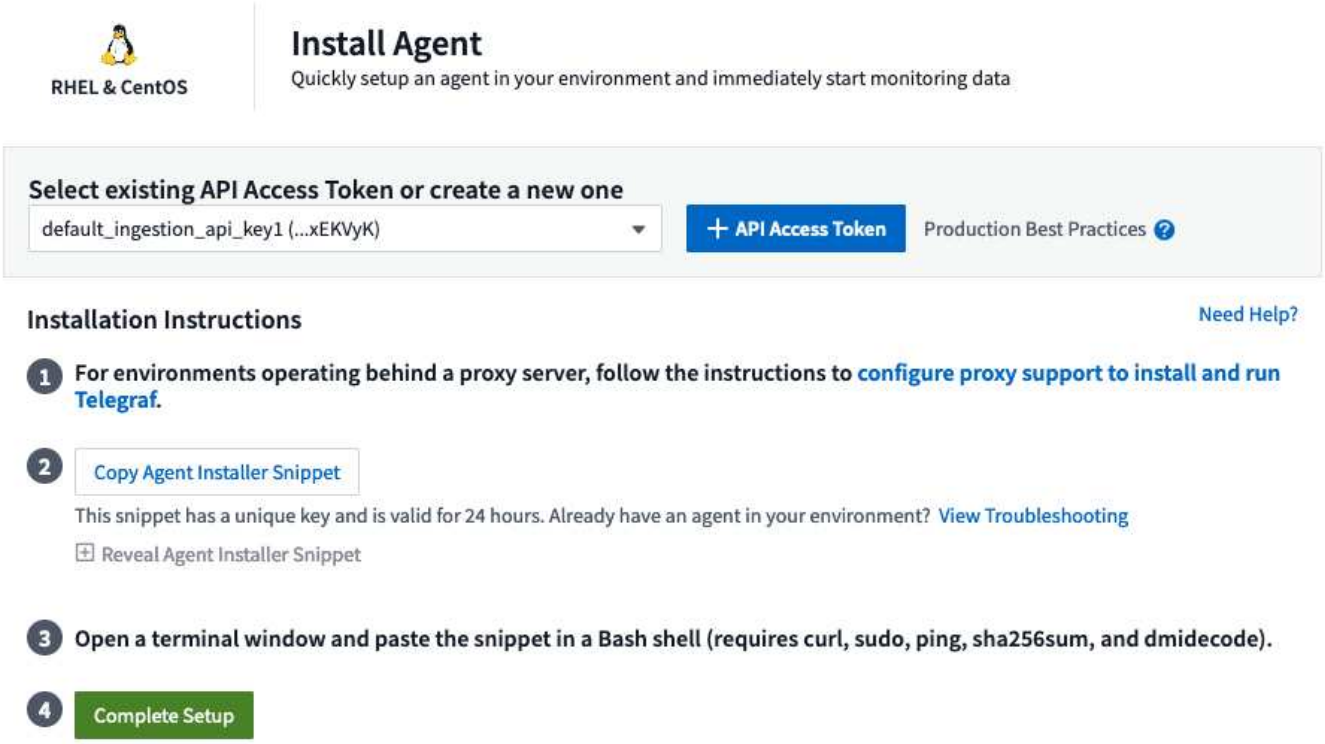
Pour les systèmes résidant derrière un proxy, effectuez les étapes suivantes **AVANT** d'installer l'agent Telegraf :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :

```
 export https_proxy=<proxy_server>:<proxy_port>
. Créez _/etc/default/telegraf_ et insérez les définitions des variables
_https_proxy_ et/ou _http_proxy_ :
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installation de l'agent



Étapes pour installer l'agent sur RHEL/CentOS :

1. Choisissez une clé d'accès d'agent.
2. Copiez le bloc de commande à partir de la boîte de dialogue d'installation de l'agent. Vous pouvez cliquer sur l'icône du presse-papiers pour copier rapidement la commande dans le presse-papiers.
3. Ouvrir une fenêtre Bash
4. Collez la commande dans la fenêtre Bash et appuyez sur Entrée.
5. La commande téléchargera le programme d'installation de l'agent approprié, l'installera et définira une configuration par défaut. Une fois terminé, le service de l'agent redémarrera. La commande possède une clé unique et est valable 24 heures.
6. Cliquez sur **Terminer** ou **Continuer**

Une fois l'agent installé, vous pouvez utiliser les commandes suivantes pour démarrer/arrêter le service :

Si votre système d'exploitation utilise systemd (CentOS 7+ et RHEL 7+) :

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Si votre système d'exploitation n'utilise pas systemd (CentOS 7+ et RHEL 7+) :

```
sudo service telegraf start
sudo service telegraf stop
```

Désinstallation de l'agent

Pour désinstaller l'agent sur RHEL/CentOS, dans un terminal Bash, procédez comme suit :

1. Arrêtez le service Telegraf :

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Supprimer l'agent Telegraf :

   ```
    yum remove telegraf
   . Supprimez tous les fichiers de configuration ou journaux qui
   pourraient être laissés derrière :
   ```

   ```
   rm -rf /etc/telegraf*
   rm -rf /var/log/telegraf*
   ```

Mise à niveau de l'agent

Pour mettre à niveau l'agent Telegraf, procédez comme suit :

1. Arrêtez le service Telegraf :

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Supprimer l'agent Telegraf précédent :

```
 yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Installer le nouvel agent"] .
```

Ubuntu et Debian

Prérequis :

- Les commandes suivantes doivent être disponibles : curl, sudo, ping, sha256sum, openssl et dmidecode
- Si vous êtes derrière un proxy, vous devez suivre les instructions de la section **Configuration de la prise en charge du proxy pour Ubuntu/Debian**.

Configuration de la prise en charge du proxy pour Ubuntu/Debian

Si votre environnement utilise un proxy, lisez cette section avant de procéder à l'installation.

Les étapes ci-dessous décrivent les actions nécessaires pour définir les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, les utilisateurs peuvent également avoir besoin de définir la variable d'environnement *no_proxy*.

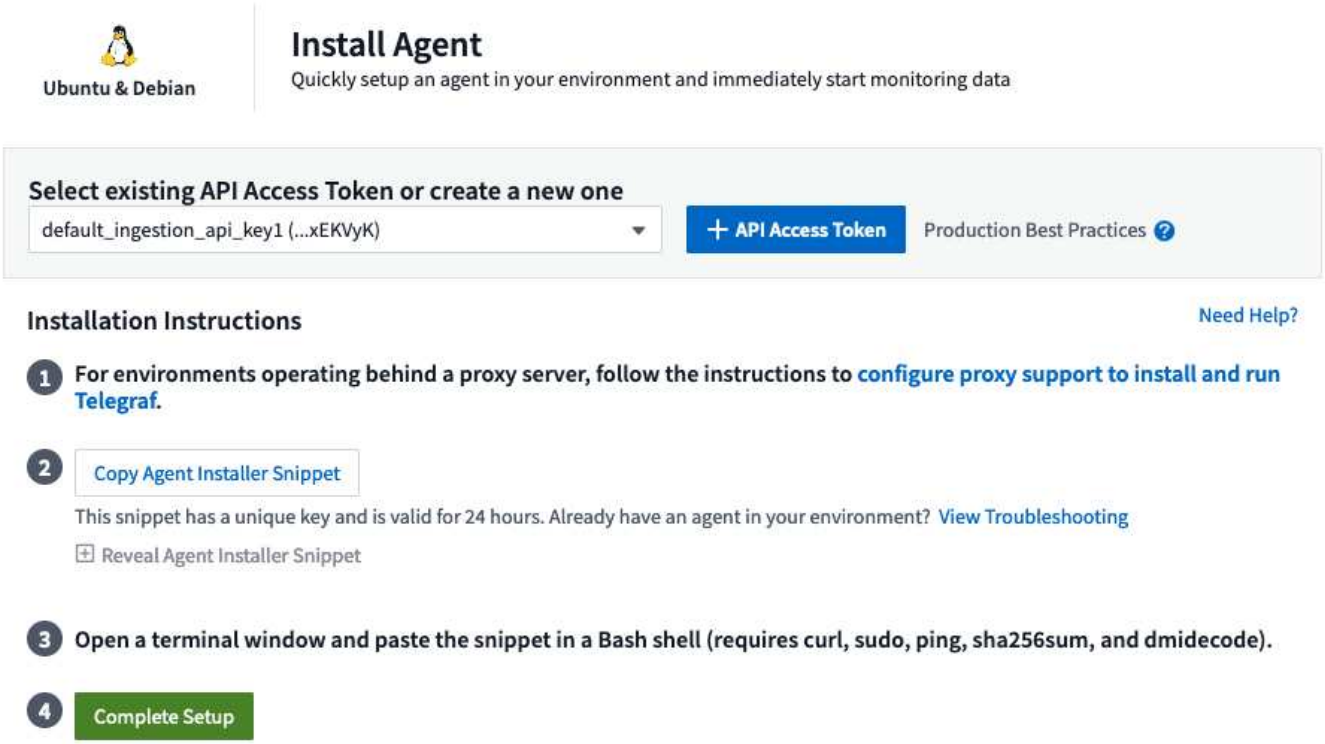
Pour les systèmes résidant derrière un proxy, effectuez les étapes suivantes **AVANT** d'installer l'agent Telegraf :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :

```
 export https_proxy=<proxy_server>:<proxy_port>
. Créez /etc/default/telegraf et insérez les définitions des variables
_https_proxy_ et/ou _http_proxy_ :
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installation de l'agent



Étapes pour installer l'agent sur Debian ou Ubuntu :

1. Choisissez une clé d'accès d'agent.
2. Copiez le bloc de commande à partir de la boîte de dialogue d'installation de l'agent. Vous pouvez cliquer sur l'icône du presse-papiers pour copier rapidement la commande dans le presse-papiers.
3. Ouvrir une fenêtre Bash
4. Collez la commande dans la fenêtre Bash et appuyez sur Entrée.
5. La commande téléchargera le programme d'installation de l'agent approprié, l'installera et définira une configuration par défaut. Une fois terminé, le service de l'agent redémarrera. La commande possède une clé unique et est valable 24 heures.
6. Cliquez sur **Terminer** ou **Continuer**

Une fois l'agent installé, vous pouvez utiliser les commandes suivantes pour démarrer/arrêter le service :

Si votre système d'exploitation utilise systemd :

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Si votre système d'exploitation n'utilise pas systemd :

```
sudo service telegraf start
sudo service telegraf stop
```

Désinstallation de l'agent

Pour désinstaller l'agent sur Ubuntu/Debian, dans un terminal Bash, exécutez ce qui suit :

1. Arrêtez le service Telegraf :

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Supprimer l'agent Telegraf :

```
 dpkg -r telegraf
. Supprimez tous les fichiers de configuration ou journaux qui
pourraient être laissés derrière :
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Mise à niveau de l'agent

Pour mettre à niveau l'agent Telegraf, procédez comme suit :

1. Arrêtez le service Telegraf :

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Supprimer l'agent Telegraf précédent :

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Installer le nouvel agent"] .
```

Vérification des sommes de contrôle des packages Telegraf

Le programme d'installation de l'agent Data Infrastructure Insights effectue des contrôles d'intégrité, mais certains utilisateurs peuvent souhaiter effectuer leurs propres vérifications avant d'installer le binaire Telegraf téléchargé. Cela peut être fait en téléchargeant le programme d'installation et en générant une somme de contrôle pour le package téléchargé, puis en comparant la somme de contrôle à la valeur indiquée dans les instructions d'installation.

Téléchargez le package d'installation sans l'installer

Pour effectuer une opération de téléchargement uniquement (par opposition au téléchargement et à l'installation par défaut), les utilisateurs peuvent modifier la commande d'installation de l'agent obtenue à partir

de l’interface utilisateur et supprimer l’option « installer ».

Suivez ces étapes :

1. Copiez l’extrait du programme d’installation de l’agent comme indiqué.
2. Au lieu de coller l’extrait dans une fenêtre de commande, collez-le dans un éditeur de texte.
3. Supprimez le « --install » (Linux) ou « -install » (Windows) de fin de la commande.
4. Copiez la commande entière depuis l’éditeur de texte.
5. Collez-le maintenant dans votre fenêtre de commande (dans un répertoire de travail) et exécutez-le.

Non-Windows (ces exemples concernent Kubernetes ; les noms de script réels peuvent varier) :

- Télécharger et installer (par défaut) :

```
 installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify && sudo -E -H ./$installerName --install
* Téléchargement uniquement :
```

```
installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify
```

Fenêtres:

- Télécharger et installer (par défaut) :

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify -install } else { Write-Host "Install
script checksum does not match"})"
* Téléchargement uniquement :
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify } else { Write-Host "Install script
checksum does not match"})"
```

La commande de téléchargement uniquement téléchargera tous les artefacts requis de Data Infrastructure Insights vers le répertoire de travail. Les artefacts comprennent, sans toutefois s’y limiter :

- un script d’installation
- un fichier d’environnement
- un binaire Telegraf

- une signature pour le binaire Telegraf
- un certificat public pour vérifier la signature binaire

L'extrait d'installation téléchargé et copié à partir de DII vérifie automatiquement le script d'installation et la signature du binaire Telegraf est vérifiée par le script d'installation.

Vérifier la valeur de la somme de contrôle

Pour générer la valeur de somme de contrôle, exécutez la commande suivante pour votre plate-forme appropriée :

- RHEL/Ubuntu :

```
 sha256sum <package_name>
* Fenêtres:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Installer le package téléchargé

Une fois que tous les artefacts ont été vérifiés de manière satisfaisante, l'installation de l'agent peut être lancée en exécutant :

Non-Windows :

```
 sudo -E -H ./<installation_script_name> --install
Fenêtres:
```

```
.\cloudinsights-windows.ps1 -install
```

Création et utilisation de jetons d'accès API

Pour créer un jeton d'accès API pour l'ingestion de données Telegraf, veuillez effectuer l'une des opérations suivantes :

Créer via la page d'installation du collecteur de données

1. Accédez à la page d'installation de Data Collector pour la plate-forme que vous souhaitez utiliser (Windows, Linux).
2. Créez un jeton avec le bouton + Jeton d'accès API.
3. Saisissez un nom et cliquez sur Enregistrer.
4. Le nom du jeton doit maintenant être sélectionné dans la liste déroulante et sera utilisé lors de l'installation du collecteur.

Créer manuellement un jeton d'accès API

1. Accédez à Admin > Accès API.
2. Cliquez sur + Jeton d'accès API.
3. Saisissez un nom et éventuellement une description.
4. Sous « Quel type d'API ce jeton sera-t-il utilisé pour appeler ? », sélectionnez uniquement « Ingestion de données », puis décochez « Unité d'acquisition ».
5. Sous « Autorisations », sélectionnez Lecture/Écriture.
6. Décochez « Faire pivoter automatiquement les jetons pour Kubernetes ».

Pour utiliser votre jeton d'accès API nouvellement créé, sélectionnez-le dans la liste déroulante « Sélectionner un jeton d'accès API existant ou en créer un nouveau » sur la page du programme d'installation. Veuillez noter que seuls les jetons possédant les propriétés suivantes peuvent être utilisés :

- Type d'API : « Ingestion de données » uniquement
- Autorisations : lecture/écriture
- Rotation automatique de Kubernetes : désactivée

Dépannage

Quelques solutions à essayer si vous rencontrez des problèmes lors de la configuration d'un agent :

Problème:	Essayez ceci:
Après avoir configuré un nouveau plugin et redémarré Telegraf, Telegraf ne parvient pas à démarrer. Les journaux indiquent une erreur semblable à ce qui suit : « [telegraf] Erreur lors de l'exécution de l'agent : Erreur lors du chargement du fichier de configuration /etc/telegraf/telegraf.d/cloudinsights-default.conf : plugin outputs.http : ligne <linenumber> : la configuration a spécifié les champs ["use_system_proxy"], mais ils n'ont pas été utilisés »	La version Telegraf installée est obsolète. Suivez les étapes sur cette page pour **mettre à niveau l'agent** pour votre plate-forme appropriée.
J'ai exécuté le script d'installation sur une ancienne installation et maintenant l'agent n'envoie plus de données	Désinstallez l'agent Telegraf, puis réexécutez le script d'installation. Suivez les étapes **Mettre à niveau l'agent** sur cette page pour votre plateforme appropriée.
J'ai déjà installé un agent à l'aide de Data Infrastructure Insights	Si vous avez déjà installé un agent sur votre hôte/VM, vous n'avez pas besoin de réinstaller l'agent. Dans ce cas, choisissez simplement la plate-forme et la clé appropriées dans l'écran d'installation de l'agent, puis cliquez sur **Continuer** ou **Terminer**.
J'ai déjà installé un agent, mais je n'utilise pas le programme d'installation de Data Infrastructure Insights.	Supprimez l'agent précédent et exécutez l'installation de l'agent Data Infrastructure Insights pour garantir des paramètres de fichier de configuration par défaut appropriés. Une fois terminé, cliquez sur **Continuer** ou **Terminer**.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration des collecteurs de données

Vous configurez des collecteurs de données dans votre environnement Data Infrastructure Insights pour collecter des données à partir des appareils du centre de données.

Avant de commencer

- Vous devez avoir configuré une unité d'acquisition avant de pouvoir commencer à collecter des données.
- Vous avez besoin d'informations d'identification pour les appareils à partir desquels vous collectez des données.
- Les adresses réseau des appareils, les informations de compte et les mots de passe sont requis pour tous les appareils à partir desquels vous collectez des données.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Collecteurs**

   Le système affiche les collecteurs de données disponibles classés par fournisseur.

2. Cliquez sur **+ Collecteur** et sélectionnez le collecteur de données à configurer.

   Dans la boîte de dialogue, vous pouvez configurer le collecteur de données et ajouter une unité d'acquisition.

3. Saisissez un nom pour le collecteur de données.
4. Cliquez sur **Configuration avancée** pour ajouter des champs de configuration supplémentaires. (Tous les collecteurs de données ne nécessitent pas de configuration avancée.)
5. Cliquez sur **Tester la configuration** pour vérifier que le collecteur de données est correctement configuré.
6. Cliquez sur **Ajouter un collecteur** pour enregistrer la configuration et ajouter le collecteur de données à votre locataire Data Infrastructure Insights .

Il peut falloir jusqu'à deux périodes d'interrogation avant que les données du service soient affichées dans les tableaux de bord ou disponibles pour l'interrogation.

- 1er sondage d'inventaire : immédiatement
- 1er sondage sur les données de performance pour établir une base de référence : immédiatement après le sondage d'inventaire
- 2e sondage de performance : dans les 15 secondes suivant la fin du 1er sondage de performance

L'interrogation se poursuit ensuite en fonction des intervalles d'interrogation d'inventaire et de performances configurés.

Déterminer l'état d'acquisition du collecteur de données

Étant donné que les collecteurs de données constituent la principale source d'informations pour Data Infrastructure Insights, il est impératif de veiller à ce qu'ils restent en état de fonctionnement.

L'état du collecteur de données s'affiche dans le coin supérieur droit de n'importe quelle page d'actif sous la forme du message « Acquis il y a N minutes », où N indique l'heure d'acquisition la plus récente du ou des collecteurs de données de l'actif. L'heure/date d'acquisition est également affichée.

Cliquer sur le message affiche un tableau avec le nom du collecteur de données, son statut et l'heure de la dernière acquisition réussie. Si vous êtes connecté en tant qu'administrateur, cliquez sur le lien du nom du collecteur de données dans le tableau pour accéder à la page de détails de ce collecteur de données.

Gestion des collecteurs de données configurés

La page Collecteurs de données installés donne accès aux collecteurs de données qui ont été configurés pour Data Infrastructure Insights. Vous pouvez utiliser cette page pour modifier les collecteurs de données existants.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Collecteurs**

   L'écran Collecteurs de données disponibles s'affiche.

2. Cliquez sur **Collecteurs de données installés**

   Une liste de tous les collecteurs de données installés s'affiche. La liste fournit le nom du collecteur, le statut, l'adresse IP à laquelle le collecteur accède et la date de la dernière acquisition des données à partir d'un périphérique. Les actions qui peuvent être effectuées sur cet écran incluent :

   - Sondage de contrôle
   - Modifier les informations d'identification du collecteur de données
   - Collecteurs de données clonés

Contrôler l'interrogation du collecteur de données

Après avoir apporté une modification à un collecteur de données, vous souhaiterez peut-être qu'il interroge immédiatement pour vérifier vos modifications, ou vous souhaiterez peut-être reporter la collecte de données sur un collecteur de données d'un, trois ou cinq jours pendant que vous travaillez sur un problème.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Collecteurs**
2. Cliquez sur **Collecteurs de données installés**
3. Cochez la case à gauche du collecteur de données que vous souhaitez modifier
4. Cliquez sur **Actions groupées** et sélectionnez l'action de sondage que vous souhaitez effectuer.

   Les actions en masse peuvent être effectuées simultanément sur plusieurs collecteurs de données. Sélectionnez les collecteurs de données et choisissez l'action à effectuer dans le menu **Action en masse**.

Modification des informations du collecteur de données

Vous pouvez modifier les informations de configuration du collecteur de données existant.

Pour modifier un seul collecteur de données :

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Collecteurs** pour ouvrir la liste des collecteurs de données installés.
2. Dans le menu d'options à droite du collecteur de données que vous souhaitez modifier, cliquez sur **Modifier**.

La boîte de dialogue Modifier le collecteur s'ouvre.

3. Saisissez les modifications et cliquez sur **Tester la configuration** pour tester la nouvelle configuration ou cliquez sur **Enregistrer** pour enregistrer la configuration.

Vous pouvez également modifier plusieurs collecteurs de données :

1. Cochez la case à gauche de chaque collecteur de données que vous souhaitez modifier.
2. Cliquez sur le bouton **Actions en masse** et choisissez **Modifier** pour ouvrir la boîte de dialogue Modifier le collecteur de données.
3. Modifiez les champs comme ci-dessus.

> Les collecteurs de données sélectionnés doivent être du même fournisseur et du même modèle, et résider sur la même unité d'acquisition.

Lors de la modification de plusieurs collecteurs de données, le champ Nom du collecteur de données affiche « Mixte » et ne peut pas être modifié. D'autres champs tels que le nom d'utilisateur et le mot de passe affichent « Mixte » et peuvent être modifiés. Les champs qui partagent la même valeur dans les collecteurs de données sélectionnés affichent les valeurs actuelles et peuvent être modifiés.

Lors de la modification de plusieurs collecteurs de données, le bouton **Tester la configuration** n'est pas disponible.

Clonage de collecteurs de données

À l'aide de la fonction de clonage, vous pouvez rapidement ajouter une source de données possédant les mêmes informations d'identification et attributs qu'une autre source de données. Le clonage vous permet de configurer facilement plusieurs instances du même type d'appareil.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Collecteurs**.
2. Cliquez sur **Collecteurs de données installés**.
3. Cliquez sur la case à cocher à gauche du collecteur de données que vous souhaitez copier.
4. Dans le menu d'options à droite du collecteur de données sélectionné, cliquez sur **Cloner**.

   La boîte de dialogue Cloner le collecteur de données s'affiche.

5. Saisissez les nouvelles informations dans les champs obligatoires.
6. Cliquez sur **Enregistrer**.

Après avoir terminé

L'opération de clonage copie tous les autres attributs et paramètres pour créer le nouveau collecteur de données.

Exécution d'actions en masse sur les collecteurs de données

Vous pouvez modifier simultanément certaines informations pour plusieurs collecteurs de données. Cette fonctionnalité vous permet de lancer un sondage, de reporter le sondage et de reprendre le sondage sur plusieurs collecteurs de données. De plus, vous pouvez supprimer plusieurs collecteurs de données.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Collecteurs**
2. Cliquez sur **Collecteurs de données installés**
3. Cliquez sur la case à cocher à gauche des collecteurs de données que vous souhaitez modifier.
4. Dans le menu d'options à droite, cliquez sur l'option que vous souhaitez exécuter.

Après avoir terminé

L'opération que vous avez sélectionnée est effectuée sur les collecteurs de données. Lorsque vous choisissez de supprimer des collecteurs de données, une boîte de dialogue s'affiche vous demandant de confirmer l'action.

Recherche sur un collecteur de données en échec

Si un collecteur de données présente un message d'échec et un impact élevé ou moyen, vous devez rechercher ce problème à l'aide de la page de résumé du collecteur de données avec ses informations liées.

Utilisez les étapes suivantes pour déterminer la cause des collecteurs de données défaillants. Les messages d'échec du collecteur de données s'affichent dans le menu **Admin** et sur la page **Collecteurs de données installés**.

Étapes

1. Cliquez sur **Admin** > **Collecteurs de données** > **Collecteurs de données installés**.
2. Cliquez sur le nom lié du collecteur de données défaillant pour ouvrir la page Résumé.
3. Sur la page Résumé, consultez la zone Commentaires pour lire les notes qui pourraient avoir été laissées par un autre ingénieur qui pourrait également enquêter sur cette panne.
4. Notez tous les messages de performance.
5. Déplacez le pointeur de votre souris sur les segments du graphique de la chronologie des événements pour afficher des informations supplémentaires.
6. Sélectionnez un message d'erreur pour un périphérique et affichez-le sous la chronologie des événements, puis cliquez sur l'icône Détails de l'erreur qui s'affiche à droite du message.

   Les détails de l'erreur incluent le texte du message d'erreur, les causes les plus probables, les informations utilisées et les suggestions de ce qui peut être essayé pour corriger le problème.

7. Dans la zone Appareils signalés par ce collecteur de données, vous pouvez filtrer la liste pour afficher uniquement les appareils qui vous intéressent, et vous pouvez cliquer sur le lien **Nom** d'un appareil pour afficher la page d'actif de cet appareil.
8. Lorsque vous revenez à la page de résumé du collecteur de données, vérifiez la zone **Afficher les modifications récentes** au bas de la page pour voir si des modifications récentes auraient pu causer le problème.

Importation de tableaux de bord

Data Infrastructure Insights fournit un certain nombre de tableaux de bord recommandés pour fournir des informations commerciales sur vos données. Chaque tableau de bord contient des widgets conçus pour aider à répondre à une question particulière ou à résoudre un problème particulier lié aux données actuellement collectées sur votre

locataire. DII vous permet également d'exporter un tableau de bord utile et de l'importer vers un autre locataire.

Importation depuis la galerie du tableau de bord

Pour importer un tableau de bord depuis la galerie, procédez comme suit :

1. Sélectionnez **Observabilité > Explorer > Tous les tableaux de bord**
2. Cliquez sur **+Importer le tableau de bord** et choisissez *Importer depuis la galerie*.

   Une liste de **tableaux de bord recommandés** s'affiche, en fonction des collecteurs de données de votre environnement. Des tableaux de bord sont disponibles pour aider à répondre aux questions sur différents types d'objets, notamment AWS, NetApp, Storage, VMware et autres.

3. Sélectionnez un ou plusieurs tableaux de bord dans la liste et cliquez sur **Ajouter des tableaux de bord**. Ces tableaux de bord s'afficheront dans votre liste de tableaux de bord.

En plus des tableaux de bord recommandés, vous pouvez également choisir d'importer des **tableaux de bord supplémentaires** qui ne sont pas pertinents pour vos données actuelles. Par exemple, si vous n'avez actuellement aucun collecteur de données de stockage installé mais que vous prévoyez d'en configurer certains à l'avenir, vous pouvez toujours choisir d'importer les tableaux de bord pertinents pour le stockage. Ces tableaux de bord seront disponibles pour l'affichage, mais peuvent ne pas afficher de données pertinentes tant qu'au moins un collecteur de données de stockage n'est pas configuré.

L'importation depuis la galerie du tableau de bord est disponible pour les utilisateurs disposant du rôle d'administrateur ou de propriétaire de compte.

Importer un tableau de bord exporté

Pour **exporter** un tableau de bord, sur la page **Observabilité > Explorer > Tous les tableaux de bord**, cliquez sur le menu à droite du tableau de bord et choisissez *Exporter*. Vous pouvez également sélectionner plusieurs tableaux de bord et choisir *Exporter* dans la liste déroulante *Actions en masse*. Les tableaux de bord sont enregistrés dans un fichier .ZIP sur votre système local.

Pour **importer** le tableau de bord, accédez au locataire souhaité et procédez comme suit :

1. Sélectionnez **Observabilité > Explorer > Tous les tableaux de bord**
2. Cliquez sur **+Importer le tableau de bord** et choisissez *Importer à partir d'un fichier*. Sélectionnez le .ZIP du fichier que vous avez précédemment exporté. Le(s) tableau(x) de bord seront importés et s'afficheront dans votre liste de tableaux de bord. Notez que si vous importez un tableau de bord portant le même nom qu'un tableau de bord existant, un « (2) » sera ajouté au nom du tableau de bord.

Comptes d'utilisateurs et rôles

Data Infrastructure Insights fournit jusqu'à quatre rôles de compte utilisateur : propriétaire du compte, administrateur, utilisateur et invité. À chaque compte sont attribués des niveaux d'autorisation spécifiques, comme indiqué dans le tableau ci-dessous. Les utilisateurs sont soit"invité" à Data Infrastructure Insights et un rôle spécifique lui est attribué, ou vous pouvez vous connecter via"Autorisation d'authentification unique (SSO)" avec un rôle par défaut. L'autorisation SSO est disponible en tant que fonctionnalité dans Data Infrastructure Insights Premium Edition.

Niveaux d’autorisation

Vous utilisez un compte disposant de privilèges d’administrateur pour créer ou modifier des comptes d’utilisateurs. À chaque compte utilisateur est attribué un rôle pour chaque fonctionnalité Data Infrastructure Insights parmi les niveaux d’autorisation suivants.

Rôle	Observabilité	Sécurité de la charge de travail	Rapports	Administrateur
Propriétaire du compte	Identique à l’administrateur	Identique à l’administrateur	Identique à l’administrateur	Identique à l’administrateur, mais gère également la configuration de l’authentification SSO et de la fédération d’identité. Il est également possible d’attribuer des propriétaires supplémentaires et d’ajouter des clients sur le locataire principal du fournisseur de services gérés (MSP).
Administrateur	Peut exécuter toutes les fonctions d’observabilité, ainsi que la gestion des collecteurs de données.	Peut exécuter toutes les fonctions de sécurité, y compris celles pour les alertes, l’analyse médico-légale, les collecteurs de données, les politiques de réponse automatisées et les jetons API pour la sécurité. Un administrateur peut également inviter d’autres utilisateurs, mais ne peut attribuer que des rôles de sécurité.	Peut exécuter toutes les fonctions utilisateur/auteur, y compris la gestion des jetons API de reporting, ainsi que toutes les tâches administratives telles que la configuration des rapports et l’arrêt et le redémarrage des tâches de reporting. Un administrateur peut également inviter d’autres utilisateurs, mais ne peut attribuer que des rôles de reporting.	Peut inviter d’autres utilisateurs mais ne peut attribuer que des rôles d’observabilité. Peut afficher mais pas modifier la configuration SSO. Peut créer et gérer des jetons d’accès API. Peut afficher les informations d’audit. Peut afficher les informations d’abonnement, l’utilisation et l’historique. Peut gérer les listes de destinataires des notifications d’alerte globale et des notifications d’abonnement.

Rôle	Observabilité	Sécurité de la charge de travail	Rapports	Administrateur
Utilisateur	Peut afficher et modifier les tableaux de bord, les requêtes, les alertes, les annotations, les règles d'annotation et les applications, et gérer la résolution des appareils.	Peut afficher et gérer les alertes et consulter les analyses médico-légales. Le rôle utilisateur peut modifier l'état de l'alerte, ajouter une note, prendre des instantanés manuellement et gérer la restriction de l'accès utilisateur.	Peut exécuter toutes les fonctions invité/consommateur ainsi que créer et gérer des rapports et des tableaux de bord.	Non disponible
Invité	Dispose d'un accès en lecture seule aux pages d'actifs, aux tableaux de bord, aux alertes et peut afficher et exécuter des requêtes.	Peut afficher les alertes et les analyses médico-légales. Le rôle d'invité ne peut pas modifier l'état de l'alerte, ajouter une note, prendre des instantanés manuellement ou restreindre l'accès des utilisateurs.	Peut afficher, planifier et exécuter des rapports et définir des préférences personnelles telles que celles concernant les langues et les fuseaux horaires. Les invités/consommateurs ne peuvent pas créer de rapports ni effectuer de tâches administratives.	Non disponible

La meilleure pratique consiste à limiter le nombre d'utilisateurs disposant d'autorisations d'administrateur. Le plus grand nombre de comptes doit être des comptes utilisateurs ou invités.

Data Infrastructure Insights : autorisations par rôle d'utilisateur

Le tableau suivant présente les autorisations Data Infrastructure Insights accordées à chaque rôle d'utilisateur.

Fonctionnalité	Administrateur/Propriétaire du compte	Utilisateur	Invité
Unités d'acquisition : ajouter/modifier/supprimer	Y	N	N
Alertes* : Créer/Modifier/Supprimer	Y	Y	N
Alertes* : Voir	Y	Y	Y
Règles d'annotation : Créer/Exécuter/Modifier/Supprimer	Y	Y	N

Annotations : Créer/Modifier/Attribuer/Afficher/Supprimer/Supprimer	Y	Y	N
Accès API* : Créer/Renommer/Désactiver/Révoquer	Y	N	N
Applications : Créer/Afficher/Modifier/Supprimer	Y	Y	N
Pages d’actifs : modifier	Y	Y	N
Pages d’actifs : vue	Y	Y	Y
Audit : Voir	Y	N	N
Coût du cloud	Y	N	N
Sécurité	Y	N	N
Tableaux de bord : Créer/Modifier/Supprimer	Y	Y	N
Tableaux de bord : vue	Y	Y	Y
Collecteurs de données : ajouter/modifier/interroger/supprimer	Y	N	N
Notifications : Afficher	Y	Y	Y
Notifications : Modifier	Y	N	N
Requêtes : Créer/Modifier/Supprimer	Y	Y	N
Requêtes : Afficher/Exécuter	Y	Y	Y
Résolution de l’appareil	Y	Y	N
Rapports* : Afficher/Exécuter	Y	Y	Y
Rapports* : Créer/Modifier/Supprimer/Planifier	Y	Y	N
Abonnement : Voir/Modifier	Y	N	N
Gestion des utilisateurs : inviter/ajouter/modifier/désactiver	Y	N	N

*Nécessite l’édition Premium

Créer des comptes en invitant des utilisateurs

La création d'un nouveau compte utilisateur s'effectue via la NetApp Console. Un utilisateur peut répondre à l'invitation envoyée par e-mail, mais si l'utilisateur n'a pas de compte avec Console, il doit s'inscrire pour pouvoir accepter l'invitation.

Avant de commencer

- Le nom d'utilisateur est l'adresse e-mail de l'invitation.
- Comprendre les rôles d'utilisateur que vous allez attribuer.
- Les mots de passe sont définis par l'utilisateur lors du processus d'inscription.

Étapes

1. Connectez-vous à Data Infrastructure Insights
2. Dans le menu, cliquez sur **Admin > Gestion des utilisateurs**

   L'écran Gestion des utilisateurs s'affiche. L'écran contient une liste de tous les comptes du système.

3. Cliquez sur **+ Utilisateur**

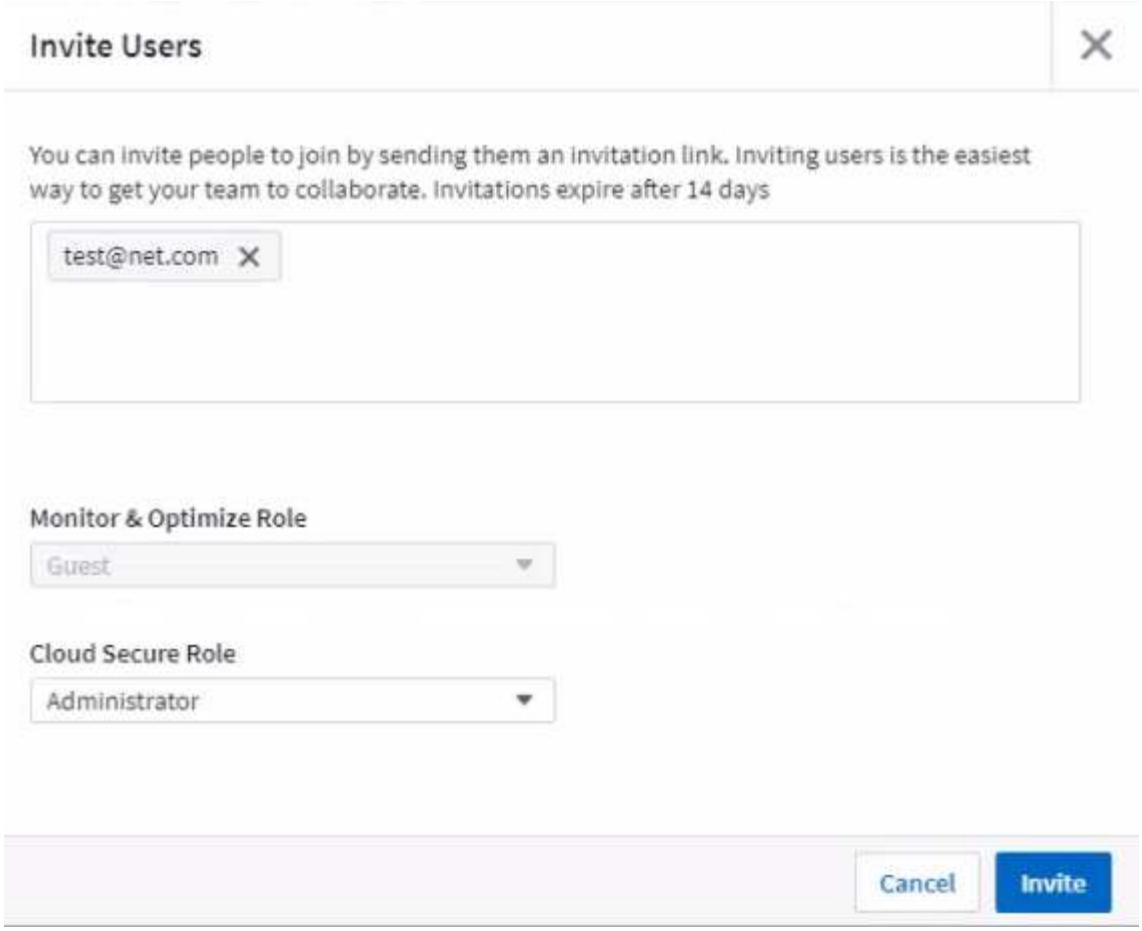
   L'écran **Inviter un utilisateur** s'affiche.

4. Saisissez une adresse e-mail ou plusieurs adresses pour les invitations.

   Remarque : lorsque vous saisissez plusieurs adresses, elles sont toutes créées avec le même rôle. Vous ne pouvez définir que plusieurs utilisateurs sur le même rôle.

5. Sélectionnez le rôle de l'utilisateur pour chaque fonctionnalité de Data Infrastructure Insights.

   Les fonctionnalités et les rôles que vous pouvez choisir dépendent des fonctionnalités auxquelles vous avez accès dans votre rôle d'administrateur particulier. Par exemple, si vous disposez du rôle d'administrateur uniquement pour les rapports, vous pourrez attribuer des utilisateurs à n'importe quel rôle dans les rapports, mais vous ne pourrez pas attribuer de rôles pour l'observabilité ou la sécurité.



6. Cliquez sur **Inviter**

   L'invitation est envoyée à l'utilisateur. Les utilisateurs auront 14 jours pour accepter l'invitation. Une fois qu'un utilisateur accepte l'invitation, il sera redirigé vers le portail NetApp Cloud, où il s'inscrira à l'aide de l'adresse e-mail indiquée dans l'invitation. S'ils disposent d'un compte existant pour cette adresse e-mail, ils peuvent simplement se connecter et pourront alors accéder à leur environnement Data Infrastructure Insights .

Modifier le rôle d'un utilisateur existant

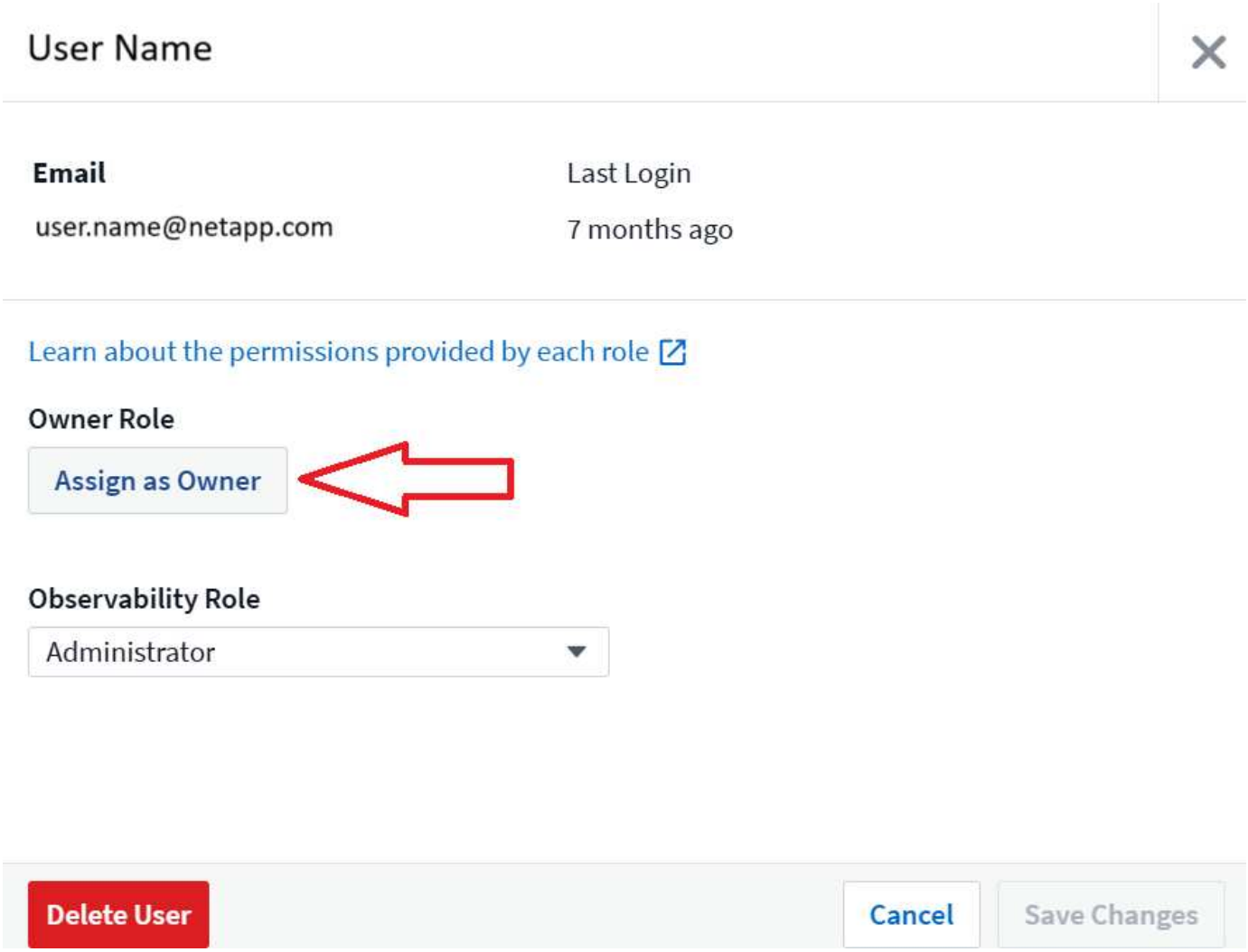
Pour modifier le rôle d'un utilisateur existant, y compris l'ajouter en tant que **propriétaire de compte secondaire**, suivez ces étapes.

1. Cliquez sur **Admin > Gestion des utilisateurs**. L'écran affiche une liste de tous les comptes du système.
2. Cliquez sur le nom d'utilisateur du compte que vous souhaitez modifier.
3. Modifiez le rôle de l'utilisateur dans chaque ensemble de fonctionnalités de Data Infrastructure Insights selon vos besoins.
4. Cliquez sur *Enregistrer les modifications*.

Pour attribuer un propriétaire de compte secondaire

Vous devez être connecté en tant que propriétaire de compte pour Observability afin d'attribuer le rôle de propriétaire de compte à un autre utilisateur.

1. Cliquez sur **Admin > Gestion des utilisateurs**.
2. Cliquez sur le nom d'utilisateur du compte que vous souhaitez modifier.
3. Dans la boîte de dialogue Utilisateur, cliquez sur **Attribuer en tant que propriétaire**.
4. Enregistrez les modifications.



Vous pouvez avoir autant de propriétaires de compte que vous le souhaitez, mais la meilleure pratique consiste à limiter le rôle de propriétaire à certaines personnes uniquement.

Suppression d'utilisateurs

Un utilisateur avec le rôle Administrateur peut supprimer un utilisateur (par exemple, une personne qui ne fait plus partie de l'entreprise) en cliquant sur le nom de l'utilisateur et en cliquant sur *Supprimer l'utilisateur* dans la boîte de dialogue. L'utilisateur sera supprimé de l'environnement Data Infrastructure Insights .

Notez que tous les tableaux de bord, requêtes, etc. créés par l'utilisateur resteront disponibles dans l'environnement Data Infrastructure Insights même après la suppression de l'utilisateur.

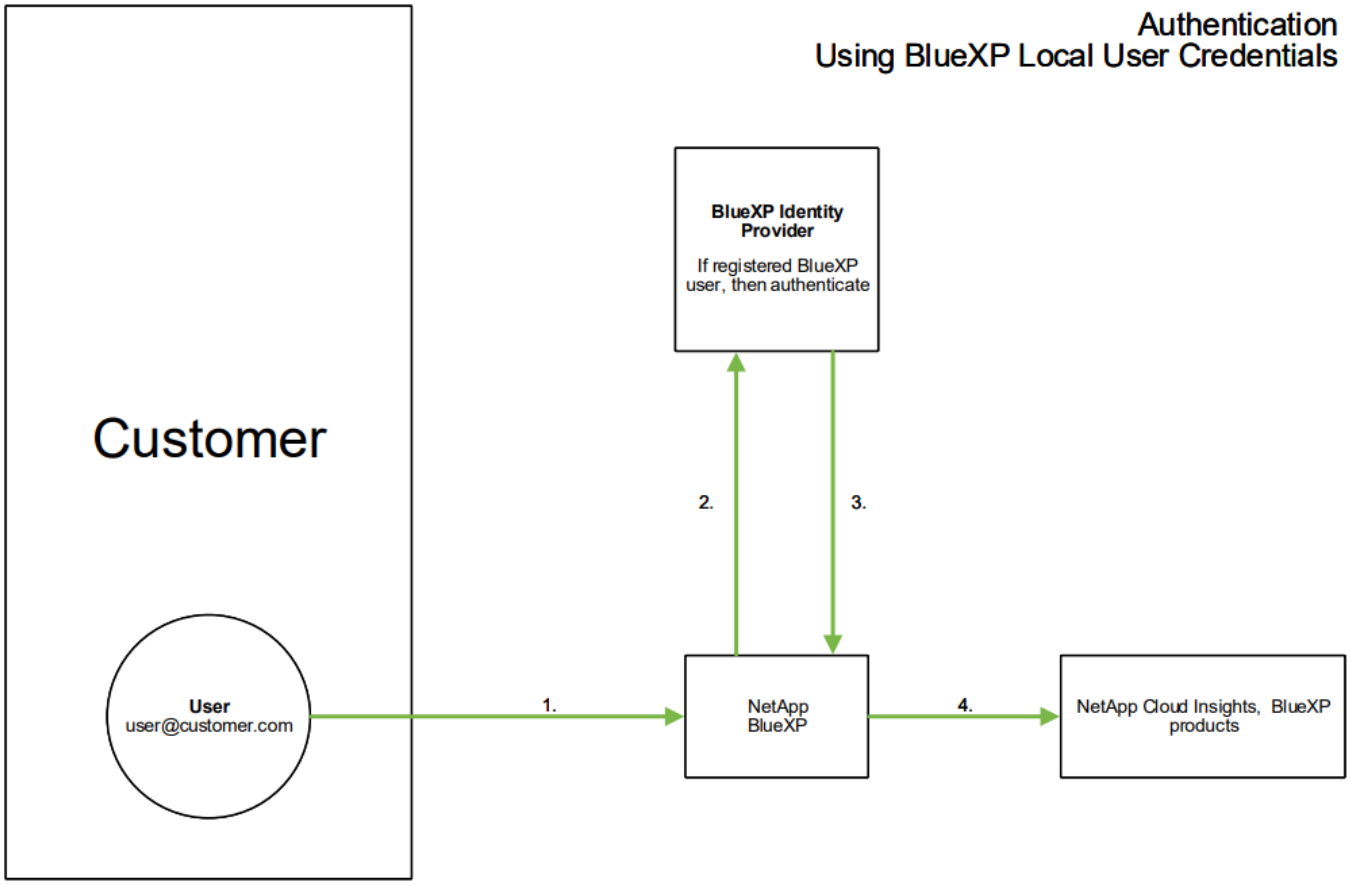
Authentification unique (SSO) et fédération d'identité

Qu’est-ce que la Fédération d’Identité ?

Avec la Fédération des identités :

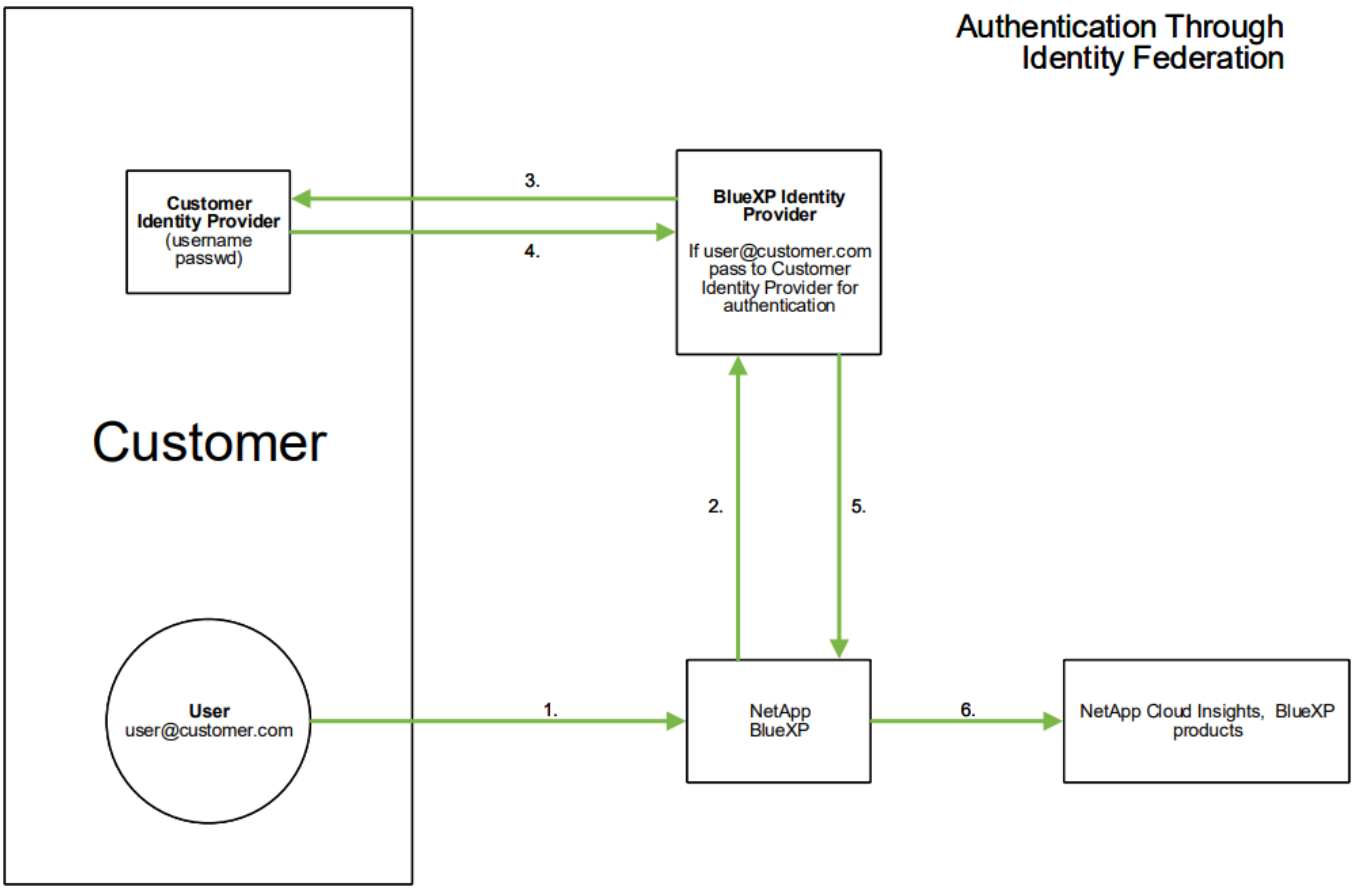
- L’authentification est déléguée au système de gestion des identités du client, à l’aide des informations d’identification du client provenant de votre annuaire d’entreprise et de politiques d’automatisation telles que l’authentification multifacteur (MFA).
- Les utilisateurs se connectent une fois à tous les services de la NetApp Console (authentification unique).

Les comptes utilisateurs sont gérés dans la NetApp Console pour tous les services cloud. Par défaut, l’authentification est effectuée à l’aide d’un profil utilisateur local de la console. Vous trouverez ci-dessous un aperçu simplifié de ce processus :



Cependant, certains clients souhaitent utiliser leur propre fournisseur d’identité pour authentifier leurs utilisateurs pour Data Infrastructure Insights et leurs autres services de NetApp Console . Avec Identity Federation, les comptes de la NetApp Console sont authentifiés à l’aide des informations d’identification de votre annuaire d’entreprise.

Voici un exemple simplifié de ce processus :



Dans le diagramme ci-dessus, lorsqu'un utilisateur accède à Data Infrastructure Insights, cet utilisateur est dirigé vers le système de gestion des identités du client pour l'authentification. Une fois le compte authentifié, l'utilisateur est dirigé vers l'URL du locataire Data Infrastructure Insights .

Activation de la fédération d'identité

La console utilise Auth0 pour implémenter la fédération d'identité et s'intégrer à des services tels que Active Directory Federation Services (ADFS) et Microsoft Azure Active Directory (AD). Pour configurer la fédération d'identité, consultez le"Instructions de la Fédération" .

Vous devez configurer la fédération d'identité avant de pouvoir utiliser SSO avec Data Infrastructure Insights.

Il est important de comprendre que la modification de la fédération d'identité s'appliquera non seulement à Data Infrastructure Insights, mais à tous les services de NetApp Console . Le client doit discuter de ce changement avec l'équipe NetApp de chaque produit qu'il possède pour s'assurer que la configuration qu'il utilise fonctionnera avec la Fédération d'identité ou si des ajustements doivent être effectués sur des comptes. Le client devra également impliquer son équipe SSO interne dans le changement vers la fédération d'identité.

Il est également important de comprendre qu'une fois la fédération d'identité activée, toute modification apportée au fournisseur d'identité de l'entreprise (comme le passage de SAML à Microsoft AD) nécessitera probablement un dépannage/des modifications/une attention particulière pour mettre à jour les profils des utilisateurs.

Pour ce problème ou tout autre problème de fédération, vous pouvez ouvrir un ticket d'assistance à l'adresse https://mysupport.netapp.com/site/help .

Provisionnement automatique des utilisateurs par authentification unique (SSO)

En plus d'inviter des utilisateurs, les administrateurs peuvent activer l'accès **Single Sign-On (SSO) User Auto-Provisioning** à Data Infrastructure Insights pour tous les utilisateurs de leur domaine d'entreprise, sans avoir à les inviter individuellement. Avec SSO activé, tout utilisateur disposant de la même adresse e-mail de domaine peut se connecter à Data Infrastructure Insights à l'aide de ses informations d'identification d'entreprise.

> *SSO User Auto-Provisioning* est disponible dans Data Infrastructure Insights Premium Edition et doit être configuré avant de pouvoir être activé pour Data Infrastructure Insights. La configuration de l'auto-approvisionnement des utilisateurs SSO comprend"Fédération d'identité" via la NetApp Console comme décrit dans la section ci-dessus. La fédération permet aux utilisateurs à authentification unique d'accéder à vos comptes NetApp Console à l'aide des informations d'identification de votre annuaire d'entreprise, en utilisant des normes ouvertes telles que Security Assertion Markup Language 2.0 (SAML) et OpenID Connect (OIDC).

Pour configurer *SSO User Auto-Provisioning*, sur la page **Admin > Gestion des utilisateurs**, vous devez d'abord avoir configuré la fédération d'identité. Sélectionnez le lien **Configurer la fédération** dans la bannière pour passer à la fédération de la console. Une fois cette configuration effectuée, les administrateurs de Data Infrastructure Insights peuvent alors activer la connexion utilisateur SSO. Lorsqu'un administrateur active le *Provisionnement automatique des utilisateurs SSO*, il choisit un rôle par défaut pour tous les utilisateurs SSO (tel qu'invité ou utilisateur). Les utilisateurs qui se connectent via SSO auront ce rôle par défaut.

Parfois, un administrateur souhaitera promouvoir un seul utilisateur hors du rôle SSO par défaut (par exemple, pour en faire un administrateur). Ils peuvent le faire sur la page **Admin > Gestion des utilisateurs** en cliquant sur le menu de droite de l'utilisateur et en sélectionnant *Attribuer un rôle*. Les utilisateurs auxquels un rôle explicite est attribué de cette manière continuent d'avoir accès à Data Infrastructure Insights même si *SSO User Auto-Provisioning* est ultérieurement désactivé.

Si l'utilisateur n'a plus besoin du rôle élevé, vous pouvez cliquer sur le menu pour *Supprimer l'utilisateur*. L'utilisateur sera supprimé de la liste. Si *SSO User Auto-Provisioning* est activé, l'utilisateur peut continuer à se connecter à Data Infrastructure Insights via SSO, avec le rôle par défaut.

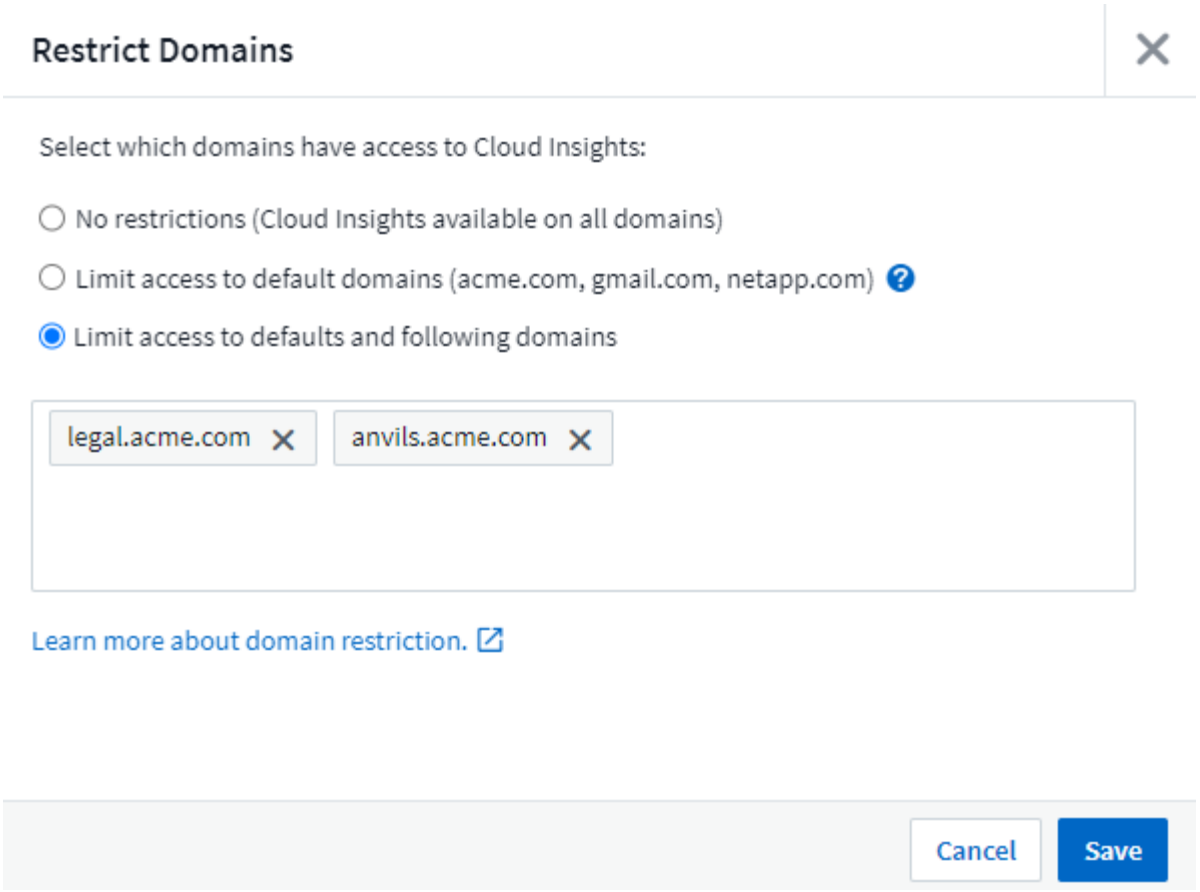
Vous pouvez choisir de masquer les utilisateurs SSO en décochant la case **Afficher les utilisateurs SSO**.

Cependant, n'activez pas *SSO User Auto-Provisioning* si l'une de ces conditions est remplie :

- Votre organisation possède plusieurs locataires Data Infrastructure Insights
- Votre organisation ne souhaite pas que tous les utilisateurs du domaine fédéré disposent d'un certain niveau d'accès automatique au locataire Data Infrastructure Insights . *À ce stade, nous n'avons pas la possibilité d'utiliser des groupes pour contrôler l'accès aux rôles avec cette option*.

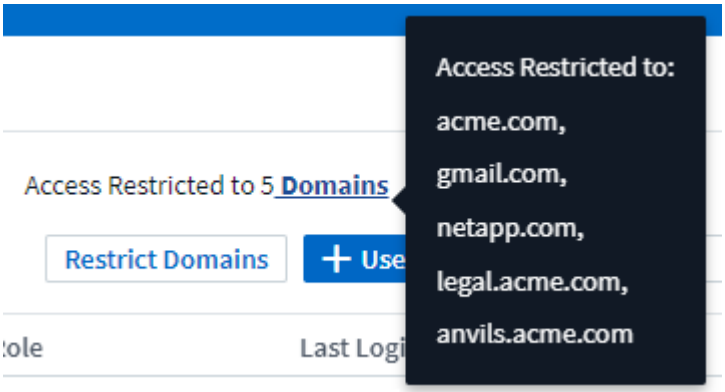
Restreindre l'accès par domaine

Data Infrastructure Insights peut restreindre l'accès des utilisateurs aux seuls domaines que vous spécifiez. Sur la page **Admin > Gestion des utilisateurs**, sélectionnez « Restreindre les domaines ».



Ces choix vous sont présentés :

- Aucune restriction : Data Infrastructure Insights reste accessible aux utilisateurs quel que soit leur domaine.
- Limiter l'accès aux domaines par défaut : les domaines par défaut sont ceux utilisés par les propriétaires de compte de votre environnement Data Infrastructure Insights . Ces domaines sont toujours accessibles.
- Limitez l'accès aux valeurs par défaut et aux domaines que vous spécifiez. Répertoriez tous les domaines auxquels vous souhaitez donner accès à votre environnement Data Infrastructure Insights , en plus des domaines par défaut.



Liste de référence des collecteurs de données Data Infrastructure Insights

Data Infrastructure Insights prend en charge une variété de collecteurs de données provenant de nombreux fournisseurs et services.

Les collecteurs de données sont classés selon ces types :

- Infrastructure : acquise auprès de périphériques fournisseurs tels que des baies de stockage, des commutateurs, des hyperviseurs ou des périphériques de sauvegarde.
- Service : acquis à partir de services tels que Kubernetes ou Docker. Également appelé *Intégration*.

Liste alphabétique des collecteurs de données pris en charge par Data Infrastructure Insights:

Collecteur de données	Type
"Amazon EC2 et EBS"	Infrastructure
"AWS S3 comme stockage"	Infrastructures
"Amazon FSx for NetApp ONTAP"	Infrastructure
"Apache"	Service
"Azure NetApp Files"	Infrastructure
"Machines virtuelles et VHD Azure"	Infrastructure
"Conseiller réseau Brocade (BNA)"	Infrastructure
"Commutateurs Fibre Channel Brocade"	Infrastructure
"Brocade FOS REST"	Infrastructure
"Commutateurs Cisco MDS Fabric"	Infrastructure
"Consul"	Service
"Couchbase"	Service
"CouchDB"	Service
"Cohesity SmartFiles"	Infrastructure
"Domaine de données Dell EMC"	Infrastructure
"Système de contrôle électronique Dell EMC"	Infrastructure
"Dell EMC PowerScale (anciennement Isilon)"	Infrastructure
"Dell EMC Isilon / PowerScale REST"	Infrastructure
"Dell EMC PowerStore"	Infrastructure
"Point de récupération Dell EMC"	Infrastructure
"Dell EMC ScaleIO/PowerFlex"	Infrastructure
"Dell EMC Unity"	Infrastructure
"Dell EMC Unisphere REST"	Infrastructure

Collecteur de données	Type
"Famille d'appareils Dell EMC VMAX/PowerMax"	Infrastructure
"Stockage en blocs Dell EMC VNX"	Infrastructure
"Fichier Dell EMC VNX"	Infrastructure
"Dell EMC VNX unifié"	Infrastructure
"Dell EMC VPLEX"	Infrastructure
"Dell EMC XtremIO"	Infrastructure
"Série Dell XC"	Infrastructure
"Docker"	Service
"Elasticsearch"	Service
"Flink"	Service
"Fujitsu ETERNUS DX"	Infrastructure
"Google Compute et Stockage"	Infrastructure
"Google Cloud NetApp Volumes"	Infrastructure
"Hadoop"	Service
"HAProxy"	Service
"Plateforme de contenu Hitachi (HCP)"	Infrastructure
"Suite de commandes Hitachi Vantara"	Infrastructure
"Plateforme NAS Hitachi Vantara"	Infrastructure
"Centre d'opérations Hitachi"	Infrastructure
"Stockage HP Enterprise Alletra 6000 (anciennement Nimble)"	Infrastructure
"Stockage HP Enterprise Alletra 9000 / Primera (anciennement 3PAR)"	Infrastructure
"Vue de commande HP Enterprise"	Infrastructure
"Appareils Huawei OceanStor et Dorado"	Infrastructure
"IBM Cleversafe"	Infrastructure
"Série IBM CS"	Infrastructure
"Contrôleur de volume SAN IBM (SVC)"	Infrastructure
"Système de stockage IBM série DS8000"	Infrastructure
"Stockages IBM XIV et A9000"	Infrastructure
"Infinidat InfiniBox"	Infrastructure
"Java"	Service
"Kafka"	Service
"Capacité"	Service

Collecteur de données	Type
"Kibana"	Service
"Kubernetes"	Service
"Série Lenovo HX"	Infrastructure
"Memcached"	Service
"Azure NetApp Files"	Infrastructure
"Microsoft Hyper-V"	Infrastructure
"MongoDB"	Service
"MySQL"	Service
"NetApp Cloud Volumes ONTAP"	Infrastructure
"Connexion au cloud NetApp pour ONTAP 9.9+"	Infrastructure
"NetApp Data ONTAP 7-Mode"	Infrastructure
"NetApp Série E"	Infrastructure
"REST NetApp Série E"	Infrastructure
"Amazon FSx for NetApp ONTAP"	Infrastructure
"Centre virtuel NetApp HCI"	Infrastructure
"Logiciel de gestion des données NetApp ONTAP"	Infrastructure
"Collecteur NetApp ONTAP REST"	Infrastructure
"NetApp ONTAP AFX"	Infrastructure
"Collecteur NetApp ONTAP ASA r2 (All-SAN Array)"	Infrastructure
"ONTAP Select NetApp ONTAP"	Infrastructure
"Baie 100 % Flash NetApp SolidFire"	Infrastructure
"NetApp StorageGRID"	Infrastructure
"Netstat"	Service
"Nginx"	Service
"Nœud"	Service
"Série Nutanix NX"	Infrastructure
"OpenZFS"	Service
"Appareil de stockage Oracle ZFS"	Infrastructure
"PostgreSQL"	Service
"Agent marionnette"	Service
"Baie Flash Pure Storage"	Infrastructure
"Virtualisation Red Hat"	Infrastructure
"Redis"	Service

Collecteur de données	Type
"Repenser la base de données"	Service
"RHEL et CentOS"	Service
"Stockage Rubrik CDM"	Infrastructure
"Ubuntu et Debian"	Service
"Magasin de données VAST"	Infrastructure
"VMware vSphere"	Infrastructure
"Windows"	Service
"Gardien de zoo"	Service

S’abonner à Data Infrastructure Insights

Démarrer avec Data Infrastructure Insights est aussi simple que trois étapes simples :

1. Inscrivez-vous pour un compte sur"* NetApp Console*" pour accéder à toutes les offres Cloud de NetApp.
2. Inscrivez-vous pour un essai gratuit de Data Infrastructure Insights pour explorer les fonctionnalités disponibles. Pour vous inscrire à un essai gratuit :
   - Aller à https://netapp.com
   - Sélectionnez **Comment acheter** en haut de la page.
   - Sélectionnez **Demander un essai**. Si vous n’êtes pas déjà inscrit sur Console, entrez vos coordonnées et inscrivez-vous. Sinon, connectez-vous.
   - Planifiez une réunion ou attendez qu’un représentant vous contacte au sujet de votre essai.
3. **Abonnez-vous** à Data Infrastructure Insights pour un accès continu et ininterrompu à vos données via une variété d’options d’abonnement flexibles :
   - "Ventes directes NetApp"
   - Place de marché AWS :
     - "Abonnement à durée déterminée"
     - "Abonnement à la carte"
     - "Abonnement base fixe + dépassements à la carte"
   - "Place de marché Azure"(toutes les options d’abonnement)

Au cours du processus d’inscription, vous pouvez choisir la région mondiale dans laquelle héberger votre environnement Data Infrastructure Insights . Pour plus d’informations, lisez Data Infrastructure Insights"Informations et région" .

Pour obtenir des informations détaillées sur les fonctionnalités et les options de tarification de Data Infrastructure Insights , consultez le"Éditions Data Infrastructure Insights" page.

Lorsque vous utilisez Data Infrastructure Insights, si vous voyez une icône de cadenas , cela signifie que la fonctionnalité n’est pas disponible dans votre abonnement actuel ou est disponible sous une forme limitée. Abonnez-vous à cette fonctionnalité pour un accès complet. Certaines fonctionnalités sont disponibles en tant queÉvaluation du module avant de souscrire.

Édition d’essai

Lorsque vous vous inscrivez à Data Infrastructure Insights et que votre environnement est actif, vous bénéficiez d’un essai gratuit de 30 jours de Data Infrastructure Insights. Au cours de cet essai, vous pouvez explorer les fonctionnalités offertes par Data Infrastructure Insights , dans votre propre environnement.

À tout moment pendant votre période d’essai, vous pouvez vous abonner à Data Infrastructure Insights. L’abonnement à Data Infrastructure Insights garantit un accès ininterrompu à vos données ainsi qu’une **"assistance produit"** options.

Data Infrastructure Insights affiche une bannière lorsque votre essai gratuit approche de sa fin. Dans cette bannière se trouve un lien *Afficher l’abonnement*, qui ouvre la page **Admin → Abonnement**. Les utilisateurs non administrateurs verront la bannière mais ne pourront pas accéder à la page d’abonnement.

Si vous avez besoin de temps supplémentaire pour évaluer Data Infrastructure Insights et que votre essai doit expirer dans 4 jours ou moins, vous pouvez prolonger votre essai de 30 jours supplémentaires. Vous ne pouvez prolonger l'essai qu'une seule fois. Vous ne pouvez pas prolonger si votre essai a expiré.

Essai via AWS Marketplace

Vous pouvez également vous inscrire pour un essai gratuit via AWS Marketplace. L'essai gratuit d'AWS Marketplace vous donne accès à Data Infrastructure Insights pour une période d'essai de 33 jours.

L'essai gratuit d'AWS Marketplace ne peut pas être prolongé.

Que faire si mon essai a expiré ?

Si votre essai gratuit a expiré et que vous n'êtes pas encore abonné à Data Infrastructure Insights, vous disposerez de fonctionnalités limitées jusqu'à votre abonnement. L'ingestion de données peut cesser et, après quelques semaines, vos données seront supprimées conformément à notre politique de conservation des données.

Que faire si mon abonnement a expiré ?

Si vous avez un abonnement à Data Infrastructure Insights, mais que cet abonnement a expiré, vous disposerez d'un délai de grâce de cinq jours pour renouveler votre abonnement. Toutes les fonctionnalités de Data Infrastructure Insights resteront actives pendant cette période de grâce.

Une fois la période de grâce écoulée, la fonctionnalité Data Infrastructure Insights est suspendue jusqu'à ce que vous renouveliez. Pour renouveler, consultez la page **Admin > Abonnement** ou contactez le service commercial NetApp .

Vos données Data Infrastructure Insights restent intactes pendant 30 jours après la période de grâce. Si vous renouvelez votre abonnement dans ce délai, toutes vos données jusqu'à l'expiration du délai de grâce seront à votre disposition.

Évaluation du module

Vous pouvez également profiter des **Évaluations de modules**. Par exemple, si vous êtes déjà abonné à Infrastructure Observability mais que vous ajoutez Kubernetes à votre environnement, vous accéderez automatiquement à une évaluation de 30 jours de Kubernetes Observability, à compter de l'installation de NetApp Kubernetes Monitoring Operator. Vous ne serez facturé que pour votre utilisation de l'unité gérée par Kubernetes Observability à la fin de la période d'évaluation.

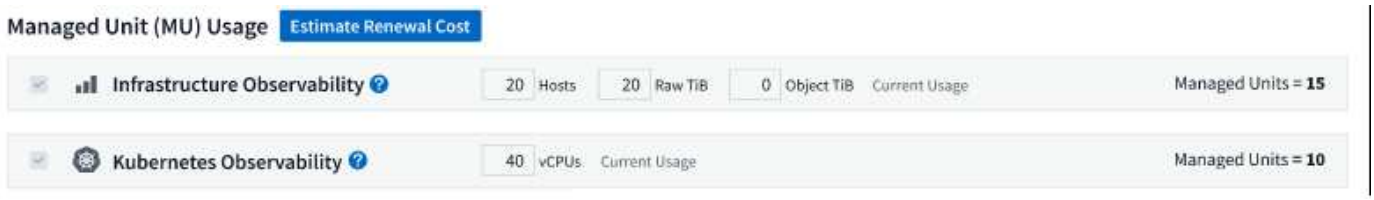
N'oubliez pas que l'utilisation de la nouvelle unité gérée (UM) vous sera facturée après l'évaluation. Assurez-vous donc de planifier en conséquence. Lorsque l'évaluation de votre module se termine, vous serez averti si vous devez ajouter d'autres MU pour éviter une interruption de service.

Vous pouvez surveiller l'utilisation de votre unité gérée sur la page **Admin > Abonnement** dans l'onglet **Utilisation**.

Une *évaluation de module* n'est pas un *essai* - nous utilisons le terme essai lorsque nous offrons aux clients une période d'essai gratuite d'utilisation du service Data Infrastructure Insights pour confirmer l'adéquation et permettre l'achat. L'évaluation d'un module est différente : c'est lorsque nous permettons à un client payant d'essayer un module de Data Infrastructure Insights qu'il n'a pas utilisé au cours des derniers mois de son abonnement payant. Lorsque l'évaluation est active, les frais pour le module nouvellement configuré sont supprimés. L'environnement de travail des clients est toujours sous abonnement et n'est pas revenu à l'essai gratuit. L'abonnement n'a pas changé.

Estimateur

Lors d'une évaluation de module, l'utilisation des MU ne vous est pas facturée pour les ressources consommées pour le module, mais vous pouvez ouvrir l'**Estimateur** (sur l'onglet *Résumé*) pour voir comment les MU seront facturées après l'évaluation, ainsi que jouer avec des scénarios « Et si » avec le nombre de MU dont vous pourriez avoir besoin à l'avenir. Réinitialisez les chiffres en quittant l'estimateur.



Cochez la case à côté d'un module pour ajouter ou supprimer l'ensemble des MU du module du coût estimé.

L'estimateur vous permet également de voir comment les chiffres s'accumulent soit pour un module complémentaire - où vous conservez votre durée d'abonnement actuelle et augmentez le nombre d'unités gérées sous licence - soit pour une option de renouvellement pour un abonnement de renouvellement que vous achèteriez à la fin de votre durée d'abonnement actuelle.

Veuillez noter que les clients ne sont éligibles à une évaluation du module qu'une seule fois par abonnement.

Options d’abonnement

Pour vous abonner, rendez-vous dans **Admin → Abonnement**. En plus des boutons **S’abonner**, vous pourrez voir vos collecteurs de données installés et calculer votre comptage estimé. Pour un environnement typique, vous pouvez cliquer sur le bouton AWS Marketplace en libre-service. Si votre environnement comprend ou devrait inclure 1 000 unités gérées ou plus, vous êtes éligible à la tarification au volume.

Mesure de l’observabilité

L’observabilité des Data Infrastructure Insights est mesurée de deux manières :

- Comptage de capacité
- Comptage unitaire géré (hérité)

Votre abonnement sera mesuré par l’une de ces méthodes, selon que vous disposez d’un abonnement existant ou que vous lancez un nouvel abonnement.

Comptage de capacité

Data Infrastructure Insights Observability mesure l’utilisation en fonction du niveau de stockage de votre locataire. Vous pouvez avoir des stockages qui entrent dans une ou plusieurs de ces catégories :

- Matières premières primaires
- Objet brut
- Cloud consommé

Chaque niveau est mesuré à un taux différent, l’ensemble étant calculé ensemble pour vous donner un droit pondéré. La formule de calcul de l’utilisation pondérée est la suivante :

```
 Weighted Capacity = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud
Tier Provisioned TiB)
Pour faciliter cela, DII calcule un seul numéro de *droit pondéré* basé
sur les quantités _souscrites_ ; il calcule ensuite ce même numéro basé
sur le stockage _découvert_ et déclare une violation uniquement si la
capacité découverte est supérieure au droit pondéré.  Cela vous donne la
flexibilité de surveiller les quantités qui varient par rapport aux
quantités souscrites pour chaque niveau, ce que DII autorise tant que le
stockage total découvert est dans les limites du droit pondéré souscrit.
```

Comptage unitaire géré (hérité)

Utilisation des compteurs d’observabilité de l’infrastructure et d’observabilité Kubernetes de Data Infrastructure Insights par **unité gérée**. L’utilisation de vos unités gérées est calculée en fonction du nombre d'**hôtes ou de machines virtuelles** et de la quantité de **capacité non formatée** gérée dans votre environnement d’infrastructure.

- 1 unité gérée = 2 hôtes (toute machine virtuelle ou physique)
- 1 unité gérée = 4 Tio de capacité non formatée de disques physiques ou virtuels

- 1 unité gérée = 40 Tio de capacité non formatée de stockage secondaire sélectionné : AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik.
- 1 unité gérée = 4 vCPU de Kuberentes.
  - 1 unité gérée K8s Adjustment = 2 nœuds ou hôtes également surveillés par l'infrastructure.

Mesure de la sécurité de la charge de travail

La sécurité de la charge de travail est mesurée par Cluster en utilisant la même approche que la mesure de l'observabilité.

Vous pouvez consulter votre utilisation de Workload Security dans la page **Admin > Abonnement** de l'onglet **Workload Security**.

L'utilisation des MU des abonnements Workload Security existants est ajustée afin que l'utilisation des nœuds ne consomme pas d'unités gérées. Data Infrastructure Insights mesure l'utilisation pour garantir la conformité avec l'utilisation sous licence.

Comment puis-je m'abonner ?

Si votre nombre d'unités gérées est inférieur à 1 000, vous pouvez vous abonner via NetApp Sales, ouauto-abonnement via AWS Marketplace.

Abonnez-vous directement via NetApp Sales

Si le nombre d'unités gérées prévu est de 1 000 ou plus, cliquez sur le bouton**"Contacter le service commercial"** bouton pour vous abonner via l'équipe commerciale NetApp .

Vous devez fournir votre **numéro de série** Data Infrastructure Insights à votre représentant commercial NetApp afin que votre abonnement payant puisse être appliqué à votre environnement Data Infrastructure Insights . Le numéro de série identifie de manière unique votre environnement d'essai Data Infrastructure Insights et peut être trouvé sur la page **Admin > Abonnement**.

Auto-abonnez-vous via AWS Marketplace

Vous devez être propriétaire ou administrateur de compte pour appliquer un abonnement AWS Marketplace à votre compte d'essai Data Infrastructure Insights existant. De plus, vous devez disposer d'un compte Amazon Web Services (AWS).

Cliquer sur le lien Amazon Marketplace ouvre AWS "Data Infrastructure Insights" page d'abonnement, où vous pouvez compléter votre abonnement. Notez que les valeurs que vous avez saisies dans la calculatrice ne sont pas renseignées dans la page d'abonnement AWS ; vous devrez saisir le nombre total d'unités gérées sur cette page.

Après avoir saisi le nombre total d'unités gérées et choisi une durée d'abonnement de 12 ou 36 mois, cliquez sur **Configurer votre compte** pour terminer le processus d'abonnement.

Une fois le processus d'abonnement AWS terminé, vous serez redirigé vers votre environnement Data Infrastructure Insights . Ou, si l'environnement n'est plus actif (par exemple, vous vous êtes déconnecté), vous

serez redirigé vers la page de connexion de la console NetAPp. Lorsque vous vous reconnectez à Data Infrastructure Insights , votre abonnement sera actif.

> Après avoir cliqué sur **Configurer votre compte** sur la page AWS Marketplace, vous devez terminer le processus d'abonnement AWS dans un délai d'une heure. Si vous ne le terminez pas dans un délai d'une heure, vous devrez cliquer à nouveau sur **Configurer votre compte** pour terminer le processus.

En cas de problème et si le processus d'abonnement ne se termine pas correctement, vous verrez toujours la bannière « Version d'essai » lorsque vous vous connecterez à votre environnement. Dans cet événement, vous pouvez aller dans **Admin > Abonnement** et répéter le processus d'abonnement.

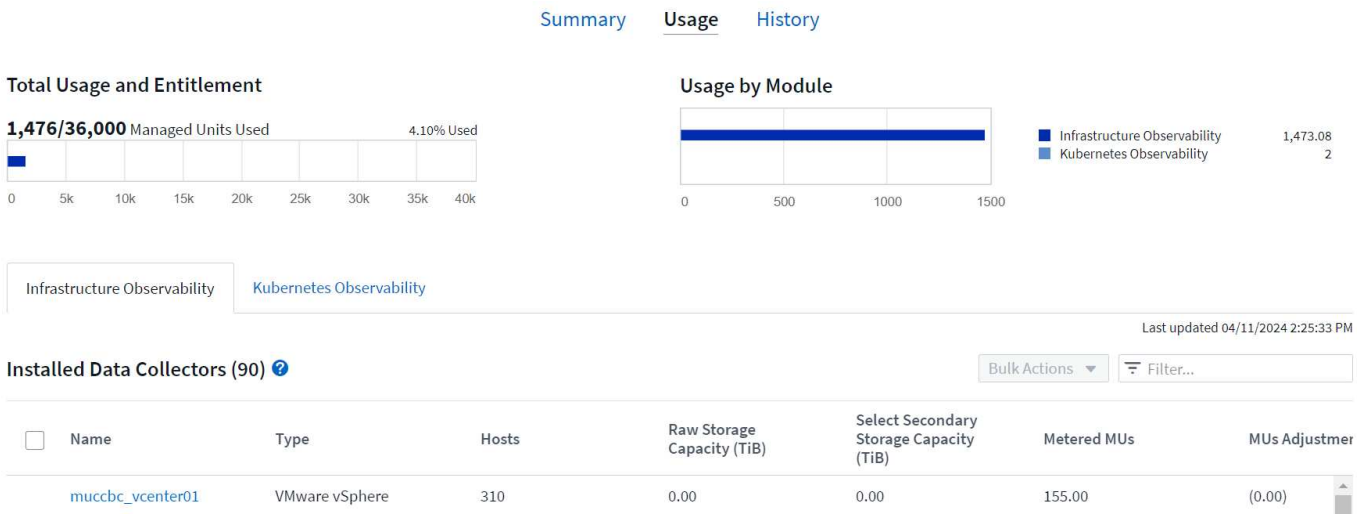
Afficher le statut de votre abonnement

Une fois votre abonnement actif, vous pouvez consulter l'état de votre abonnement et l'utilisation de l'unité gérée à partir de la page **Admin > Abonnement**.

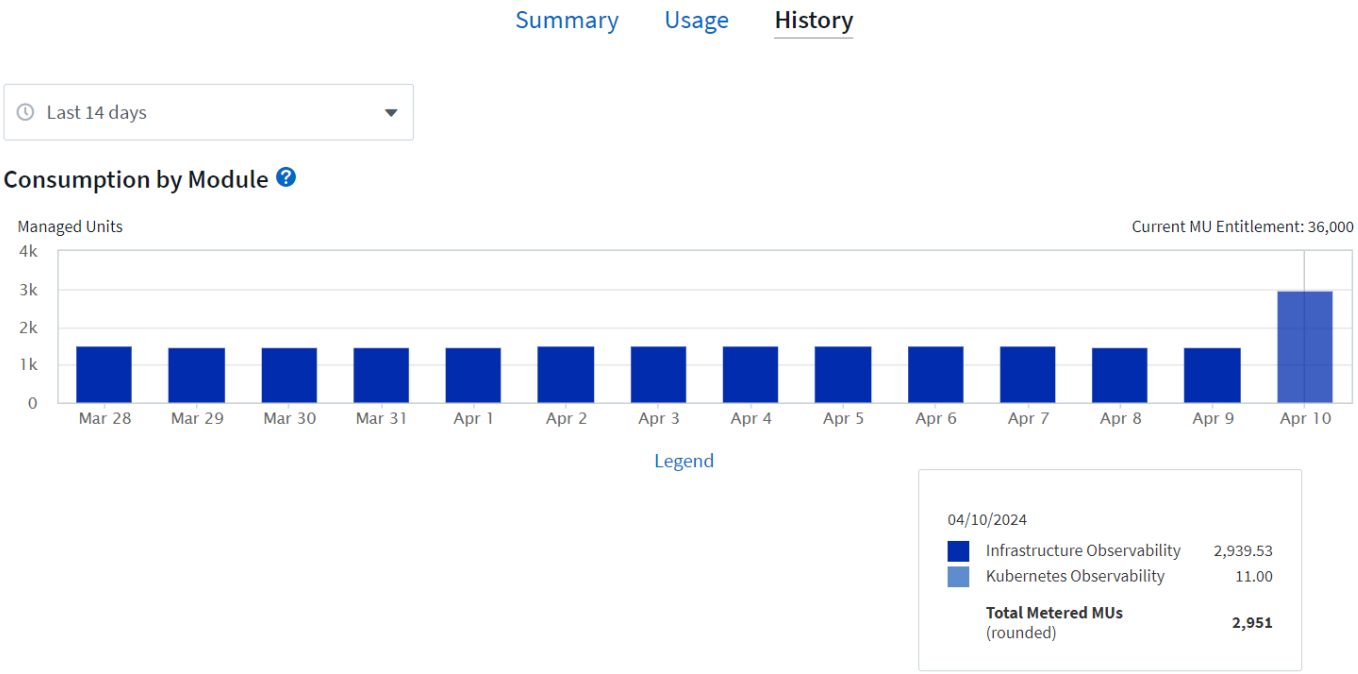
L'onglet **Résumé** de l'abonnement affiche des éléments tels que les suivants :

- Édition actuelle
- Numéro de série d'abonnement
- Droits actuels de l'UM

L'onglet **Utilisation** vous montre votre utilisation actuelle de MU et comment cette utilisation se répartit par collecteur de données.



L'onglet **Historique** vous donne un aperçu de votre utilisation de MU au cours des 7 à 90 derniers jours. En survolant une colonne du graphique, vous obtenez une répartition par module (c'est-à-dire Observabilité, Kubernetes).



Consultez votre gestion d'utilisation

L'onglet Gestion de l'utilisation affiche un aperçu de l'utilisation de l'unité gérée, ainsi que des onglets décomposant la consommation de l'unité gérée par collecteur ou cluster Kubernetes.

Le nombre d'unités gérées de capacité non formatée reflète la somme de la capacité brute totale de l'environnement et est arrondi à l'unité gérée la plus proche.

La somme des unités gérées peut différer légèrement du nombre de collecteurs de données dans la section récapitulative. Cela est dû au fait que le nombre d'unités gérées est arrondi à l'unité gérée la plus proche. La somme de ces nombres dans la liste des collecteurs de données peut être légèrement supérieure au total des unités gérées dans la section Statut. La section récapitulative reflète le nombre réel d'unités gérées pour votre abonnement.

Si votre utilisation approche ou dépasse votre montant souscrit, vous pouvez réduire votre utilisation en supprimant les collecteurs de données ou en arrêtant la surveillance des clusters Kubernetes. Supprimez un élément de cette liste en cliquant sur le menu « trois points » et en sélectionnant *Supprimer*.

Que se passe-t-il si je dépasse mon utilisation souscrite ?

Des avertissements s'affichent lorsque votre utilisation de l'unité gérée dépasse 80 %, 90 % et 100 % du montant total souscrit :

Lorsque l'utilisation dépasse :	Cela se produit / Action recommandée :
80%	Une bannière d'information est affichée. Aucune action n'est nécessaire.

Lorsque l'utilisation dépasse :	Cela se produit / Action recommandée :
90%	Une bannière d'avertissement s'affiche. Vous souhaiterez peut-être augmenter le nombre d'unités gérées auxquelles vous êtes abonné.
100%	Une bannière d'erreur s'affiche jusqu'à ce que vous effectuiez l'une des opérations suivantes : • Supprimez les collecteurs de données afin que votre utilisation de l'unité gérée soit égale ou inférieure à votre quantité souscrite • Modifiez votre abonnement pour augmenter le nombre d'unités gérées souscrites

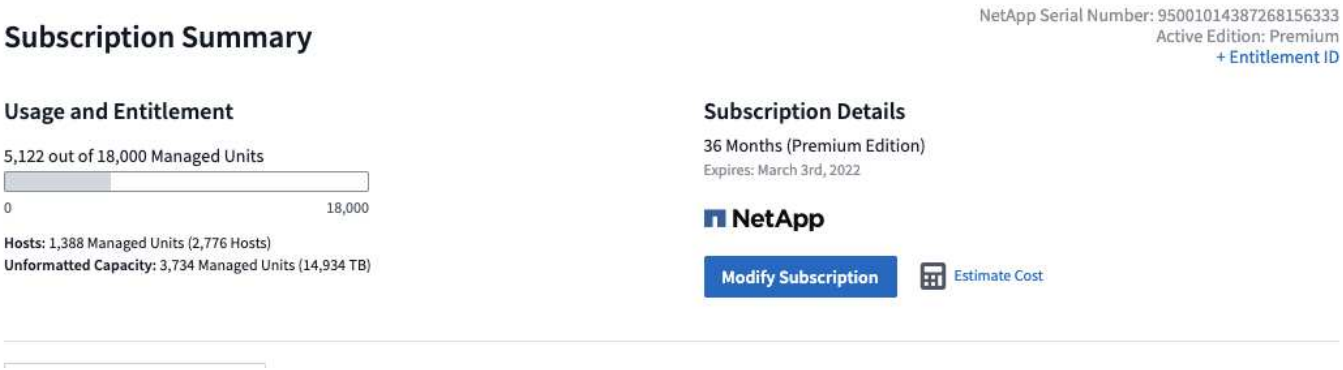
Abonnez-vous directement et évitez l'essai

Vous pouvez également vous abonner à Data Infrastructure Insights directement depuis le "Place de marché AWS" , sans créer au préalable un environnement d'essai. Une fois votre abonnement terminé et votre environnement configuré, vous serez immédiatement abonné.

Ajout d'un identifiant d'autorisation

Si vous possédez un produit NetApp valide fourni avec Data Infrastructure Insights, vous pouvez ajouter ce numéro de série de produit à votre abonnement Data Infrastructure Insights existant. Par exemple, si vous avez acheté NetApp Astra Control Center, le numéro de série de la licence Astra Control Center peut être utilisé pour identifier l'abonnement dans Data Infrastructure Insights. Data Infrastructure Insights fait référence à cela comme un *ID d'autorisation*.

Pour ajouter un ID d'autorisation à votre abonnement Data Infrastructure Insights , sur la page **Admin > Abonnement**, cliquez sur *+ID d'autorisation*.



Observabilité

Création de tableaux de bord

Présentation des tableaux de bord

Data Infrastructure Insights offre aux utilisateurs la flexibilité de créer des vues opérationnelles des données d'infrastructure, en vous permettant de créer des tableaux de bord personnalisés avec une variété de widgets, chacun offrant une grande flexibilité dans l'affichage et la représentation graphique de vos données.

> Les exemples dans ces sections sont fournis à titre explicatif uniquement et ne couvrent pas tous les scénarios possibles. Les concepts et les étapes présentés ici peuvent être utilisés pour créer vos propres tableaux de bord afin de mettre en évidence les données spécifiques à vos besoins particuliers.

Créer un tableau de bord

Vous créez un nouveau tableau de bord à l'un des deux endroits suivants :

- **Tableaux de bord > [+Nouveau tableau de bord]**
- **Tableaux de bord > Afficher tous les tableaux de bord >** cliquez sur le bouton **[+Tableau de bord]**

Voyez-le en action

Créez des tableaux de bord puissants avec NetApp (vidéo),window=read-later

Commandes du tableau de bord

L'écran du tableau de bord comporte plusieurs commandes :

- **Sélecteur de temps** : vous permet d'afficher les données du tableau de bord pour une plage de temps allant des 15 dernières minutes aux 30 derniers jours, ou une plage de temps personnalisée allant jusqu'à 31 jours. Vous pouvez choisir de remplacer cette plage horaire globale dans des widgets individuels.
- Bouton **Enregistrer** : permet d'enregistrer ou de supprimer le tableau de bord.

  Vous pouvez renommer le tableau de bord actuel en cliquant sur **Renommer** dans le menu Enregistrer.

- **+ Bouton Ajouter un widget**, qui vous permet d'ajouter n'importe quel nombre de tableaux, de graphiques ou d'autres widgets au tableau de bord.

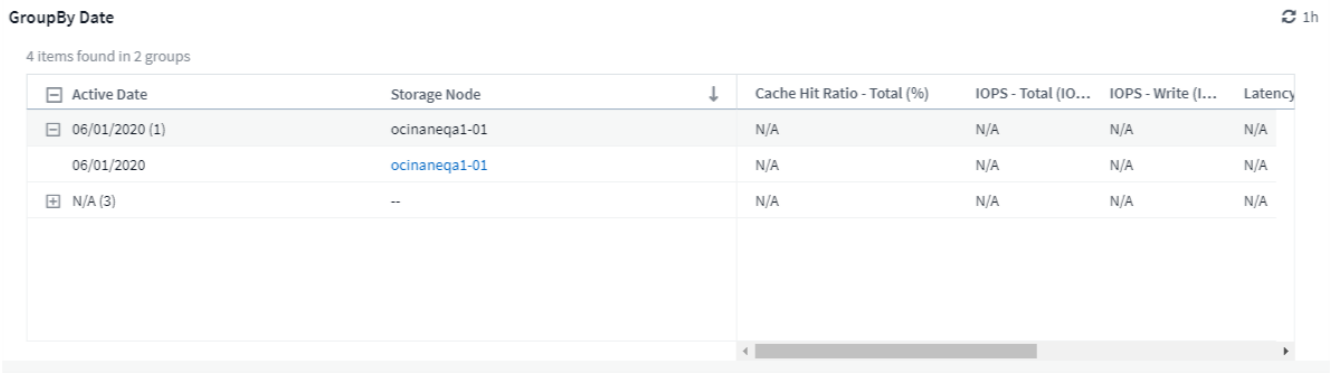
  Les widgets peuvent être redimensionnés et déplacés vers différentes positions dans le tableau de bord, pour vous offrir la meilleure vue de vos données en fonction de vos besoins actuels.

- **+ Bouton Ajouter une variable**, qui vous permet d'utiliser des variables pour filtrer activement les données du tableau de bord.

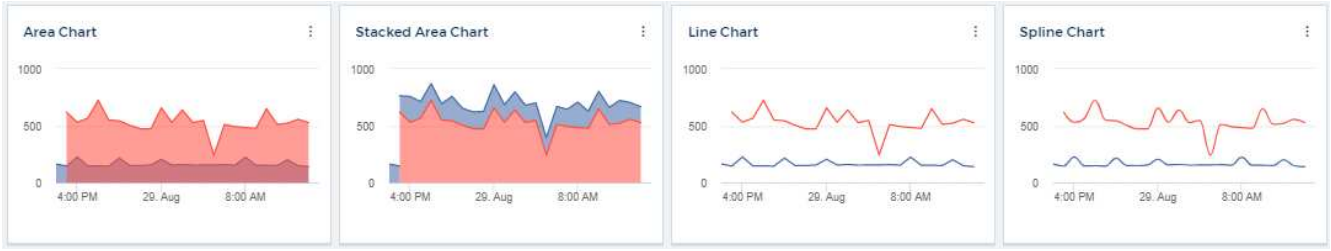
Types de widgets

Vous pouvez choisir parmi les types de widgets suivants :

- **Widget de tableau** : un tableau affichant des données en fonction des filtres et des colonnes que vous choisissez. Les données du tableau peuvent être combinées en groupes qui peuvent être réduits et développés.

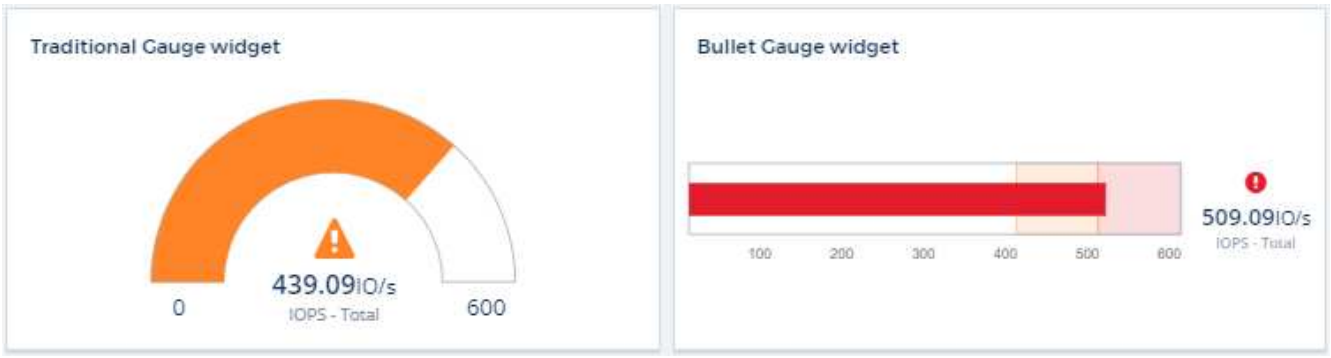


- * Graphiques linéaires, splines, de surface, à aires empilées * : il s'agit de widgets de graphiques de séries chronologiques sur lesquels vous pouvez afficher les performances et d'autres données au fil du temps.

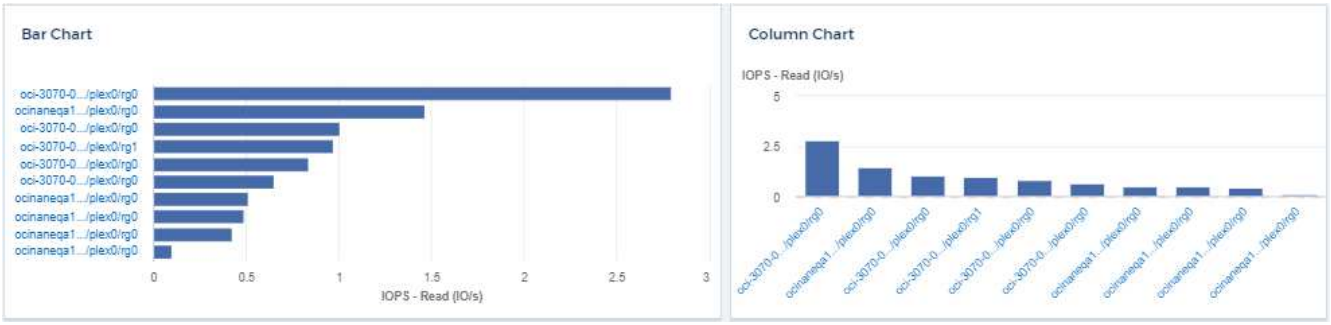


- **Widget à valeur unique** : un widget vous permettant d'afficher une valeur unique qui peut être dérivée directement d'un compteur ou calculée à l'aide d'une requête ou d'une expression. Vous pouvez définir des seuils de formatage des couleurs pour indiquer si la valeur est dans la plage attendue, d'avertissement ou critique.

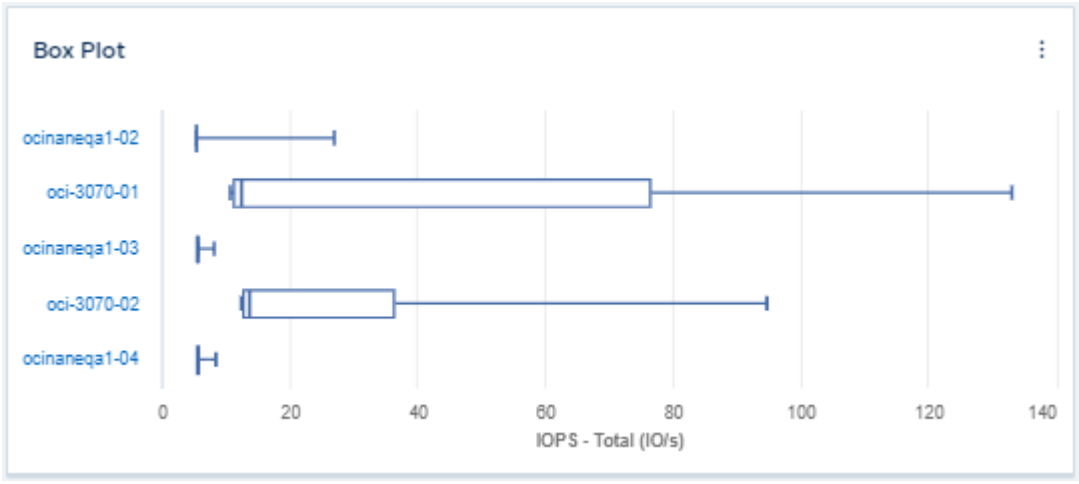
- **Widget de jauge** : affiche des données à valeur unique dans une jauge traditionnelle (solide) ou une jauge à puces, avec des couleurs basées sur les valeurs « Avertissement » ou « Critique » que vous"personnaliser" .



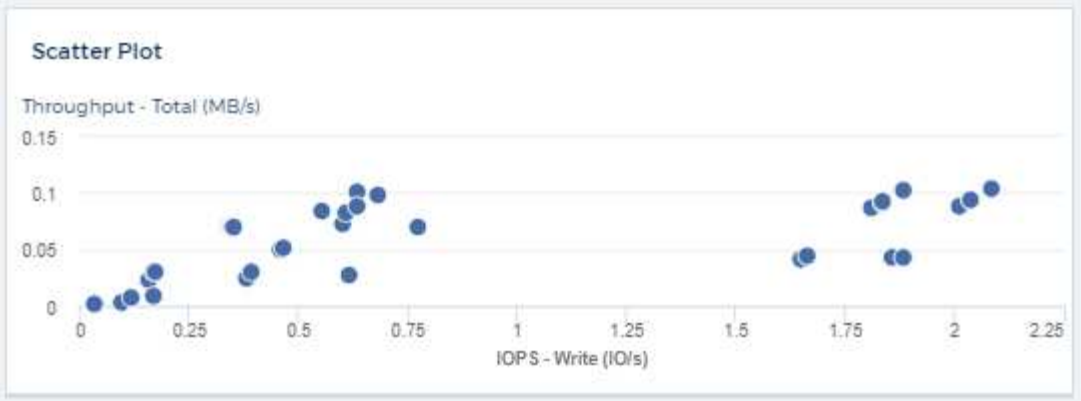
- **Graphiques à barres et à colonnes** : affiche les valeurs N supérieures ou inférieures, par exemple, les 10 premiers stockages par capacité ou les 5 derniers volumes par IOPS.



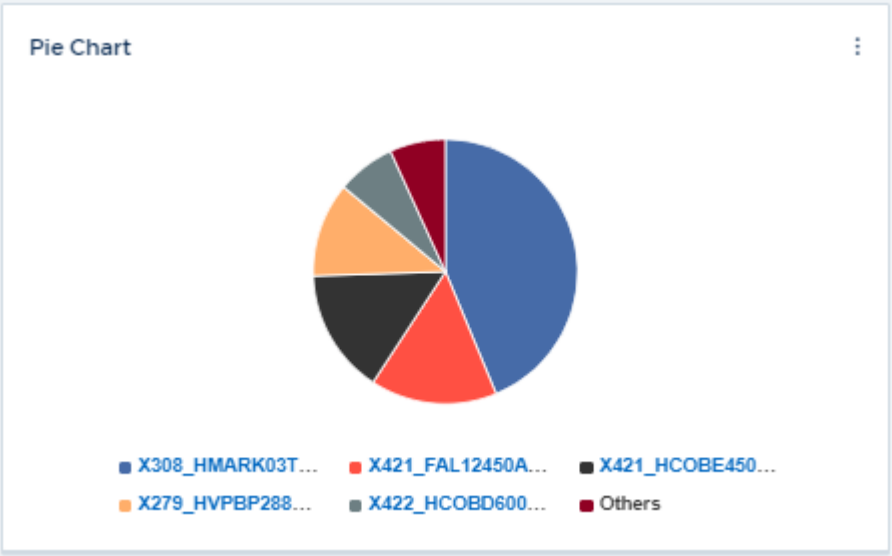
- * Graphique en boîte à moustaches * : Un tracé du minimum, du maximum, de la médiane et de la plage entre le quartile inférieur et supérieur des données dans un seul graphique.



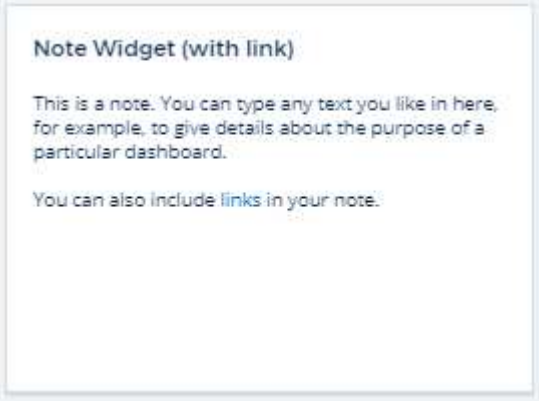
- **Graphique en nuage de points** : trace les données associées sous forme de points, par exemple, les IOPS et la latence. Dans cet exemple, vous pouvez localiser rapidement des actifs avec un débit élevé et un faible nombre d'IOPS.



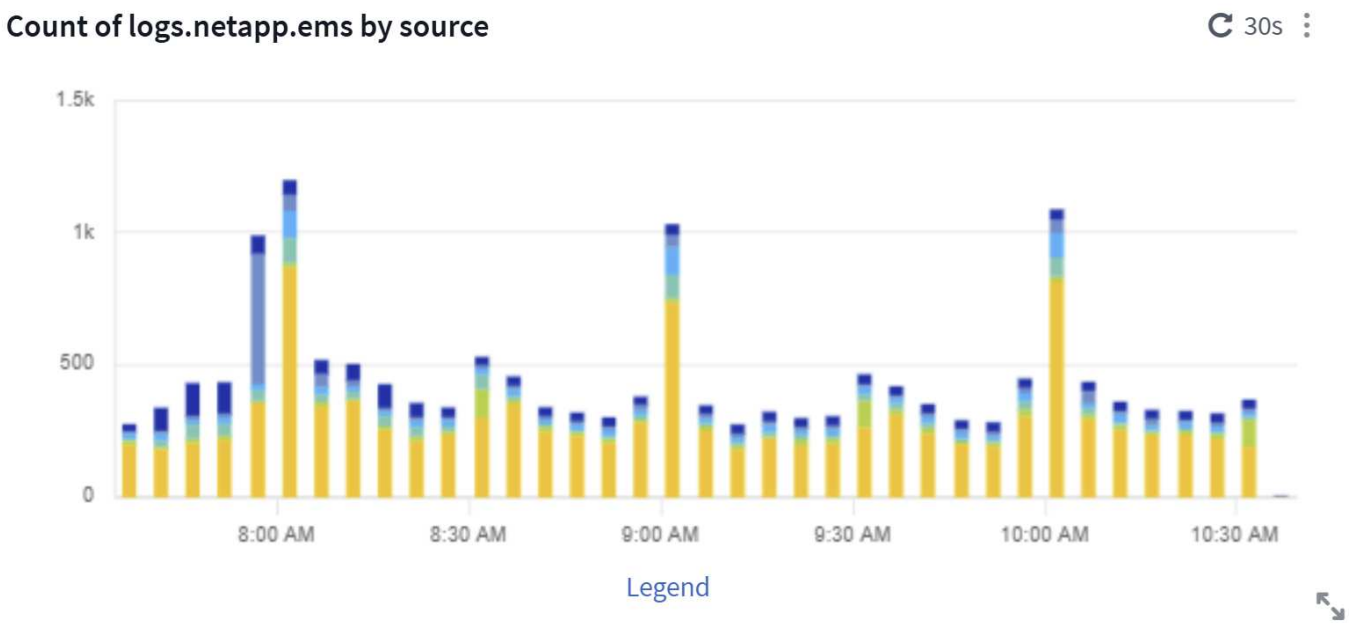
- **Graphique à secteurs** : un graphique à secteurs traditionnel pour afficher les données comme une partie du total.



- **Widget de note** : Jusqu'à 1 000 caractères de texte libre.



- **Graphique à barres temporelles** : affiche les données du journal ou des métriques au fil du temps.



- **Tableau des alertes** : affiche jusqu'aux 1 000 dernières alertes.

Pour des explications plus détaillées sur ces fonctionnalités et d'autres fonctionnalités du tableau de bord,"Cliquez ici" .

Définir un tableau de bord comme page d'accueil

Vous pouvez choisir le tableau de bord à définir comme **page d'accueil** de votre locataire en utilisant l'une des méthodes suivantes :

- Accédez à **Tableaux de bord > Afficher tous les tableaux de bord** pour afficher la liste des tableaux de bord de votre locataire. Cliquez sur le menu d'options à droite du tableau de bord souhaité et sélectionnez **Définir comme page d'accueil**.
- Cliquez sur un tableau de bord de la liste pour ouvrir le tableau de bord. Cliquez sur le menu déroulant dans le coin supérieur et sélectionnez **Définir comme page d'accueil**.

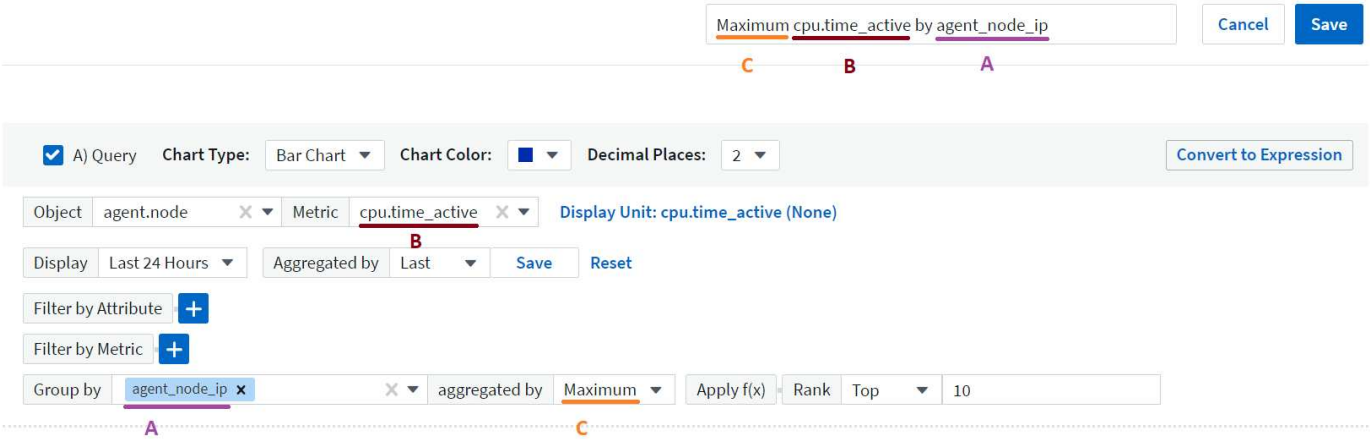
Fonctionnalités du tableau de bord

Les tableaux de bord et les widgets offrent une grande flexibilité dans la façon dont les données sont affichées. Voici quelques concepts pour vous aider à tirer le meilleur parti de vos tableaux de bord personnalisés.

toc:[]

Nommage des widgets

Les widgets sont automatiquement nommés en fonction de l'objet, de la métrique ou de l'attribut sélectionné pour la première requête de widget. Si vous choisissez également un regroupement pour le widget, les attributs « Grouper par » sont inclus dans la dénomination automatique (méthode d'agrégation et métrique).



La sélection d'un nouvel objet ou d'un attribut de regroupement met à jour le nom automatique.

Si vous ne souhaitez pas utiliser le nom automatique du widget, vous pouvez simplement saisir un nouveau nom.

Placement et taille des widgets

Tous les widgets du tableau de bord peuvent être positionnés et dimensionnés en fonction de vos besoins pour chaque tableau de bord particulier.

Dupliquer un widget

En mode Édition du tableau de bord, cliquez sur le menu du widget et sélectionnez **Dupliquer**. L'éditeur de widgets est lancé, pré-rempli avec la configuration du widget d'origine et avec un suffixe « copie » dans le nom du widget. Vous pouvez facilement apporter les modifications nécessaires et enregistrer le nouveau widget. Le widget sera placé en bas de votre tableau de bord et vous pourrez le positionner selon vos besoins. N'oubliez pas de sauvegarder votre tableau de bord lorsque toutes les modifications sont terminées.

Affichage des légendes des widgets

La plupart des widgets des tableaux de bord peuvent être affichés avec ou sans légendes. Les légendes dans les widgets peuvent être activées ou désactivées sur un tableau de bord par l'une des méthodes suivantes :

- Lors de l'affichage du tableau de bord, cliquez sur le bouton **Options** du widget et sélectionnez **Afficher les légendes** dans le menu.

À mesure que les données affichées dans le widget changent, la légende de ce widget est mise à jour de manière dynamique.

Lorsque les légendes sont affichées, si la page de destination de l'actif indiqué par la légende est accessible, la légende s'affichera sous la forme d'un lien vers cette page d'actif. Si la légende affiche « tous », cliquer sur le lien affichera une page de requête correspondant à la première requête du widget.

Transformer les métriques

Data Infrastructure Insights fournit différentes options de **transformation** pour certaines métriques dans les widgets (en particulier, les métriques appelées « Personnalisées » ou métriques d'intégration, telles que celles de Kubernetes, ONTAP Advanced Data, des plugins Telegraf, etc.), vous permettant d'afficher les données de plusieurs manières. Lorsque vous ajoutez des métriques transformables à un widget, une liste déroulante vous propose les choix de transformation suivants :

Aucun : les données sont affichées telles quelles, sans aucune manipulation.

Taux : Valeur actuelle divisée par la plage de temps depuis l'observation précédente.

Cumulatif : L'accumulation de la somme des valeurs précédentes et de la valeur actuelle.

Delta : La différence entre la valeur d'observation précédente et la valeur actuelle.

Taux Delta : Valeur Delta divisée par la plage de temps depuis l'observation précédente.

Taux cumulé : valeur cumulée divisée par la plage de temps depuis l'observation précédente.

Notez que la transformation des métriques ne modifie pas les données sous-jacentes elles-mêmes, mais uniquement la manière dont ces données sont affichées.

Requêtes et filtres des widgets du tableau de bord

Requêtes

La requête dans un widget de tableau de bord est un outil puissant pour gérer l'affichage de vos données. Voici quelques éléments à noter sur les requêtes de widgets.

Certains widgets peuvent avoir jusqu'à cinq requêtes. Chaque requête tracera son propre ensemble de lignes ou de graphiques dans le widget. La définition du cumul, du regroupement, des résultats supérieurs/inférieurs, etc. sur une requête n'affecte aucune autre requête pour le widget.

Vous pouvez cliquer sur l'icône en forme d'œil pour masquer temporairement une requête. L'affichage du widget se met à jour automatiquement lorsque vous masquez ou affichez une requête. Cela vous permet de vérifier vos données affichées pour des requêtes individuelles lorsque vous créez votre widget.

Les types de widgets suivants peuvent avoir plusieurs requêtes :

- Graphique en aires
- Graphique à aires empilées
- Graphique linéaire
- Graphique spline
- Widget à valeur unique

Les autres types de widgets ne peuvent avoir qu'une seule requête :

- Tableau
- Graphique à barres
- Boîte à moustaches
- Nuage de points

Filtrage dans les requêtes des widgets du tableau de bord

Voici quelques mesures que vous pouvez prendre pour tirer le meilleur parti de vos filtres.

Filtrage de correspondance exacte

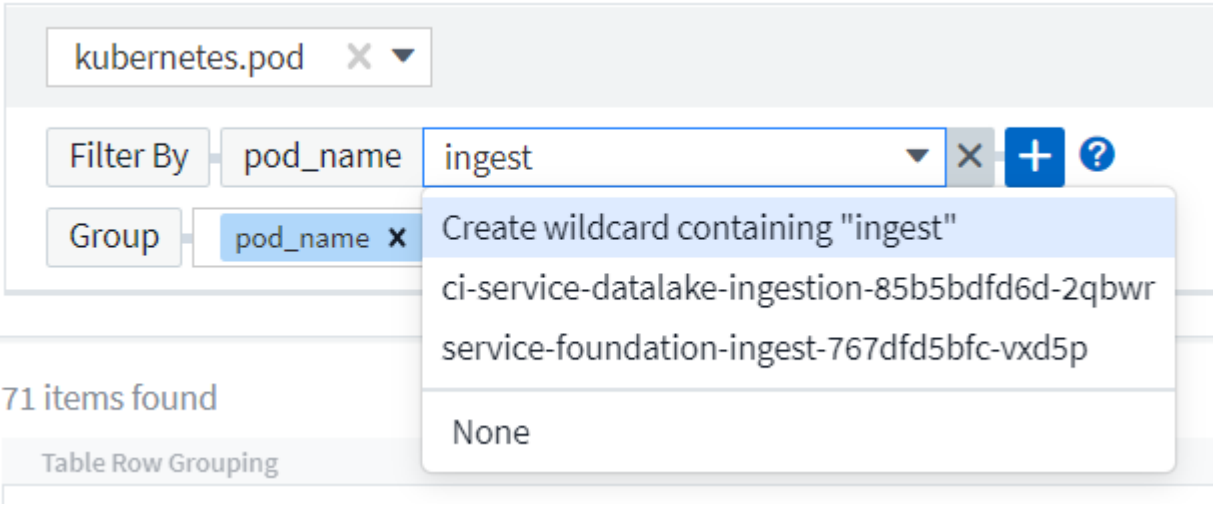
Si vous placez une chaîne de filtre entre guillemets doubles, Insight traite tout ce qui se trouve entre le premier

et le dernier guillemet comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs à l'intérieur des guillemets seront traités comme des littéraux. Par exemple, le filtrage par « * » renverra des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs AND, OR et NOT seront également traités comme des chaînes littérales lorsqu'ils sont placés entre guillemets.

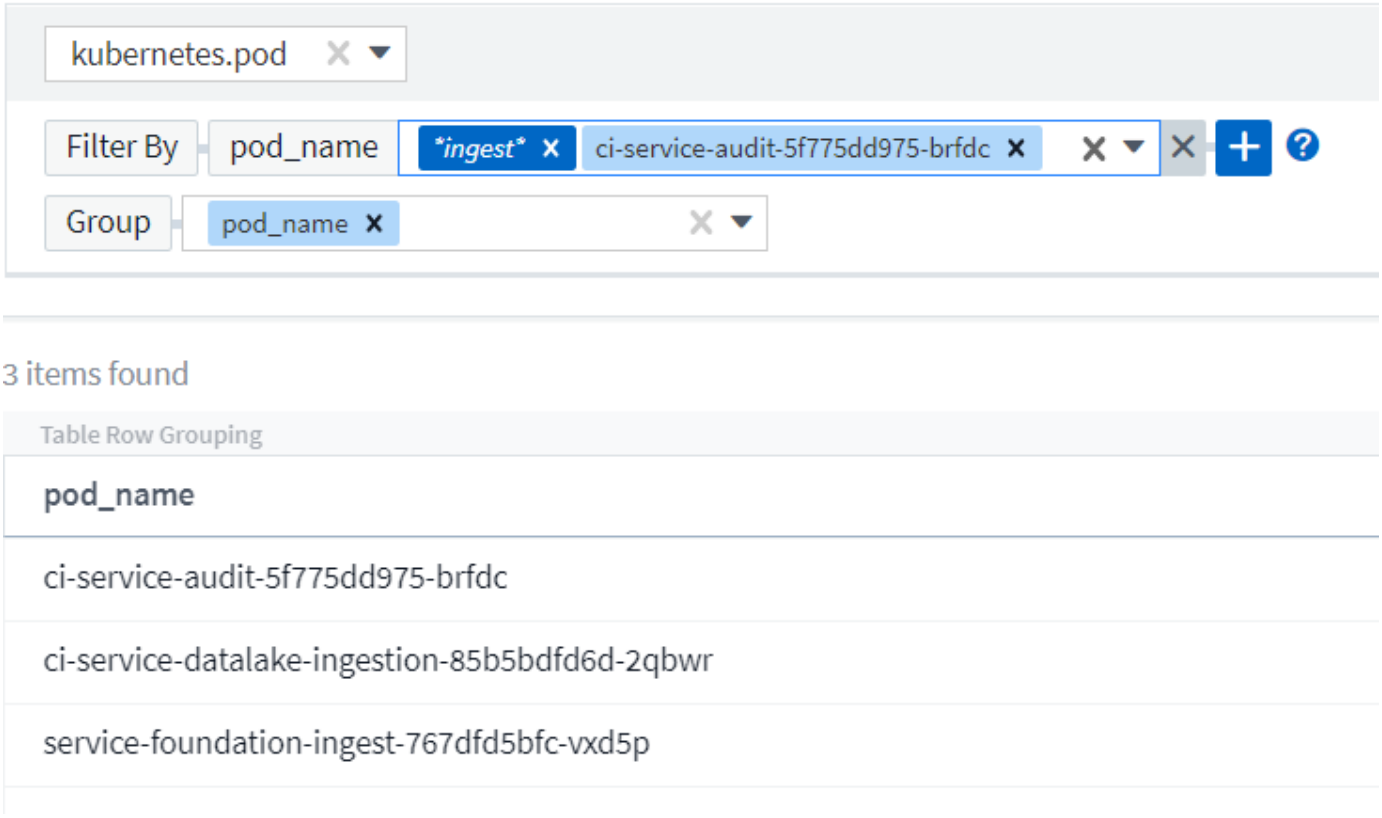
Vous pouvez utiliser des filtres de correspondance exacte pour trouver des ressources spécifiques, par exemple le nom d'hôte. Si vous souhaitez rechercher uniquement le nom d'hôte « marketing » mais exclure « marketing01 », « marketing-boston », etc., placez simplement le nom « marketing » entre guillemets.

Caractères génériques et expressions

Lorsque vous filtrez des valeurs de texte ou de liste dans des requêtes ou des widgets de tableau de bord, lorsque vous commencez à saisir, vous avez la possibilité de créer un **filtre générique** basé sur le texte actuel. La sélection de cette option renverra tous les résultats correspondant à l'expression générique. Vous pouvez également créer des **expressions** en utilisant NOT ou OR, ou vous pouvez sélectionner l'option « Aucun » pour filtrer les valeurs nulles dans le champ.



Les filtres basés sur des caractères génériques ou des expressions (par exemple NOT, OR, « Aucun », etc.) s'affichent en bleu foncé dans le champ de filtre. Les éléments que vous sélectionnez directement dans la liste sont affichés en bleu clair.



Notez que le filtrage par caractères génériques et par expressions fonctionne avec du texte ou des listes, mais pas avec des nombres, des dates ou des booléens.

Filtrage de texte avancé avec suggestions contextuelles de saisie semi-automatique

Le filtrage dans les requêtes de widgets est *contextuel* ; lorsque vous sélectionnez une ou plusieurs valeurs de filtre pour un champ, les autres filtres pour cette requête afficheront les valeurs pertinentes pour ce filtre. Par exemple, lors de la définition d'un filtre pour un objet spécifique *Nom*, le champ à filtrer pour *Modèle* affichera uniquement les valeurs pertinentes pour ce nom d'objet.

Le filtrage contextuel s'applique également aux variables de page du tableau de bord (attributs de type texte ou annotations uniquement). Lorsque vous sélectionnez une valeur de filtre pour une variable, toutes les autres variables utilisant des objets associés afficheront uniquement les valeurs de filtre possibles en fonction du contexte de ces variables associées.

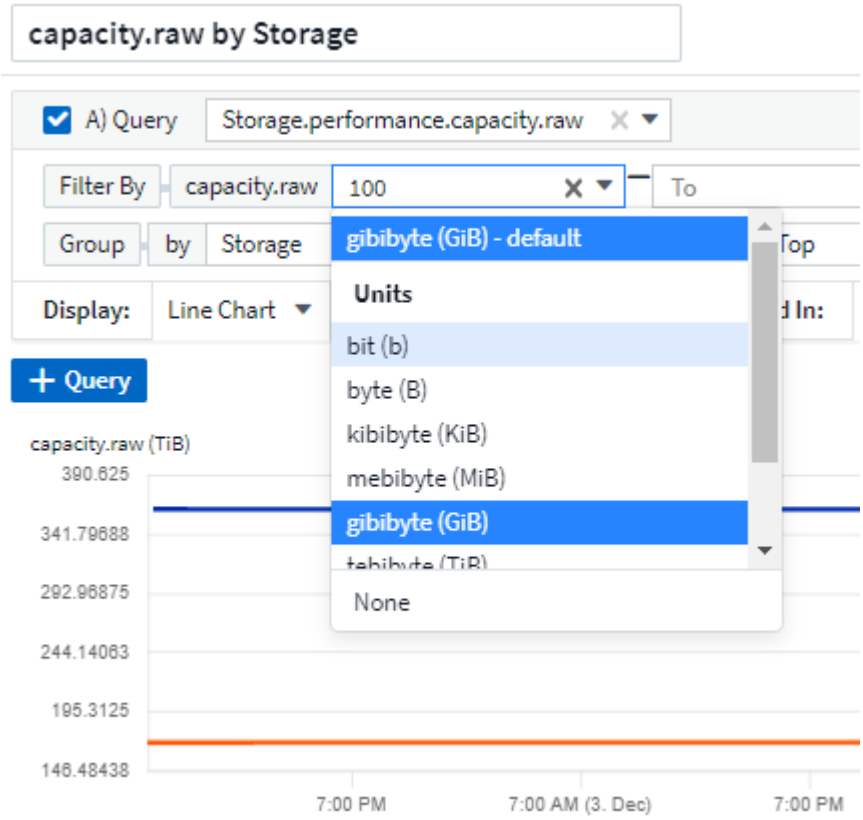
Notez que seuls les filtres de texte afficheront des suggestions contextuelles de saisie semi-automatique. La date, l'énumération (liste), etc. n'afficheront pas les suggestions de saisie semi-automatique. Cela dit, vous *pouvez* définir un filtre sur un champ Enum (c'est-à-dire une liste) et faire en sorte que d'autres champs de texte soient filtrés dans le contexte. Par exemple, en sélectionnant une valeur dans un champ Enum comme Centre de données, les autres filtres afficheront uniquement les modèles/noms de ce centre de données, mais pas l'inverse.

La plage horaire sélectionnée fournira également un contexte pour les données affichées dans les filtres.

Choix des unités de filtrage

Lorsque vous saisissez une valeur dans un champ de filtre, vous pouvez sélectionner les unités dans lesquelles afficher les valeurs sur le graphique. Par exemple, vous pouvez filtrer sur la capacité brute et choisir d'afficher le Gio par défaut, ou sélectionner un autre format tel que Tio. Ceci est utile si vous avez un certain

nombre de graphiques sur votre tableau de bord affichant des valeurs en Tio et que vous souhaitez que tous vos graphiques affichent des valeurs cohérentes.



Affinements de filtrage supplémentaires

Les éléments suivants peuvent être utilisés pour affiner davantage vos filtres.

- Un astérisque vous permet de rechercher tout. Par exemple,

  ```
  vol*rhel
  ```

  affiche toutes les ressources qui commencent par « vol » et se terminent par « rhel ».

- Le point d'interrogation vous permet de rechercher un nombre spécifique de caractères. Par exemple,

  ```
  BOS-PRD??-S12
  ```

  affiche *BOS-PRD12-S12*, *BOS-PRD13-S12*, etc.

- L'opérateur OR vous permet de spécifier plusieurs entités. Par exemple,

  ```
  FAS2240 OR CX600 OR FAS3270
  ```

trouve plusieurs modèles de stockage.

- L'opérateur NOT vous permet d'exclure du texte des résultats de la recherche. Par exemple,

```
NOT EMC*
```

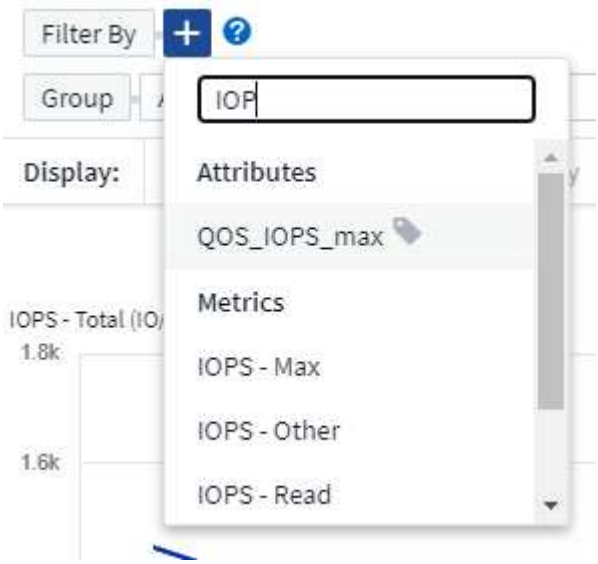
trouve tout ce qui ne commence pas par « EMC ». Vous pouvez utiliser

```
NOT *
```

pour afficher les champs qui ne contiennent aucune valeur.

Identification des objets renvoyés par les requêtes et les filtres

Les objets renvoyés par les requêtes et les filtres ressemblent à ceux présentés dans l'illustration suivante. Les objets avec des « balises » qui leur sont attribuées sont des annotations tandis que les objets sans balises sont des compteurs de performances ou des attributs d'objet.



Regroupement, identification et agrégation

Regroupement (enroulement)

Les données affichées dans un widget sont regroupées (parfois appelées cumulées) à partir des points de données sous-jacents collectés lors de l'acquisition. Par exemple, si vous disposez d'un widget de graphique linéaire affichant les IOPS de stockage au fil du temps, vous souhaiterez peut-être voir une ligne distincte pour chacun de vos centres de données, pour une comparaison rapide. Dans le champ « Grouper par », sélectionnez le type d'objet lui-même pour afficher les lignes, zones, barres, colonnes, etc. (selon le type de widget) individuelles pour chaque objet. Vous pouvez choisir de regrouper les données selon n'importe quel attribut disponible dans la liste pour cet objet. Par exemple, lors de la consultation des données d'un volume interne, vous pouvez souhaiter regrouper les données par nom de stockage.

Pour afficher les données consolidées, supprimez tout attribut Group By, le regroupement s'effectuant par défaut par « Tous ».

Vous pouvez choisir d'agréger ces données de plusieurs manières :

- **Moyenne** : affiche chaque ligne comme la *moyenne* des données sous-jacentes.
- **Maximum** : affiche chaque ligne comme le *maximum* des données sous-jacentes.
- **Minimum** : affiche chaque ligne comme le *minimum* des données sous-jacentes.
- **Somme** : affiche chaque ligne comme la *somme* des données sous-jacentes.

Lors de la consultation du tableau de bord, la sélection de la légende d'un widget dont les données sont regroupées par « Tous » ouvre une page de requête affichant les résultats de la première requête utilisée dans le widget.

Si vous avez défini un filtre pour la requête, les données sont regroupées en fonction des données filtrées.

Identification des données personnalisées

Lorsque vous créez ou modifiez un widget basé sur vos propres données personnalisées, ces données peuvent ne pas être correctement représentées dans le widget sans attribut d'identification. Si DII ne parvient pas à identifier l'objet que vous avez sélectionné pour votre widget, il vous présentera un lien *Configuration avancée* dans la zone « Grouper par ». Développez cette section pour sélectionner l'attribut qui vous permettra d'identifier vos données.

Agrégation de données

Vous pouvez affiner davantage vos graphiques en regroupant les points de données par intervalles de minutes, d'heures ou de jours avant que ces données ne soient ensuite agrégées par attribut (si cette option est choisie). Vous pouvez choisir d'agréger des points de données en fonction de leur *Moyenne, Maximum, Minimum, Somme* ou *Nombre*.

Un petit intervalle combiné à une longue plage de temps peut entraîner un avertissement « L'intervalle d'agrégation a généré trop de points de données ». Vous pourriez voir cela si vous avez un petit intervalle et augmentez la période du tableau de bord à 7 jours. Dans ce cas, Insight augmentera temporairement l'intervalle d'agrégation jusqu'à ce que vous sélectionniez une période plus petite.

La plupart des compteurs d'actifs s'agrègent sur *Moyenne* par défaut. Certains compteurs s'agrègent sur *Max, Min* ou *Sum* par défaut. Par exemple, les erreurs de port sont regroupées par défaut sur *Sum*, tandis que les IOPS de stockage sont regroupées sur *Average*.

Affichage des résultats supérieurs/inférieurs

Dans un widget graphique, vous pouvez afficher les résultats **Meilleurs** ou **Inférieurs** pour les données

cumulées et choisir le nombre de résultats affichés dans la liste déroulante fournie. Dans un widget de tableau, vous pouvez trier par n'importe quelle colonne.

Widget graphique haut/bas

Dans un widget graphique, lorsque vous choisissez de regrouper les données par un attribut spécifique, vous avez la possibilité d'afficher les N premiers ou les N derniers résultats. Notez que vous ne pouvez pas choisir les résultats supérieurs ou inférieurs lorsque vous choisissez de cumuler par *tous* les attributs.

Vous pouvez choisir les résultats à afficher en choisissant **Haut** ou **Bas** dans le champ **Afficher** de la requête et en sélectionnant une valeur dans la liste fournie.

Le widget de tableau affiche les entrées

Dans un widget de tableau, vous pouvez sélectionner le nombre de résultats affichés dans les résultats du tableau. Vous n'avez pas la possibilité de choisir les résultats supérieurs ou inférieurs, car le tableau vous permet de trier par ordre croissant ou décroissant selon n'importe quelle colonne à la demande.

Vous pouvez choisir le nombre de résultats à afficher dans le tableau du tableau de bord en sélectionnant une valeur dans le champ **Afficher les entrées** de la requête.

Widget de regroupement dans le tableau

Les données d'un widget de tableau peuvent être regroupées par n'importe quel attribut disponible, vous permettant de voir un aperçu de vos données et de les explorer en profondeur pour plus de détails. Les mesures du tableau sont regroupées pour une visualisation facile dans chaque ligne réduite.

Les widgets de tableau vous permettent de regrouper vos données en fonction des attributs que vous définissez. Par exemple, vous souhaiterez peut-être que votre tableau affiche le nombre total d'IOPS de stockage regroupés par centres de données dans lesquels ces stockages se trouvent. Ou vous souhaiterez peut-être afficher un tableau de machines virtuelles regroupées en fonction de l'hyperviseur qui les héberge. À partir de la liste, vous pouvez développer chaque groupe pour afficher les actifs de ce groupe.

Le regroupement n'est disponible que dans le type de widget Tableau.

Exemple de regroupement (avec explication du cumul)

Les widgets de tableau vous permettent de regrouper des données pour un affichage plus facile.

Dans cet exemple, nous allons créer un widget de tableau affichant toutes les machines virtuelles regroupées par centre de données.

Étapes

1. Créez ou ouvrez un tableau de bord et ajoutez un widget **Tableau**.
2. Sélectionnez *Machine virtuelle* comme type d'actif pour ce widget.
3. Cliquez sur le sélecteur de colonnes et choisissez *Nom de l'hyperviseur* et *IOPS - Total*.

   Ces colonnes sont maintenant affichées dans le tableau.

4. Ignorons toutes les machines virtuelles sans IOPS et incluons uniquement les machines virtuelles dont le total des IOPS est supérieur à 1. Cliquez sur le bouton **Filtrer par [+]** et sélectionnez *IOPS - Total*. Cliquez sur *Any*, et dans le champ **de**, tapez **1**. Laissez le champ **à** vide. Appuyez sur Entrée ou cliquez sur le champ de filtre pour appliquer le filtre.

Le tableau affiche désormais toutes les machines virtuelles avec un nombre total d'IOPS supérieur ou égal à 1. Notez qu'il n'y a pas de regroupement dans le tableau. Toutes les machines virtuelles sont affichées.

5. Cliquez sur le bouton **Grouper par [+]**.

   Vous pouvez regrouper par n'importe quel attribut ou annotation affiché. Choisissez *Tout* pour afficher toutes les machines virtuelles dans un seul groupe.

   Tout en-tête de colonne pour une mesure de performance affiche un menu « trois points » contenant une option **Récapitulatif** . La méthode de cumul par défaut est *Average*. Cela signifie que le nombre affiché pour le groupe est la moyenne de tous les IOPS totaux signalés pour chaque machine virtuelle à l'intérieur du groupe. Vous pouvez choisir de regrouper cette colonne par *Moyenne, Somme, Minimum* ou *Maximum*. Toute colonne que vous affichez et qui contient des mesures de performances peut être regroupée individuellement.

6. Cliquez sur *Tous* et sélectionnez *Nom de l'hyperviseur*.

   La liste des machines virtuelles est désormais regroupée par hyperviseur. Vous pouvez développer chaque hyperviseur pour afficher les machines virtuelles hébergées par celui-ci.

7. Cliquez sur **Enregistrer** pour enregistrer le tableau dans le tableau de bord. Vous pouvez redimensionner ou déplacer le widget comme vous le souhaitez.
8. Cliquez sur **Enregistrer** pour enregistrer le tableau de bord.

Synthèse des données de performance

Si vous incluez une colonne pour les données de performances (par exemple, *IOPS - Total*) dans un widget de tableau, lorsque vous choisissez de regrouper les données, vous pouvez alors choisir une méthode de cumul pour cette colonne. La méthode de cumul par défaut consiste à afficher la moyenne (*avg*) des données sous-jacentes dans la ligne de groupe. Vous pouvez également choisir d'afficher la somme, le minimum ou le maximum des données.

Sélecteur de plage horaire du tableau de bord

Vous pouvez sélectionner la plage horaire pour les données de votre tableau de bord. Seules les données pertinentes pour la plage horaire sélectionnée seront affichées dans les widgets du tableau de bord. Vous

pouvez sélectionner parmi les plages horaires suivantes :

- Les 15 dernières minutes
- Les 30 dernières minutes
- Les 60 dernières minutes
- Les 2 dernières heures
- 3 dernières heures (c'est la valeur par défaut)
- Les 6 dernières heures
- Les 12 dernières heures
- Dernières 24 heures
- Les 2 derniers jours
- Les 3 derniers jours
- Les 7 derniers jours
- Les 30 derniers jours
- Plage horaire personnalisée

  La plage horaire personnalisée vous permet de sélectionner jusqu'à 31 jours consécutifs. Vous pouvez également définir l'heure de début et l'heure de fin de la journée pour cette plage. L'heure de début par défaut est 00h00 le premier jour sélectionné et l'heure de fin par défaut est 23h59 le dernier jour sélectionné. Cliquez sur **Appliquer** pour appliquer la plage horaire personnalisée au tableau de bord.

Zoom sur une plage horaire

Lorsque vous visualisez un widget de série chronologique (Ligne, Spline, Zone, Zone empilée) ou un graphique sur une page de destination, vous pouvez faire glisser la souris sur le graphique pour effectuer un zoom avant. Dans le coin supérieur droit de l'écran, vous pouvez ensuite verrouiller cette plage de temps afin que les graphiques sur d'autres pages reflètent les données de cette plage de temps verrouillée. Pour déverrouiller, sélectionnez une plage horaire différente dans la liste.

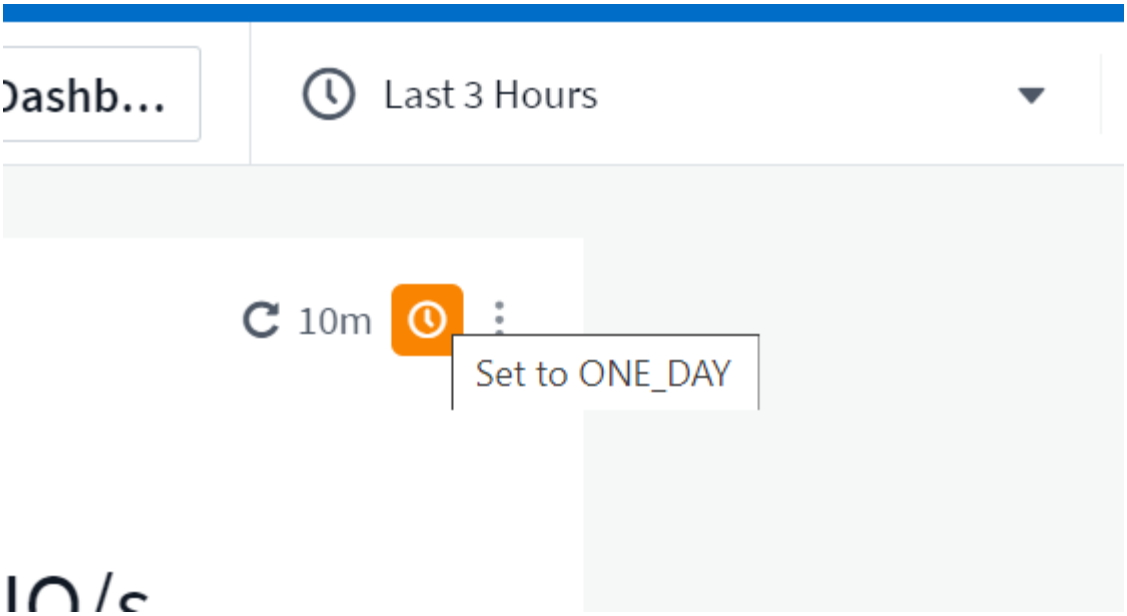
Remplacement de l'heure du tableau de bord dans les widgets individuels

Vous pouvez remplacer le paramètre de plage horaire du tableau de bord principal dans des widgets individuels. Ces widgets afficheront les données en fonction de leur période définie, et non de la période du tableau de bord.

Pour remplacer l'heure du tableau de bord et forcer un widget à utiliser sa propre période, dans le mode d'édition du widget, choisissez la plage horaire souhaitée et enregistrez le widget sur le tableau de bord.

Le widget affichera ses données en fonction de la période définie, quelle que soit la période que vous sélectionnez sur le tableau de bord lui-même.

La période que vous définissez pour un widget n'affectera aucun autre widget du tableau de bord.



Axe primaire et secondaire

Différentes mesures utilisent différentes unités de mesure pour les données qu'elles rapportent dans un graphique. Par exemple, lorsque l'on examine les IOPS, l'unité de mesure est le nombre d'opérations d'E/S par seconde (IO/s), tandis que la latence est purement une mesure du temps (millisecondes, microsecondes, secondes, etc.). Lors de la représentation graphique des deux métriques sur un graphique à ligne unique à l'aide d'un seul ensemble de valeurs pour l'axe Y, les nombres de latence (généralement une poignée de millisecondes) sont représentés sur la même échelle que les IOPS (généralement numérotés en milliers), et la ligne de latence se perd à cette échelle.

Mais il est possible de représenter graphiquement les deux ensembles de données sur un seul graphique significatif, en plaçant une unité de mesure sur l'axe Y principal (côté gauche) et l'autre unité de mesure sur l'axe Y secondaire (côté droit). Chaque mesure est représentée à sa propre échelle.

Étapes

Cet exemple illustre le concept des axes primaires et secondaires dans un widget de graphique.

1. Créer ou ouvrir un tableau de bord. Ajoutez un widget de graphique linéaire, de graphique spline, de graphique à aires ou de graphique à aires empilées au tableau de bord.
2. Sélectionnez un type d'actif (par exemple *Stockage*) et choisissez *IOPS - Total* pour votre première métrique. Définissez les filtres de votre choix et choisissez une méthode de regroupement si vous le souhaitez.

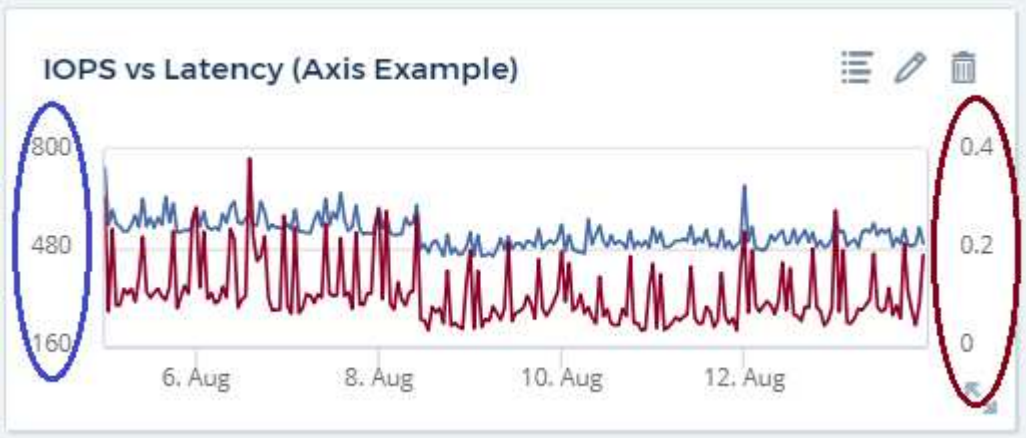
   La ligne IOPS est affichée sur le graphique, avec son échelle indiquée sur la gauche.

3. Cliquez sur **[+Requête]** pour ajouter une deuxième ligne au graphique. Pour cette ligne, choisissez *Latence - Total* pour la métrique.

   Notez que la ligne est affichée à plat en bas du graphique. C'est parce qu'il est dessiné à la même échelle que la ligne IOPS.

4. Dans la requête Latence, sélectionnez **Axe Y : Secondaire**.

   La ligne de latence est désormais dessinée à sa propre échelle, qui est affichée sur le côté droit du graphique.



Expressions dans les widgets

Dans un tableau de bord, n'importe quel widget de série chronologique (ligne, spline, zone, zone empilée), graphique à barres, graphique à colonnes, graphique à secteurs ou widget de tableau vous permet de créer des expressions à partir des mesures que vous choisissez et d'afficher le résultat de ces expressions dans un seul graphique (ou colonne dans le cas duwidget de tableau). Les exemples suivants utilisent des expressions pour résoudre des problèmes spécifiques. Dans le premier exemple, nous souhaitons afficher les IOPS de lecture sous forme de pourcentage du total des IOPS pour tous les actifs de stockage de votre locataire. Le deuxième exemple donne une visibilité sur les IOPS « système » ou « surcharge » qui se produisent sur votre locataire, c'est-à-dire les IOPS qui ne proviennent pas directement de la lecture ou de l'écriture de données.

Vous pouvez utiliser des variables dans des expressions (par exemple, *$Var1 * 100*)

Exemple d'expressions : Lire le pourcentage d'IOPS

Dans cet exemple, nous souhaitons afficher les IOPS de lecture en pourcentage du total des IOPS. Vous pouvez considérer cela comme la formule suivante :

```
 Read Percentage = (Read IOPS / Total IOPS) x 100
Ces données peuvent être affichées sous forme de graphique linéaire sur
votre tableau de bord.  Pour ce faire, suivez ces étapes :
```

Étapes

1. Créez un nouveau tableau de bord ou ouvrez un tableau de bord existant en mode édition.
2. Ajoutez un widget au tableau de bord. Choisissez **Graphique en aires**.

   Le widget s'ouvre en mode édition. Par défaut, une requête s'affiche indiquant *IOPS - Total* pour les actifs *Storage*. Si vous le souhaitez, sélectionnez un autre type d'actif.

3. Cliquez sur le lien **Convertir en expression** à droite.

   La requête actuelle est convertie en mode Expression. Notez que vous ne pouvez pas modifier le type d'actif en mode Expression. Lorsque vous êtes en mode Expression, le lien devient **Revenir à la requête**. Cliquez ici si vous souhaitez revenir au mode Requête à tout moment. Sachez que le passage d'un mode à l'autre réinitialisera les champs à leurs valeurs par défaut.

   Pour l'instant, restez en mode Expression.

4. La métrique **IOPS - Total** se trouve désormais dans le champ de variable alphabétique « **a** ». Dans le champ variable « **b** », cliquez sur **Sélectionner** et choisissez **IOPS - Lecture**.

   Vous pouvez ajouter jusqu'à un total de cinq variables alphabétiques pour votre expression en cliquant sur le bouton + suivant les champs de variables. Pour notre exemple de pourcentage de lecture, nous n'avons besoin que du total des IOPS (« **a** ») et des IOPS de lecture (« **b** »).

5. Dans le champ **Expression**, vous utilisez les lettres correspondant à chaque variable pour construire votre expression. Nous savons que le pourcentage de lecture = (IOPS de lecture / IOPS totales) x 100, nous écririons donc cette expression comme suit :

   ```
    (b / a) * 100
   . Le champ *Label* identifie l'expression.  Modifiez l'étiquette en
   « Pourcentage de lecture » ou en quelque chose d'aussi significatif pour
   vous.
   . Modifiez le champ *Unités* en « % » ou « Pourcentage ».
   ```

   Le graphique affiche le pourcentage de lecture IOPS au fil du temps pour les périphériques de stockage choisis. Si vous le souhaitez, vous pouvez définir un filtre ou choisir une autre méthode de cumul. Sachez que si vous sélectionnez Somme comme méthode de cumul, toutes les valeurs de pourcentage sont additionnées, ce qui peut potentiellement dépasser 100 %.

6. Cliquez sur **Enregistrer** pour enregistrer le graphique sur votre tableau de bord.

Exemple d'expressions : E/S « Système »

Exemple 2 : Parmi les mesures collectées à partir des sources de données figurent la lecture, l'écriture et le nombre total d'E/S par seconde. Cependant, le nombre total d'IOPS signalé par une source de données inclut parfois les IOPS « système », qui sont les opérations d'E/S qui ne font pas directement partie de la lecture ou de l'écriture de données. Ces E/S système peuvent également être considérées comme des E/S « en hauteur », nécessaires au bon fonctionnement du système mais non directement liées aux opérations de données.

Pour afficher ces E/S système, vous pouvez soustraire les IOPS en lecture et en écriture du total des IOPS signalés depuis l'acquisition. La formule pourrait ressembler à ceci :

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Ces données peuvent ensuite être affichées sous forme de graphique
linéaire sur votre tableau de bord.  Pour ce faire, suivez ces étapes :
```

Étapes

1. Créez un nouveau tableau de bord ou ouvrez un tableau de bord existant en mode édition.
2. Ajoutez un widget au tableau de bord. Choisissez **Graphique linéaire**.

   Le widget s'ouvre en mode édition. Par défaut, une requête s'affiche indiquant *IOPS - Total* pour les actifs *Storage*. Si vous le souhaitez, sélectionnez un autre type d'actif.

3. Dans le champ **Regrouper**, choisissez *Somme* par *Tous*.

   Le graphique affiche une ligne indiquant la somme des IOPS totales.

4. Cliquez sur l'icône *Dupliquer cette requête* pour créer une copie de la requête.

   Un duplicata de la requête est ajouté sous l'original.

5. Dans la deuxième requête, cliquez sur le bouton **Convertir en expression**.

   La requête actuelle est convertie en mode Expression. Cliquez sur **Revenir à la requête** si vous souhaitez revenir au mode Requête à tout moment. Sachez que le passage d'un mode à l'autre réinitialisera les champs à leurs valeurs par défaut.

   Pour l'instant, restez en mode Expression.

6. La métrique *IOPS - Total* se trouve désormais dans le champ de variable alphabétique « **a** ». Cliquez sur *IOPS - Total* et remplacez-le par *IOPS - Lecture*.
7. Dans le champ variable « **b** », cliquez sur **Sélectionner** et choisissez *IOPS - Écriture*.
8. Dans le champ **Expression**, vous utilisez les lettres correspondant à chaque variable pour construire votre expression. Nous écririons notre expression simplement comme :

   ```
   a + b
   ```

   Dans la section Affichage, choisissez **Graphique en aires** pour cette expression.

9. Le champ **Label** identifie l'expression. Modifiez l'étiquette en « IOPS système » ou en quelque chose d'aussi significatif pour vous.

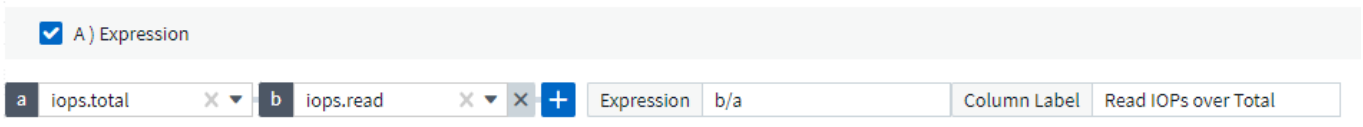
   Le graphique affiche le total des IOPS sous forme de graphique linéaire, avec un graphique en aires indiquant la combinaison des IOPS en lecture et en écriture en dessous. L'écart entre les deux montre les IOPS qui ne sont pas directement liées aux opérations de lecture ou d'écriture de données. Il s'agit de vos IOPS « système ».

10. Cliquez sur **Enregistrer** pour enregistrer le graphique sur votre tableau de bord.

Pour utiliser une variable dans une expression, saisissez simplement le nom de la variable, par exemple *$var1 * 100*. Seules les variables numériques peuvent être utilisées dans les expressions.

Expressions dans un widget de tableau

Les widgets de tableau gèrent les expressions un peu différemment. Vous pouvez avoir jusqu'à cinq expressions dans un seul widget de tableau, chacune d'entre elles étant ajoutée en tant que nouvelle colonne au tableau. Chaque expression peut inclure jusqu'à cinq valeurs sur lesquelles effectuer son calcul. Vous pouvez facilement nommer la colonne avec un nom significatif.



Variables

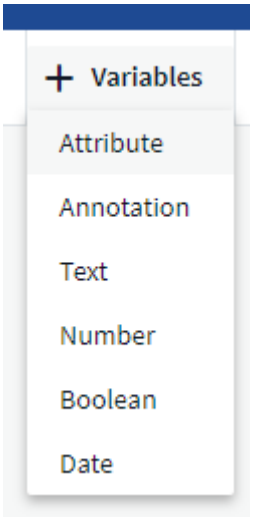
Les variables vous permettent de modifier les données affichées dans certains ou tous les widgets d'un tableau de bord à la fois. En définissant un ou plusieurs widgets pour utiliser une variable commune, les modifications apportées à un endroit entraînent la mise à jour automatique des données affichées dans

chaque widget.

Types de variables

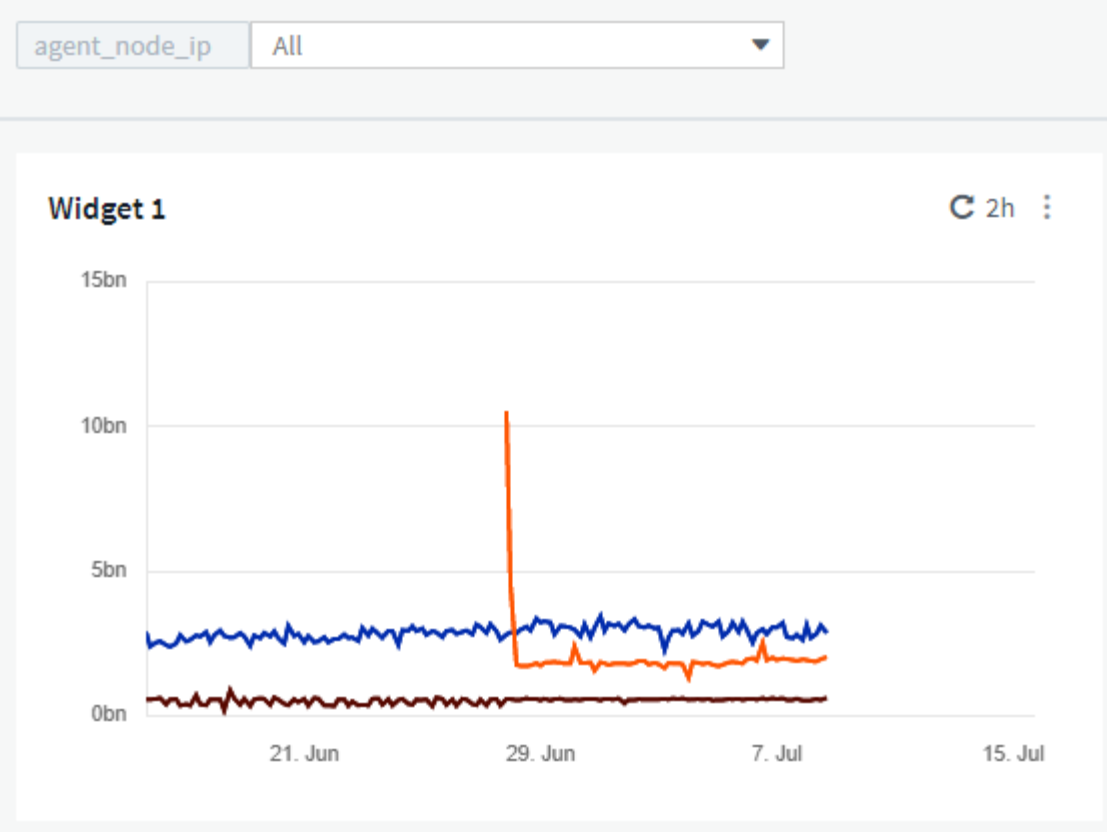
Une variable peut être de l'un des types suivants :

- **Attribut** : utilisez les attributs ou les métriques d'un objet pour filtrer
- **Annotation** : Utilisez un"Annotation" pour filtrer les données du widget.
- **Texte** : Une chaîne alphanumérique.
- **Numérique** : Une valeur numérique. À utiliser seul ou comme valeur « de » ou « à », selon le champ de votre widget.
- **Booléen** : À utiliser pour les champs avec des valeurs Vrai/Faux, Oui/Non, etc. Pour la variable booléenne, les choix sont Oui, Non, Aucun, N'importe lequel.
- **Date** : une valeur de date. À utiliser comme valeur « de » ou « à », selon la configuration de votre widget.

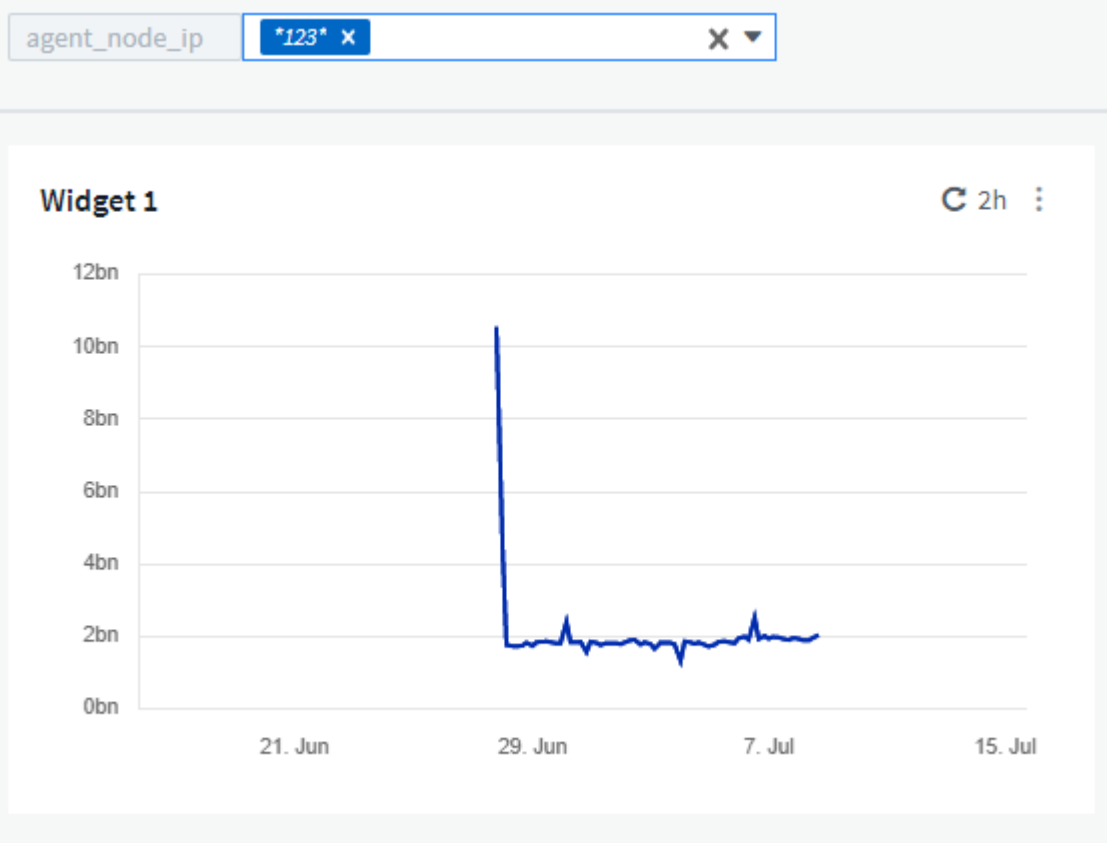


Variables d'attribut

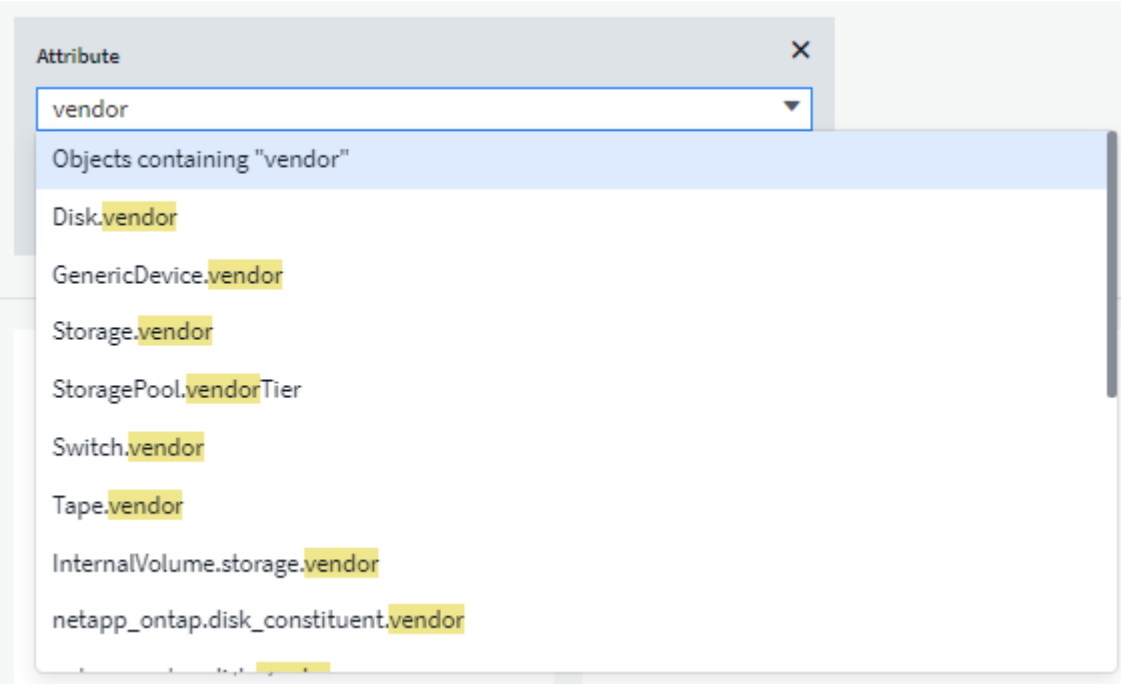
La sélection d'une variable de type Attribut vous permet de filtrer les données du widget contenant la ou les valeurs d'attribut spécifiées. L'exemple ci-dessous montre un widget de ligne affichant les tendances de mémoire libre pour les nœuds d'agent. Nous avons créé une variable pour les adresses IP des nœuds d'agent, actuellement configurée pour afficher toutes les adresses IP :



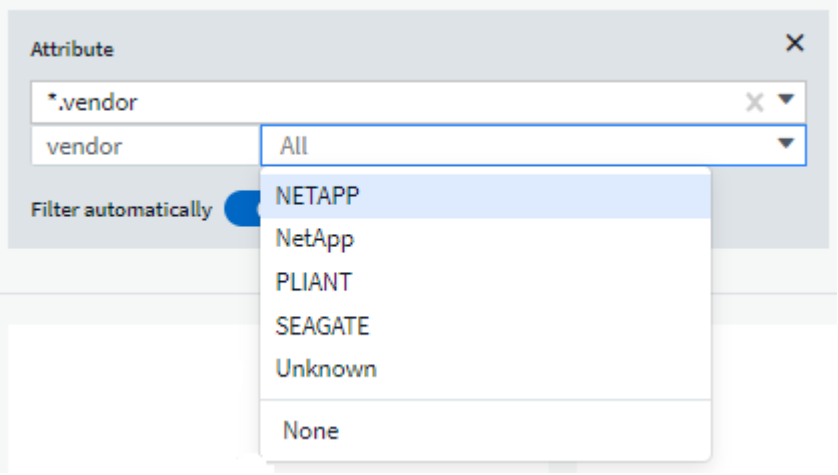
Mais si vous souhaitez temporairement voir uniquement les nœuds sur des sous-réseaux individuels de votre locataire, vous pouvez définir ou modifier la variable sur une ou plusieurs adresses IP de nœud d'agent spécifiques. Ici, nous visualisons uniquement les nœuds du sous-réseau « 123 » :



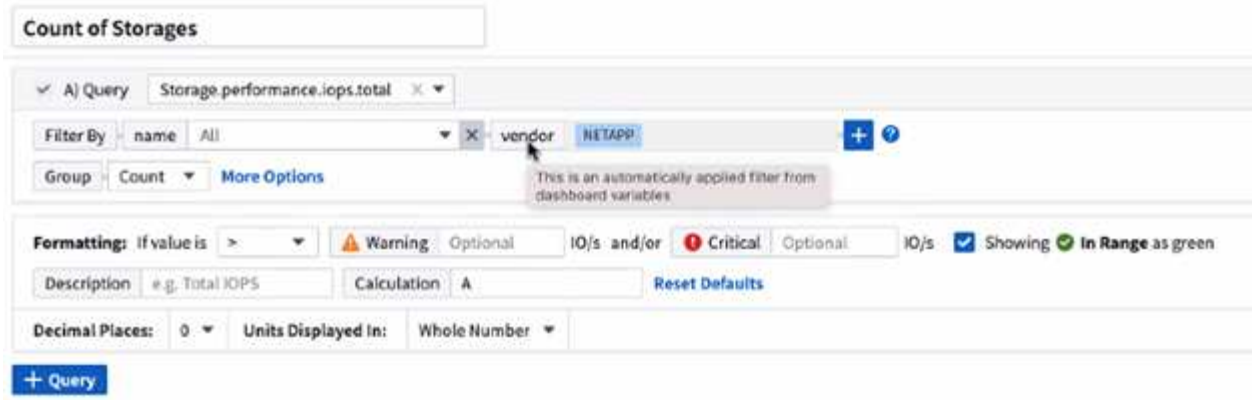
Vous pouvez également définir une variable pour filtrer sur *tous* les objets avec un attribut particulier quel que soit le type d'objet, par exemple les objets avec un attribut « vendor », en spécifiant **.vendor* dans le champ variable. Vous n'avez pas besoin de saisir le caractère « * ». Data Infrastructure Insights le fournira si vous sélectionnez l'option générique.



Lorsque vous déroulez la liste des choix pour la valeur de la variable, les résultats sont filtrés afin d'afficher uniquement les fournisseurs disponibles en fonction des objets de votre tableau de bord.



Si vous modifiez un widget sur votre tableau de bord où le filtre d'attribut est pertinent (ce qui signifie que les objets du widget contiennent un attribut **.vendor*), cela vous montre que le filtre d'attribut est automatiquement appliqué.

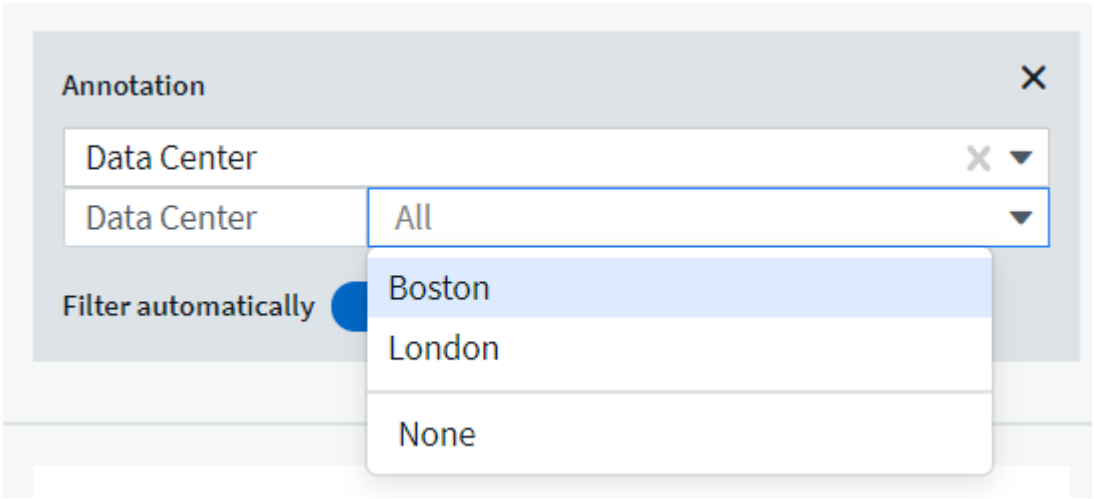


14

Appliquer des variables est aussi simple que de modifier les données d'attribut de votre choix.

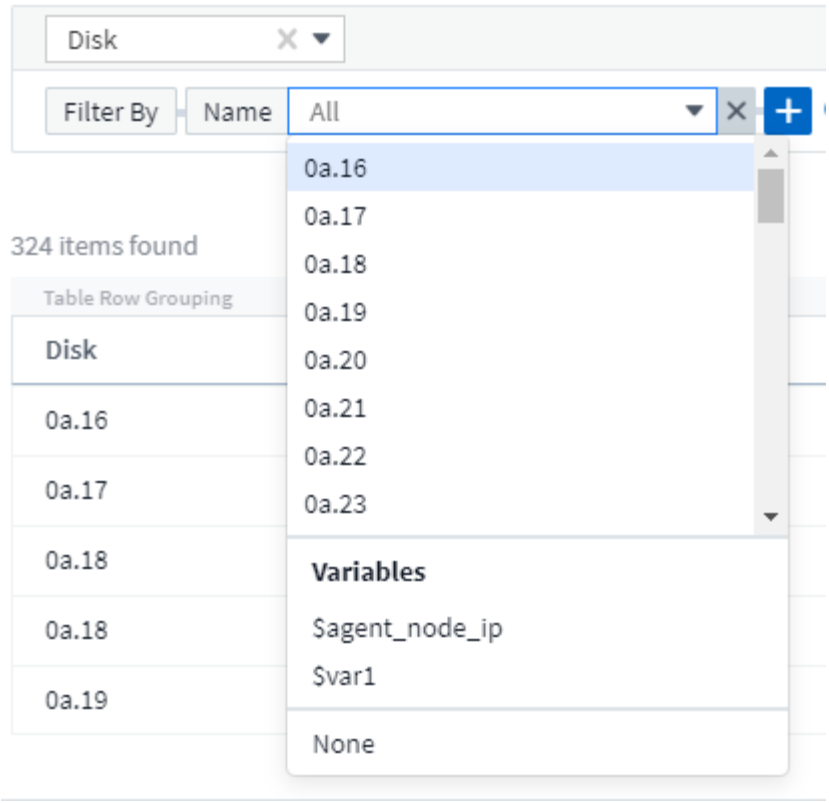
Variables d'annotation

Le choix d'une variable d'annotation vous permet de filtrer les objets associés à cette annotation, par exemple ceux appartenant au même centre de données.



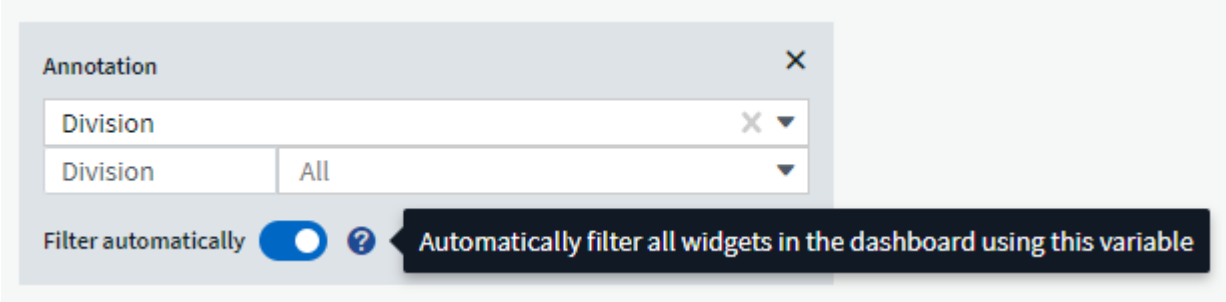
Variable texte, nombre, date ou booléenne

Vous pouvez créer des variables génériques qui ne sont pas associées à un attribut particulier en sélectionnant un type de variable *Texte*, *Nombre*, *Booléen* ou *Date*. Une fois la variable créée, vous pouvez la sélectionner dans un champ de filtre de widget. Lors de la définition d'un filtre dans un widget, en plus des valeurs spécifiques que vous pouvez sélectionner pour le filtre, toutes les variables qui ont été créées pour le tableau de bord sont affichées dans la liste. Elles sont regroupées sous la section « Variables » dans la liste déroulante et ont des noms commençant par « $ ». Choisir une variable dans ce filtre vous permettra de rechercher les valeurs que vous saisissez dans le champ variable du tableau de bord lui-même. Tous les widgets utilisant cette variable dans un filtre seront mis à jour de manière dynamique.



Portée du filtre variable

Lorsque vous ajoutez une variable d'annotation ou d'attribut à votre tableau de bord, la variable peut être appliquée à *tous* les widgets du tableau de bord, ce qui signifie que tous les widgets de votre tableau de bord afficheront des résultats filtrés en fonction de la valeur que vous avez définie dans la variable.



Notez que seules les variables d'attribut et d'annotation peuvent être filtrées automatiquement de cette manière. Les variables non annotées ou attributaires ne peuvent pas être filtrées automatiquement. Chaque widget individuel doit être configuré pour utiliser des variables de ces types.

Pour désactiver le filtrage automatique afin que la variable s'applique uniquement aux widgets pour lesquels vous l'avez spécifiquement définie, cliquez sur le curseur « Filtrer automatiquement » pour le désactiver.

Pour définir une variable dans un widget individuel, ouvrez le widget en mode édition et sélectionnez l'annotation ou l'attribut spécifique dans le champ *Filtrer par*. Avec une variable d'annotation, vous pouvez sélectionner une ou plusieurs valeurs spécifiques, ou sélectionner le nom de la variable (indiqué par le « $ » initial) pour permettre la saisie de la variable au niveau du tableau de bord. La même chose s'applique aux variables d'attribut. Seuls les widgets pour lesquels vous définissez la variable afficheront les résultats filtrés.

Le filtrage des variables est *contextuel* ; lorsque vous sélectionnez une ou plusieurs valeurs de filtre pour une

variable, les autres variables de votre page afficheront uniquement les valeurs pertinentes pour ce filtre. Par exemple, lors de la définition d'un filtre de variable sur un *modèle* de stockage spécifique, toutes les variables définies pour filtrer le *nom* de stockage afficheront uniquement les valeurs pertinentes pour ce modèle.

Pour utiliser une variable dans une expression, saisissez simplement le nom de la variable dans le cadre de l'expression, par exemple, *$var1 * 100*. Seules les variables numériques peuvent être utilisées dans les expressions. Vous ne pouvez pas utiliser de variables d'annotation ou d'attribut numériques dans les expressions.

Le filtrage des variables est *contextuel* ; lorsque vous sélectionnez une ou plusieurs valeurs de filtre pour une variable, les autres variables de votre page afficheront uniquement les valeurs pertinentes pour ce filtre. Par exemple, lors de la définition d'un filtre de variable sur un *modèle* de stockage spécifique, toutes les variables définies pour filtrer le *nom* de stockage afficheront uniquement les valeurs pertinentes pour ce modèle.

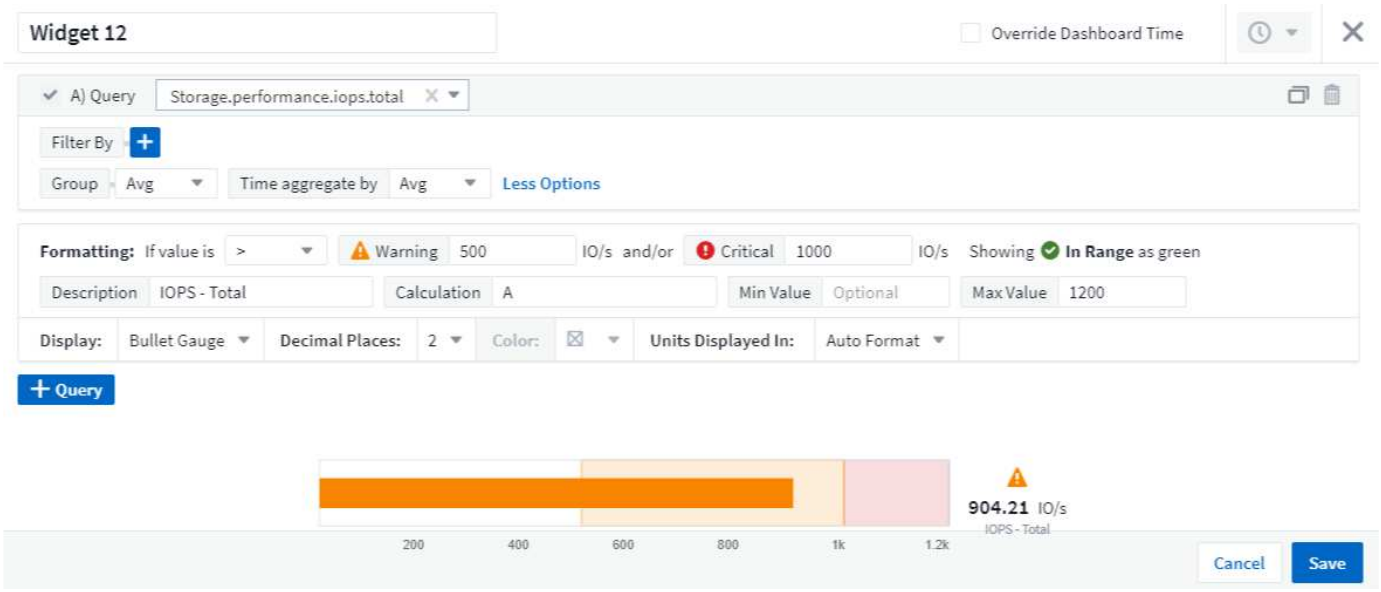
Nommage des variables

Noms des variables :

- Doit inclure uniquement les lettres a à z, les chiffres 0 à 9, le point (.), le trait de soulignement (_) et l'espace ( ).
- Ne peut pas dépasser 20 caractères.
- Sont sensibles à la casse : $CityName et $cityname sont des variables différentes.
- Ne peut pas être identique à un nom de variable existant.
- Ne peut pas être vide.

Widgets de jauge de formatage

Les widgets Solid et Bullet Gauge vous permettent de définir des seuils pour les niveaux *Avertissement* et/ou *Critique*, fournissant une représentation claire des données que vous spécifiez.



Pour définir la mise en forme de ces widgets, suivez ces étapes :

1. Choisissez si vous souhaitez mettre en évidence les valeurs supérieures (>) ou inférieures (<) à vos seuils. Dans cet exemple, nous mettrons en évidence les valeurs supérieures (>) aux niveaux de seuil.

2. Choisissez une valeur pour le seuil « Avertissement ». Lorsque le widget affiche des valeurs supérieures à ce niveau, il affiche la jauge en orange.
3. Choisissez une valeur pour le seuil « Critique ». Les valeurs supérieures à ce niveau entraîneront l'affichage de la jauge en rouge.

Vous pouvez éventuellement choisir une valeur minimale et maximale pour la jauge. Les valeurs inférieures au minimum n'afficheront pas la jauge. Les valeurs supérieures au maximum afficheront une jauge pleine. Si vous ne choisissez pas de valeurs minimales ou maximales, le widget sélectionne les valeurs minimales et maximales optimales en fonction de la valeur du widget.

Formatage d'un widget à valeur unique

dans le widget Valeur unique, en plus de définir les seuils d'avertissement (orange) et critique (rouge), vous pouvez choisir d'afficher les valeurs « Dans la plage » (celles en dessous du niveau d'avertissement) avec un arrière-plan vert ou blanc.

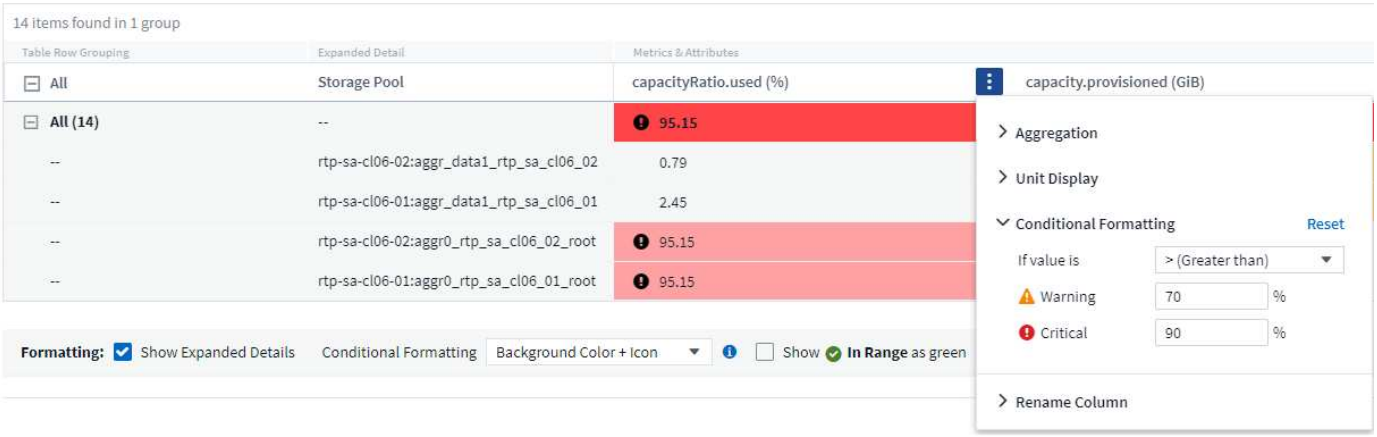
Cliquer sur le lien dans un widget à valeur unique ou dans un widget de jauge affichera une page de requête

correspondant à la première requête du widget.

Widgets de tableau de formatage

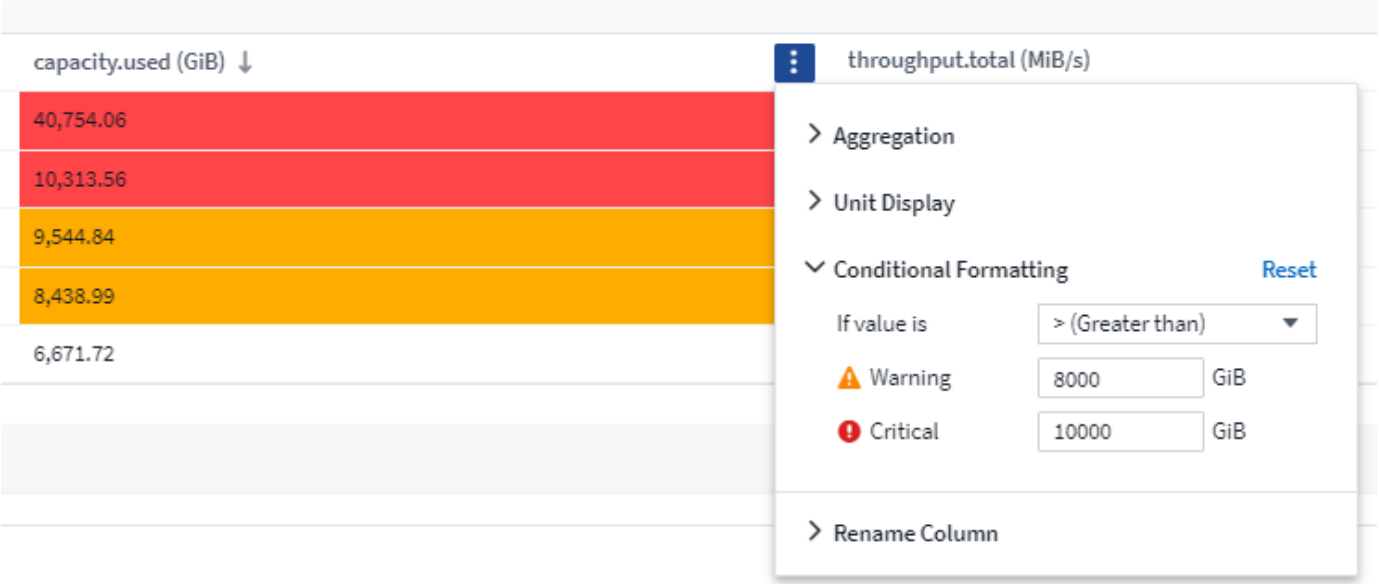
Comme les widgets à valeur unique et à jauge, vous pouvez définir une mise en forme conditionnelle dans les widgets de tableau, vous permettant de mettre en évidence les données avec des couleurs et/ou des icônes spéciales.

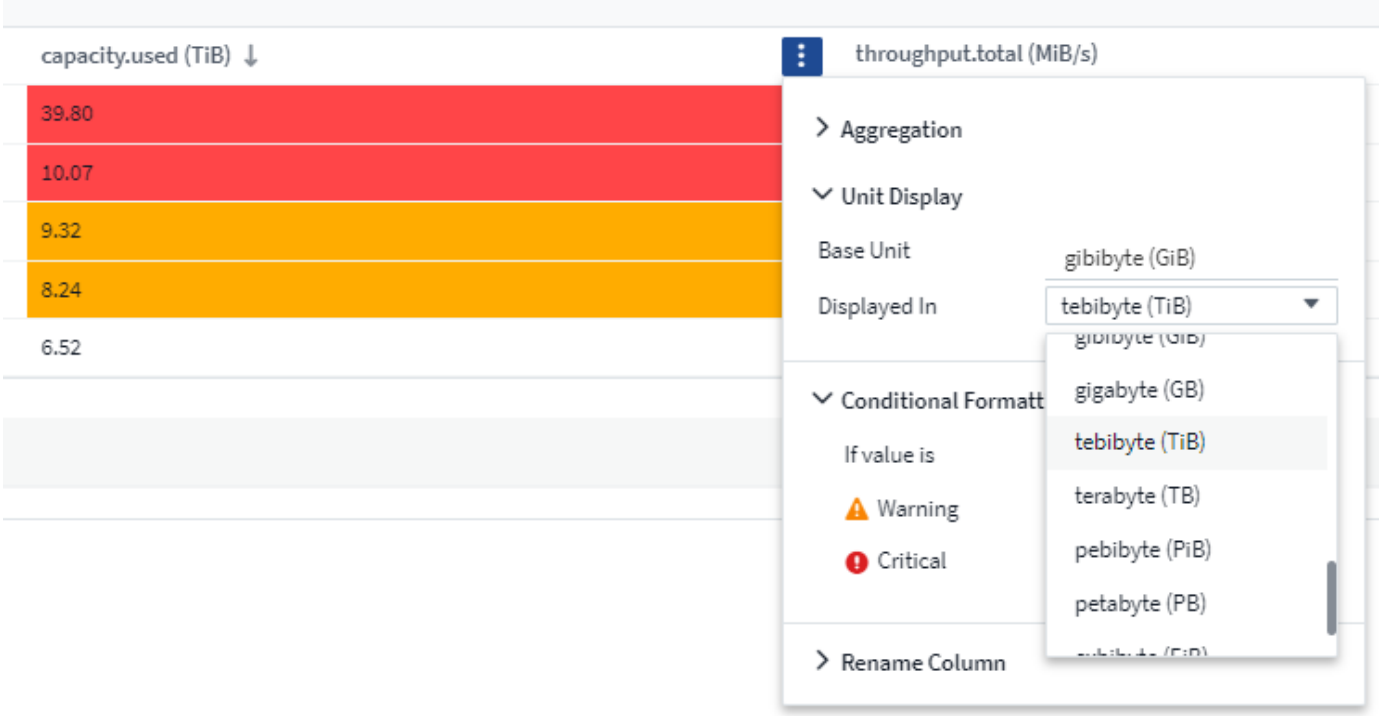
La mise en forme conditionnelle vous permet de définir et de mettre en évidence les seuils de niveau d'avertissement et de niveau critique dans les widgets de tableau, offrant une visibilité instantanée sur les valeurs aberrantes et les points de données exceptionnels.



La mise en forme conditionnelle est définie séparément pour chaque colonne d'un tableau. Par exemple, vous pouvez choisir un ensemble de seuils pour une colonne de capacité et un autre ensemble pour une colonne de débit.

Si vous modifiez l'affichage de l'unité pour une colonne, la mise en forme conditionnelle reste la même et reflète la modification des valeurs. Les images ci-dessous montrent la même mise en forme conditionnelle même si l'unité d'affichage est différente.



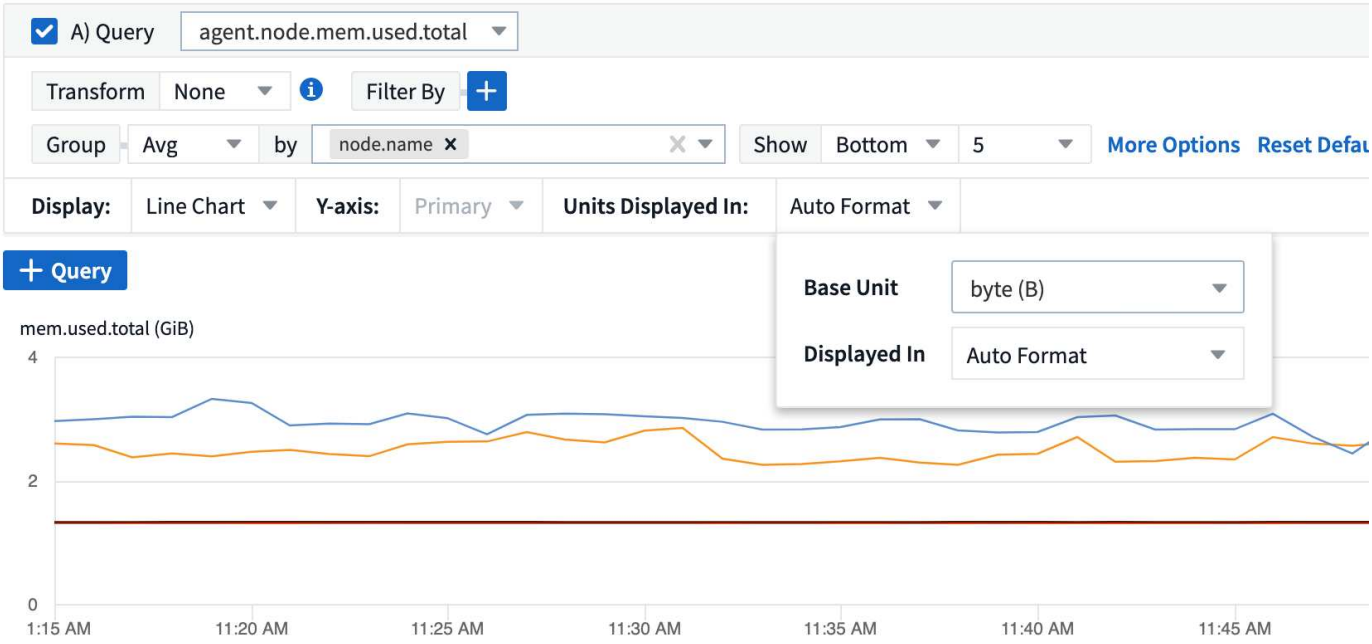


Vous pouvez choisir d'afficher la mise en forme des conditions sous forme de couleur, d'icônes ou les deux.

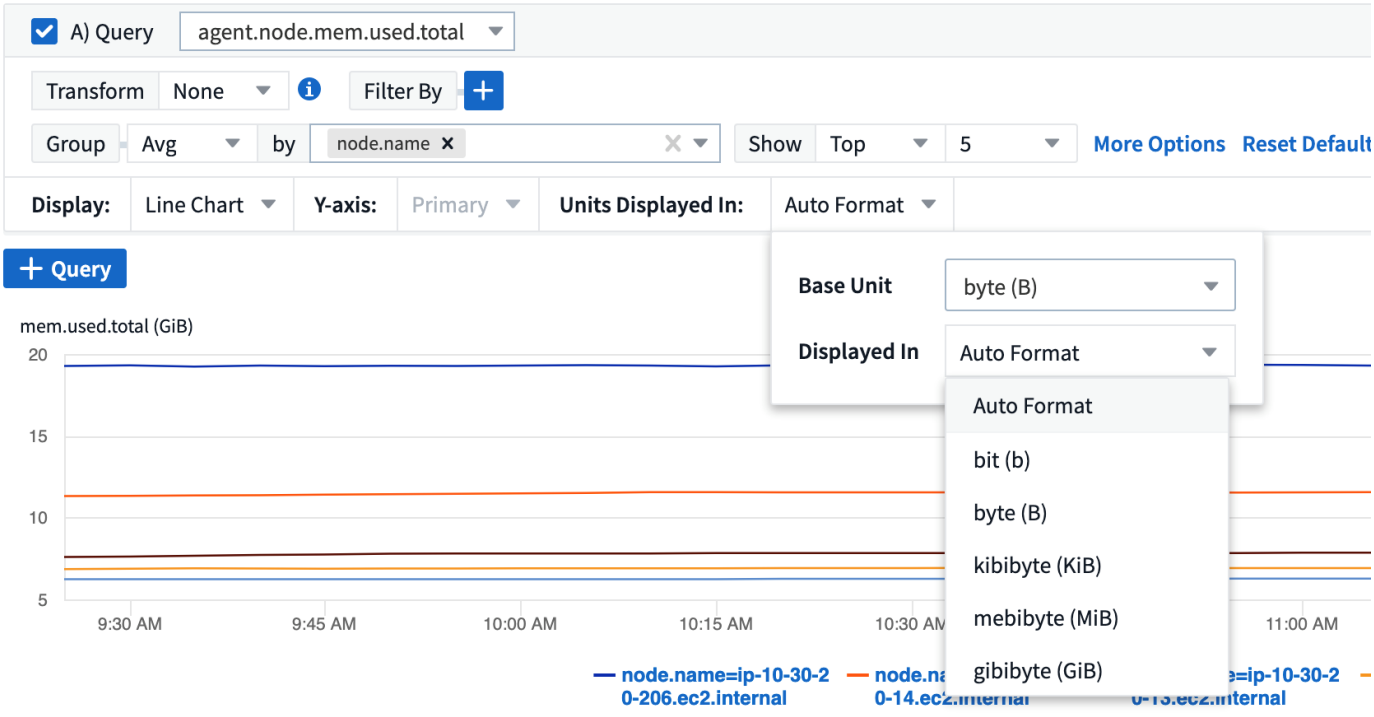
Choix de l'unité d'affichage des données

La plupart des widgets d'un tableau de bord vous permettent de spécifier les unités dans lesquelles afficher les valeurs, par exemple *Mégaoctets*, *Milliers*, *Pourcentage*, *Millisecondes (ms)*, etc. Dans de nombreux cas, Data Infrastructure Insights connaît le meilleur format pour les données acquises. Dans les cas où le meilleur format n'est pas connu, vous pouvez définir le format souhaité.

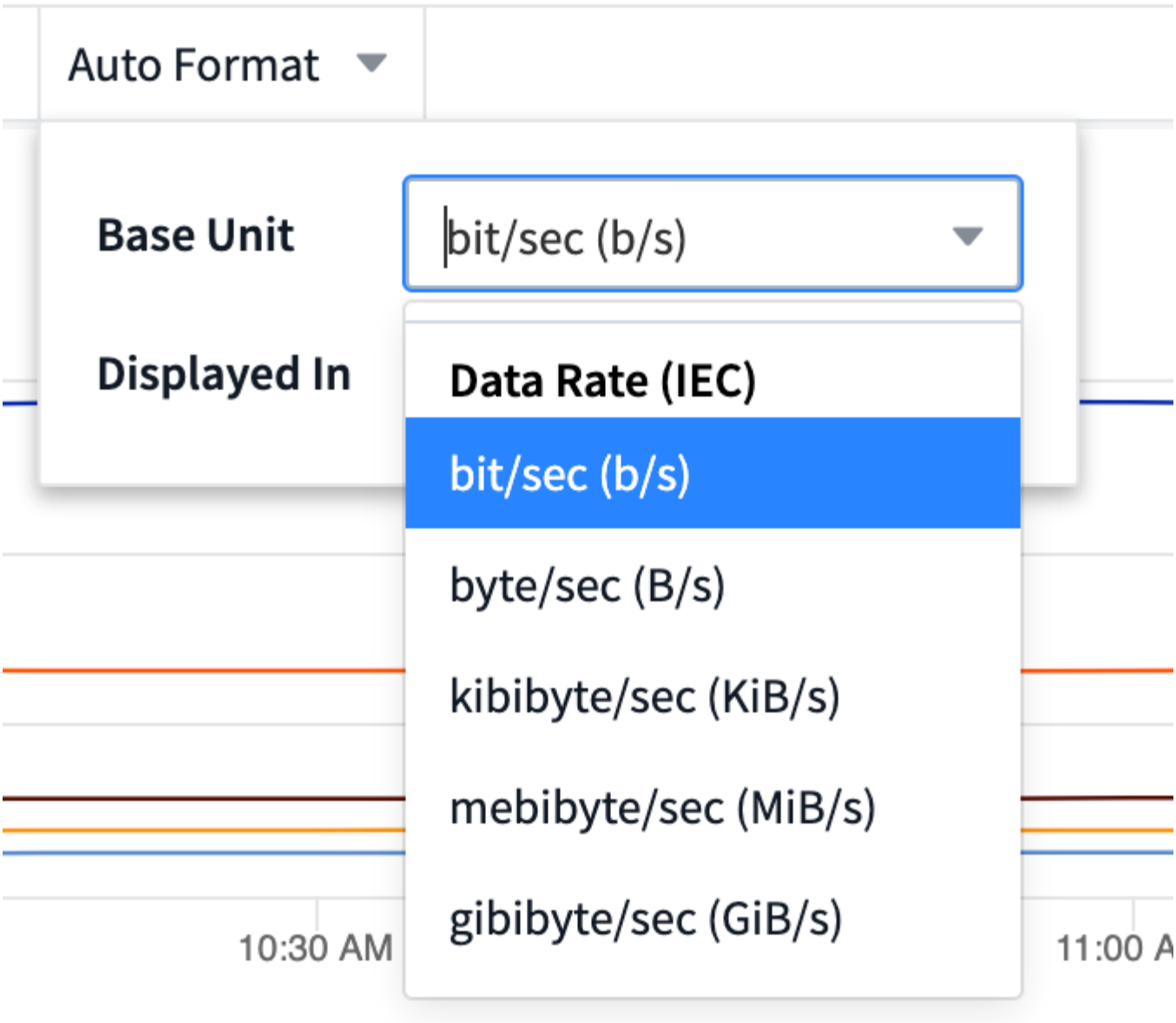
Dans l'exemple de graphique linéaire ci-dessous, les données sélectionnées pour le widget sont connues pour être en *octets* (l'unité de données IEC de base : voir le tableau ci-dessous), donc l'unité de base est automatiquement sélectionnée comme « octet (B) ». Cependant, les valeurs de données sont suffisamment grandes pour être présentées sous forme de gibioctets (Gio), donc Data Infrastructure Insights formate automatiquement par défaut les valeurs en Gio. L'axe Y du graphique indique « Gio » comme unité d'affichage et toutes les valeurs sont affichées en fonction de cette unité.



Si vous souhaitez afficher le graphique dans une unité différente, vous pouvez choisir un autre format dans lequel afficher les valeurs. Étant donné que l'unité de base dans cet exemple est *octet*, vous pouvez choisir parmi les formats « basés sur les octets » pris en charge : bit (b), octet (B), kibioctet (Kio), mébioctet (Mio), gibioctet (Gio). L'étiquette et les valeurs de l'axe Y changent en fonction du format que vous choisissez.



Dans les cas où l'unité de base n'est pas connue, vous pouvez attribuer une unité parmi les"unités disponibles" , ou saisissez le vôtre. Une fois que vous avez attribué une unité de base, vous pouvez ensuite choisir d'afficher les données dans l'un des formats pris en charge appropriés.



Pour effacer vos paramètres et recommencer, cliquez sur **Réinitialiser les valeurs par défaut**.

Un mot sur le formatage automatique

La plupart des mesures sont rapportées par les collecteurs de données dans la plus petite unité, par exemple sous la forme d'un nombre entier tel que 1 234 567 890 octets. Par défaut, Data Infrastructure Insights formatera automatiquement la valeur pour l'affichage le plus lisible. Par exemple, une valeur de données de 1 234 567 890 octets serait automatiquement formatée à 1,23 *Gibioctets*. Vous pouvez choisir de l'afficher dans un autre format, tel que *Mébioctets*. La valeur s'affichera en conséquence.

Data Infrastructure Insights utilise les normes de dénomination des nombres en anglais américain. Le « milliard » américain équivaut à « mille millions ».

Widgets avec requêtes multiples

Si vous disposez d'un widget de série chronologique (c'est-à-dire une ligne, une spline, une zone, une zone empilée) comportant deux requêtes où les deux sont tracées sur l'axe Y principal, l'unité de base n'est pas affichée en haut de l'axe Y. Cependant, si votre widget comporte une requête sur l'axe Y principal et une

requête sur l'axe Y secondaire, les unités de base de chacun sont affichées.

Si votre widget comporte trois requêtes ou plus, les unités de base ne sont pas affichées sur l'axe Y.

Unités disponibles

Le tableau suivant présente toutes les unités disponibles par catégorie.

Catégorie	Unités
Devise	cent dollar
Données (CEI)	bit octet kibioctet mébioctet gibioctet tébioctet pébioctet exbioctet
Débit de données (CEI)	bit/sec octet/sec kibioctet/sec mébioctet/sec gibioctet/sec tébioctet/sec pébioctet/sec
Données (métriques)	kilooctet mégaoctet gigaoctet téraoctet pétaoctet exaoctet
Débit de données (métrique)	kilooctet/sec mégaoctet/sec gigaoctet/sec téraoctet/sec pétaoctet/sec exaoctet/sec
CEI	kibi mebi gibi tebi pebi exbi
Décimal	nombre entier mille millions milliards mille milliards
Pourcentage	pourcentage
Durée	nanoseconde microseconde milliseconde seconde minute heure
Température	Celsius Fahrenheit
Fréquence	hertz kilohertz mégahertz gigahertz
processeur	nanocores microcores millicores coeurs kilocores mégacores gigacores teracores petacores exacores
Débit	E/S ops/sec ops/sec requêtes/sec lectures/sec écritures/sec ops/min lectures/min écritures/min

Mode TV et rafraîchissement automatique

Les données des widgets des tableaux de bord et des pages de destination des ressources s'actualisent automatiquement en fonction d'un intervalle d'actualisation déterminé par la plage horaire du tableau de bord sélectionnée. L'intervalle d'actualisation est basé sur le fait que le widget est une série chronologique (graphique linéaire, spline, aire, aire empilée) ou non chronologique (tous les autres graphiques).

Plage de temps du tableau de bord	Intervalle de rafraîchissement des séries chronologiques	Intervalle de rafraîchissement non chronologique
Les 15 dernières minutes	10 secondes	1 minute
Les 30 dernières minutes	15 secondes	1 minute
Les 60 dernières minutes	15 secondes	1 minute
Les 2 dernières heures	30 secondes	5 minutes
Les 3 dernières heures	30 secondes	5 minutes
Les 6 dernières heures	1 minute	5 minutes
Les 12 dernières heures	5 minutes	10 minutes
Dernières 24 heures	5 minutes	10 minutes
Les 2 derniers jours	10 minutes	10 minutes
Les 3 derniers jours	15 minutes	15 minutes
Les 7 derniers jours	1 heure	1 heure
Les 30 derniers jours	2 heures	2 heures

Chaque widget affiche son intervalle d'actualisation automatique dans le coin supérieur droit du widget.

L'actualisation automatique n'est pas disponible pour la plage horaire du tableau de bord personnalisé.

Associé au **Mode TV**, l'actualisation automatique permet un affichage en temps quasi réel des données sur un tableau de bord ou une page d'actif. Le mode TV offre un affichage épuré ; le menu de navigation est masqué, offrant plus d'espace à l'écran pour l'affichage de vos données, tout comme le bouton Modifier. Le mode TV ignore les délais d'expiration typiques de Data Infrastructure Insights , laissant l'affichage en direct jusqu'à la déconnexion manuelle ou automatique par les protocoles de sécurité d'autorisation.

Étant donné que la NetApp Console dispose de son propre délai d'expiration de connexion utilisateur de 7 jours, Data Infrastructure Insights doit également se déconnecter avec cet événement. Vous pouvez simplement vous reconnecter et votre tableau de bord continuera à s'afficher.

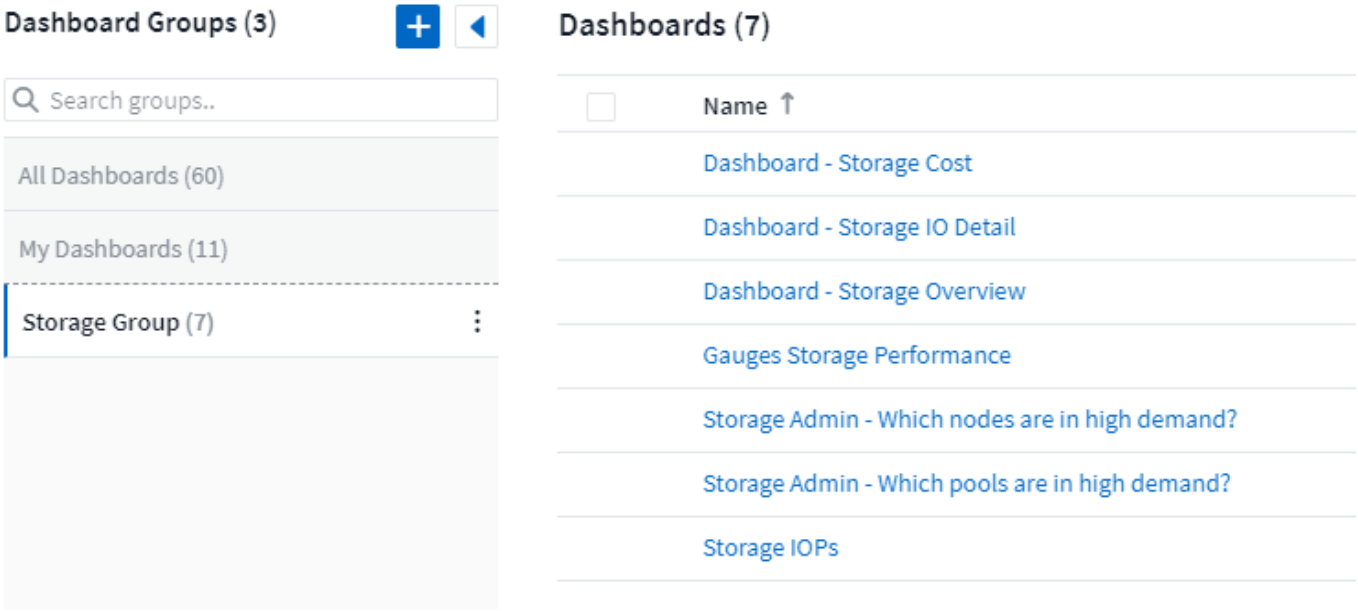
- Pour activer le mode TV, cliquez sur le bouton Mode TV.
- Pour désactiver le mode TV, cliquez sur le bouton **Quitter** en haut à gauche de l'écran.

Vous pouvez suspendre temporairement l'actualisation automatique en cliquant sur le bouton Pause dans le coin supérieur droit. En pause, le champ de plage horaire du tableau de bord affichera la plage horaire active des données en pause. Vos données sont toujours en cours d'acquisition et de mise à jour pendant que l'actualisation automatique est suspendue. Cliquez sur le bouton Reprendre pour continuer l'actualisation automatique des données.

Groupes de tableaux de bord

Le regroupement vous permet de visualiser et de gérer les tableaux de bord associés. Par exemple, vous pouvez avoir un groupe de tableaux de bord dédié au stockage sur votre locataire. Les groupes de tableaux de

bord sont gérés sur la page **Tableaux de bord > Afficher tous les tableaux de bord**.



Deux groupes sont affichés par défaut :

- **Tous les tableaux de bord** répertorie tous les tableaux de bord qui ont été créés, quel que soit le propriétaire.
- **Mes tableaux de bord** répertorie uniquement les tableaux de bord créés par l'utilisateur actuel.

Le nombre de tableaux de bord contenus dans chaque groupe est indiqué à côté du nom du groupe.

Pour créer un nouveau groupe, cliquez sur le bouton **"+" Créer un nouveau groupe de tableau de bord**. Saisissez un nom pour le groupe et cliquez sur **Créer un groupe**. Un groupe vide est créé avec ce nom.

Pour ajouter des tableaux de bord au groupe, cliquez sur le groupe *Tous les tableaux de bord* pour afficher tous les tableaux de bord de votre locataire, ou cliquez sur *Mes tableaux de bord* si vous souhaitez uniquement voir les tableaux de bord que vous possédez, puis effectuez l'une des opérations suivantes :

- Pour ajouter un seul tableau de bord, cliquez sur le menu à droite du tableau de bord et sélectionnez *Ajouter au groupe*.
- Pour ajouter plusieurs tableaux de bord à un groupe, sélectionnez-les en cliquant sur la case à cocher en regard de chaque tableau de bord, puis cliquez sur le bouton **Actions en masse** et sélectionnez *Ajouter au groupe*.

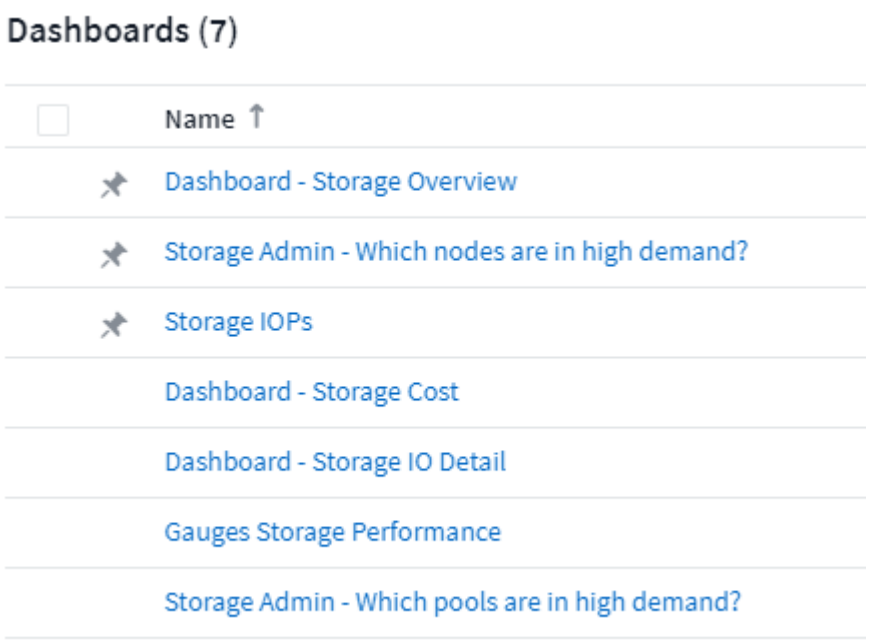
Supprimez les tableaux de bord du groupe actuel de la même manière en sélectionnant *Supprimer du groupe*. Vous ne pouvez pas supprimer les tableaux de bord du groupe *Tous les tableaux de bord* ou *Mes tableaux de bord*.

La suppression d'un tableau de bord d'un groupe ne supprime pas le tableau de bord de Data Infrastructure Insights. Pour supprimer complètement un tableau de bord, sélectionnez le tableau de bord et cliquez sur *Supprimer*. Cela le supprime de tous les groupes auxquels il appartenait et il n'est plus disponible pour aucun utilisateur.

Épinglez vos tableaux de bord préférés

Vous pouvez gérer davantage vos tableaux de bord en épinglant vos favoris en haut de votre liste de tableaux de bord. Pour épingler un tableau de bord, cliquez simplement sur le bouton en forme de punaise affiché lorsque vous survolez un tableau de bord dans n'importe quelle liste.

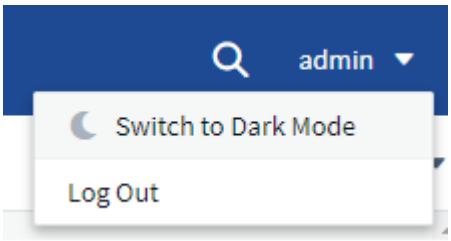
L'épinglage/désépinglage du tableau de bord est une préférence individuelle de l'utilisateur et indépendante du groupe (ou des groupes) auquel appartient le tableau de bord.



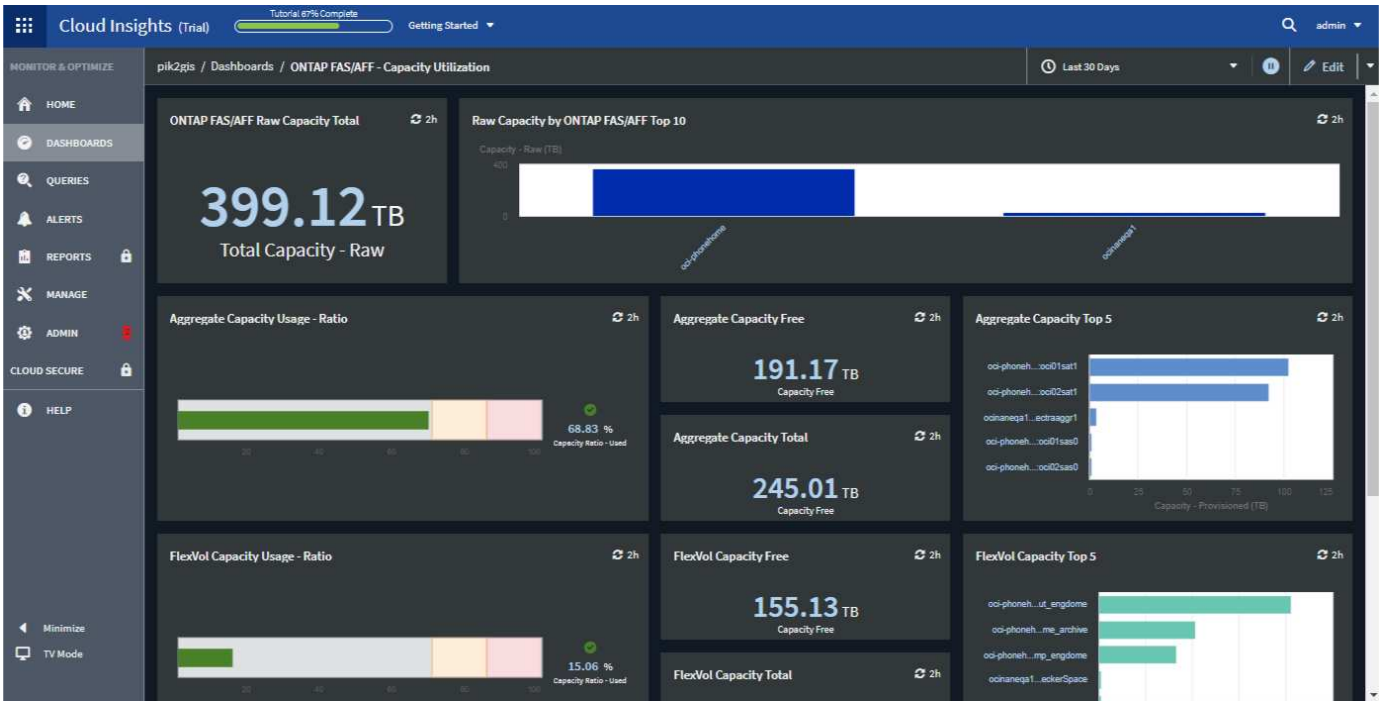
Thème sombre

Vous pouvez choisir d'afficher Data Infrastructure Insights à l'aide d'un thème clair (par défaut), qui affiche la plupart des écrans avec un arrière-plan clair et du texte sombre, ou d'un thème sombre qui affiche la plupart des écrans avec un arrière-plan sombre et du texte clair.

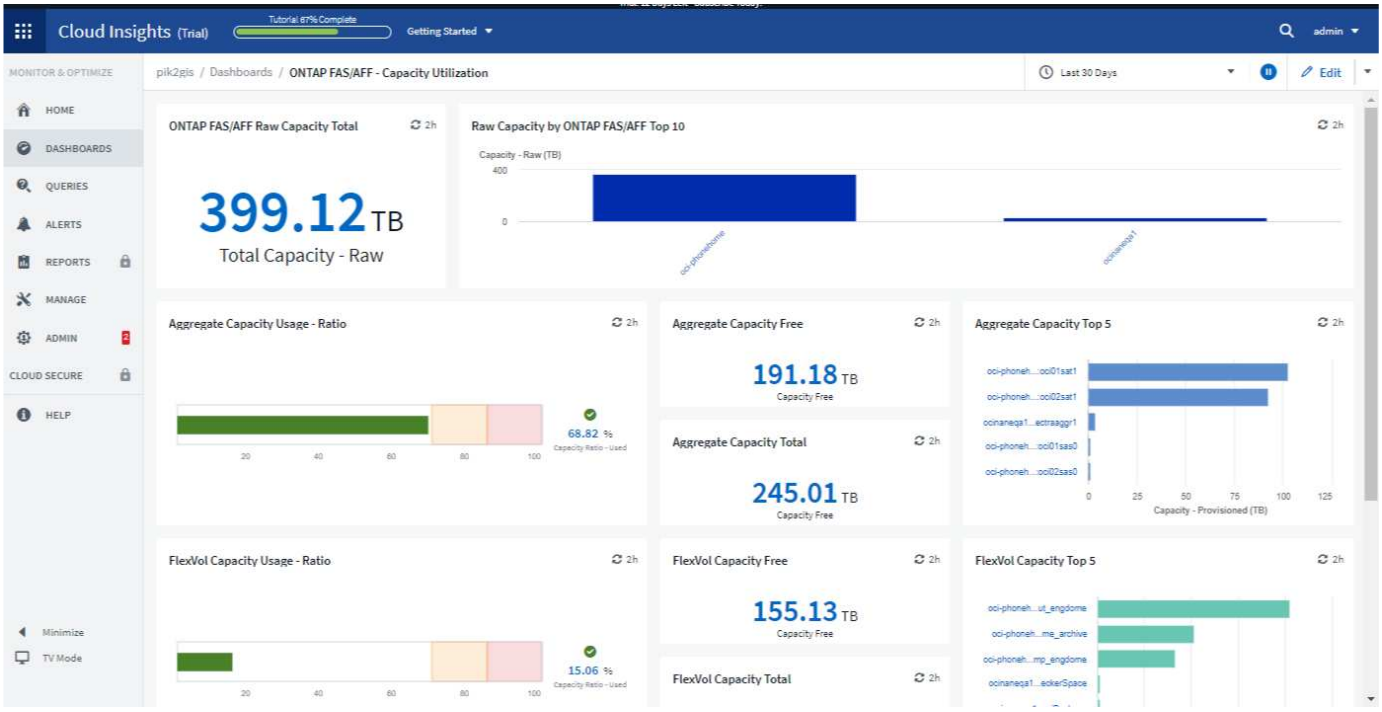
Pour basculer entre les thèmes clairs et sombres, cliquez sur le bouton du nom d'utilisateur dans le coin supérieur droit de l'écran et choisissez le thème souhaité.



Vue du tableau de bord du thème sombre :



Vue du tableau de bord du thème clair :



Certaines zones de l'écran, telles que certains graphiques de widgets, affichent toujours des arrière-plans clairs même lorsqu'elles sont visualisées dans un thème sombre.

Interpolation de graphique linéaire

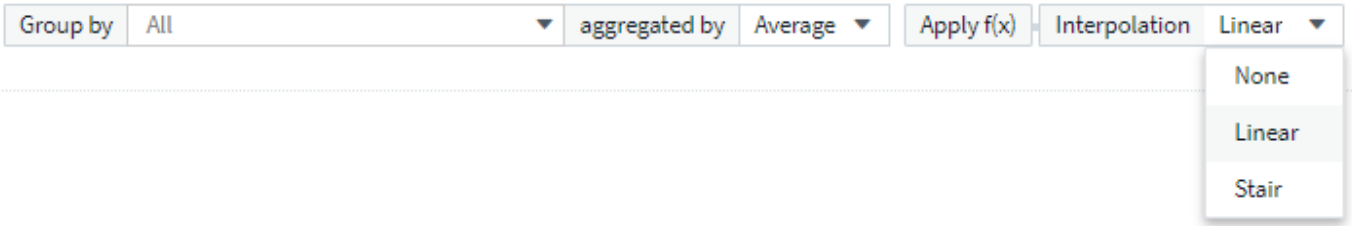
Différents collecteurs de données interrogent souvent leurs données à des intervalles différents. Par exemple, le collecteur de données A peut interroger toutes les 15 minutes tandis que le collecteur de données B interroge toutes les cinq minutes. Lorsqu'un widget de graphique linéaire (également des graphiques splines, à aires et à aires empilées) regroupe ces données provenant de plusieurs collecteurs de données en une seule

ligne (par exemple, lorsque le widget regroupe par « tous ») et actualise la ligne toutes les cinq minutes, les données du collecteur B peuvent être affichées avec précision tandis que les données du collecteur A peuvent comporter des lacunes, affectant ainsi l'agrégat jusqu'à ce que le collecteur A interroge à nouveau.

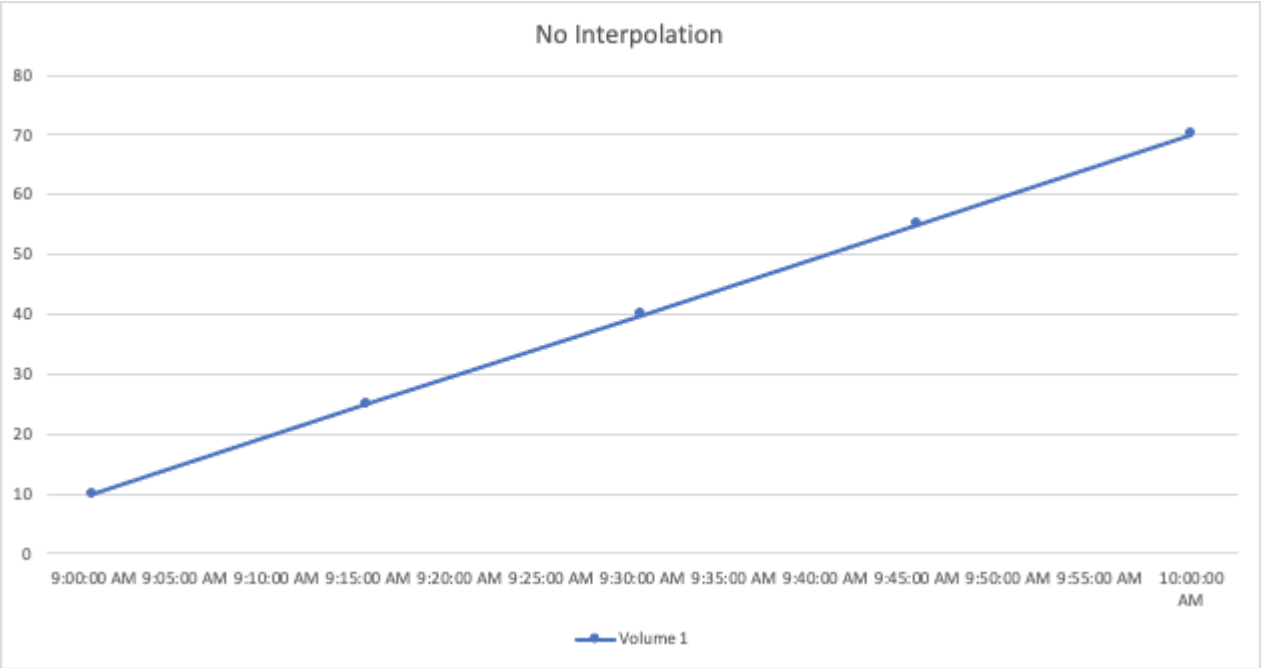
Pour remédier à ce problème, Data Infrastructure Insights interpole les données lors de l'agrégation, en utilisant les points de données environnants pour faire une « meilleure estimation » des données jusqu'à ce que les collecteurs de données effectuent une nouvelle interrogation. Vous pouvez toujours afficher les données d'objet de chaque collecteur de données individuellement en ajustant le regroupement du widget.

Méthodes d'interpolation

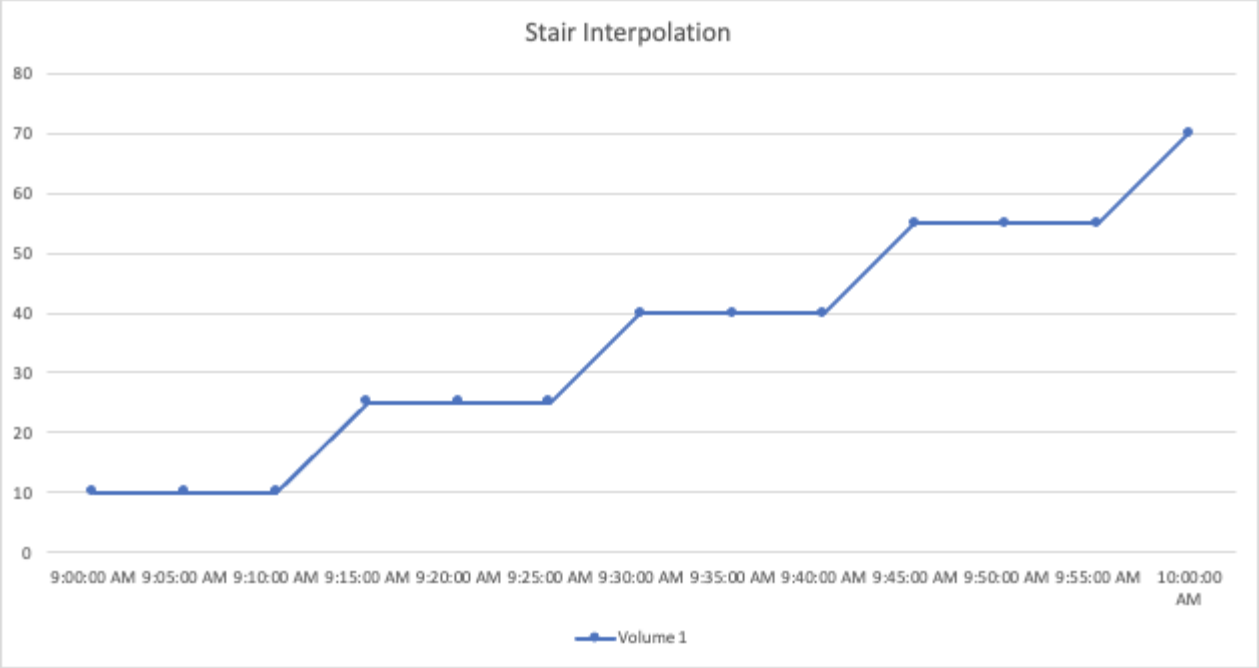
Lors de la création ou de la modification d'un graphique linéaire (ou d'un graphique spline, à aires ou à aires empilées), vous pouvez définir la méthode d'interpolation sur l'un des trois types suivants. Dans la section « Grouper par », choisissez l'interpolation souhaitée.



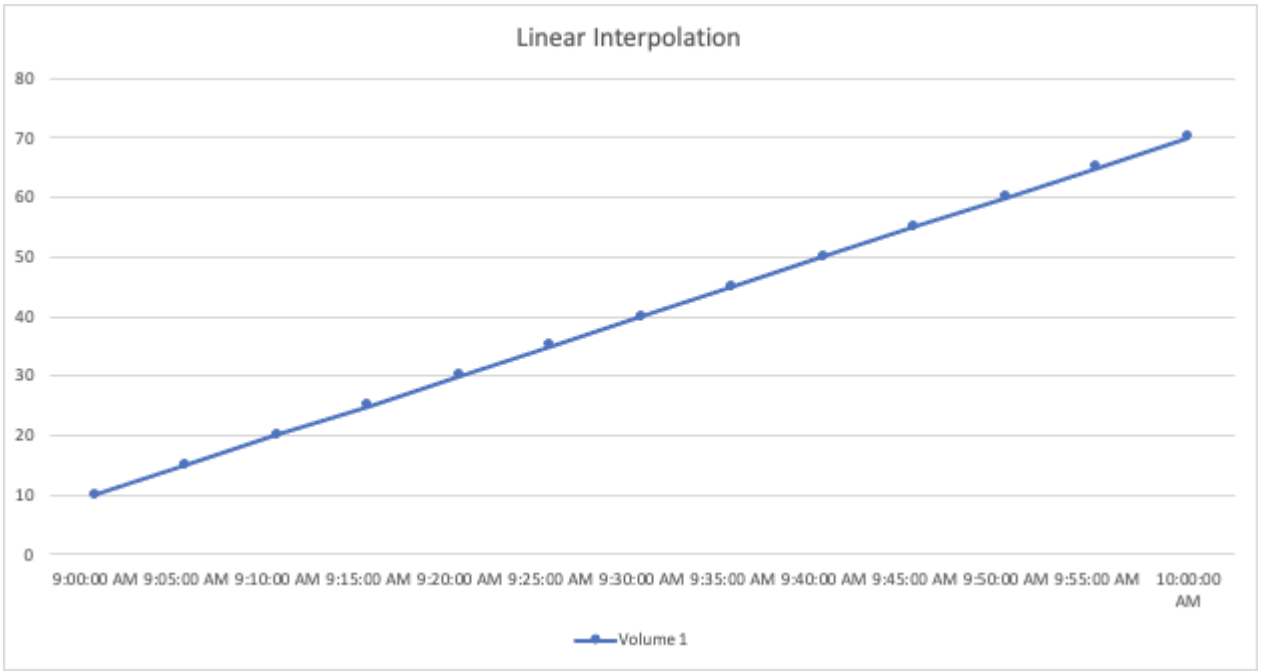
- **Aucun** : Ne rien faire, c'est-à-dire ne pas générer de points entre les deux.



- **Escalier** : Un point est généré à partir de la valeur du point précédent. En ligne droite, cela s'afficherait comme une disposition « en escalier » typique.



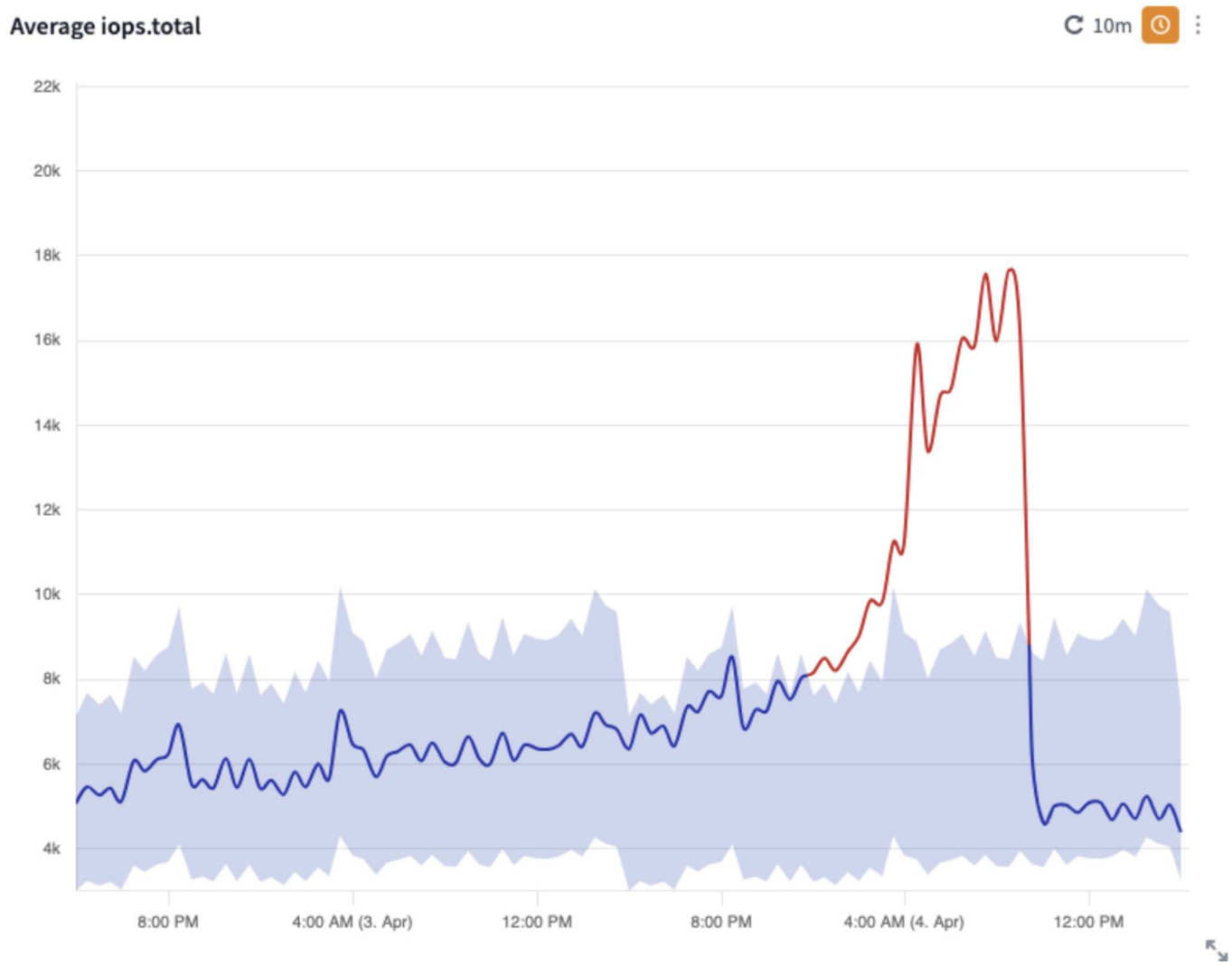
- **Linéaire** : un point est généré comme valeur entre la connexion des deux points. Génère une ligne qui ressemble à la ligne reliant les deux points, mais avec des points de données supplémentaires (interpolés).



Limites d'anomalie dans les widgets de ligne

Lorsque vous incluez un widget de graphique linéaire ou spline sur un tableau de bord ou une page de destination, vous pouvez choisir d'afficher le graphique dans le contexte des **limites attendues** pour les données. Vous pouvez considérer cela comme une recherche d'anomalies dans les modèles de vos données.

DII utilise des données saisonnières (horaires ou quotidiennes) pour définir des limites supérieures et inférieures sur lesquelles il s'attend à ce que les données tombent à un moment donné. Si les données dépassent ou chutent en dessous des limites attendues, le graphique mettra cela en évidence comme une anomalie.



Pour afficher les limites d'anomalie, modifiez le widget et choisissez *Afficher les limites d'anomalie*. Vous pouvez choisir entre deux algorithmes de détection :

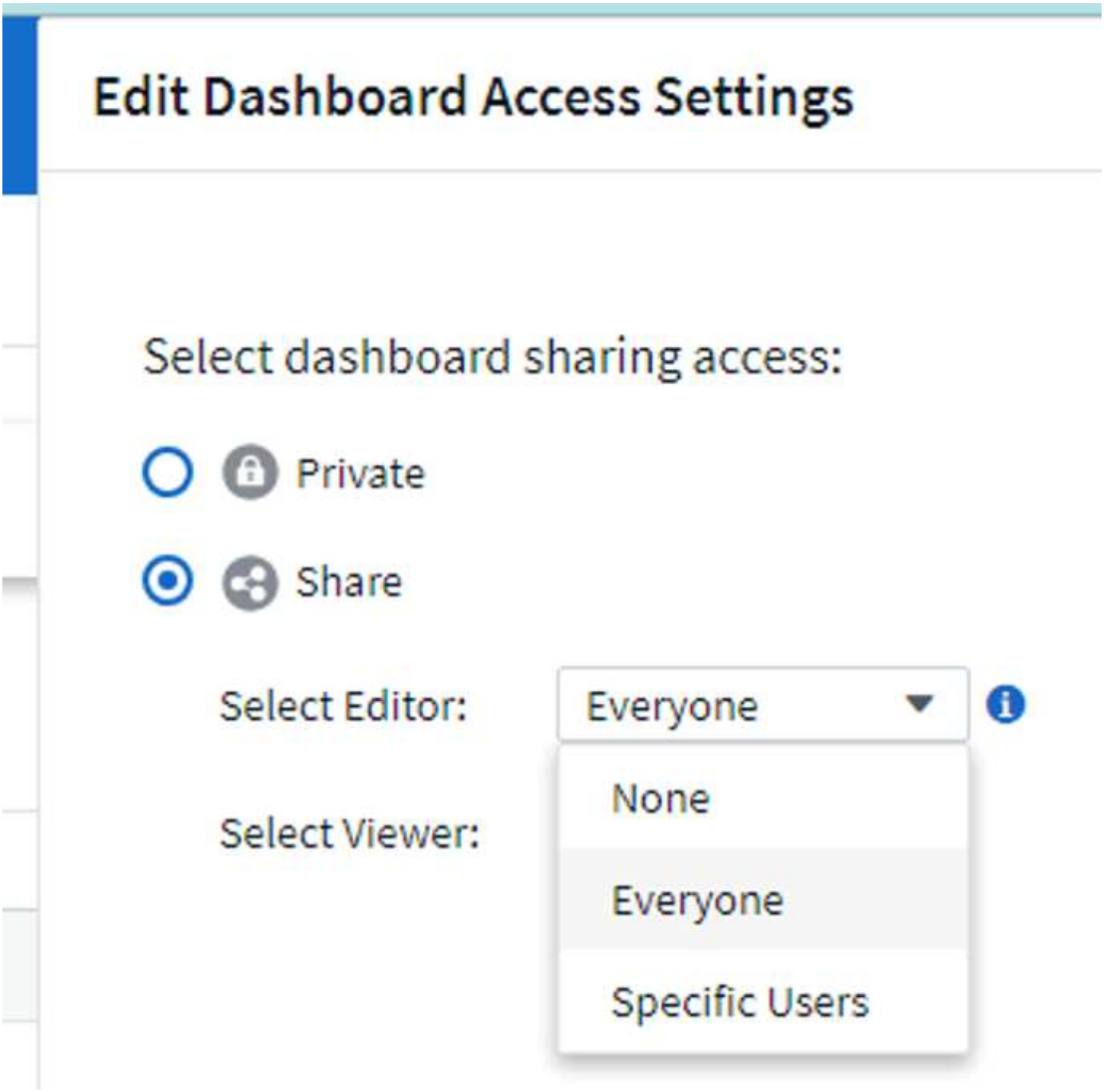
- **Détecteur adaptatif** s'adapte rapidement aux changements, ce qui le rend utile pour les enquêtes détaillées.
- **Smooth Detector** minimise le bruit et les faux positifs, filtrant les fluctuations à court terme tout en détectant les changements significatifs.

De plus, vous pouvez choisir d'afficher la saisonnalité *horaire* ou *quotidienne*, ainsi que de définir la sensibilité de détection. Une sensibilité *élevée* détecte davantage de franchissements de limites, une sensibilité *faible* en détecte moins.

Gardez à l'esprit que vous ne pouvez afficher les limites attendues que lorsque le graphique est configuré pour afficher une seule ligne. Si vos paramètres ou filtres de regroupement affichent plusieurs lignes, ou si vous avez défini plusieurs requêtes pour le widget, l'option permettant d'afficher les limites attendues sera désactivée.

Gestion des accès au tableau de bord

Data Infrastructure Insights vous offre désormais un meilleur contrôle sur l'accès aux tableaux de bord que vous créez. Vous choisissez qui peut modifier vos graphiques. Vous contrôlez l'exposition aux informations potentiellement sensibles. Garder un tableau de bord privé vous permet de finaliser vos visualisations jusqu'à ce qu'elles soient prêtes à être utilisées par d'autres personnes de votre organisation.

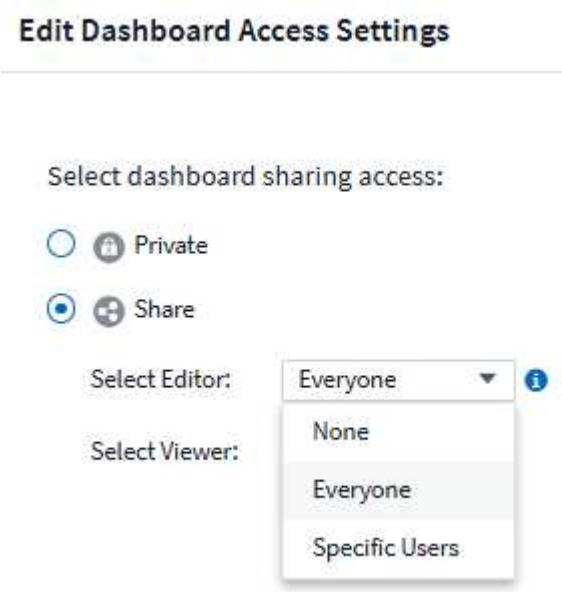


Par défaut, lorsque vous créez un nouveau tableau de bord, ce tableau de bord n'est visible que par vous, le créateur. Aucun autre utilisateur ne peut voir ou modifier le tableau de bord.

Une fois votre tableau de bord finalisé, vous pouvez choisir d'autoriser d'autres membres de votre organisation à le consulter. Pour partager un tableau de bord, dans la liste des tableaux de bord, sélectionnez *Partager*

dans le menu de droite.

Vous pouvez choisir de partager le tableau de bord avec tout le monde ou de sélectionner des utilisateurs, avec des autorisations de modification ou de lecture seule.



Bonnes pratiques pour les tableaux de bord et les widgets

Conseils et astuces pour vous aider à tirer le meilleur parti des puissantes fonctionnalités des tableaux de bord et des widgets.

Trouver la bonne métrique

Data Infrastructure Insights acquiert des compteurs et des mesures à l'aide de noms qui diffèrent parfois d'un collecteur de données à l'autre.

Lorsque vous recherchez la bonne métrique ou le bon compteur pour votre widget de tableau de bord, gardez à l'esprit que la métrique que vous souhaitez peut être sous un nom différent de celui auquel vous pensez. Bien que les listes déroulantes de Data Infrastructure Insights soient généralement classées par ordre alphabétique, il arrive qu'un terme n'apparaisse pas dans la liste là où vous pensez qu'il devrait l'être. Par exemple, des termes tels que « capacité brute » et « capacité utilisée » n'apparaissent pas ensemble dans la plupart des listes.

Meilleure pratique : utilisez la fonction de recherche dans des champs tels que Filtrer par ou des emplacements comme le sélecteur de colonnes pour trouver ce que vous cherchez. Par exemple, la recherche de « cap » affichera toutes les mesures contenant « capacité » dans leur nom, quel que soit leur emplacement

dans la liste. Vous pouvez ensuite facilement sélectionner les mesures souhaitées dans cette liste plus courte.

Voici quelques expressions alternatives que vous pouvez essayer lors de la recherche de métriques :

Lorsque vous souhaitez trouver :	Essayez également de rechercher :
processeur	Processeur
Capacité	Capacité utilisée Capacité brute Capacité provisionnée Capacité des pools de stockage <autre type d'actif> Capacité écrite
Vitesse du disque	Vitesse de disque la plus faible Type de disque le moins performant
Hôte	Hôtes hyperviseurs
Hyperviseur	L'hôte est un hyperviseur
Microcode	Micrologiciel
Nom	Alias Nom de l'hyperviseur Nom de stockage Nom de <autre type d'actif> Nom simple Nom de la ressource Fabric Alias
Lire / Écrire	Écritures partielles en attente de lecture/écriture IOPS - Capacité d'écriture Latence - Lecture Utilisation du cache - Lecture
Machine virtuelle	VM est virtuelle

Cette liste n'est pas exhaustive. Ce ne sont que des exemples de termes de recherche possibles.

Trouver les bons actifs

Les ressources que vous pouvez référencer dans les filtres et les recherches de widgets varient d'un type de ressource à l'autre.

Dans les tableaux de bord et les pages d'actifs, le type d'actif autour duquel vous construisez votre widget détermine les autres compteurs de type d'actif pour lesquels vous pouvez filtrer ou ajouter une colonne. Gardez les points suivants à l'esprit lors de la création de votre widget :

Ce type d'actif / compteur :	Peut être filtré sous ces actifs :
Machine virtuelle	VMDK
Magasin(s) de données	Volume interne Volume de machine virtuelle VMDK
Hyperviseur	La machine virtuelle est un hôte hyperviseur
Hôte(s)	Volume interne Cluster de volumes Hôte Machine virtuelle
Tissu	Port

Cette liste n'est pas exhaustive.

Meilleure pratique : Si vous filtrez un type d'actif particulier qui n'apparaît pas dans la liste, essayez de créer votre requête autour d'un autre type d'actif.

Exemple de nuage de points : connaître votre axe

La modification de l'ordre des compteurs dans un widget de nuage de points modifie les axes sur lesquels les données sont affichées.

À propos de cette tâche

Cet exemple créera un nuage de points qui vous permettra de voir les machines virtuelles sous-performantes qui ont une latence élevée par rapport aux IOPS faibles.

Étapes

1. Créez ou ouvrez un tableau de bord en mode édition et ajoutez un widget * Graphique en nuage de points *.
2. Sélectionnez un type d'actif, par exemple, *Machine virtuelle*.
3. Sélectionnez le premier compteur que vous souhaitez tracer. Pour cet exemple, sélectionnez *Latence - Total*.

   Latence - Total est représenté sur l'axe des X du graphique.

4. Sélectionnez le deuxième compteur que vous souhaitez tracer. Pour cet exemple, sélectionnez *IOPS - Total*.

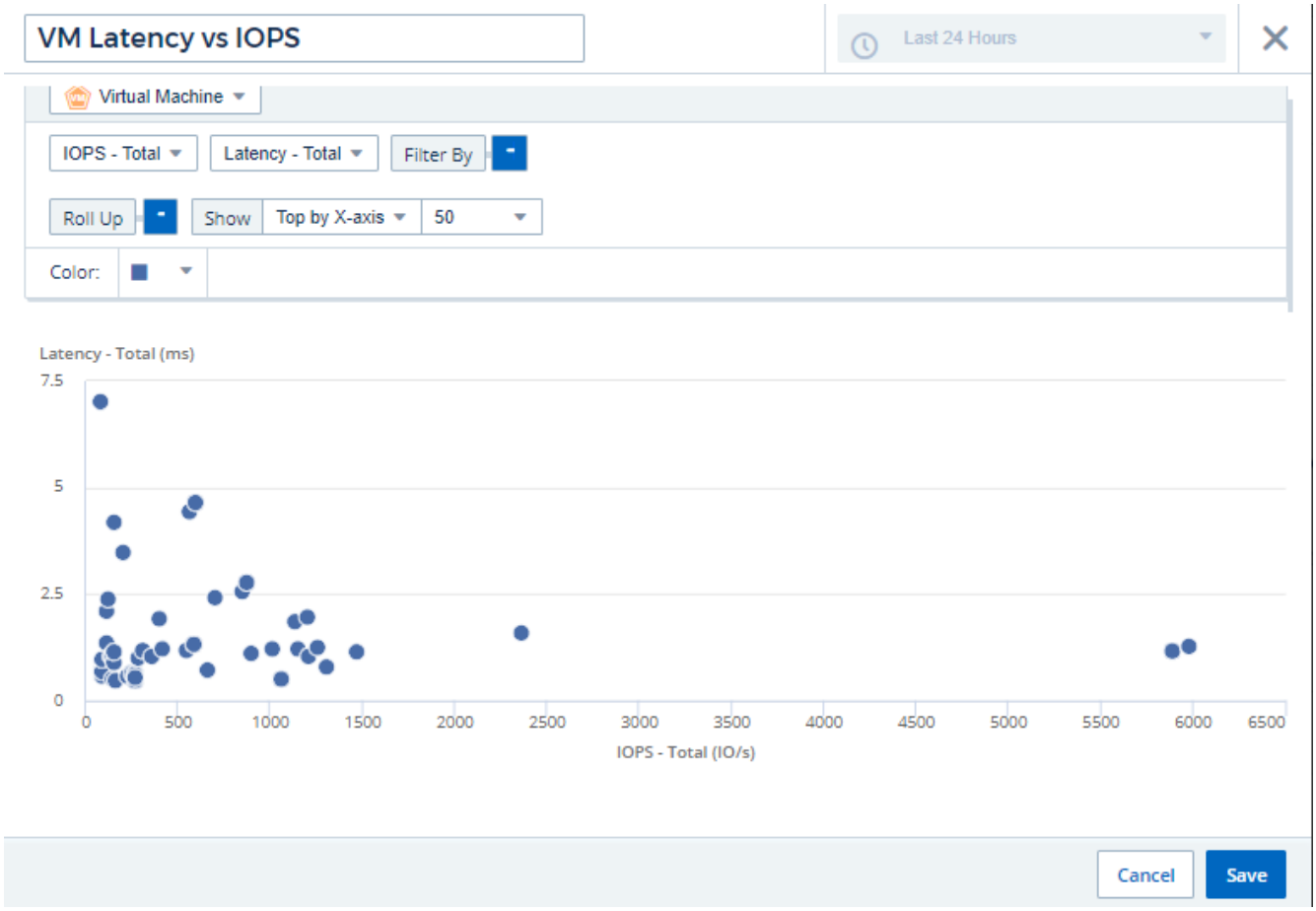
   IOPS - Total est représenté le long de l'axe Y du graphique. Les machines virtuelles avec une latence plus élevée s'affichent sur le côté droit du graphique. Seules les 100 machines virtuelles présentant la latence la plus élevée sont affichées, car le paramètre **Top par axe X** est actuel.

5. Inversez maintenant l'ordre des compteurs en définissant le premier compteur sur *IOPS - Total* et le

second sur *Latency - Total*.

Latency-Total est désormais représenté sur l'axe Y du graphique et *IOPS - Total* sur l'axe X. Les machines virtuelles avec des IOPS plus élevées s'affichent désormais sur le côté droit du graphique.

Notez que, comme nous n'avons pas modifié le paramètre **Top par axe X**, le widget affiche désormais les 100 machines virtuelles avec les IOPS les plus élevées, car c'est ce qui est actuellement tracé le long de l'axe X.



Vous pouvez choisir que le graphique affiche les N premiers sur l'axe X, les N premiers sur l'axe Y, les N derniers sur l'axe X ou les N derniers sur l'axe Y. Dans notre dernier exemple, le graphique affiche les 100 principales machines virtuelles qui ont le nombre total d'IOPS le plus élevé. Si nous le modifions en **Top par axe Y**, le graphique affichera à nouveau les 100 premières machines virtuelles qui ont la latence totale la plus élevée.

Notez que dans un graphique en nuage de points, vous pouvez cliquer sur un point pour accéder à la page d'actif de cette ressource.

Exemples de tableaux de bord

Exemple de tableau de bord : performances d'une machine virtuelle

Les opérations informatiques sont aujourd'hui confrontées à de nombreux défis. On demande aux administrateurs de faire plus avec moins, et avoir une visibilité complète sur vos centres de données dynamiques est indispensable. Dans cet exemple, nous

allons vous montrer comment créer un tableau de bord avec des widgets qui vous donnent des informations opérationnelles sur les performances de la machine virtuelle (VM) sur votre locataire. En suivant cet exemple et en créant des widgets pour cibler vos besoins spécifiques, vous pouvez effectuer des opérations telles que la visualisation des performances de stockage back-end par rapport aux performances de la machine virtuelle front-end, ou l'affichage de la latence de la machine virtuelle par rapport à la demande d'E/S.

À propos de cette tâche

Ici, nous allons créer un tableau de bord des performances de la machine virtuelle contenant les éléments suivants :

- un tableau répertoriant les noms des machines virtuelles et les données de performances
- un graphique comparant la latence des machines virtuelles à la latence du stockage
- un graphique montrant les lectures, les écritures et le total des IOPS pour les machines virtuelles
- un graphique montrant le débit maximal de vos machines virtuelles

Ceci n'est qu'un exemple de base. Vous pouvez personnaliser votre tableau de bord pour mettre en évidence et comparer toutes les données de performance que vous choisissez, afin de cibler vos propres meilleures pratiques opérationnelles.

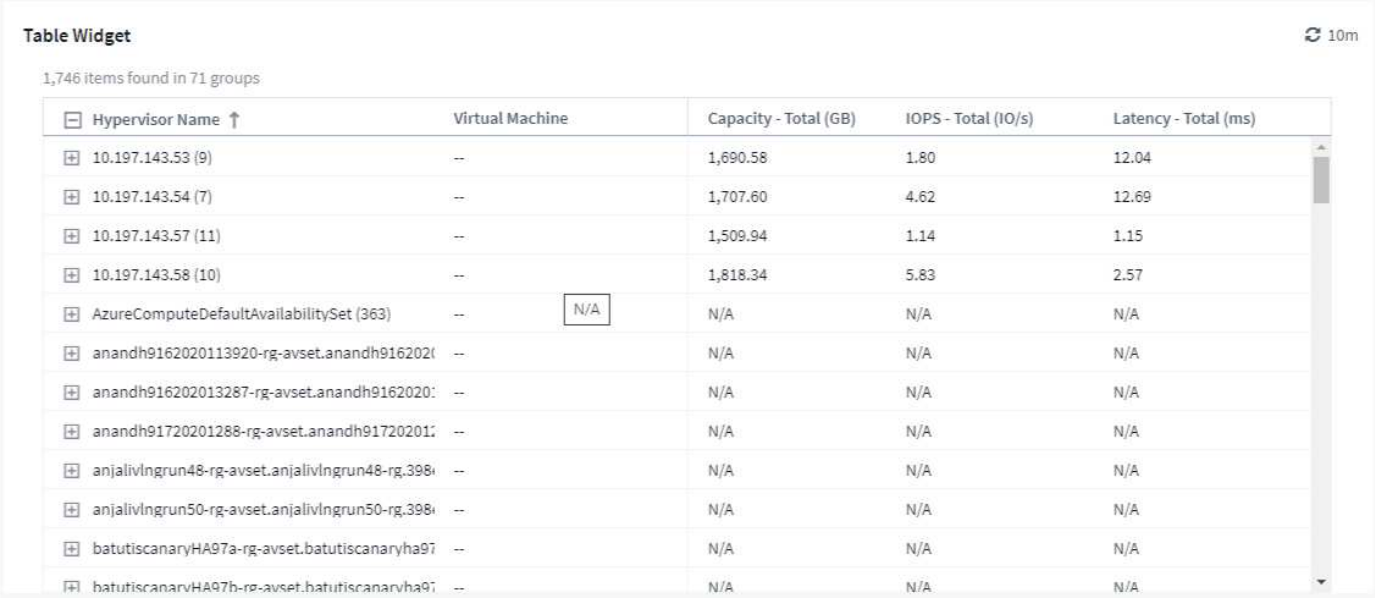
Étapes

1. Connectez-vous à Insight en tant qu'utilisateur disposant d'autorisations administratives.
2. Dans le menu **Tableaux de bord**, sélectionnez **[+Nouveau tableau de bord]**.

   La page **Nouveau tableau de bord** s'ouvre.

3. En haut de la page, saisissez un nom unique pour le tableau de bord, par exemple « Performances des machines virtuelles par application ».
4. Cliquez sur **Enregistrer** pour enregistrer le tableau de bord avec le nouveau nom.
5. Commençons à ajouter nos widgets. Si nécessaire, cliquez sur l'icône **Modifier** pour activer le mode Édition.
6. Cliquez sur l'icône **Ajouter un widget** et sélectionnez **Tableau** pour ajouter un nouveau widget de tableau au tableau de bord.

   La boîte de dialogue Modifier le widget s'ouvre. Les données par défaut affichées concernent tous les stockages de votre locataire.



1. Nous pouvons personnaliser ce widget. Dans le champ Nom en haut, supprimez « Widget 1 » et saisissez « Tableau des performances de la machine virtuelle ».
2. Cliquez sur la liste déroulante du type d'actif et remplacez *Stockage* par *Machine virtuelle*.

   Les données du tableau changent pour afficher toutes les machines virtuelles de votre locataire.

3. Ajoutons quelques colonnes au tableau. Cliquez sur l'icône d'engrenage à droite et sélectionnez *Nom de l'hyperviseur*, *IOPS - Total* et *Latence - Total*. Vous pouvez également essayer de saisir le nom dans la recherche pour afficher rapidement le champ souhaité.

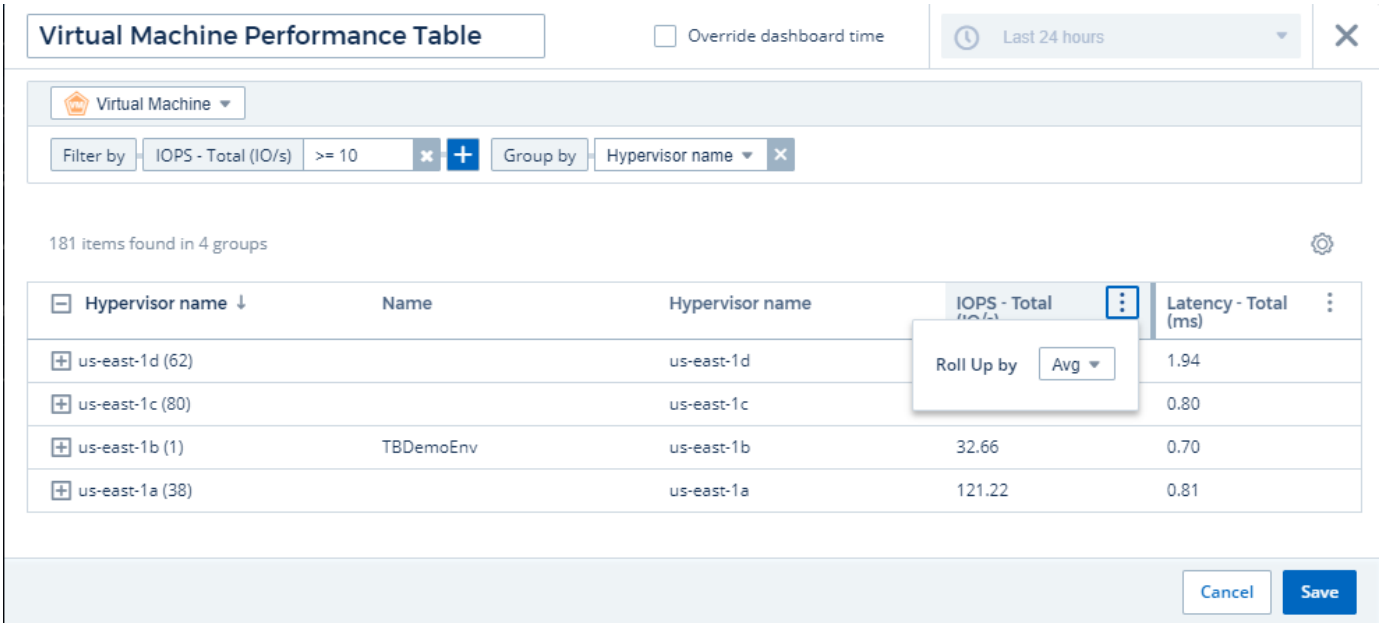
   Ces colonnes sont désormais affichées dans le tableau. Vous pouvez trier le tableau selon n'importe laquelle de ces colonnes. Notez que les colonnes sont affichées dans l'ordre dans lequel elles ont été ajoutées au widget.

4. Pour cet exercice, nous exclurons les machines virtuelles qui ne sont pas activement utilisées. Nous allons donc filtrer tout ce qui a moins de 10 IOPS au total. Cliquez sur le bouton **[+]** à côté de **Filtrer par** et sélectionnez *IOPS - Total*. Cliquez sur **N'importe lequel** et entrez « 10 » dans le champ **de**. Laissez le champ **à** vide. Cliquez en dehors du champ de filtre ou appuyez sur Entrée pour définir le filtre.

   Le tableau affiche désormais uniquement les machines virtuelles avec un total de 10 IOPS ou plus.

5. Nous pouvons encore réduire le tableau en regroupant les résultats. Cliquez sur le bouton **[+]** à côté de **Grouper par** et sélectionnez un champ par lequel regrouper, tel que *Application* ou *Nom de l'hyperviseur*. Le regroupement est appliqué automatiquement.

   Les lignes du tableau sont désormais regroupées en fonction de vos paramètres. Vous pouvez développer et réduire les groupes selon vos besoins. Les lignes groupées affichent les données cumulées pour chacune des colonnes. Certaines colonnes vous permettent de choisir la méthode de cumul pour cette colonne.



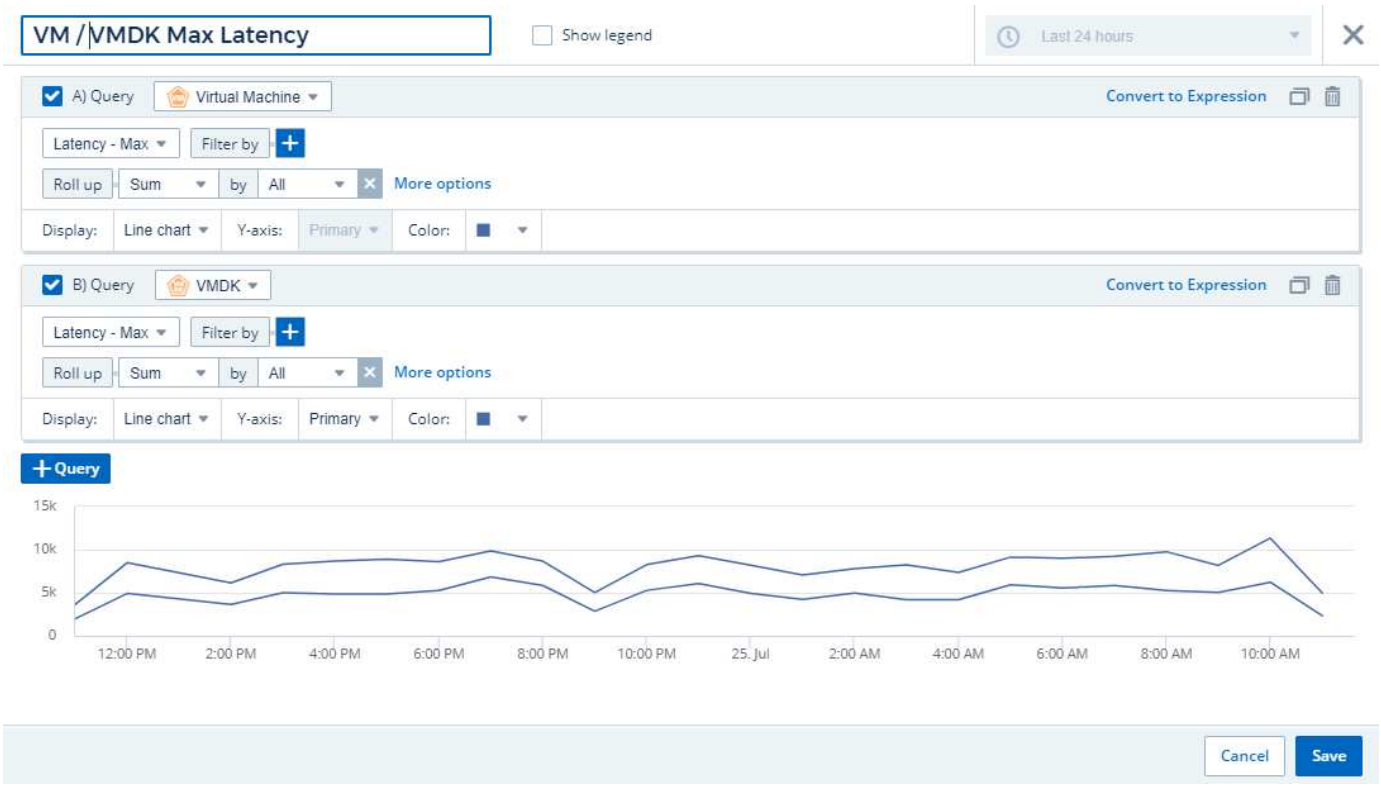
1. Lorsque vous avez personnalisé le widget de tableau à votre convenance, cliquez sur le bouton **[Enregistrer]**.

   Le widget de tableau est enregistré dans le tableau de bord.

Vous pouvez redimensionner le widget sur le tableau de bord en faisant glisser le coin inférieur droit. Agrandissez le widget pour afficher clairement toutes les colonnes. Cliquez sur **Enregistrer** pour enregistrer le tableau de bord actuel.

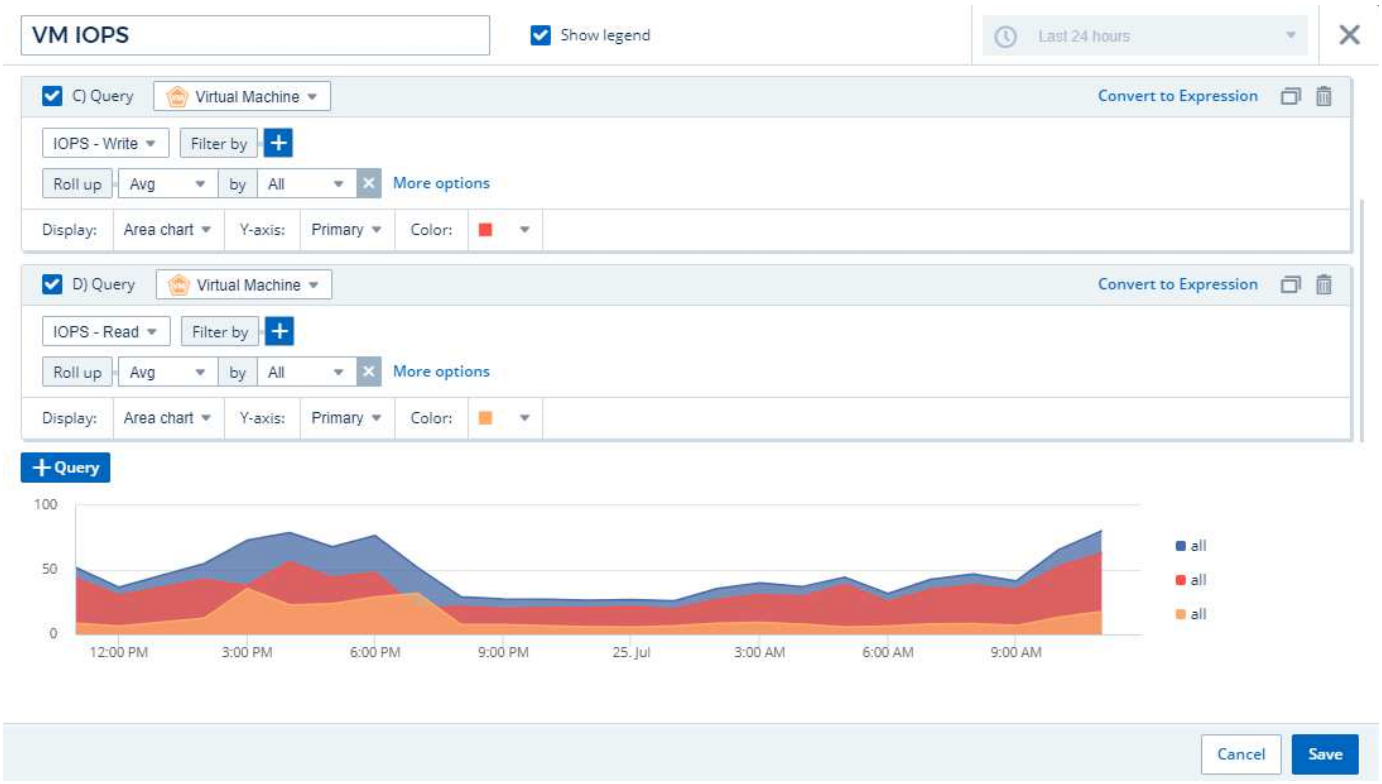
Ensuite, nous ajouterons quelques graphiques pour montrer les performances de notre machine virtuelle. Créons un graphique linéaire comparant la latence de la VM avec la latence de VMDK.

1. Si nécessaire, cliquez sur l'icône **Modifier** sur le tableau de bord pour activer le mode Édition.
2. Cliquez sur l'icône **[Ajouter un widget]** et sélectionnez *Graphique linéaire* pour ajouter un nouveau widget de graphique linéaire au tableau de bord.
3. La boîte de dialogue **Modifier le widget** s'ouvre. Nommez ce widget « VM / VMDK Max Latency »
4. Sélectionnez **Machine virtuelle** et choisissez *Latence - Max*. Définissez les filtres que vous souhaitez ou laissez **Filtrer par** vide. Pour **Regrouper**, choisissez *Somme* par *Tous*. Affichez ces données sous forme de *graphique linéaire* et laissez *axe Y* comme *principal*.
5. Cliquez sur le bouton **[+Requête]** pour ajouter une deuxième ligne de données. Pour cette ligne, sélectionnez *VMDK* et *Latency - Max*. Définissez les filtres que vous souhaitez ou laissez **Filtrer par** vide. Pour **Regrouper**, choisissez *Somme* par *Tous*. Affichez ces données sous forme de *graphique linéaire* et laissez *axe Y* comme *principal*.
6. Cliquez sur **[Enregistrer]** pour ajouter ce widget au tableau de bord.



Ensuite, nous ajouterons un graphique montrant la lecture, l'écriture et le nombre total d'IOPS de la machine virtuelle dans un seul graphique.

1. Cliquez sur l'icône **[Ajouter un widget]** et sélectionnez *Graphique en aires* pour ajouter un nouveau widget de graphique en aires au tableau de bord.
2. La boîte de dialogue Modifier le widget s'ouvre. Nommez ce widget « VM IOPS »
3. Sélectionnez **Machine virtuelle** et choisissez *IOPS - Total*. Définissez les filtres que vous souhaitez ou laissez **Filtrer par** vide. Pour **Réduire**, choisissez *Somme* par *Tous*. Affichez ces données sous forme de *graphique à aires* et laissez *axe Y* comme *principal*.
4. Cliquez sur le bouton **[+Requête]** pour ajouter une deuxième ligne de données. Pour cette ligne, sélectionnez **Machine virtuelle** et choisissez *IOPS - Lecture*.
5. Cliquez sur le bouton **[+Requête]** pour ajouter une troisième ligne de données. Pour cette ligne, sélectionnez **Machine virtuelle** et choisissez *IOPS - Écriture*.
6. Cliquez sur **Afficher la légende** pour afficher une légende pour ce widget sur le tableau de bord.



1. Cliquez sur **[Enregistrer]** pour ajouter ce widget au tableau de bord.

Ensuite, nous ajouterons un graphique montrant le débit de la machine virtuelle pour chaque application associée à la machine virtuelle. Nous utiliserons la fonction Roll Up pour cela.

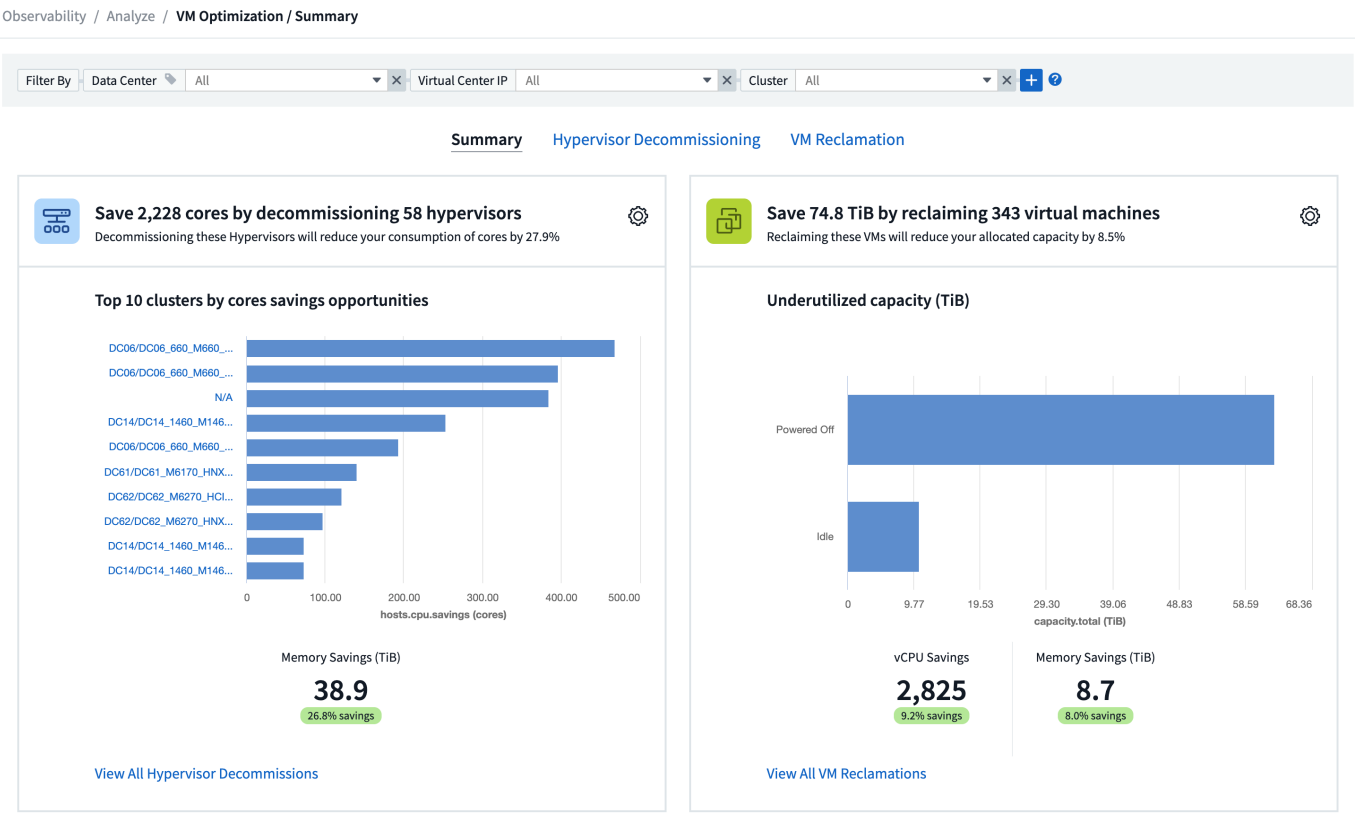
1. Cliquez sur l'icône **[Ajouter un widget]** et sélectionnez *Graphique linéaire* pour ajouter un nouveau widget de graphique linéaire au tableau de bord.
2. La boîte de dialogue Modifier le widget s'ouvre. Nommez ce widget « Débit VM par application »
3. Sélectionnez Machine virtuelle et choisissez Débit - Total. Définissez les filtres souhaités ou laissez Filtrer par vide. Pour Roll up, choisissez « Max » et sélectionnez par « Application » ou « Nom ». Afficher les 10 meilleures applications. Affichez ces données sous forme de graphique linéaire et laissez l'axe Y comme axe principal.
4. Cliquez sur **[Enregistrer]** pour ajouter ce widget au tableau de bord.

Vous pouvez déplacer des widgets sur le tableau de bord en maintenant le bouton de la souris enfoncé n'importe où en haut du widget et en le faisant glisser vers un nouvel emplacement.

Vous pouvez redimensionner les widgets en faisant glisser le coin inférieur droit.

Assurez-vous de **[Enregistrer]** le tableau de bord après avoir effectué vos modifications.

Votre tableau de bord final des performances de la machine virtuelle ressemblera à ceci :



Travailler avec des requêtes

Interrogation des assets et des métriques

Interrogez les ressources physiques et virtuelles de votre infrastructure pour surveiller les performances, résoudre les problèmes et effectuer des recherches précises selon des critères personnalisés comme des annotations. Data Infrastructure Insights permet d'interroger différents types de ressources — des baies de stockage et hôtes aux applications et machines virtuelles — ainsi que d'intégrer des indicateurs provenant de Kubernetes, Docker et ONTAP Advanced Data pour une visibilité complète.

Notez que les règles d'annotation, qui attribuent automatiquement des annotations aux ressources, nécessitent une requête partagée avec tout le monde. Voir ci-dessous pour plus d'informations sur le partage des requêtes.

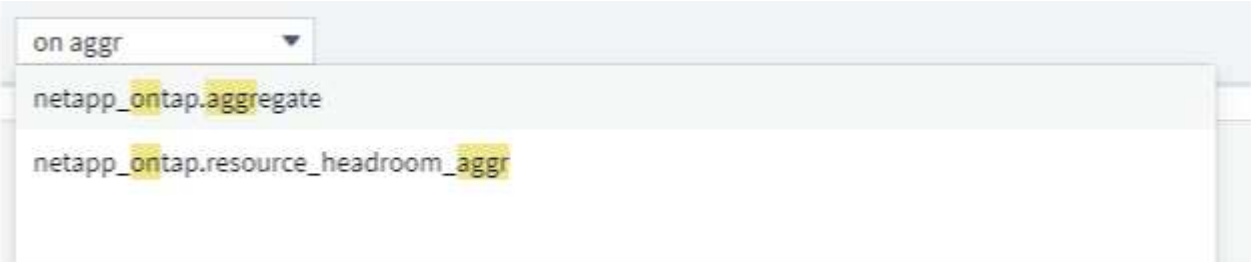
Vous pouvez interroger les actifs d'inventaire physiques ou virtuels (et leurs métriques associées) sur votre locataire, ou les métriques fournies avec l'intégration telle que Kubernetes ou ONTAP Advanced Data.

Actifs d'inventaire

Tous les types d'actifs d'inventaire (également appelés infrastructure) (stockage, switch, VM, Application, etc.) peuvent être utilisés dans les requêtes, les widgets de tableau de bord et les pages d'accueil personnalisées des actifs. Les champs et compteurs disponibles pour les filtres, les expressions et l'affichage varient selon les types d'actifs.

Mesures d'intégration

Outre l'interrogation des actifs d'inventaire et de leurs mesures de performances associées, vous pouvez également interroger les mesures de **données d'intégration**, telles que celles générées par Kubernetes ou Docker, ou fournies avec ONTAP Advanced Metrics.



Partage de requêtes

Contrôlez l'accès à vos requêtes en choisissant qui peut les consulter et les modifier. Par défaut, les nouvelles requêtes sont privées et visibles uniquement par vous, et vous pouvez choisir de les partager avec des utilisateurs spécifiques ou avec l'ensemble de votre organisation grâce à des niveaux d'autorisation flexibles (lecture seule ou modification).

Vous pouvez choisir de partager la requête avec Everyone ou avec certains utilisateurs, avec des autorisations de modification ou de lecture seule.

Les utilisateurs disposant de l'autorisation Account Owner peuvent voir toutes les requêtes, quel que soit le paramètre de confidentialité.

Créer des requêtes

Les requêtes vous permettent de rechercher les actifs de votre locataire à un niveau granulaire, ce qui vous permet de filtrer les données souhaitées et de trier les résultats à votre guise.

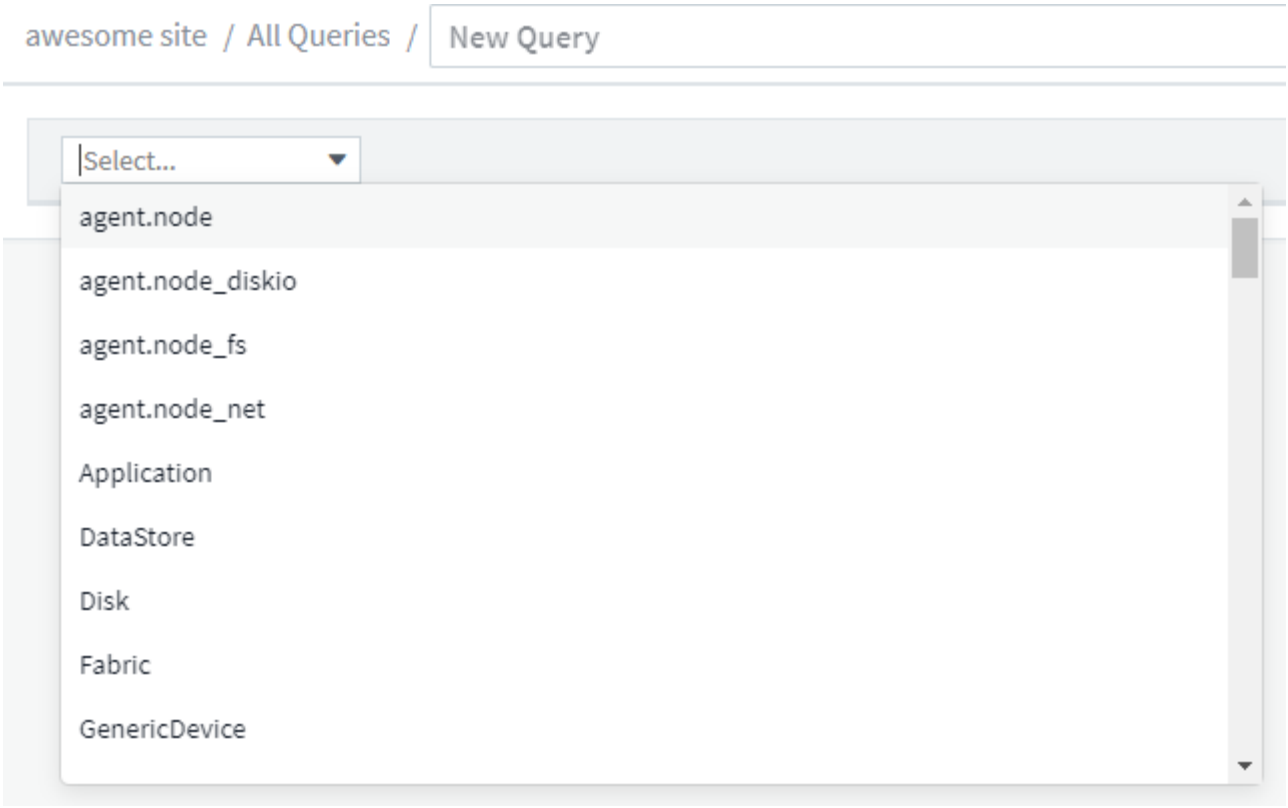
Par exemple, vous pouvez créer une requête pour les *volumes*, ajouter un filtre pour rechercher des *stockages* particuliers associés aux volumes sélectionnés, ajouter un autre filtre pour rechercher une *annotation* particulière telle que « Niveau 1 » sur les stockages sélectionnés, et enfin ajouter un autre filtre pour rechercher tous les stockages avec *IOPS - Lecture (IO/s)* supérieur à 25. Lorsque les résultats sont affichés, vous pouvez ensuite trier les colonnes d'informations associées à la requête par ordre croissant ou décroissant.

Remarque : lorsqu'un nouveau collecteur de données est ajouté et acquiert des ressources, ou que des annotations ou des affectations d'application sont effectuées, vous pouvez interroger ces nouvelles ressources, annotations ou applications uniquement après l'indexation des requêtes. L'indexation se produit à un intervalle régulier ou lors de certains événements tels que l'exécution de règles d'annotation.

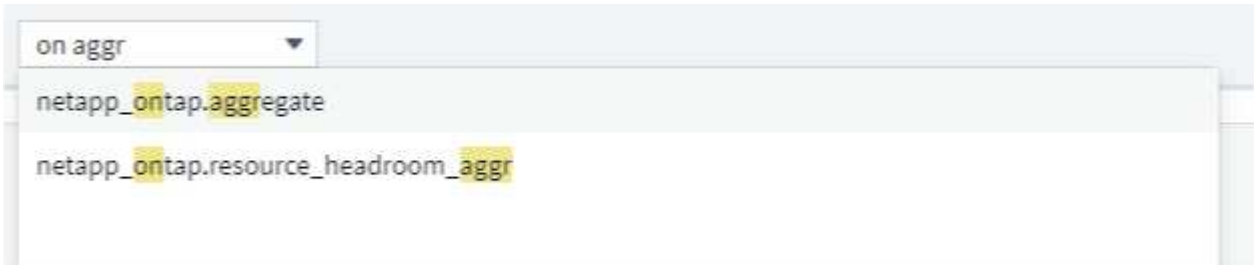
Créer une requête est très simple :

1. Accédez à **Requêtes > *+Nouvelle requête**.
2. Dans la liste « Sélectionner… », sélectionnez le type d'objet que vous souhaitez interroger. Vous pouvez faire défiler la liste ou commencer à taper pour trouver plus rapidement ce que vous recherchez.

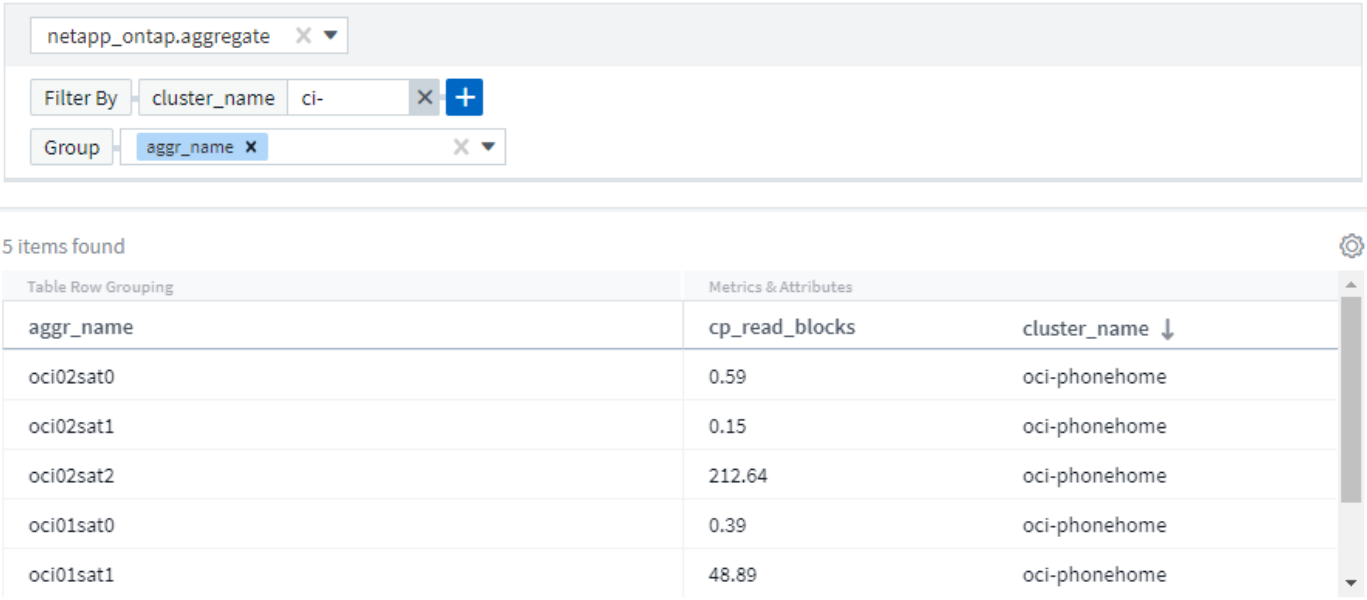
Liste déroulante :



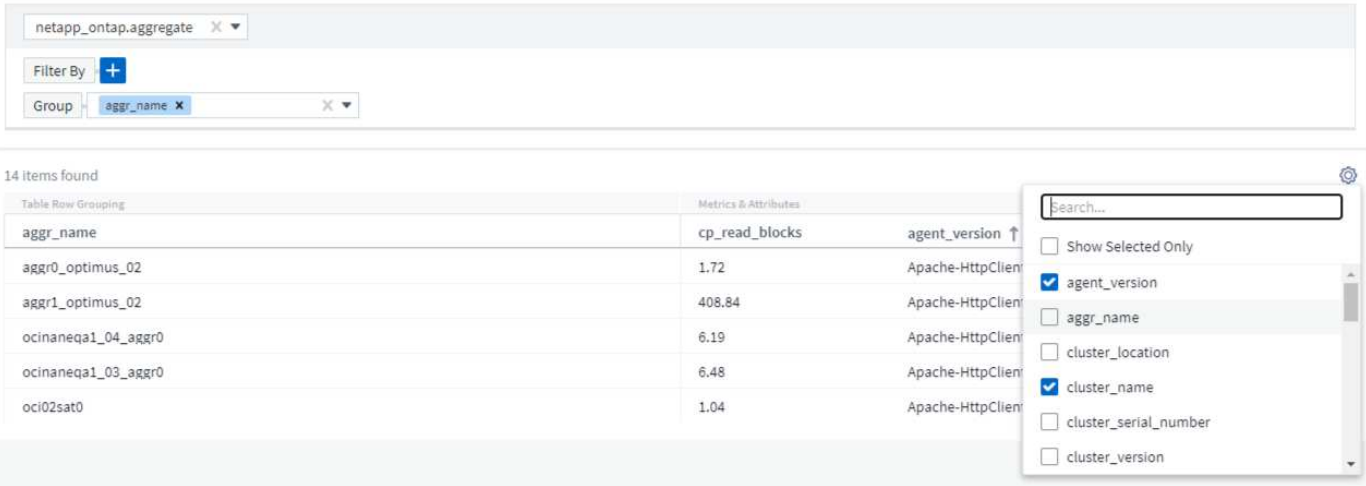
Tapez pour rechercher :



Vous pouvez ajouter des filtres pour affiner davantage votre requête en cliquant sur le bouton **+** dans le champ **Filtrer par**. Regrouper les lignes par objet ou par attribut. Lorsque vous travaillez avec des données d'intégration (Kubernetes, ONTAP Advanced Metrics, etc.), vous pouvez regrouper par plusieurs attributs, si vous le souhaitez.



La liste des résultats de la requête affiche un certain nombre de colonnes par défaut, en fonction du type d'objet recherché. Pour ajouter, supprimer ou modifier les colonnes, cliquez sur l'icône d'engrenage à droite du tableau. Les colonnes disponibles varient en fonction du type d'actif/métrique.



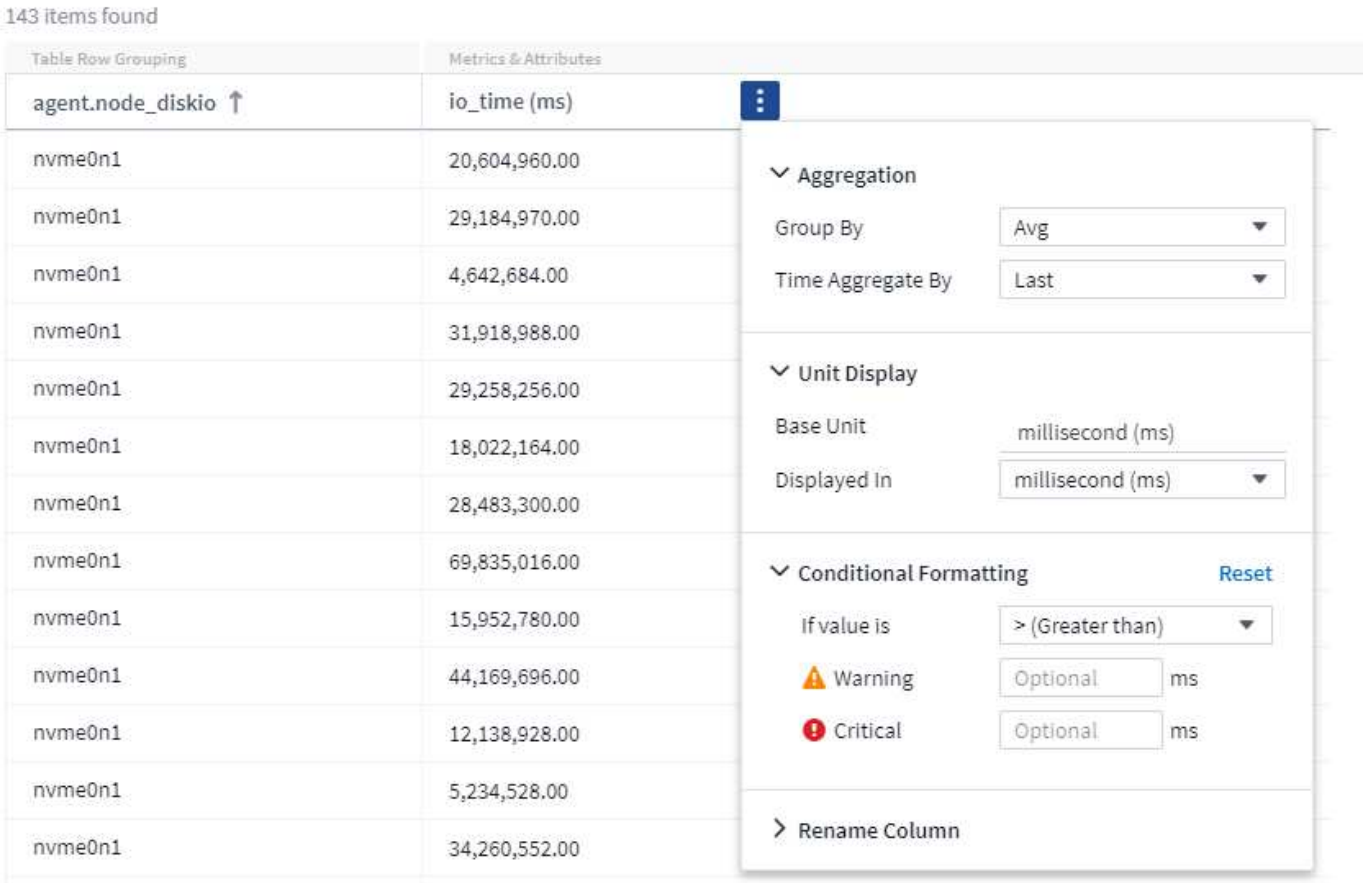
Voyez-le en action

"Explorer et analyser avec des requêtes dans Data Infrastructure Insights (Vidéo)"

Choix de l'agrégation, des unités et de la mise en forme conditionnelle

Agrégation et unités

Pour les colonnes « valeur », vous pouvez affiner davantage les résultats de votre requête en choisissant la manière dont les valeurs affichées sont agrégées ainsi qu'en sélectionnant les unités dans lesquelles ces valeurs sont affichées. Ces options se trouvent en sélectionnant le menu « trois points » dans le coin supérieur d'une colonne.



Unités

Vous pouvez sélectionner les unités dans lesquelles afficher les valeurs. Par exemple, si la colonne sélectionnée affiche la capacité brute et que les valeurs sont affichées en Gio, mais que vous préférez les afficher en Tio, sélectionnez simplement Tio dans la liste déroulante Affichage de l'unité.

Agrégation

De la même manière, si les valeurs affichées sont agrégées à partir des données sous-jacentes sous la forme « Moyenne », mais que vous préférez afficher la somme de toutes les valeurs, sélectionnez « Somme » dans la liste déroulante *Grouper par* (si vous souhaitez que les valeurs groupées affichent les sommes) ou dans la liste déroulante *Agréger par heure* (si vous souhaitez que les valeurs de ligne affichent les sommes des données sous-jacentes).

Vous pouvez choisir d'agréger des points de données groupés par *Moyenne, Max, Min ou Somme*.

Vous pouvez regrouper les données de lignes individuelles par *Moyenne, Dernier point de données acquis, Maximum, Minimum ou Somme*.

Mise en forme conditionnelle

La mise en forme conditionnelle vous permet de mettre en évidence les seuils de niveau d'avertissement et de niveau critique dans la liste des résultats de la requête, offrant ainsi une visibilité instantanée sur les valeurs aberrantes et les points de données exceptionnels.

La mise en forme conditionnelle est définie séparément pour chaque colonne. Par exemple, vous pouvez choisir un ensemble de seuils pour une colonne de capacité et un autre ensemble pour une colonne de débit.

Renommer la colonne

Renommer une colonne modifie le nom affiché dans la liste des résultats de la requête. Le nouveau nom de colonne est également affiché dans le fichier résultant si vous exportez la liste de requêtes au format .CSV.

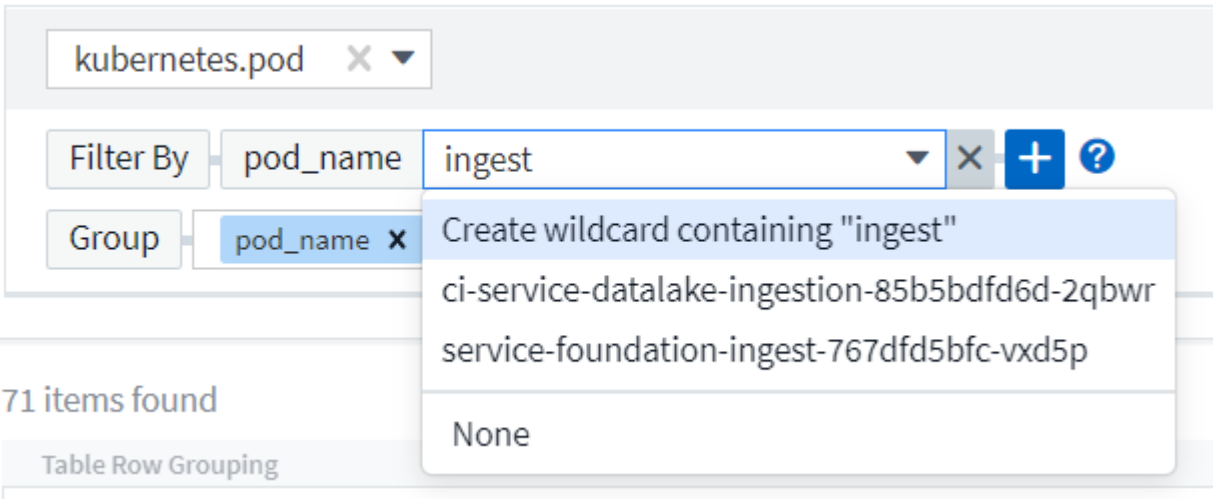
Enregistrer

Après avoir configuré votre requête pour afficher les résultats souhaités, vous pouvez cliquer sur le bouton **Enregistrer** pour enregistrer la requête pour une utilisation ultérieure. Donnez-lui un nom significatif et unique.

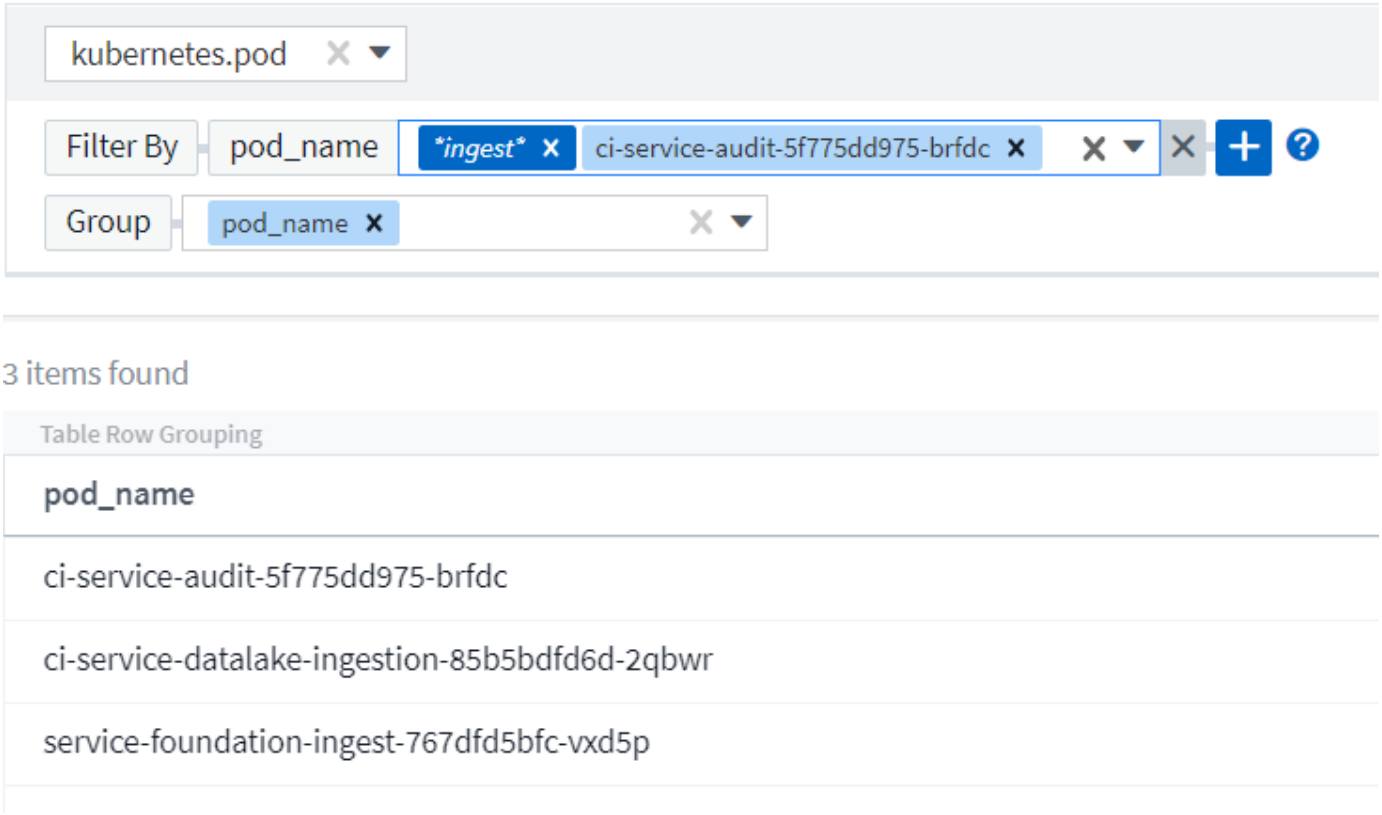
En savoir plus sur le filtrage

Caractères génériques et expressions

Lorsque vous filtrez des valeurs de texte ou de liste dans des requêtes ou des widgets de tableau de bord, lorsque vous commencez à saisir, vous avez la possibilité de créer un **filtre générique** basé sur le texte actuel. La sélection de cette option renverra tous les résultats correspondant à l'expression générique. Vous pouvez également créer des **expressions** en utilisant NOT ou OR, ou vous pouvez sélectionner l'option « Aucun » pour filtrer les valeurs nulles dans le champ.



Les filtres basés sur des caractères génériques ou des expressions (par exemple NOT, OR, « Aucun », etc.) s'affichent en bleu foncé dans le champ de filtre. Les éléments que vous sélectionnez directement dans la liste sont affichés en bleu clair.



Notez que le filtrage par caractères génériques et par expressions fonctionne avec du texte ou des listes, mais pas avec des nombres, des dates ou des booléens.

Filtres de raffinage

Vous pouvez utiliser les éléments suivants pour affiner votre filtre :

Filtre	Ce qu'il fait	Exemple	Résultat
* (Astérisque)	vous permet de rechercher tout ce que vous voulez	vol*rhel	renvoie toutes les ressources commençant par « vol » et se terminant par « rhel »
? (point d'interrogation)	vous permet de rechercher un nombre spécifique de caractères	BOS-PRD??-S12	renvoie BOS-PRD***12***-S12, BOS-PRD***23***-S12, et ainsi de suite
OU	vous permet de spécifier plusieurs entités	FAS2240 OU CX600 OU FAS3270	renvoie l'un des FAS2440, CX600 ou FAS3270
PAS	vous permet d'exclure du texte des résultats de recherche	NON EMC*	renvoie tout ce qui ne commence pas par « EMC »

Aucun	recherche les valeurs NULL dans tous les champs	*Aucun*	renvoie les résultats lorsque le champ cible est vide
Pas *	recherche les valeurs NULL dans les champs *texte uniquement*	Pas *	renvoie les résultats lorsque le champ cible est vide

Si vous placez une chaîne de filtre entre guillemets doubles, Insight traite tout ce qui se trouve entre le premier et le dernier guillemet comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs à l'intérieur des guillemets seront traités comme des littéraux. Par exemple, le filtrage par « * » renverra des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OR et NOT seront également traités comme des chaînes littérales lorsqu'ils sont placés entre guillemets.

Filtrage des valeurs booléennes

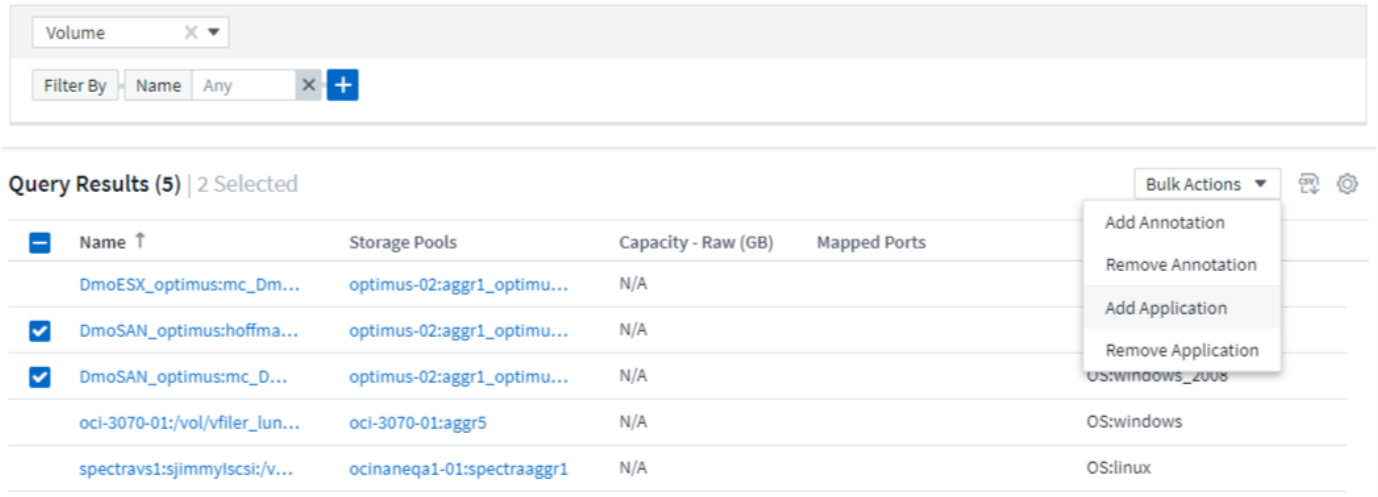
Lorsque vous filtrez une valeur booléenne, les choix suivants peuvent vous être proposés pour filtrer :

- **Tout** : cela renverra *tous* les résultats, y compris les résultats définis sur « Oui », « Non » ou pas définis du tout.
- **Oui** : renvoie uniquement les résultats « Oui ». Notez que DII affiche « Oui » comme coche dans la plupart des tableaux. Les valeurs peuvent être définies sur « Vrai », « Activé », etc. DII traite toutes ces valeurs comme « Oui ».
- **Non** : renvoie uniquement les résultats « Non ». Notez que DII affiche « Non » sous la forme d'un « X » dans la plupart des tableaux. Les valeurs peuvent être définies sur « Faux », « Désactivé », etc. DII traite toutes ces valeurs comme « Non ».
- **Aucun** : renvoie uniquement les résultats pour lesquels la valeur n'a pas été définie du tout. Également appelées valeurs « nulles ».

Que dois-je faire maintenant que j'ai les résultats de la requête ?

L'interrogation fournit un endroit simple pour ajouter des annotations ou attribuer des applications à des actifs. Notez que vous ne pouvez attribuer des applications ou des annotations qu'à vos ressources d'inventaire (disque, stockage, etc.). Les mesures d'intégration ne peuvent pas prendre en charge les annotations ou les affectations d'application.

Pour attribuer une annotation ou une application aux ressources résultant de votre requête, sélectionnez simplement la ou les ressources à l'aide de la colonne de cases à cocher à gauche du tableau des résultats, puis cliquez sur le bouton **Actions en masse** à droite. Choisissez l'action souhaitée à appliquer aux actifs sélectionnés.



Les règles d'annotation nécessitent une requête

Si vous configurez"Règles d'annotation" , chaque règle doit avoir une requête sous-jacente avec laquelle travailler. Mais comme vous l'avez vu ci-dessus, les requêtes peuvent être aussi larges ou aussi étroites que vous le souhaitez.

Consultation des requêtes

Vous pouvez afficher vos requêtes pour surveiller vos actifs et modifier la manière dont vos requêtes affichent les données liées à vos actifs.

Étapes

1. Connectez-vous à votre locataire Data Infrastructure Insights .
2. Cliquez sur **Requêtes** et sélectionnez **Afficher toutes les requêtes**. Vous pouvez modifier la façon dont les requêtes s'affichent en effectuant l'une des opérations suivantes :
3. Vous pouvez saisir du texte dans la zone de filtre pour rechercher et afficher des requêtes spécifiques.
4. Vous pouvez modifier l'ordre de tri des colonnes dans le tableau des requêtes en ordre croissant (flèche vers le haut) ou décroissant (flèche vers le bas) en cliquant sur la flèche dans l'en-tête de la colonne.
5. Pour redimensionner une colonne, passez la souris sur l'en-tête de la colonne jusqu'à ce qu'une barre bleue apparaisse. Placez la souris sur la barre et faites-la glisser vers la droite ou vers la gauche.
6. Pour déplacer une colonne, cliquez sur l'en-tête de la colonne et faites-le glisser vers la droite ou vers la gauche.

Lorsque vous faites défiler les résultats de la requête, sachez que les résultats peuvent changer à mesure que Data Infrastructure Insights interroge automatiquement vos collecteurs de données. Cela peut entraîner l'absence de certains éléments ou l'affichage de certains éléments dans le désordre, selon la façon dont ils sont triés.

Exportation des résultats de la requête vers un fichier .CSV

Vous pouvez exporter les résultats de n'importe quelle requête vers un fichier .CSV, ce qui vous permettra d'analyser les données ou de les importer dans une autre application.

Étapes

1. Connectez-vous à Data Infrastructure Insights.
2. Cliquez sur **Requêtes** et sélectionnez **Afficher toutes les requêtes**.

   La page Requêtes s'affiche.

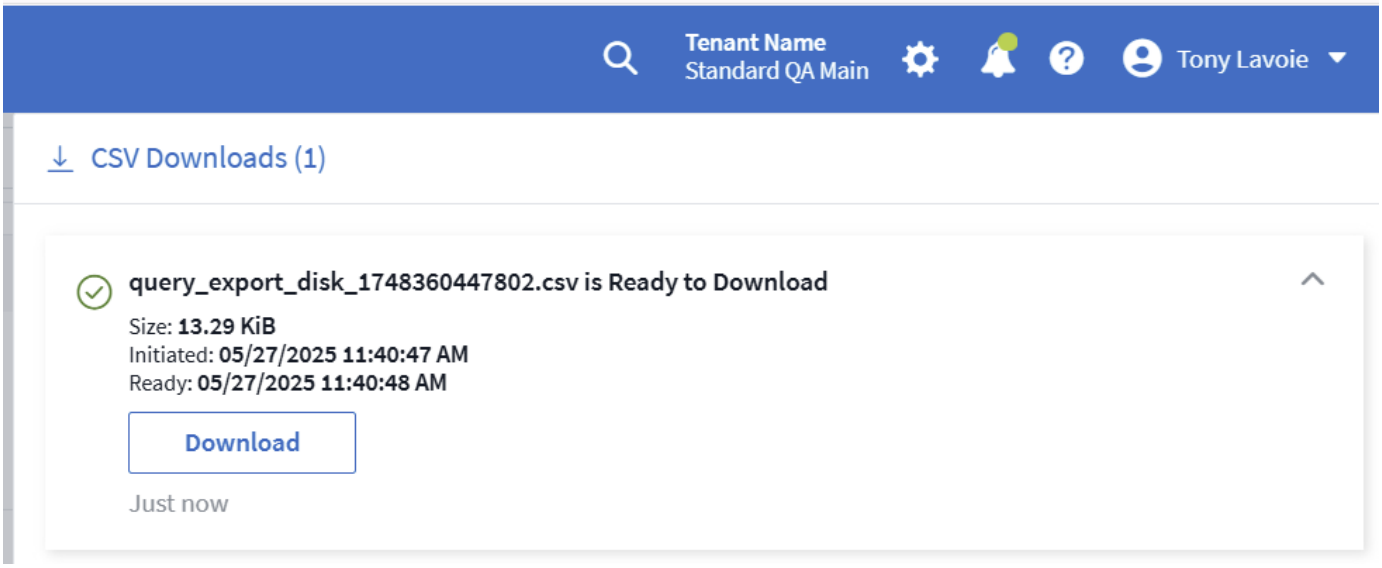
3. Cliquez sur une requête.
4. Cliquez pour exporter les résultats de la requête vers un fichier .CSV.

L'exportation vers .CSV est également disponible dans le menu « trois points » des widgets de tableau de bord ainsi que dans la plupart des tableaux de page de destination.

Exportation asynchrone

L'exportation de données au format .CSV peut prendre de quelques secondes à plusieurs heures, selon la quantité de données à exporter. Data Infrastructure Insights exporte ces données de manière asynchrone, ce qui vous permet de continuer à travailler pendant la compilation du fichier .CSV.

Affichez et téléchargez vos exportations .CSV en sélectionnant l'icône « Cloche » dans la barre d'outils en haut à droite.



Les données exportées refléteront le filtrage actuel, les colonnes et les noms de colonnes affichés.

Virgules dans les noms d'actifs

Remarque : lorsqu'une virgule apparaît dans le nom d'un actif, l'exportation place le nom entre guillemets, préservant ainsi le nom de l'actif et le format .csv approprié.

Format de l'heure ou pas format de l'heure ?

Lors de l'ouverture d'un fichier .CSV exporté avec Excel, si vous avez un nom d'objet ou un autre champ au format NN:NN (deux chiffres suivis de deux points suivis de deux autres chiffres), Excel interprétera parfois ce nom comme un format d'heure, au lieu d'un format de texte. Cela peut entraîner l'affichage par Excel de valeurs incorrectes dans ces colonnes. Par exemple, un objet nommé « 81:45 » s'afficherait dans Excel sous la forme « 81:45:00 ».

Pour contourner ce problème, importez le fichier .CSV dans Excel en suivant les étapes suivantes :

1. Ouvrez une nouvelle feuille dans Excel.
2. Dans l'onglet « Données », choisissez « À partir du texte ».
3. Localisez le fichier .CSV souhaité et cliquez sur « Importer ».
4. Dans l'assistant d'importation, choisissez « Délimité » et cliquez sur Suivant.
5. Choisissez « Virgule » comme délimiteur et cliquez sur Suivant.
6. Sélectionnez les colonnes souhaitées et choisissez « Texte » pour le format des données de la colonne.
7. Cliquez sur Terminer.

   Vos objets doivent s'afficher dans Excel au format approprié.

Modifier ou supprimer une requête

Vous pouvez modifier les critères associés à une requête lorsque vous souhaitez modifier les critères de recherche des actifs que vous interrogez.

Modifier une requête

Étapes

1. Cliquez sur **Explorer** et sélectionnez **Toutes les requêtes de métriques**.

   La page Requêtes s'affiche.

2. Cliquez sur le nom de la requête
3. Pour ajouter un critère à la requête, cliquez sur l'icône Colonnes et sélectionnez une métrique ou un attribut dans la liste.

Une fois que vous avez effectué toutes les modifications nécessaires, effectuez l'une des opérations suivantes :

- Cliquez sur le bouton **Enregistrer** pour enregistrer la requête avec le nom utilisé initialement.
- Cliquez sur le menu déroulant à côté du bouton **Enregistrer** et sélectionnez **Enregistrer sous** pour enregistrer la requête sous un autre nom. Cela n'écrase pas la requête d'origine.
- Cliquez sur le menu déroulant à côté du bouton **Enregistrer** et sélectionnez **Renommer** pour modifier le nom de la requête que vous aviez utilisé initialement. Cela écrase la requête d'origine.
- Cliquez sur le menu déroulant à côté du bouton **Enregistrer** et sélectionnez **Annuler les modifications** pour rétablir la requête aux dernières modifications enregistrées.

Suppression d'une requête

Pour supprimer une requête, cliquez sur **Requêtes** et sélectionnez **Afficher toutes les requêtes**, puis effectuez l'une des opérations suivantes :

1. Cliquez sur le menu « trois points » à droite de la requête et cliquez sur **Supprimer**.
2. Cliquez sur le nom de la requête et sélectionnez **Supprimer** dans le menu déroulant **Enregistrer**.

Affectation ou suppression de plusieurs applications à des actifs

Vous pouvez attribuer plusieurs"applications" pour supprimer plusieurs applications des

actifs à l'aide d'une requête au lieu de devoir les attribuer ou les supprimer manuellement.

Vous pouvez utiliser ces étapes pour ajouter ou supprimer"annotations" de la même façon.

Avant de commencer

Vous devez déjà avoir créé une requête qui trouve tous les actifs que vous souhaitez modifier.

Étapes

1. Cliquez sur **Explorer** et sélectionnez **Requêtes métriques**.

   La page Requêtes s'affiche.

2. Cliquez sur le nom de la requête qui recherche les actifs.

   La liste des actifs associés à la requête s'affiche.

3. Sélectionnez les actifs souhaités dans la liste ou cliquez sur la case à cocher supérieure pour sélectionner Tous.

   La liste déroulante Actions en masse s'affiche.

4. Pour ajouter une application aux ressources sélectionnées, cliquez sur Actions groupées et sélectionnez **Ajouter une application**.
5. Sélectionnez une ou plusieurs applications.

   Vous pouvez sélectionner plusieurs applications pour les hôtes, les volumes internes, les qtrees et les machines virtuelles ; cependant, vous ne pouvez sélectionner qu'une seule application pour un volume ou un partage.

6. Cliquez sur **Enregistrer**.
7. Pour supprimer une application attribuée aux actifs, cliquez sur Actions groupées et sélectionnez **Supprimer l'application**.
8. Sélectionnez l'application ou les applications que vous souhaitez supprimer.
9. Cliquez sur **Supprimer**.

Toutes les nouvelles applications que vous attribuez remplacent toutes les applications de l'actif dérivées d'un autre actif. Par exemple, les volumes héritent des applications des hôtes et lorsque de nouvelles applications sont attribuées à un volume, la nouvelle application a la priorité sur l'application dérivée.

Après avoir cliqué sur *Enregistrer* lors d'un ajout groupé ou sur *Supprimer* lors d'une action de suppression groupée, Data Infrastructure Insights vous informe que l'action prendra un certain temps. Vous pouvez ignorer ce message ; l'action continuera en arrière-plan.

Pour les environnements comportant de grandes quantités d'actifs associés, l'héritage des affectations d'application à ces actifs peut prendre plusieurs minutes. Veuillez prévoir plus de temps pour que l'héritage se produise si vous avez de nombreux biens liés.

Copie des valeurs du tableau

Vous pouvez copier les valeurs des tableaux dans le presse-papiers pour les utiliser dans

les zones de recherche ou d'autres applications.

À propos de cette tâche

Il existe deux méthodes que vous pouvez utiliser pour copier des valeurs de tables ou des résultats de requête dans le presse-papiers.

Étapes

1. Méthode 1 : Mettez en surbrillance le texte souhaité avec la souris, copiez-le et collez-le dans les champs de recherche ou d'autres applications.
2. Méthode 2 : pour les champs à valeur unique, passez la souris sur le champ et cliquez sur l'icône du presse-papiers qui apparaît. La valeur est copiée dans le presse-papiers pour être utilisée dans les champs de recherche ou d'autres applications.

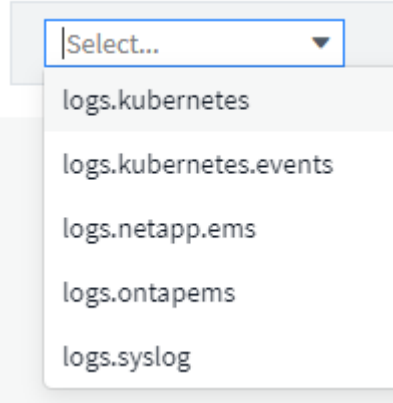
   Notez que seules les valeurs qui sont des liens vers des actifs peuvent être copiées à l'aide de cette méthode. Seuls les champs qui incluent des valeurs uniques (c'est-à-dire non des listes) ont l'icône de copie.

Explorateur de journaux

Data Infrastructure Insights Log Explorer est un outil puissant permettant d'interroger les journaux système. En plus d'aider aux enquêtes, vous pouvez également enregistrer une requête de journal dans un moniteur pour fournir des alertes lorsque ces déclencheurs de journal particuliers sont activés.

Pour commencer à explorer les journaux, cliquez sur **Requêtes de journal > +Nouvelle requête de journal**.

Sélectionnez un journal disponible dans la liste.

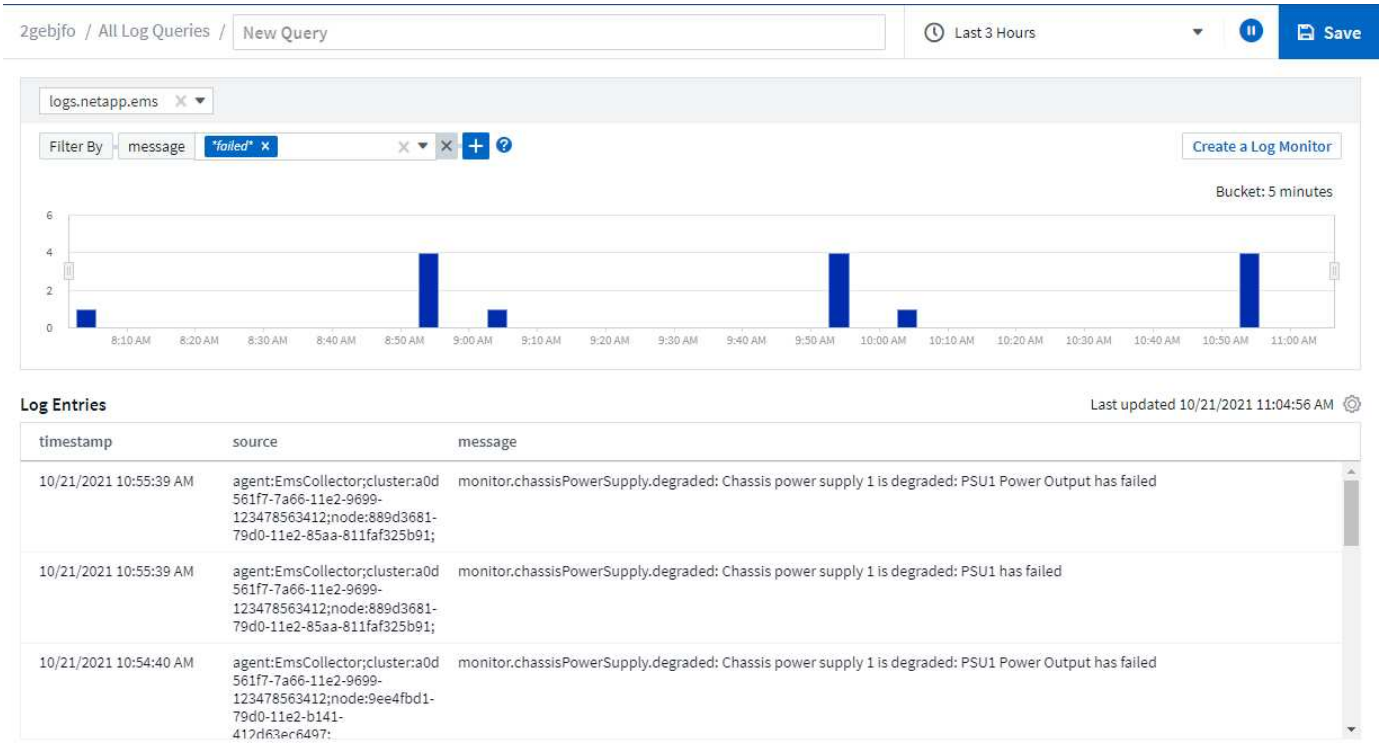


Les types de journaux disponibles pour l'interrogation peuvent varier en fonction de votre environnement. Des types de journaux supplémentaires peuvent être ajoutés au fil du temps.

Vous pouvez définir des filtres pour affiner davantage les résultats de la requête. Par exemple, pour rechercher tous les messages de journal indiquant un échec, définissez un filtre pour *Messages* contenant le mot « échec ».

Vous pouvez commencer à saisir le texte souhaité dans le champ de filtre ; Data Infrastructure Insights vous invitera à créer une recherche générique contenant la chaîne au fur et à mesure de la saisie.

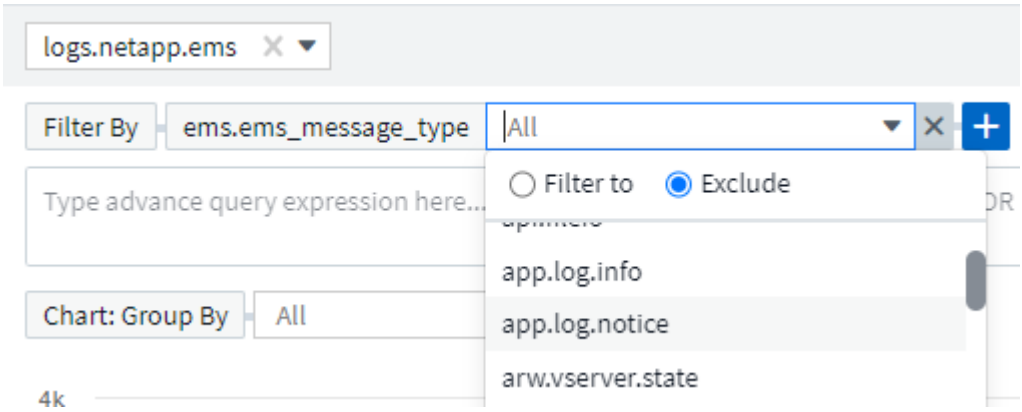
Les résultats sont affichés dans un graphique indiquant le nombre d'instances de journal dans chaque période indiquée. Sous le graphique se trouvent les entrées du journal elles-mêmes. Le graphique et les entrées s'actualisent automatiquement en fonction de la plage horaire sélectionnée.



Filtration

Inclure / Exclure

Lors du filtrage des journaux, vous pouvez choisir d'**inclure** (c'est-à-dire « Filtrer sur ») ou d'**exclure** les chaînes que vous saisissez. Les chaînes exclues sont affichées dans le filtre complété comme « PAS <chaîne> ».



Les filtres basés sur des caractères génériques ou des expressions (par exemple NOT, OR, « Aucun », etc.) s'affichent en bleu foncé dans le champ de filtre. Les éléments que vous sélectionnez directement dans la liste sont affichés en bleu clair.

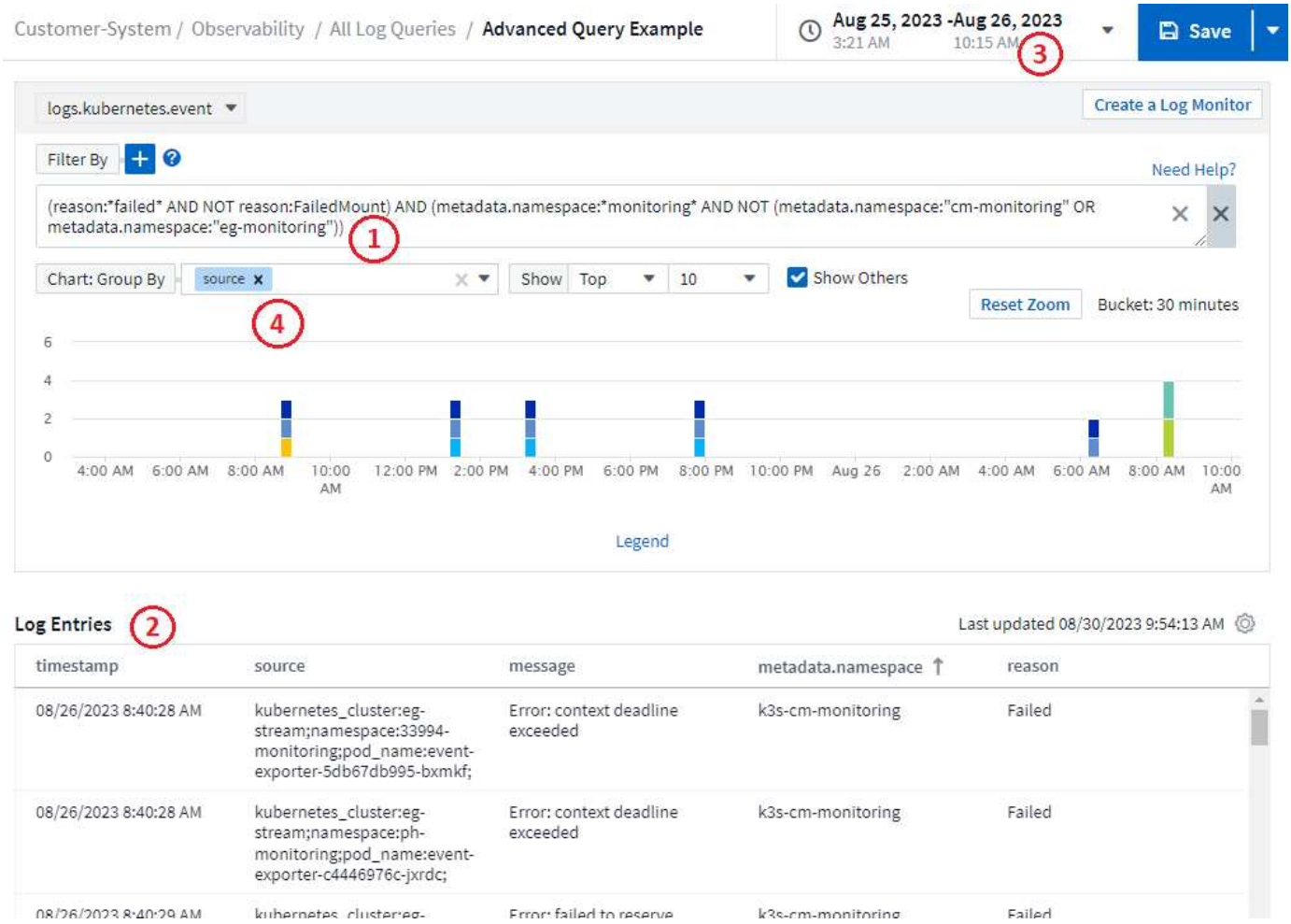
À tout moment, vous pouvez cliquer sur *Créer un moniteur de journal* pour créer un nouveau moniteur basé sur le filtre actuel.

Filtrage avancé

Lorsque vous filtrez des valeurs de texte ou de liste dans des requêtes ou des widgets de tableau de bord, lorsque vous commencez à saisir, vous avez la possibilité de créer un **filtre générique** basé sur le texte actuel. La sélection de cette option renverra tous les résultats correspondant à l'expression générique. Vous pouvez également créer des expressions en utilisant NOT, AND ou OR, ou vous pouvez sélectionner l'option « Aucun » pour filtrer les valeurs nulles.

> Assurez-vous d'enregistrer votre requête tôt et souvent lorsque vous créez votre filtrage. L'interrogation avancée est une entrée de chaîne « de forme libre » et des erreurs d'analyse peuvent se produire au fur et à mesure de la création.

Jetez un œil à cette image d'écran montrant les résultats filtrés pour une requête avancée du journal *logs.kubernetes.event*. Il se passe beaucoup de choses sur cette page, ce qui est expliqué sous l'image :

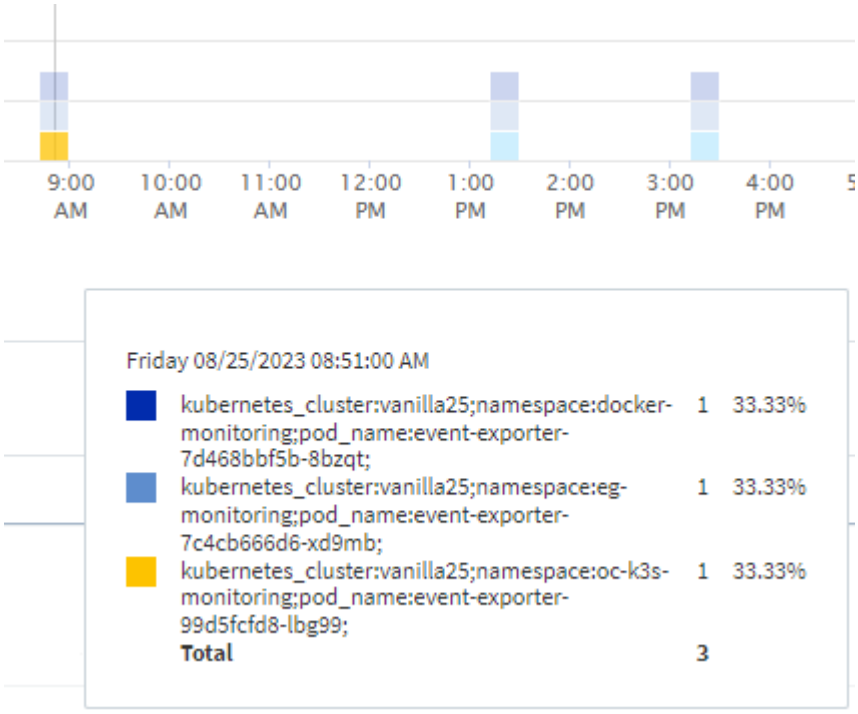


1. Cette chaîne de requête avancée filtre les éléments suivants :
   - Filtrez les entrées de journal avec une *raison* qui inclut le mot « échec », mais rien avec la raison spécifique « FailedMount ».
   - Incluez toutes les entrées qui incluent également un *metadata.namespace* incluant le mot « monitoring », mais excluez les espaces de noms spécifiques « cm-monitoring » ou « eg-monitoring ».

     Notez que dans le cas ci-dessus, puisque « cm-monitoring » et « eg-monitoring » contiennent tous deux un tiret (« - »), les chaînes doivent être incluses entre guillemets, sinon une erreur d'analyse sera affichée. Les chaînes qui n'incluent pas de tirets, d'espaces, etc. n'ont pas besoin d'être placées entre

guillemets. En cas de doute, essayez de mettre la chaîne entre guillemets.

2. Les résultats du filtre actuel, y compris toutes les valeurs « Filtrer par » ET le filtre de requête avancée, sont affichés dans la liste des résultats. La liste peut être triée par n'importe quelle colonne affichée. Pour afficher des colonnes supplémentaires, sélectionnez l'icône « engrenage ».
3. Le graphique a été agrandi pour afficher uniquement les résultats du journal qui se sont produits dans une période donnée. La plage horaire affichée ici reflète le niveau de zoom actuel. Sélectionnez le bouton *Réinitialiser le zoom* pour rétablir le niveau de zoom sur la plage horaire actuelle de Data Infrastructure Insights .
4. Les résultats du graphique ont été regroupés par le champ *source*. Le graphique montre les résultats dans chaque colonne regroupés par couleurs. Survoler une colonne du graphique affichera certains détails sur les entrées spécifiques.



Filtres de raffinage

Vous pouvez utiliser les éléments suivants pour affiner votre filtre :

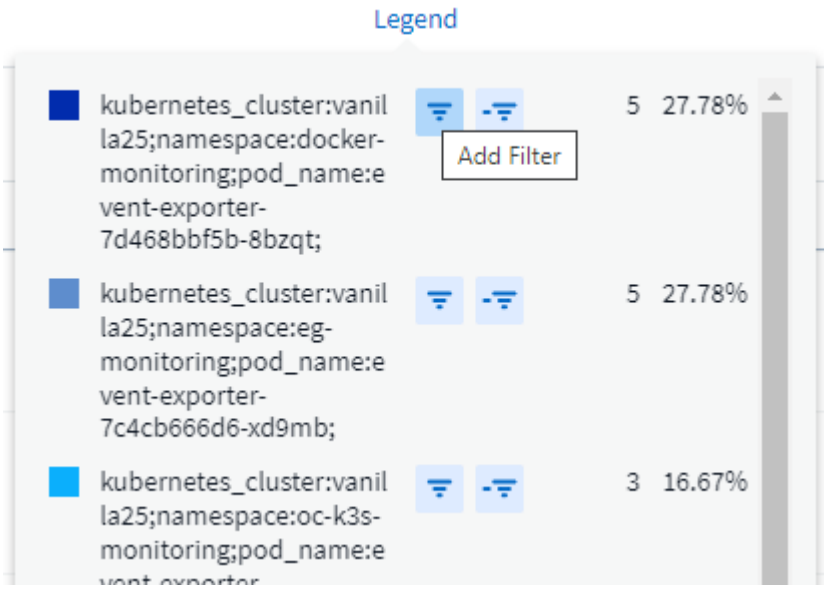
Filtre	Ce qu'il fait
* (Astérisque)	vous permet de rechercher tout ce que vous voulez
? (point d'interrogation)	vous permet de rechercher un nombre spécifique de caractères
OU	vous permet de spécifier plusieurs entités
PAS	vous permet d'exclure du texte des résultats de recherche
Aucun	recherche les valeurs NULL dans tous les champs
Pas *	recherche les valeurs NULL dans les champs *texte uniquement*

Si vous placez une chaîne de filtre entre guillemets doubles, Insight traite tout ce qui se trouve entre le premier et le dernier guillemet comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs à l'intérieur des guillemets seront traités comme des littéraux. Par exemple, le filtrage par « * » renverra des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OR et NOT seront également traités comme des chaînes littérales lorsqu'ils sont placés entre guillemets.

Vous pouvez combiner un filtre simple avec un filtre de requête avancé ; le filtre résultant est un « ET » des deux.

La légende du graphique

La *Légende* sous le graphique réserve également quelques surprises. Pour chaque résultat (basé sur le filtre actuel) affiché dans la légende, vous avez la possibilité d'afficher uniquement les résultats de cette ligne (Ajouter un filtre) ou d'afficher tous les résultats NON pour cette ligne (Ajouter un filtre d'exclusion). Le graphique et la liste des entrées de journal sont mis à jour pour afficher les résultats en fonction de votre sélection. Pour supprimer ce filtrage, ouvrez à nouveau la légende et sélectionnez le [X] pour effacer le filtre basé sur la légende.

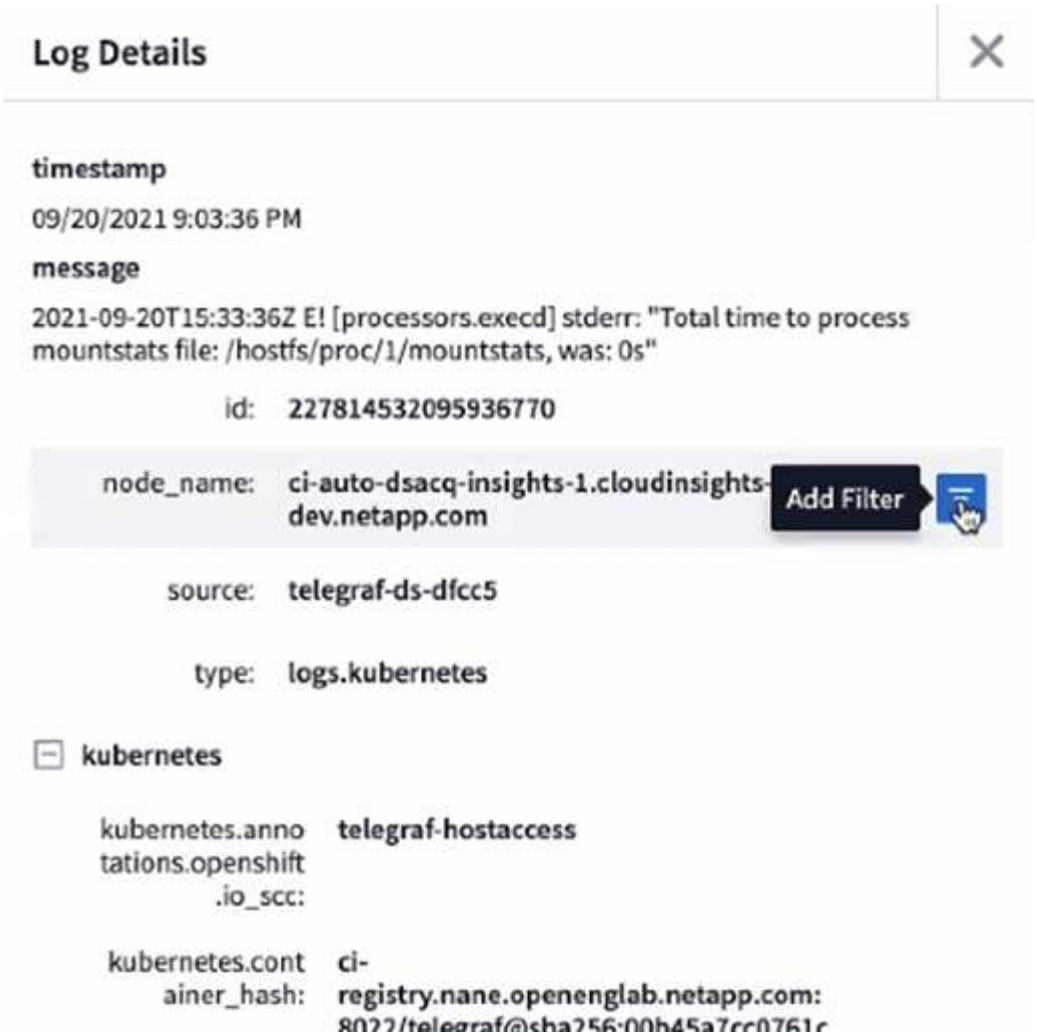


Détails du journal

Cliquer n'importe où dans une entrée de journal dans la liste ouvrira un volet de détails pour cette entrée. Ici, vous pouvez explorer plus d'informations sur l'événement.

Cliquez sur « Ajouter un filtre » pour ajouter le champ sélectionné au filtre actuel. La liste des entrées du journal sera mise à jour en fonction du nouveau filtre.

Notez que certains champs ne peuvent pas être ajoutés en tant que filtres ; dans ces cas, l'icône *Ajouter un filtre* n'est pas disponible.



Dépannage

Vous trouverez ici des suggestions pour résoudre les problèmes liés aux requêtes de journal.

Problème:	Essayez ceci :
Je ne vois pas de messages « debug » dans ma requête de journal	Les messages du journal de débogage ne sont pas collectés. Pour capturer les messages souhaités, modifiez le niveau de gravité du message concerné en *informationnel, erreur, alerte, urgence* ou *avis*.

Identifier les appareils inactifs

Identifier les actifs dont vous disposez et qui les utilise est essentiel pour « ajuster la taille » et libérer l'infrastructure inutilisée. Vous pouvez facilement réaffecter ou désactiver les ressources sous-utilisées et éviter les achats inutiles.

Utilisez les étapes suivantes pour identifier les actifs inactifs.

Étapes

- Accédez à **Observabilité > Explorer** → **+Nouvelle requête de métrique**.
- Sélectionnez *Stockage* dans la liste déroulante.

- Cliquez sur l'engrenage et ajoutez *isActive* comme colonne.

  Les lignes affichant une coche sont actives. « X » indique les appareils inactifs.

Pour supprimer les appareils inactifs, sélectionnez simplement les appareils à supprimer et dans la liste déroulante **Actions en masse**, sélectionnez *Supprimer les appareils inactifs*.

Connaissances

Connaissances

Les informations vous permettent d'examiner des éléments tels que l'utilisation des ressources et la manière dont elle affecte les autres ressources, ou des analyses de temps de traitement complet.

Un certain nombre d'informations sont disponibles. Accédez à **Tableaux de bord > Insights** pour commencer à vous plonger dans le sujet. Vous pouvez afficher les Insights actifs (Insights en cours d'exécution) sur l'onglet principal ou les Insights inactifs sur l'onglet *Insights inactifs*. Les informations inactives sont celles qui étaient auparavant actives mais qui ne se produisent plus.

Types d'informations

Ressources partagées sous pression

Les charges de travail à fort impact peuvent réduire les performances d'autres charges de travail dans une ressource partagée. Cela met la ressource partagée sous pression. Data Infrastructure Insights fournit des outils pour vous aider à étudier la saturation des ressources et son impact sur votre locataire."En savoir plus"

Les espaces de noms Kubernetes manquent d'espace

L'aperçu des espaces de noms Kubernetes manquant d'espace vous donne un aperçu des charges de travail sur vos espaces de noms Kubernetes qui risquent de manquer d'espace, avec une estimation du nombre de jours restants avant que chaque espace ne soit plein."En savoir plus"

Récupérez le stockage à froid ONTAP

Reclaim ONTAP Cold Storage Insight fournit des données sur la capacité de réfrigération, les économies potentielles de coûts/d'énergie et les éléments d'action recommandés pour les volumes sur les systèmes ONTAP ."En savoir plus"

> Il s'agit d'une fonctionnalité *Aperçu* et elle peut changer au fil du temps à mesure que des améliorations sont apportées. "Apprendre encore plus" à propos des fonctionnalités de Data Infrastructure Insights Preview.

Perspectives : Les ressources partagées sous pression

Les charges de travail à fort impact peuvent réduire les performances d'autres charges de travail dans une ressource partagée. Cela met la ressource partagée sous pression. Data Infrastructure Insights fournit des outils pour vous aider à étudier la saturation des ressources et son impact sur votre locataire.

Terminologie

Lorsqu'on parle de charge de travail ou d'impact sur les ressources, les définitions suivantes sont utiles.

Une **charge de travail exigeante** est une charge de travail actuellement identifiée comme ayant un impact sur d'autres ressources du pool de stockage partagé. Ces charges de travail génèrent des IOPS plus élevées (par exemple), réduisant ainsi les IOPS dans les charges de travail impactées. Les charges de travail exigeantes sont parfois appelées « charges de travail à forte consommation ».

Une **charge de travail impactée** est une charge de travail affectée par une charge de travail à forte consommation dans le pool de stockage partagé. Ces charges de travail connaissent une réduction des IOPS et/ou une latence plus élevée, causées par les charges de travail exigeantes.

Notez que si Data Infrastructure Insights n'a pas découvert la charge de travail de calcul principale, le volume ou le volume interne lui-même sera reconnu comme la charge de travail. Cela s'applique aussi bien aux charges de travail exigeantes qu'aux charges impactées.

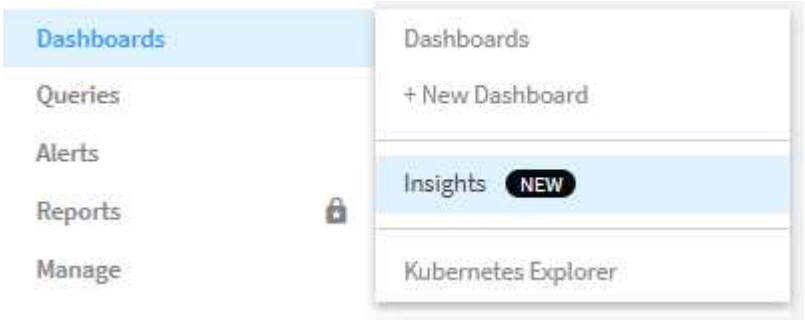
La saturation des ressources partagées est le rapport entre les IOPS impactées et la *ligne de base*.

La ligne de base est définie comme le point de données maximal signalé pour chaque charge de travail dans l'heure précédant immédiatement la saturation détectée.

Une **Contention** ou une **Saturation** se produit lorsque les IOPS sont déterminées comme affectant d'autres ressources ou charges de travail dans le pool de stockage partagé.

Charges de travail exigeantes

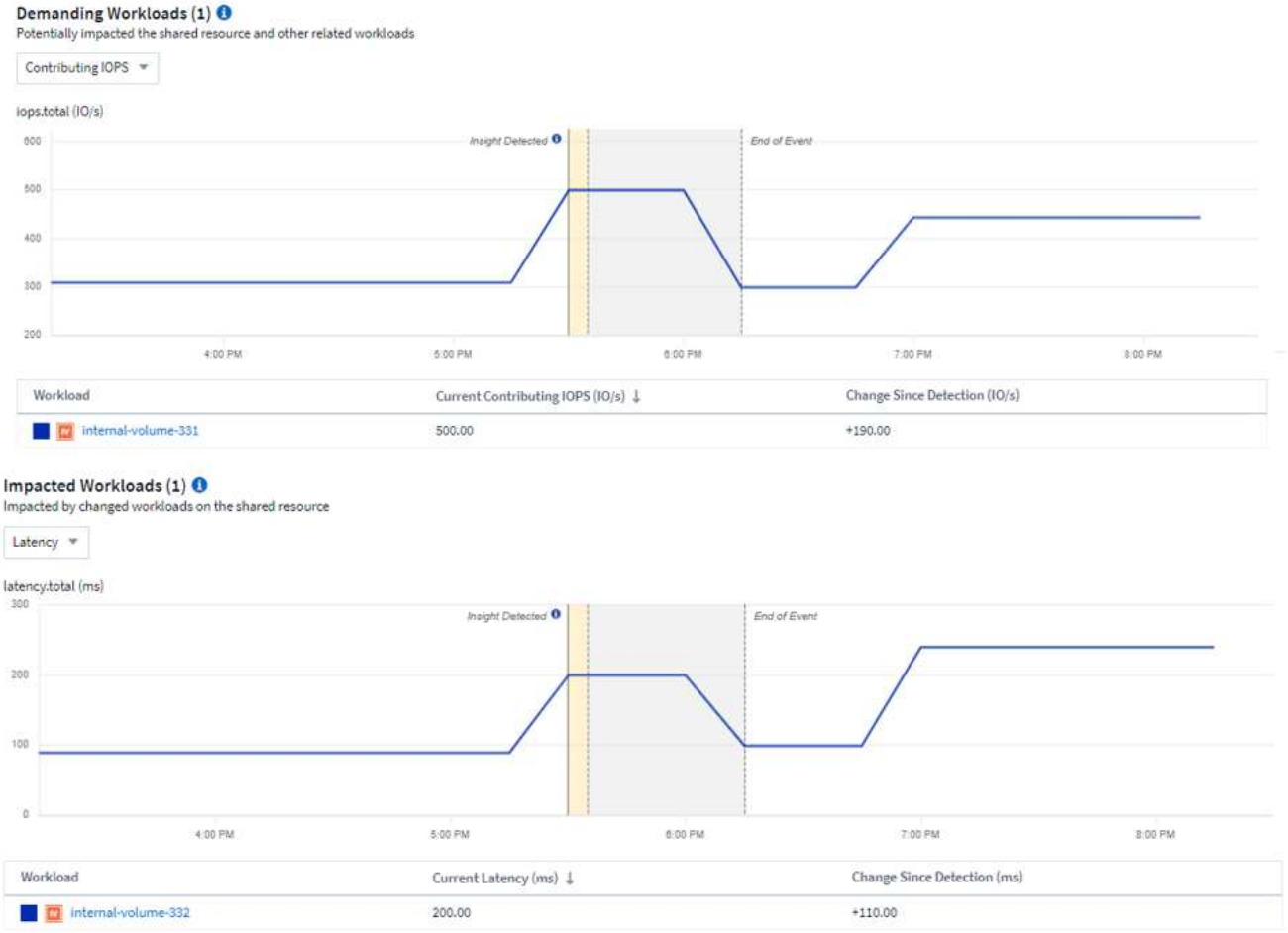
Pour commencer à examiner les charges de travail exigeantes et impactées dans vos ressources partagées, cliquez sur **Tableaux de bord > Informations** et sélectionnez l'information **Ressources partagées sous stress**.



Data Infrastructure Insights affiche une liste de toutes les charges de travail pour lesquelles une saturation a été détectée. Notez que Data Infrastructure Insights affichera les charges de travail pour lesquelles au moins une *ressource exigeante* **ou** *ressource impactée* a été détectée.

Cliquez sur une charge de travail pour afficher la page de détails correspondante. Le graphique supérieur montre l'activité sur la ressource partagée (par exemple, un pool de stockage) sur laquelle la contention/saturation se produit.

Ci-dessous se trouvent deux graphiques montrant les charges de travail *exigeantes* et les charges de travail qui sont *impactées* par ces charges de travail exigeantes.



Sous chaque tableau se trouve une liste des charges de travail et/ou des ressources affectant ou affectées par la contention. Cliquer sur une ressource (par exemple, une machine virtuelle) ouvre une page de détails pour cette ressource. Cliquer sur une charge de travail ouvre une page de requête affichant les pods impliqués. Notez que si le lien ouvre une requête vide, cela peut être dû au fait que le pod affecté ne fait plus partie de la contention active. Vous pouvez modifier la plage horaire de la requête pour afficher la liste des pods dans une plage horaire plus grande ou plus ciblée.

Que dois-je faire pour résoudre la saturation ?

Il existe un certain nombre de mesures que vous pouvez prendre pour réduire ou éliminer le risque de

saturation de votre locataire. Ceux-ci sont affichés en développant le lien **+Afficher les recommandations** sur la page. Voici quelques choses que vous pouvez essayer.

- Déplacer les consommateurs à IOPS élevés

  Déplacez les charges de travail « gourmandes » vers des pools de stockage moins saturés. Il est recommandé d'évaluer le niveau et la capacité de ces pools avant de déplacer les charges de travail, afin d'éviter des coûts inutiles ou des conflits supplémentaires.

- Mettre en œuvre une politique de qualité de service (QoS)

  La mise en œuvre d'une politique QoS par charge de travail pour garantir que suffisamment de ressources libres sont disponibles atténuera la saturation du pool de stockage. C'est une solution à long terme.

- Ajouter des ressources supplémentaires

  Si la ressource partagée (par exemple, le pool de stockage) a atteint le point de saturation IOPS, l'ajout de disques plus nombreux ou plus rapides au pool garantira suffisamment de ressources libres disponibles pour atténuer la saturation.

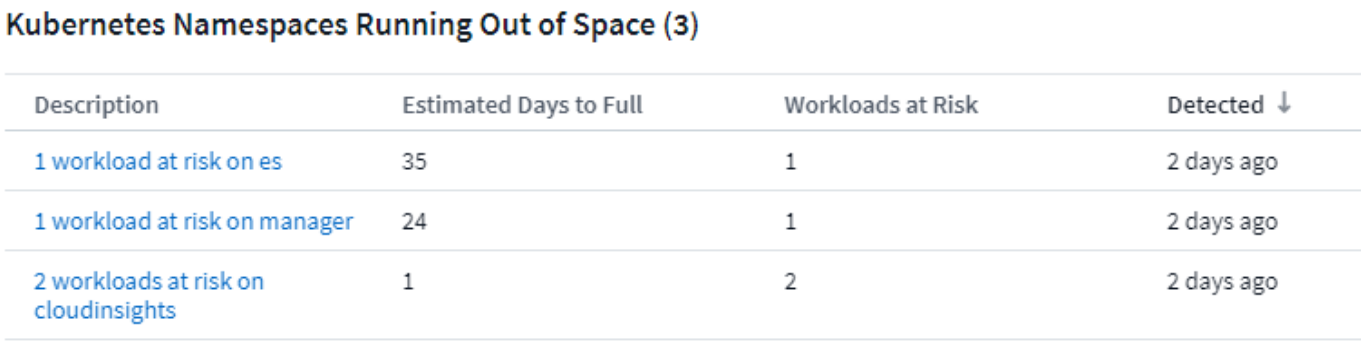
Enfin, vous pouvez cliquer sur **Copier le lien Insight** pour copier l'URL de la page dans le presse-papiers, afin de la partager plus facilement avec vos collègues.

Aperçu : les espaces de noms Kubernetes manquent d'espace

Manquer d'espace sur votre locataire n'est jamais une bonne situation. Data Infrastructure Insights vous aide à prévoir le temps dont vous disposez avant que les volumes persistants Kubernetes ne soient pleins.

L'aperçu *Kubernetes Namespaces Running Out of Space* vous donne un aperçu des charges de travail sur vos espaces de noms Kubernetes qui risquent de manquer d'espace, avec une estimation du nombre de jours restants avant que chaque volume persistant ne soit plein.

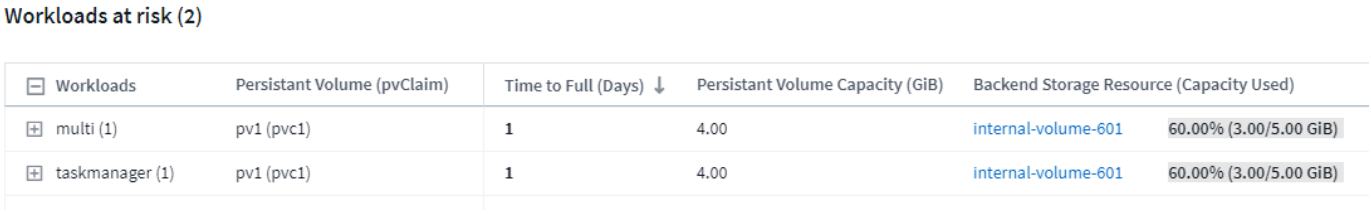
Vous pouvez consulter cet aperçu en accédant à **Tableaux de bord > Aperçus**.



Cliquez sur une charge de travail pour ouvrir une page de détails pour Insight. Sur cette page, vous verrez un graphique montrant les tendances de la capacité de charge de travail ainsi qu'un tableau montrant les éléments suivants :

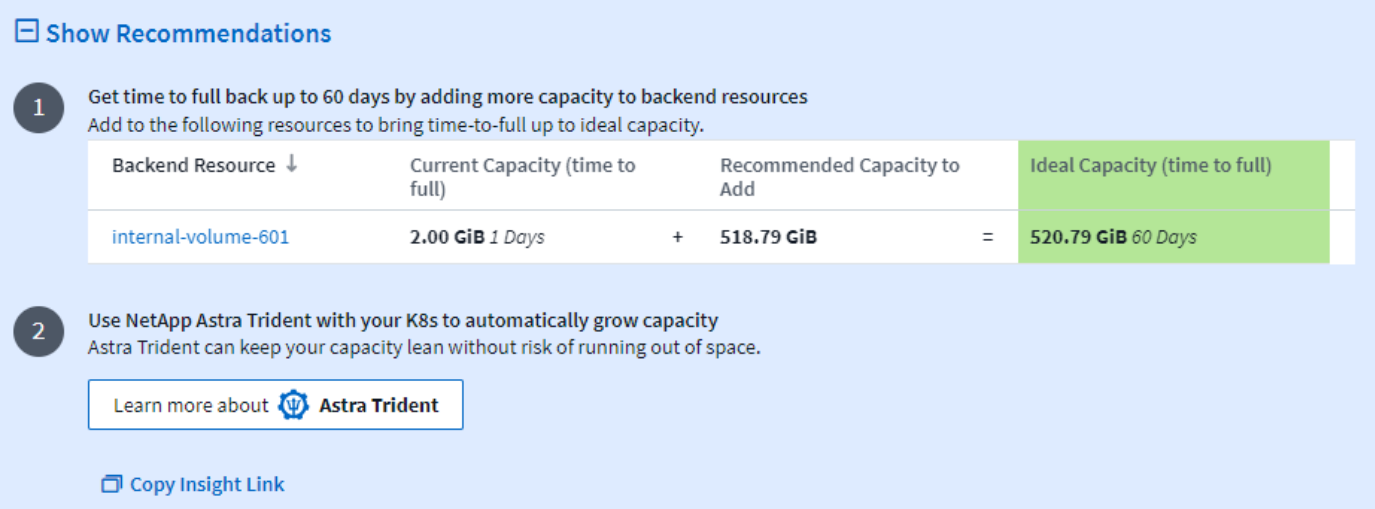
- Nom de la charge de travail
- Volume persistant affecté

- Temps de remplissage prévu en jours
- Capacité du volume persistant
- Ressource de stockage backend affectée, avec capacité actuelle utilisée sur la capacité totale. Cliquer sur ce lien ouvrira la page de destination détaillée du volume backend.



Que puis-je faire si je manque d'espace ?

Sur la page Insight, cliquez sur **+Afficher les recommandations** pour afficher les solutions possibles. L'option la plus simple lorsque vous manquez d'espace est toujours d'ajouter plus de capacité, et Data Infrastructure Insights vous montre la capacité optimale à ajouter pour augmenter le délai d'attente jusqu'à une prévision cible de 60 jours. D'autres recommandations sont également présentées.



C'est également ici que vous pouvez copier un lien pratique vers cet Insight, pour ajouter la page à vos favoris ou pour la partager facilement avec votre équipe.

Aperçu : Récupérez le stockage à froid ONTAP

Reclaim ONTAP Cold Storage Insight fournit des données sur la capacité de réfrigération, les économies potentielles de coûts/d'énergie et les éléments d'action recommandés pour les volumes sur les systèmes ONTAP .

Pour afficher ces informations, accédez à **Tableaux de bord > Informations** et consultez l'information *Reclaim ONTAP Cold Storage*. Notez que cet Insight ne répertoriera les stockages concernés que si Data Infrastructure Insights a détecté un stockage à froid, sinon vous verrez un message « tout est clair ».

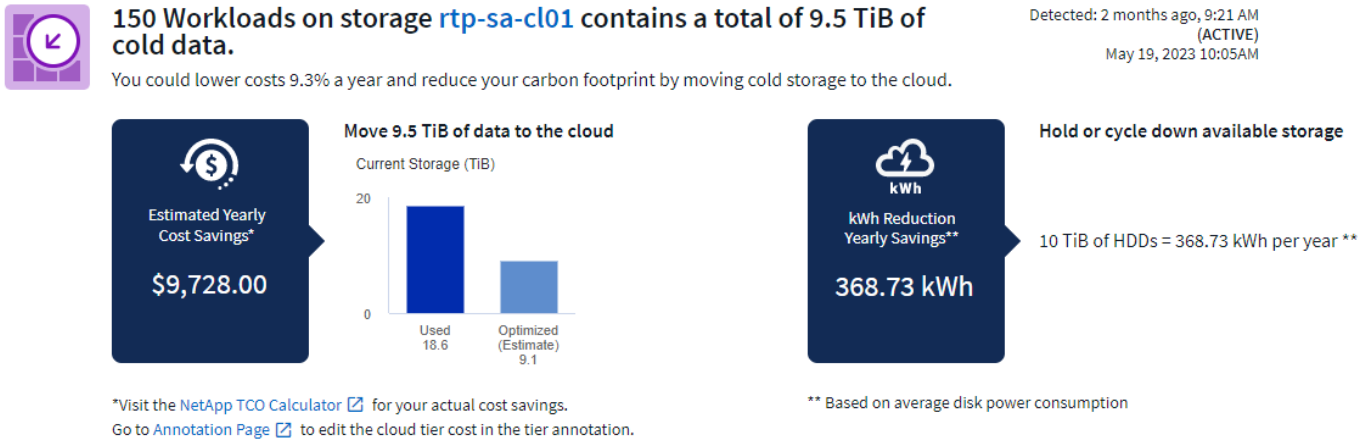
Gardez à l'esprit que les données froides datant de moins de 30 jours ne sont pas affichées.

Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected ↓
0.30 TiB of cold data on storage rtp-sa-cl04	0.30	45	an hour ago
1.22 TiB of cold data on storage umeng-aff300-01-02	1.22	84	16 days ago
11.62 TiB of cold data on storage rtp-sa-cl01	11.62	171	16 days ago

La description d'Insight donne une indication rapide de la quantité de données détectées comme « froides » et du stockage sur lequel résident ces données. Le tableau fournit également un décompte des charges de travail avec des données froides.

La sélection d'un Insight dans la liste ouvre une page affichant plus de détails, notamment des recommandations pour déplacer les données vers le Cloud ou réduire le nombre de disques unifiés, ainsi que les économies de coûts et d'énergie estimées que vous pourriez potentiellement réaliser en mettant en œuvre ces recommandations. La page fournit même un lien pratique vers"Calculateur TCO de NetApp" afin que vous puissiez expérimenter avec les chiffres.



Recommandations

Sur la page Insight, développez les **Recommandations** pour explorer les options suivantes :

- Déplacez les charges de travail inutilisées (zombies) vers un niveau de stockage à moindre coût (HDD)

  En utilisant l'indicateur zombie, le stockage à froid et le nombre de jours, recherchez la quantité de données la plus froide et la plus importante et déplacez la charge de travail vers un niveau de stockage à moindre coût (tel qu'un pool de stockage utilisant un stockage sur disque dur). Une charge de travail est considérée comme un « zombie » lorsqu'elle n'a reçu aucune demande d'E/S significative pendant 30 jours ou plus.

- Supprimer les charges de travail inutilisées

  Vérifiez quelles charges de travail ne sont pas utilisées et envisagez de les archiver ou de les supprimer du système de stockage.

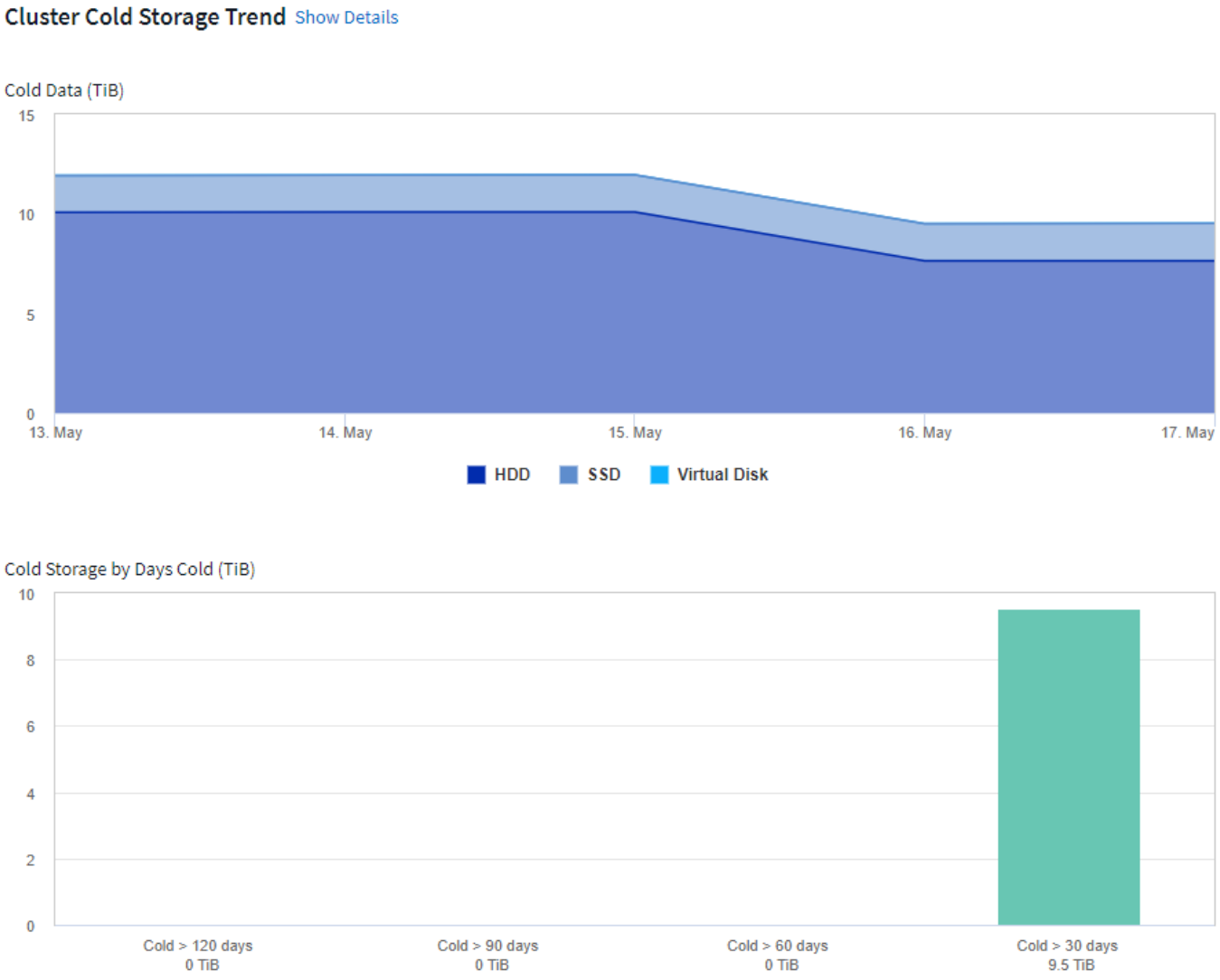
- Envisagez la solution Fabric Pool de NetApp

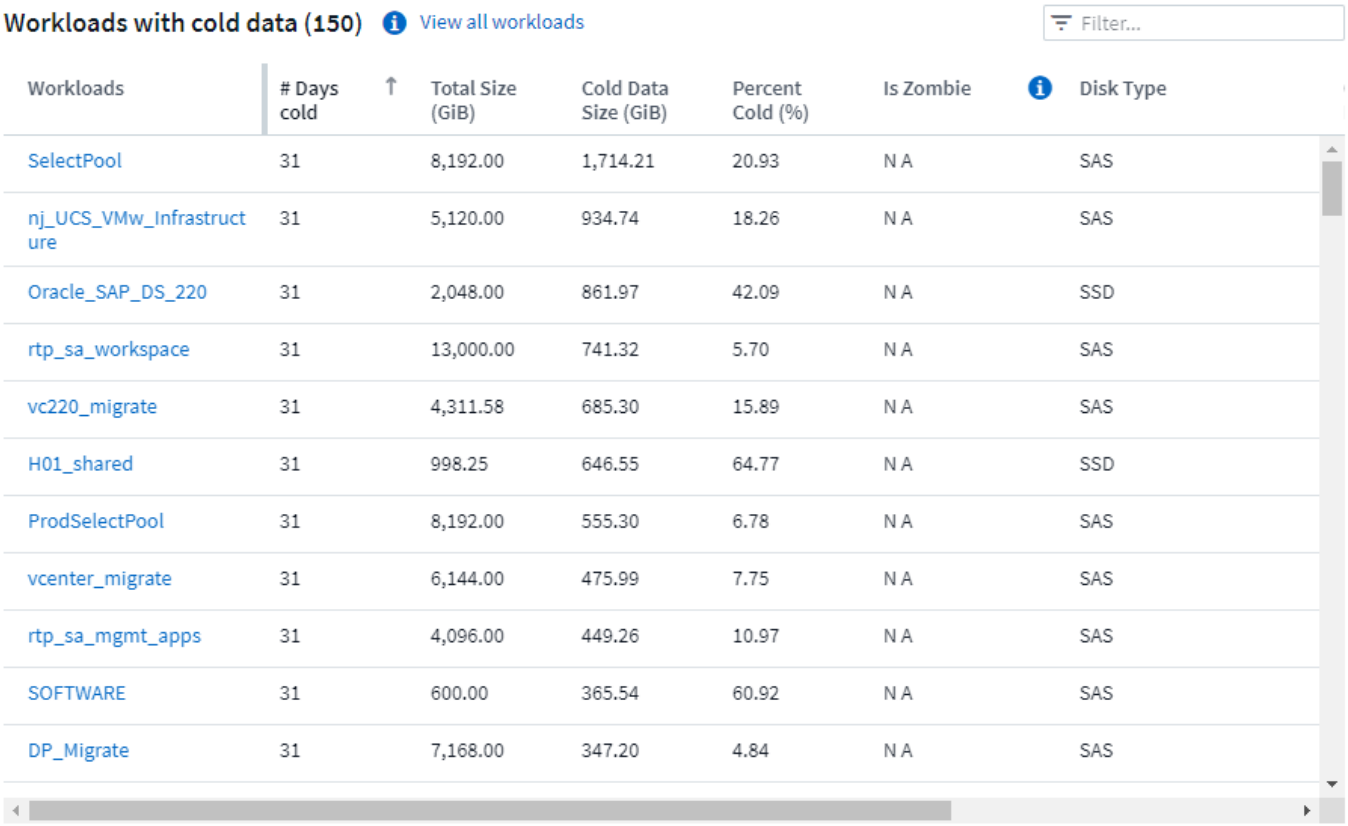
  NetApp"Solution de piscine en tissu" hiérarchise automatiquement les données froides vers un stockage cloud à faible coût, augmentant ainsi l'efficacité de votre niveau de performance tout en offrant une

protection des données à distance.

Visualiser et explorer

Les graphiques et le tableau fournissent des informations de tendance supplémentaires et vous permettent d'explorer en détail les charges de travail individuelles.





Workloads with cold data (150) View all workloads

Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

Moniteurs et alertes

Alertes avec moniteurs

Configurez des moniteurs pour suivre les seuils de performances, consigner les événements et les anomalies sur l'ensemble de vos ressources d'infrastructure. Créez des alertes personnalisées pour des mesures telles que la latence d'écriture des nœuds, la capacité de stockage ou les performances des applications, et recevez des notifications lorsque ces conditions sont remplies.

Les moniteurs vous permettent de définir des seuils sur les métriques générées par les objets « d'infrastructure » tels que le stockage, la VM, EC2 et les ports, ainsi que pour les données « d'intégration » telles que celles collectées pour Kubernetes, les métriques avancées ONTAP et les plugins Telegraf. Ces moniteurs *métriques* vous alertent lorsque les seuils de niveau d'avertissement ou de niveau critique sont dépassés.

Vous pouvez également créer des moniteurs pour déclencher des alertes de niveau avertissement, critique ou informatif lorsque des *événements de journal* spécifiés sont détectés.

Data Infrastructure Insights fournit un certain nombre de"Moniteurs définis par le système" également, en fonction de votre environnement.

Meilleures pratiques de sécurité

Les alertes Data Infrastructure Insights sont conçues pour mettre en évidence les points de données et les tendances de votre locataire, et Data Infrastructure Insights vous permet de saisir n'importe quelle adresse e-

mail valide comme destinataire d'alerte. Si vous travaillez dans un environnement sécurisé, soyez particulièrement attentif à qui reçoit la notification ou a accès à l'alerte.

Moniteur métrique ou journal ?

1. Dans le menu Data Infrastructure Insights , cliquez sur **Alertes > Gérer les moniteurs**

   La page de liste des moniteurs s'affiche, affichant les moniteurs actuellement configurés.

2. Pour modifier un moniteur existant, cliquez sur le nom du moniteur dans la liste.
3. Pour ajouter un moniteur, cliquez sur **+ Moniteur**.

   Lorsque vous ajoutez un nouveau moniteur, vous êtes invité à créer un moniteur de métriques ou un moniteur de journaux.

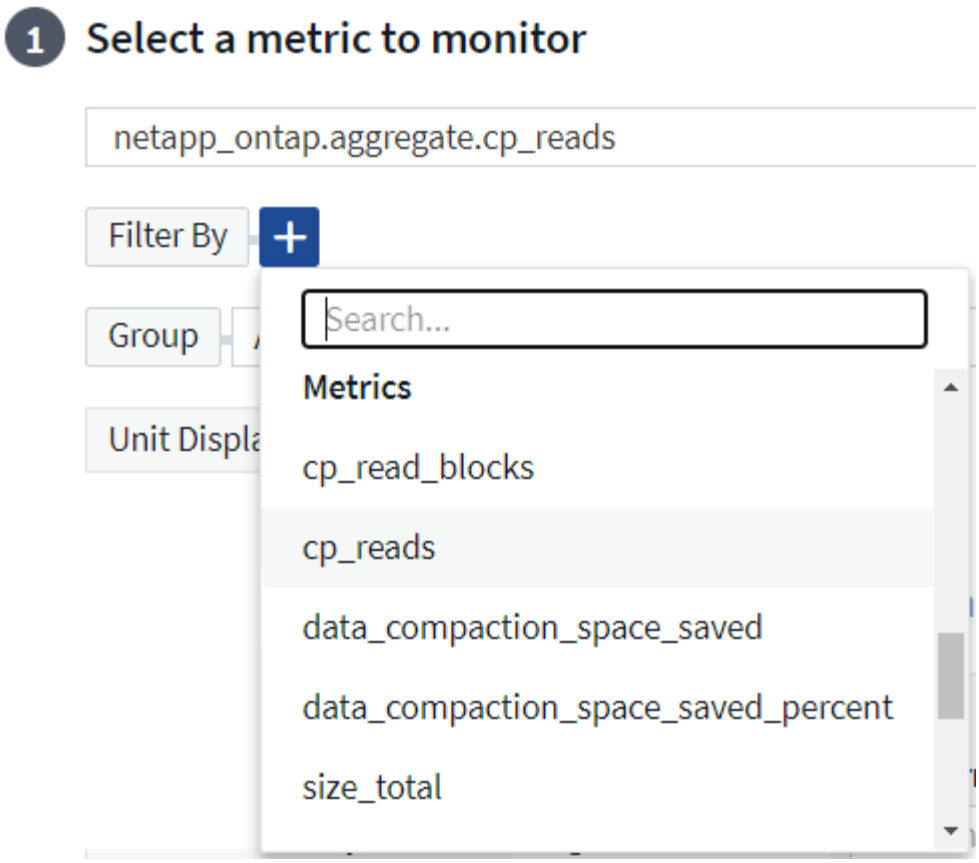
   - *Metric* surveille les alertes sur les déclencheurs liés à l'infrastructure ou aux performances
   - *Log* surveille les alertes sur l'activité liée au journal

   Après avoir choisi votre type de moniteur, la boîte de dialogue Configuration du moniteur s'affiche. La configuration varie en fonction du type de moniteur que vous créez.

Moniteur métrique

1. Dans la liste déroulante, recherchez et choisissez un type d'objet et une métrique à surveiller.

Vous pouvez définir des filtres pour affiner les attributs d'objet ou les mesures à surveiller.

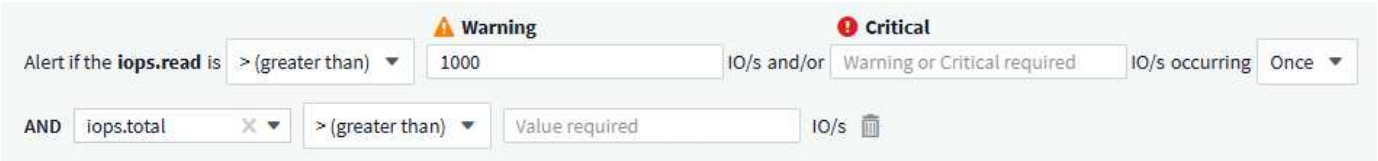


Lorsque vous travaillez avec des données d'intégration (Kubernetes, ONTAP Advanced Data, etc.), le filtrage des métriques supprime les points de données individuels/non appariés de la série de données tracées, contrairement aux données d'infrastructure (stockage, VM, ports, etc.) où les filtres fonctionnent sur la valeur agrégée de la série de données et suppriment potentiellement l'objet entier du graphique.

Les moniteurs de métriques s'appliquent aux objets d'inventaire tels que le stockage, le commutateur, l'hôte, la machine virtuelle, etc., ainsi qu'aux métriques d'intégration telles que les données ONTAP Advanced ou Kubernetes. Lors de la surveillance des objets d'inventaire, notez que vous ne pouvez pas sélectionner une méthode « Grouper par ». Cependant, le regroupement est autorisé lors de la surveillance des données d'intégration.

Moniteurs multi-conditions

Vous pouvez choisir d'affiner davantage votre surveillance métrique en ajoutant une deuxième condition. Développez simplement l'invite « + Ajouter une condition de métrique secondaire » et configurez la condition supplémentaire.



Le moniteur émettra une alerte si les deux conditions sont remplies.

Notez que vous ne pouvez utiliser qu'un « ET » pour une deuxième condition ; vous ne pouvez pas choisir d'alerter sur une condition OU sur l'autre.

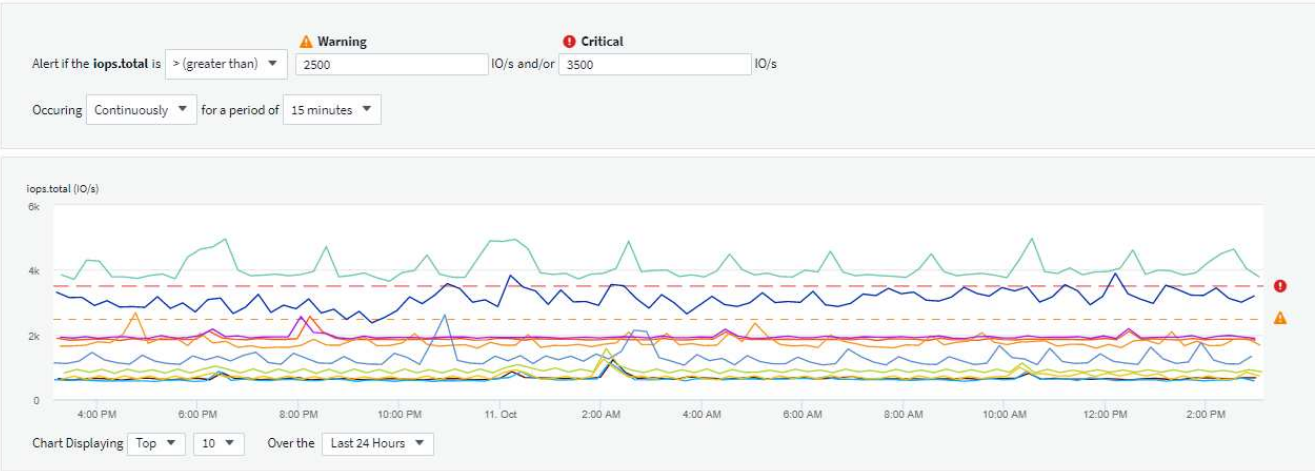
Définir les conditions du moniteur.

1. Après avoir choisi l'objet et la métrique à surveiller, définissez les seuils de niveau d'avertissement et/ou de niveau critique.
2. Pour le niveau *Avertissement*, entrez 200 pour notre exemple. La ligne pointillée indiquant ce niveau d'avertissement s'affiche dans l'exemple de graphique.
3. Pour le niveau *Critique*, entrez 400. La ligne pointillée indiquant ce niveau critique s'affiche dans l'exemple de graphique.

   Le graphique affiche les données historiques. Les lignes de niveau d'avertissement et critique sur le graphique sont une représentation visuelle du moniteur, vous pouvez donc facilement voir quand le moniteur peut déclencher une alerte dans chaque cas.

4. Pour l'intervalle d'occurrence, choisissez *En continu* pour une période de *15 minutes*.

   Vous pouvez choisir de déclencher une alerte dès qu'un seuil est dépassé ou d'attendre que le seuil soit dépassé en continu pendant un certain temps. Dans notre exemple, nous ne souhaitons pas être alertés à chaque fois que le nombre total d'IOPS dépasse le niveau d'avertissement ou critique, mais uniquement lorsqu'un objet surveillé dépasse en continu l'un de ces niveaux pendant au moins 15 minutes.



Définir le comportement de résolution des alertes

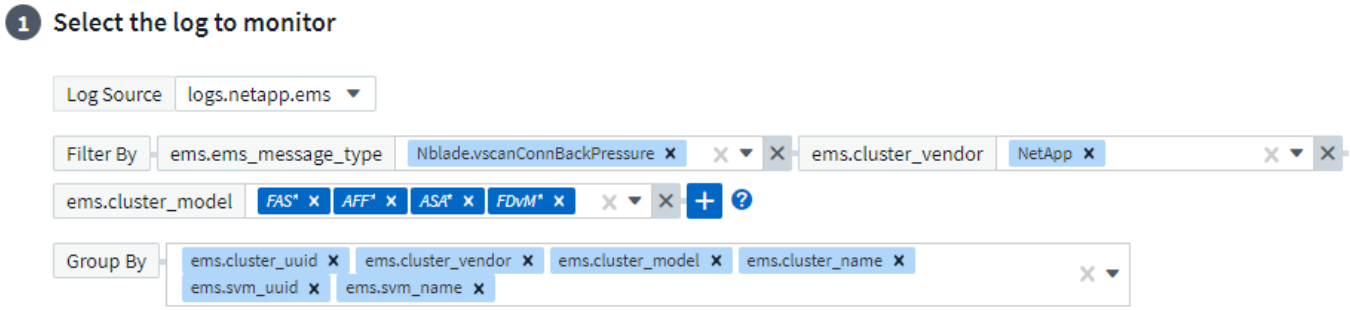
Vous pouvez choisir comment une alerte de surveillance métrique est résolue. Deux choix s'offrent à vous :

- Résoudre le problème lorsque la métrique revient dans la plage acceptable.
- Résoudre lorsque la métrique se situe dans la plage acceptable pendant une durée spécifiée, de 1 minute à 7 jours.

Moniteur de journal

Lors de la création d'un **Moniteur de journaux**, choisissez d'abord le journal à surveiller dans la liste des journaux disponibles. Vous pouvez ensuite filtrer en fonction des attributs disponibles comme ci-dessus. Vous pouvez également choisir un ou plusieurs attributs « Grouper par ».

Le filtre Log Monitor ne peut pas être vide.



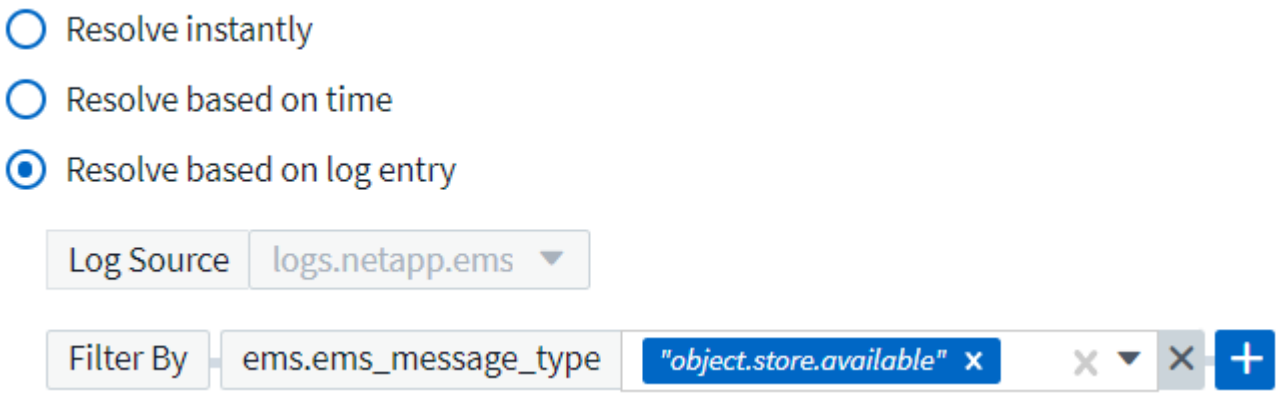
Définir le comportement de l'alerte

Vous pouvez créer le moniteur pour alerter avec un niveau de gravité *Critique*, *Avertissement* ou *Informationnel*, lorsque les conditions que vous avez définies ci-dessus se produisent une fois (c'est-à-dire immédiatement), ou attendre d'alerter jusqu'à ce que les conditions se produisent 2 fois ou plus.

Définir le comportement de résolution des alertes

Vous pouvez choisir comment une alerte de surveillance de journal est résolue. Trois choix s'offrent à vous :

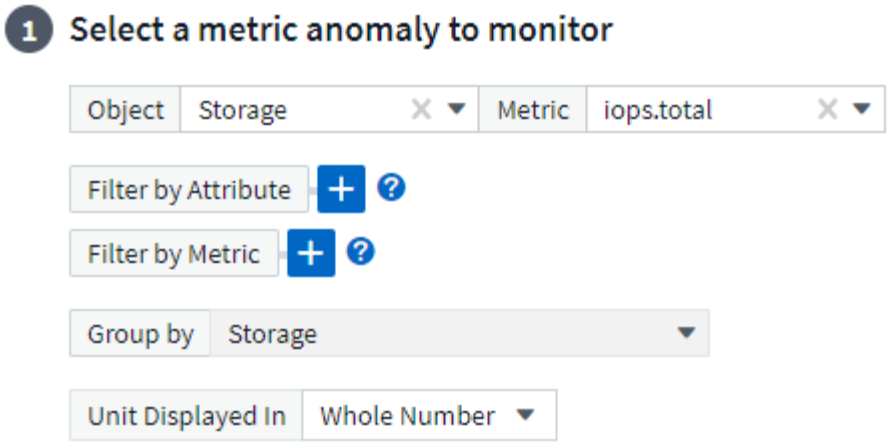
- **Résoudre instantanément** : L'alerte est immédiatement résolue sans aucune autre action nécessaire
- **Résolution en fonction du temps** : L'alerte est résolue une fois le temps spécifié écoulé
- **Résolution basée sur l'entrée de journal** : L'alerte est résolue lorsqu'une activité de journal ultérieure s'est produite. Par exemple, lorsqu'un objet est enregistré comme « disponible ».



Moniteur de détection d'anomalies

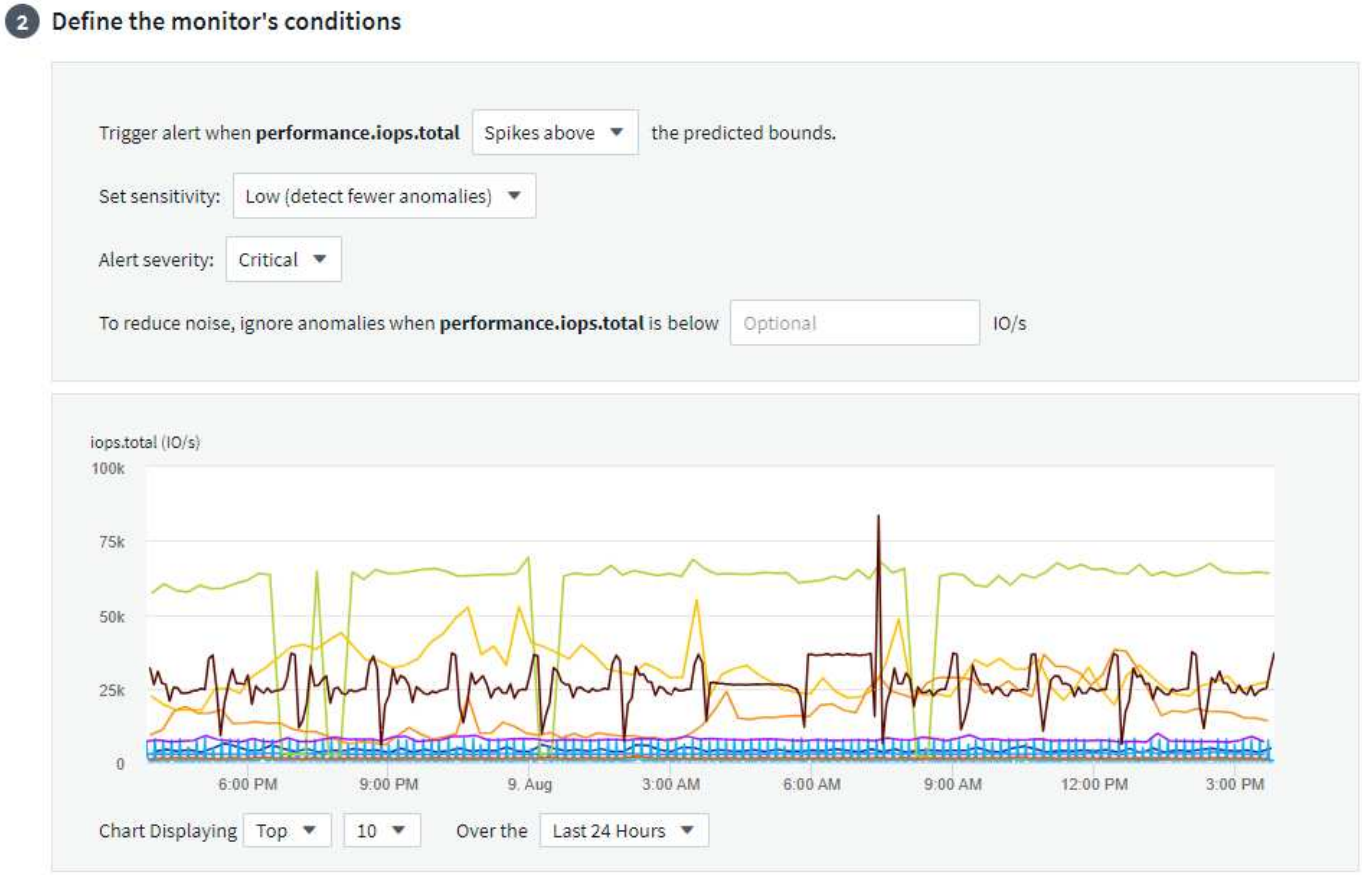
1. Dans la liste déroulante, recherchez et choisissez un type d'objet et une métrique à surveiller.

Vous pouvez définir des filtres pour affiner les attributs d'objet ou les mesures à surveiller.



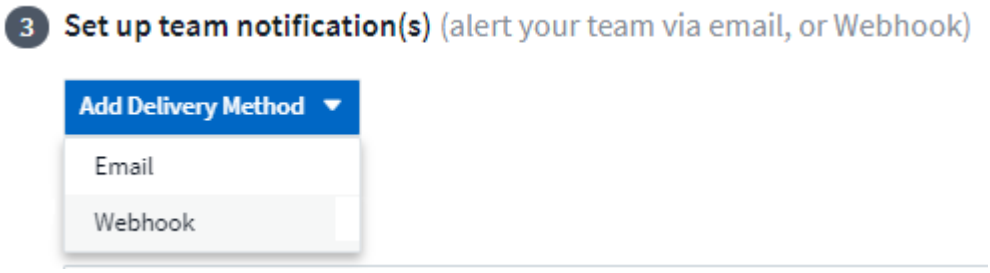
Définir les conditions du moniteur.

1. Après avoir choisi l'objet et la métrique à surveiller, vous définissez les conditions dans lesquelles une anomalie est détectée.
   - Choisissez de détecter une anomalie lorsque la métrique choisie **monte au-dessus** des limites prédites, **descend en dessous** de ces limites, ou **monte au-dessus ou descend en dessous** des limites.
   - Définissez la **sensibilité** de détection. **Faible** (moins d'anomalies sont détectées), **Moyen** ou **Élevé** (plus d'anomalies sont détectées).
   - Définissez les alertes sur **Avertissement** ou **Critique**.
   - Si vous le souhaitez, vous pouvez choisir de réduire le bruit, en ignorant les anomalies lorsque la métrique choisie est inférieure à un seuil que vous avez défini.



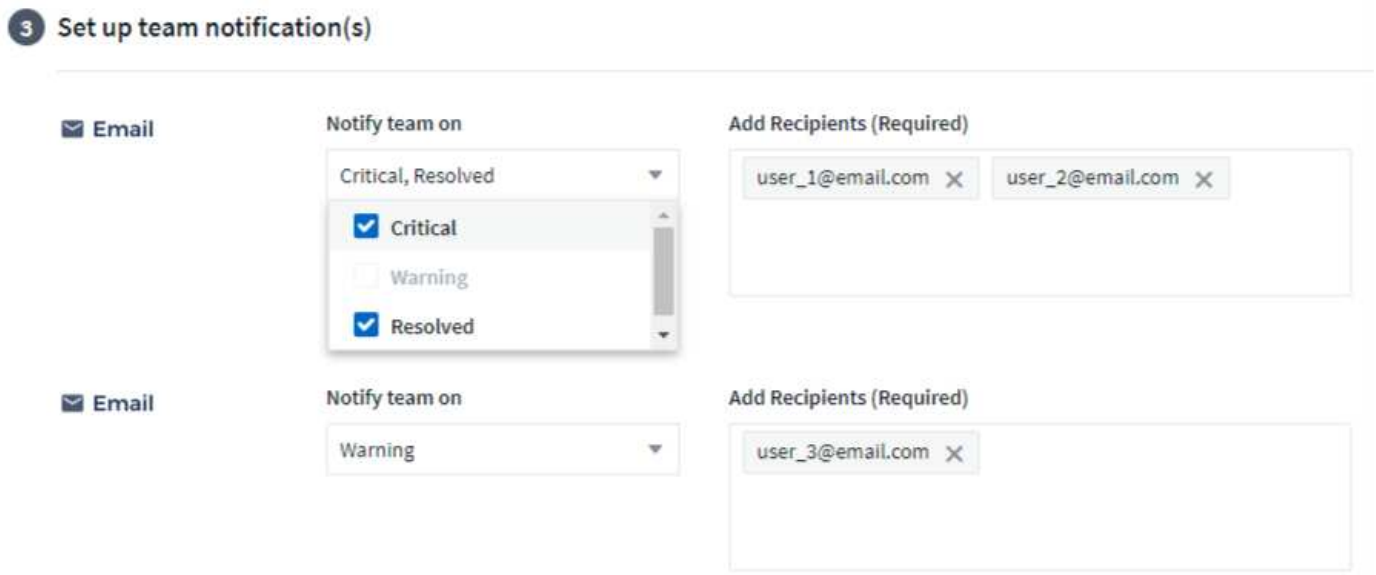
Sélectionnez le type de notification et les destinataires

Dans la section *Configurer les notifications d'équipe*, vous pouvez choisir d'alerter votre équipe par e-mail ou par Webhook.



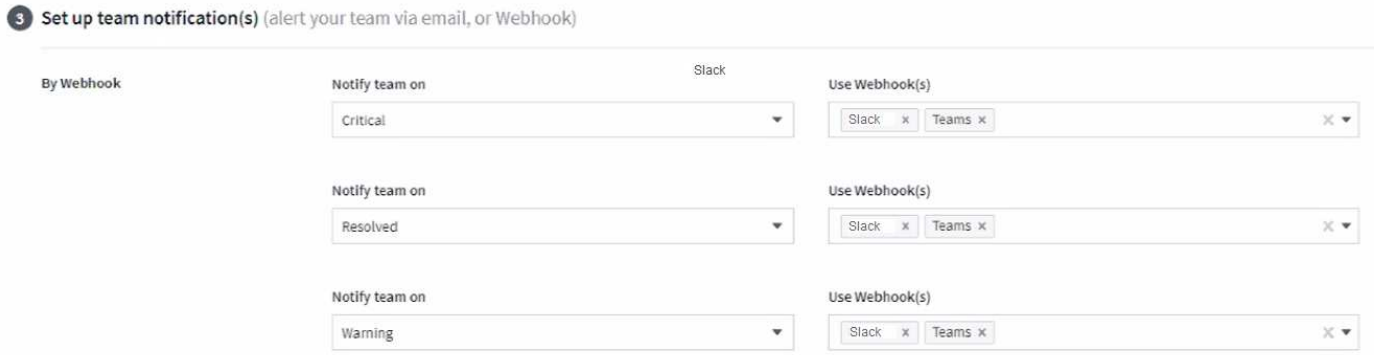
Alerte par e-mail :

Spécifiez les destinataires de courrier électronique pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents destinataires pour les avertissements ou les alertes critiques.



Alerte via Webhook :

Spécifiez le(s) webhook(s) pour les notifications d'alerte. Si vous le souhaitez, vous pouvez choisir différents webhooks pour les alertes d'avertissement ou critiques.



Les notifications du collecteur de données ONTAP ont priorité sur toutes les notifications de surveillance spécifiques pertinentes pour le cluster/collecteur de données. La liste de destinataires que vous avez définie pour le collecteur de données lui-même recevra les alertes du collecteur de données. S'il n'y a pas d'alertes de collecteur de données actives, les alertes générées par le moniteur seront envoyées à des destinataires de moniteur spécifiques.

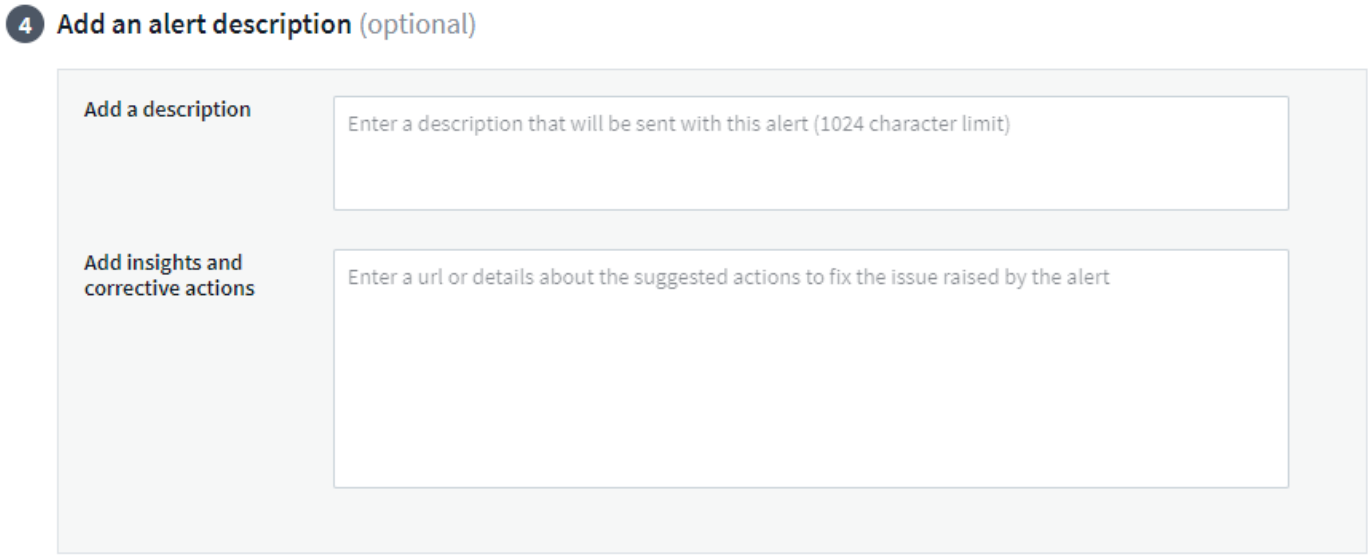
Définition d'actions correctives ou d'informations supplémentaires

Vous pouvez ajouter une description facultative ainsi que des informations supplémentaires et/ou des actions correctives en remplissant la section **Ajouter une description d'alerte**. La description peut contenir jusqu'à 1024 caractères et sera envoyée avec l'alerte. Le champ Informations/Actions correctives peut contenir jusqu'à 67 000 caractères et sera affiché dans la section récapitulative de la page de destination de l'alerte.

Dans ces champs, vous pouvez fournir des notes, des liens ou des étapes à suivre pour corriger ou traiter l'alerte.

Vous pouvez ajouter n'importe quel attribut d'objet (par exemple, le nom de stockage) comme paramètre à une description d'alerte. Par exemple, vous pouvez définir des paramètres pour le nom du volume et le nom du stockage dans une description telle que : « Latence élevée pour le volume :

%%relatedObject.volume.name%%, Stockage : *%%relatedObject.storage.name%%* ».



Sauvegardez votre moniteur

1. Si vous le souhaitez, vous pouvez ajouter une description du moniteur.
2. Donnez au moniteur un nom significatif et cliquez sur **Enregistrer**.

   Votre nouveau moniteur est ajouté à la liste des moniteurs actifs.

Liste des moniteurs

La page Moniteur répertorie les moniteurs actuellement configurés, affichant les éléments suivants :

- Nom du moniteur
- Statut
- Objet/métrique surveillé
- Conditions du moniteur

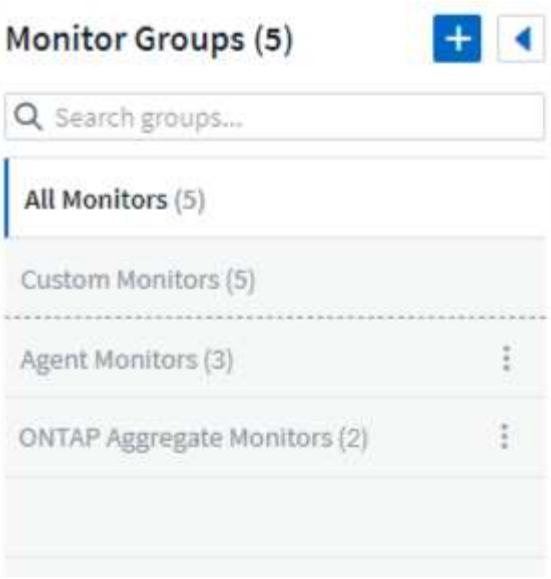
Vous pouvez choisir de suspendre temporairement la surveillance d'un type d'objet en cliquant sur le menu à droite du moniteur et en sélectionnant **Pause**. Lorsque vous êtes prêt à reprendre la surveillance, cliquez sur **Reprendre**.

Vous pouvez copier un moniteur en sélectionnant **Dupliquer** dans le menu. Vous pouvez ensuite modifier le nouveau moniteur et changer l'objet/la métrique, le filtre, les conditions, les destinataires des e-mails, etc.

Si un moniteur n'est plus nécessaire, vous pouvez le supprimer en sélectionnant **Supprimer** dans le menu.

Groupes de surveillance

Le regroupement vous permet d'afficher et de gérer les moniteurs associés. Par exemple, vous pouvez disposer d'un groupe de surveillance dédié au stockage sur votre locataire ou de surveillances pertinentes pour une certaine liste de destinataires.



Les groupes de moniteurs suivants sont affichés. Le nombre de moniteurs contenus dans un groupe est indiqué à côté du nom du groupe.

- **Tous les moniteurs** répertorie tous les moniteurs.
- **Moniteurs personnalisés** répertorie tous les moniteurs créés par l'utilisateur.
- **Moniteurs suspendus** répertorie tous les moniteurs système qui ont été suspendus par Data Infrastructure Insights.
- Data Infrastructure Insights affichera également un certain nombre de **Groupes de surveillance système**, qui répertorieront un ou plusieurs groupes de"moniteurs définis par le système" , y compris les moniteurs d'infrastructure et de charge de travail ONTAP .

Les moniteurs personnalisés peuvent être suspendus, repris, supprimés ou déplacés vers un autre groupe. Les moniteurs définis par le système peuvent être suspendus et repris, mais ne peuvent pas être supprimés ou déplacés.

Moniteurs suspendus

Ce groupe ne sera affiché que si Data Infrastructure Insights a suspendu un ou plusieurs moniteurs. Un moniteur peut être suspendu s'il génère des alertes excessives ou continues. Si le moniteur est un moniteur personnalisé, modifiez les conditions pour empêcher l'alerte continue, puis reprenez le moniteur. Le moniteur sera supprimé du groupe Moniteurs suspendus lorsque le problème à l'origine de la suspension sera résolu.

Moniteurs définis par le système

Ces groupes afficheront les moniteurs fournis par Data Infrastructure Insights, à condition que votre environnement contienne les périphériques et/ou la disponibilité des journaux requis par les moniteurs.

Les moniteurs définis par le système ne peuvent pas être modifiés, déplacés vers un autre groupe ou supprimés. Cependant, vous pouvez dupliquer un moniteur système et modifier ou déplacer le doublon.

Les moniteurs système peuvent inclure des moniteurs pour l'infrastructure ONTAP (stockage, volume, etc.) ou les charges de travail (c'est-à-dire les moniteurs de journaux) ou d'autres groupes. NetApp évalue en permanence les besoins des clients et les fonctionnalités des produits, et mettra à jour ou ajoutera des moniteurs et des groupes système selon les besoins.

Groupes de moniteurs personnalisés

Vous pouvez créer vos propres groupes pour contenir des moniteurs en fonction de vos besoins. Par exemple, vous souhaiterez peut-être un groupe pour tous vos moniteurs liés au stockage.

Pour créer un nouveau groupe de moniteurs personnalisé, cliquez sur le bouton **"+" Créer un nouveau groupe de moniteurs**. Saisissez un nom pour le groupe et cliquez sur **Créer un groupe**. Un groupe vide est créé avec ce nom.

Pour ajouter des moniteurs au groupe, accédez au groupe *Tous les moniteurs* (recommandé) et effectuez l'une des opérations suivantes :

- Pour ajouter un seul moniteur, cliquez sur le menu à droite du moniteur et sélectionnez *Ajouter au groupe*. Choisissez le groupe auquel ajouter le moniteur.
- Cliquez sur le nom du moniteur pour ouvrir la vue d'édition du moniteur et sélectionnez un groupe dans la section *Associer à un groupe de moniteurs*.

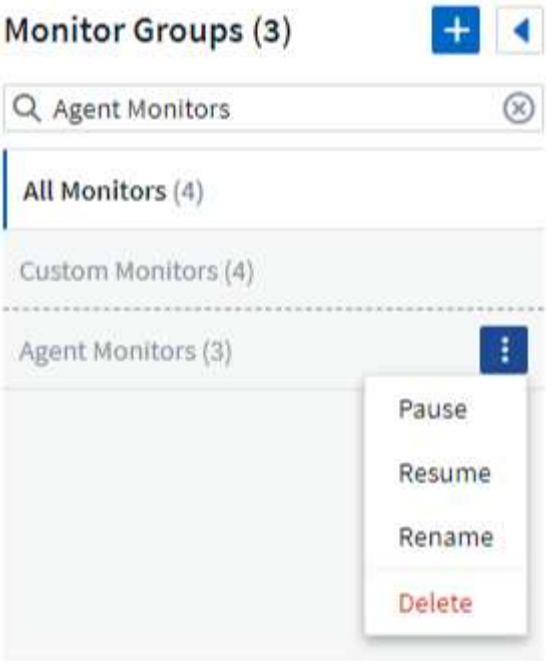
Supprimez les moniteurs en cliquant sur un groupe et en sélectionnant *Supprimer du groupe* dans le menu. Vous ne pouvez pas supprimer des moniteurs du groupe *Tous les moniteurs* ou *Moniteurs personnalisés*. Pour supprimer un moniteur de ces groupes, vous devez supprimer le moniteur lui-même.

> La suppression d'un moniteur d'un groupe ne supprime pas le moniteur de Data Infrastructure Insights. Pour supprimer complètement un moniteur, sélectionnez le moniteur et cliquez sur *Supprimer*. Cela le supprime également du groupe auquel il appartenait et il n'est plus disponible pour aucun utilisateur.

Vous pouvez également déplacer un moniteur vers un groupe différent de la même manière, en sélectionnant *Déplacer vers le groupe*.

Pour mettre en pause ou reprendre tous les moniteurs d'un groupe à la fois, sélectionnez le menu du groupe et cliquez sur *Pause* ou *Reprendre*.

Utilisez le même menu pour renommer ou supprimer un groupe. La suppression d'un groupe ne supprime pas les moniteurs de Data Infrastructure Insights; ils sont toujours disponibles dans *Tous les moniteurs*.



Moniteurs définis par le système

Data Infrastructure Insights comprend un certain nombre de moniteurs définis par le système pour les métriques et les journaux. Les moniteurs système disponibles dépendent des collecteurs de données présents sur votre locataire. De ce fait, les moniteurs disponibles dans Data Infrastructure Insights peuvent changer à mesure que des collecteurs de données sont ajoutés ou que leurs configurations sont modifiées.

Voir le"Moniteurs définis par le système" page pour les descriptions des moniteurs inclus avec Data Infrastructure Insights.

Plus d'informations

- "Affichage et suppression des alertes"

Affichage et gestion des alertes des moniteurs

Data Infrastructure Insights affiche des alertes lorsque"seuils surveillés" sont dépassés.

Les moniteurs et les alertes sont disponibles dans Data Infrastructure Insights Standard Edition et versions ultérieures.

Affichage et gestion des alertes

Pour afficher et gérer les alertes, procédez comme suit.

1. Accédez à la page **Alertes > Toutes les alertes**.
2. Une liste contenant jusqu'aux 1 000 alertes les plus récentes s'affiche. Vous pouvez trier cette liste sur n'importe quel champ en cliquant sur l'en-tête de colonne du champ. La liste affiche les informations suivantes. Notez que toutes ces colonnes ne sont pas affichées par défaut. Vous pouvez sélectionner les colonnes à afficher en cliquant sur l'icône « engrenage » :
   - **ID d'alerte** : ID d'alerte unique généré par le système

- **Heure de déclenchement** : L'heure à laquelle le moniteur concerné a déclenché l'alerte
- **Gravité actuelle** (onglet Alertes actives) : la gravité actuelle de l'alerte active
- **Gravité maximale** (onglet Alertes résolues) ; la gravité maximale de l'alerte avant sa résolution
- **Moniteur** : Le moniteur configuré pour déclencher l'alerte
- **Déclenché le** : L'objet sur lequel le seuil surveillé a été dépassé
- **Statut** : État d'alerte actuel, *Nouveau* ou *En cours*
- **Statut actif** : *Actif* ou *Résolu*
- **Condition** : La condition de seuil qui a déclenché l'alerte
- **Métrique** : La métrique de l'objet sur laquelle le seuil surveillé a été dépassé
- **État du moniteur** : État actuel du moniteur qui a déclenché l'alerte
- **A une action corrective** : L'alerte a suggéré des actions correctives. Ouvrez la page d'alerte pour les afficher.

Vous pouvez gérer une alerte en cliquant sur le menu à droite de l'alerte et en choisissant l'une des options suivantes :

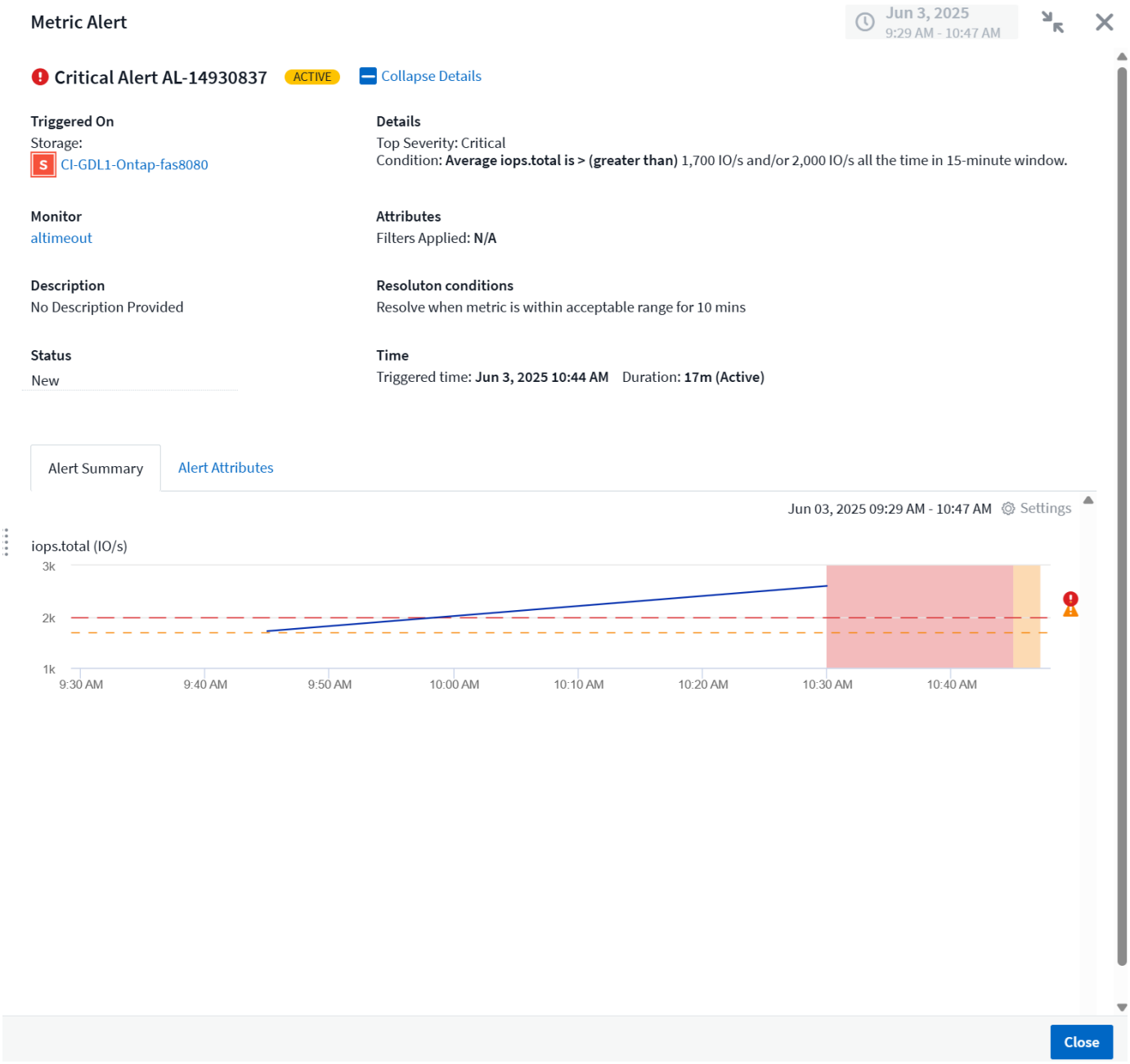
- **En cours** pour indiquer que l'alerte fait l'objet d'une enquête ou doit rester ouverte
- **Ignorer** pour supprimer l'alerte de la liste des alertes actives.

Vous pouvez gérer plusieurs alertes en sélectionnant la case à cocher à gauche de chaque alerte et en cliquant sur *Modifier le statut des alertes sélectionnées*.

Cliquer sur un ID d'alerte ouvre la page de détails de l'alerte.

Panneau de détails des alertes

Sélectionnez n'importe quelle ligne d'alerte pour ouvrir le panneau de détails de l'alerte. Le panneau de détails de l'alerte fournit des détails supplémentaires sur l'alerte, notamment un *Résumé*, une section *Performances* affichant des graphiques liés aux données de l'objet, tous les *Actifs associés* et les *Commentaires* saisis par les enquêteurs de l'alerte.



Alertes lorsque des données sont manquantes

Dans un système en temps réel tel que Data Infrastructure Insights, pour déclencher l'analyse d'un moniteur afin de décider si une alerte doit être générée, nous nous appuyons sur l'une des deux choses suivantes :

- le prochain point de données à arriver
- un minuteur à déclencher lorsqu'il n'y a pas de point de données et que vous avez attendu suffisamment longtemps

Comme c'est le cas avec une arrivée lente des données (ou aucune arrivée de données), le mécanisme de minuterie doit prendre le relais car le taux d'arrivée des données est insuffisant pour déclencher des alertes en « temps réel ». La question devient donc généralement : « Combien de temps dois-je attendre avant de fermer la fenêtre d'analyse et de regarder ce que j'ai ? » Si vous attendez trop longtemps, vous ne générez pas les alertes assez rapidement pour être utiles.

Si vous disposez d'un moniteur avec une fenêtre de 30 minutes qui détecte qu'une condition est violée par le dernier point de données avant une perte de données à long terme, une alerte sera générée car le moniteur n'a reçu aucune autre information à utiliser pour confirmer une récupération de la métrique ou pour signaler que la condition a persisté.

Alertes « actives en permanence »

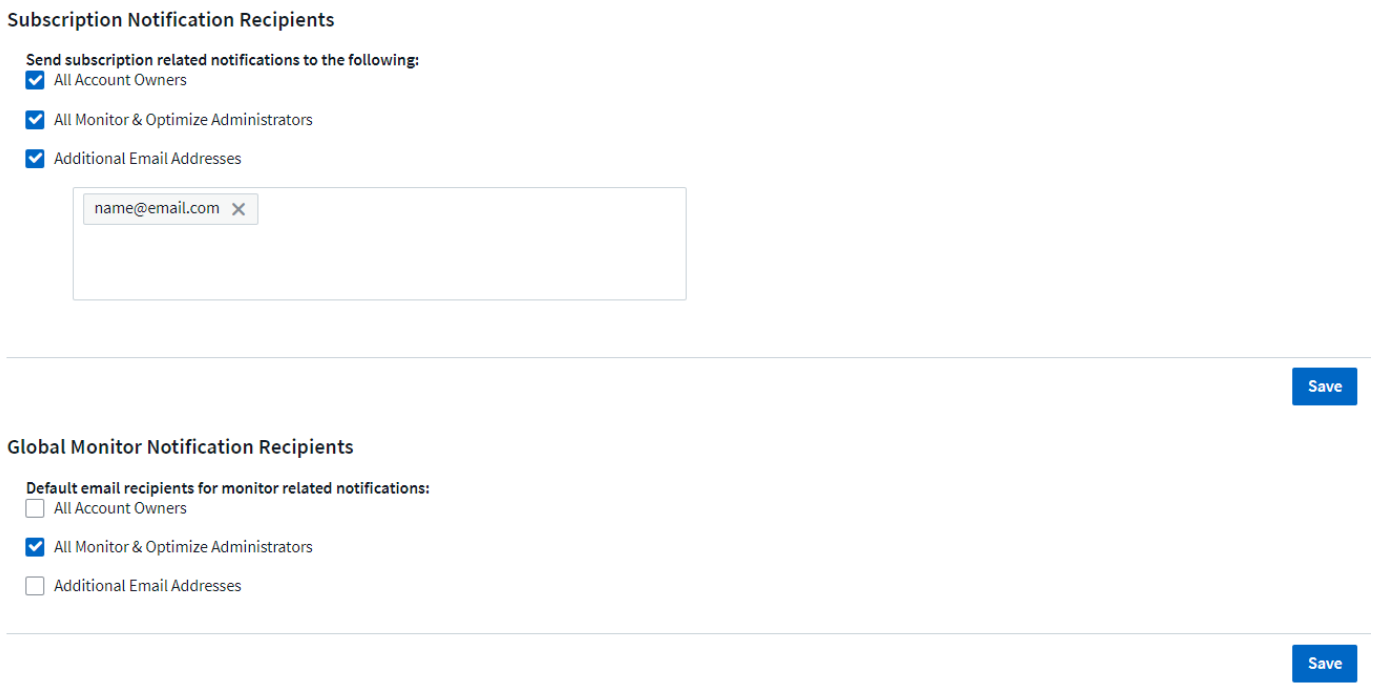
Il est possible de configurer un moniteur de telle manière que la condition existe **toujours** sur l'objet surveillé, par exemple, IOPS > 1 ou latence > 0. Ceux-ci sont souvent créés comme moniteurs « de test » puis oubliés. Ces moniteurs créent des alertes qui restent ouvertes en permanence sur les objets constitutifs, ce qui peut entraîner des problèmes de stress et de stabilité du système au fil du temps.

Pour éviter cela, Data Infrastructure Insights fermera automatiquement toute alerte « active en permanence » après 7 jours. Notez que les conditions de surveillance sous-jacentes peuvent (probablement) continuer à exister, provoquant l'émission d'une nouvelle alerte presque immédiatement, mais cette fermeture des alertes « toujours actives » atténue une partie du stress du système qui peut autrement se produire.

Configuration des notifications par e-mail

Vous pouvez configurer une liste de courrier électronique pour les notifications liées à l'abonnement, ainsi qu'une liste de courrier électronique globale de destinataires pour la notification des violations de seuil de politique de performances.

Pour configurer les paramètres des destinataires des e-mails de notification, accédez à la page **Admin > Notifications** et sélectionnez l'onglet *E-mail*.



Destinataires des notifications d'abonnement

Pour configurer les destinataires des notifications d'événements liés à l'abonnement, accédez à la section « Destinataires des notifications d'abonnement ». Vous pouvez choisir de recevoir des notifications par e-mail pour les événements liés à l'abonnement à tout ou partie des destinataires suivants :

- Tous les propriétaires de compte
- Tous les administrateurs *Monitor & Optimize*
- Adresses e-mail supplémentaires que vous spécifiez

Voici des exemples des types de notifications qui peuvent être envoyées et des actions utilisateur que vous pouvez effectuer.

Notification:	**Action de l'utilisateur :**
L'essai ou l'abonnement a été mis à jour	Consultez les détails de l'abonnement sur le"Abonnement" page
L'abonnement expirera dans 90 jours L'abonnement expirera dans 30 jours	Aucune action n'est nécessaire si le « Renouvellement automatique » est activé. Contactez le service commercial NetApp pour renouveler l'abonnement.
Le procès se termine dans 2 jours	Renouveler l'essai à partir du"Abonnement" page. Vous pouvez renouveler un essai une fois. Contactez le service commercial de NetApp pour acheter un abonnement
L'essai ou l'abonnement a expiré Le compte cessera de collecter des données dans 48 heures Le compte sera supprimé après 48 heures	Contactez le service commercial de NetApp pour acheter un abonnement

Pour garantir que vos destinataires reçoivent les notifications de Data Infrastructure Insights, ajoutez les adresses e-mail suivantes à toutes les listes « autorisées » :

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Liste globale des destinataires des alertes

Les notifications par courrier électronique des alertes sont envoyées à la liste des destinataires des alertes pour chaque action sur l'alerte. Vous pouvez choisir d'envoyer des notifications d'alerte à une liste de destinataires globale.

Pour configurer les destinataires d'alerte globale, choisissez les destinataires souhaités dans la section **Destinataires des notifications du moniteur global**.

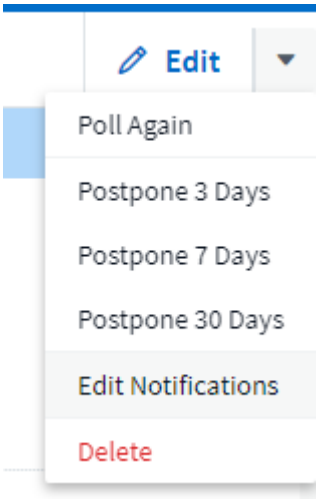
Vous pouvez toujours remplacer la liste des destinataires globaux pour un moniteur individuel lors de la création ou de la modification du moniteur.

Les notifications du collecteur de données ONTAP ont priorité sur toutes les notifications de surveillance spécifiques pertinentes pour le cluster/collecteur de données. La liste de destinataires que vous avez définie pour le collecteur de données lui-même recevra les alertes du collecteur de données. S'il n'y a pas d'alertes de collecteur de données actives, les alertes générées par le moniteur seront envoyées à des destinataires de moniteur spécifiques.

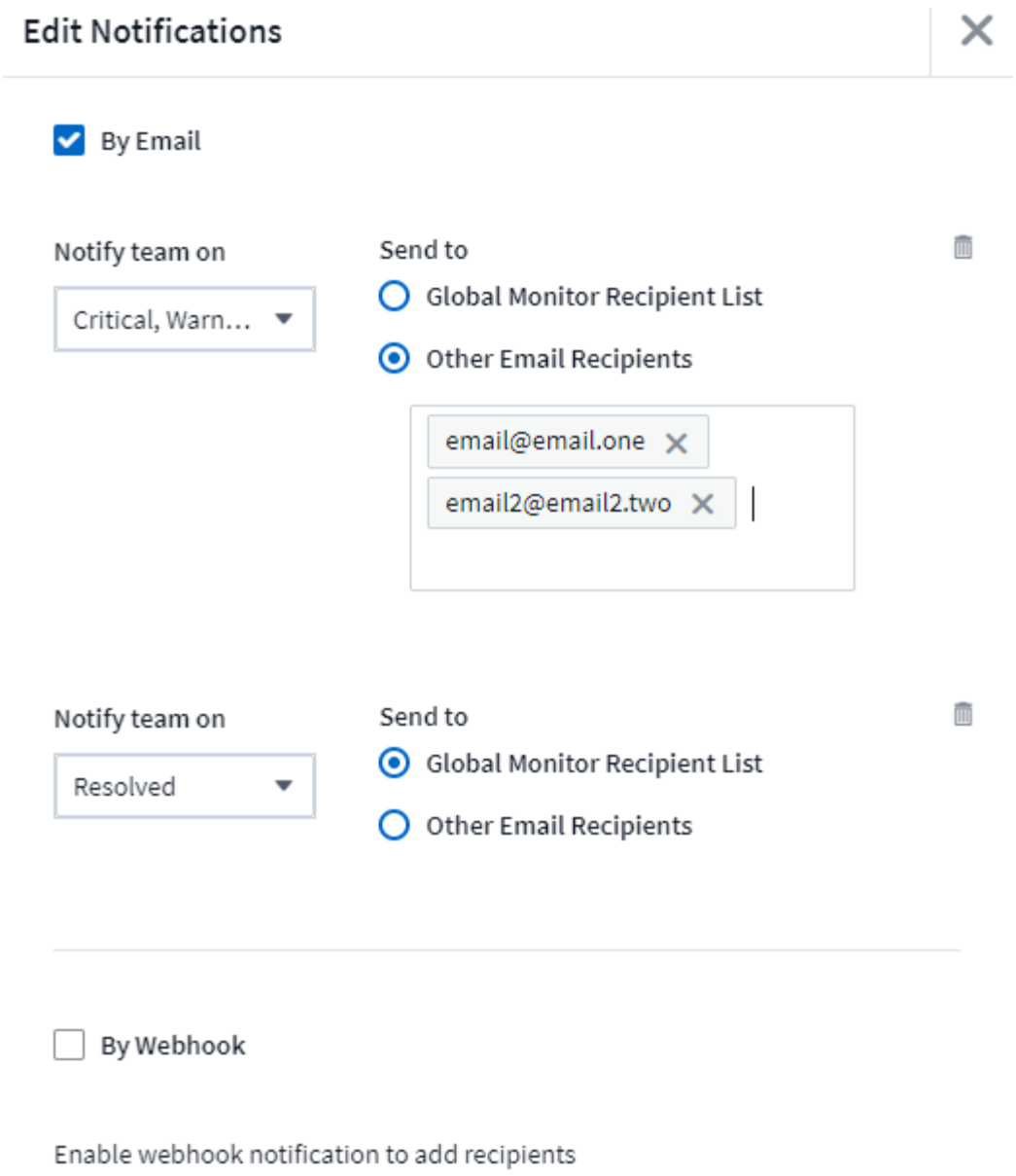
Modification des notifications pour ONTAP

Vous pouvez modifier les notifications pour les clusters ONTAP en sélectionnant *Modifier les notifications* dans

la liste déroulante supérieure droite d'une page de destination de stockage.



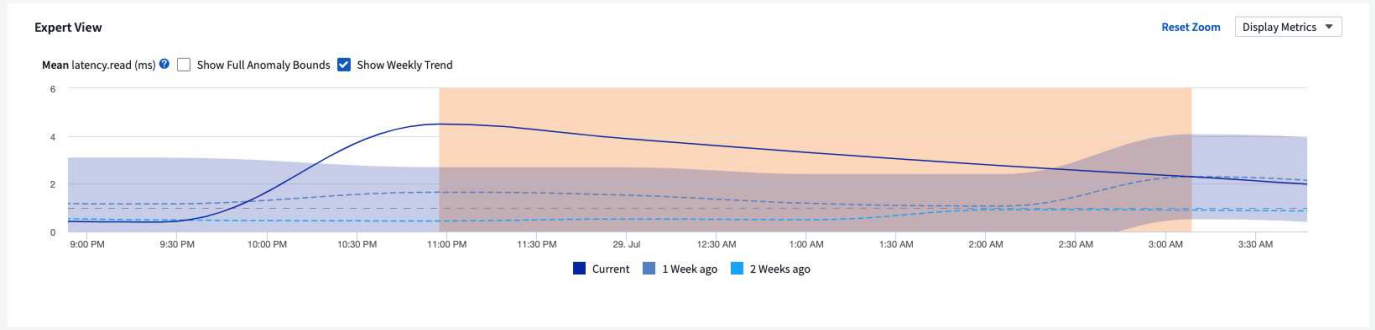
À partir de là, vous pouvez définir des notifications pour les alertes critiques, d'avertissement, d'information et/ou résolues. Chaque scénario peut notifier la liste des destinataires globaux ou d'autres destinataires de votre choix.



Moniteurs de détection d'anomalies

La détection des anomalies fournit un aperçu des changements inattendus dans les modèles de données de votre locataire. Une anomalie se produit lorsque le modèle de comportement d'un objet change, par exemple, si un objet subit un certain niveau de latence à un certain moment le mercredi, mais que la latence dépasse ce niveau à ce moment-là le mercredi suivant, ce pic serait considéré comme une anomalie. Data Infrastructure Insights permet la création de moniteurs pour alerter lorsque des anomalies telles que celle-ci se produisent.

La détection d'anomalies convient aux mesures d'objets qui présentent un modèle récurrent et prévisible. Lorsque ces mesures d'objet dépassent ou chutent en dessous de leurs niveaux attendus, Data Infrastructure Insights peut générer une alerte pour inciter à une enquête.



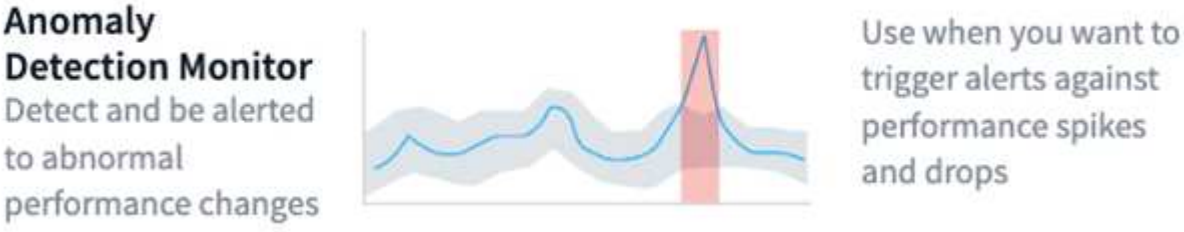
Qu'est-ce que la détection d'anomalies ?

Une anomalie se produit lorsque la valeur moyenne d'une mesure est éloignée d'un certain nombre d'écarts types de la moyenne pondérée de cette mesure pour les semaines précédentes, les semaines récentes ayant plus de poids que les semaines précédentes. Data Infrastructure Insights offre la possibilité de surveiller les données et d'alerter lorsque des anomalies sont détectées. Vous avez le choix de définir les niveaux de « sensibilité » de détection. Par exemple, une sensibilité plus élevée serait obtenue lorsque la valeur moyenne présente moins d'écarts types par rapport à la moyenne, ce qui entraînerait la génération d'un plus grand nombre d'alertes. À l'inverse, une sensibilité plus faible = plus d'écarts types par rapport à la moyenne = moins d'alertes.

La surveillance de la détection des anomalies diffère de la surveillance des seuils.

- **La surveillance basée sur des seuils** fonctionne lorsque vous avez des seuils prédéfinis pour des mesures spécifiques. En d'autres termes, lorsque vous avez une compréhension claire de ce qui est attendu (c'est-à-dire dans une fourchette normale).

- **La surveillance de détection d'anomalies** utilise des algorithmes d'apprentissage automatique pour identifier les valeurs aberrantes qui s'écartent de la norme, lorsque la définition de « normal » n'est pas claire.



Quand aurais-je besoin de la détection d'anomalies ?

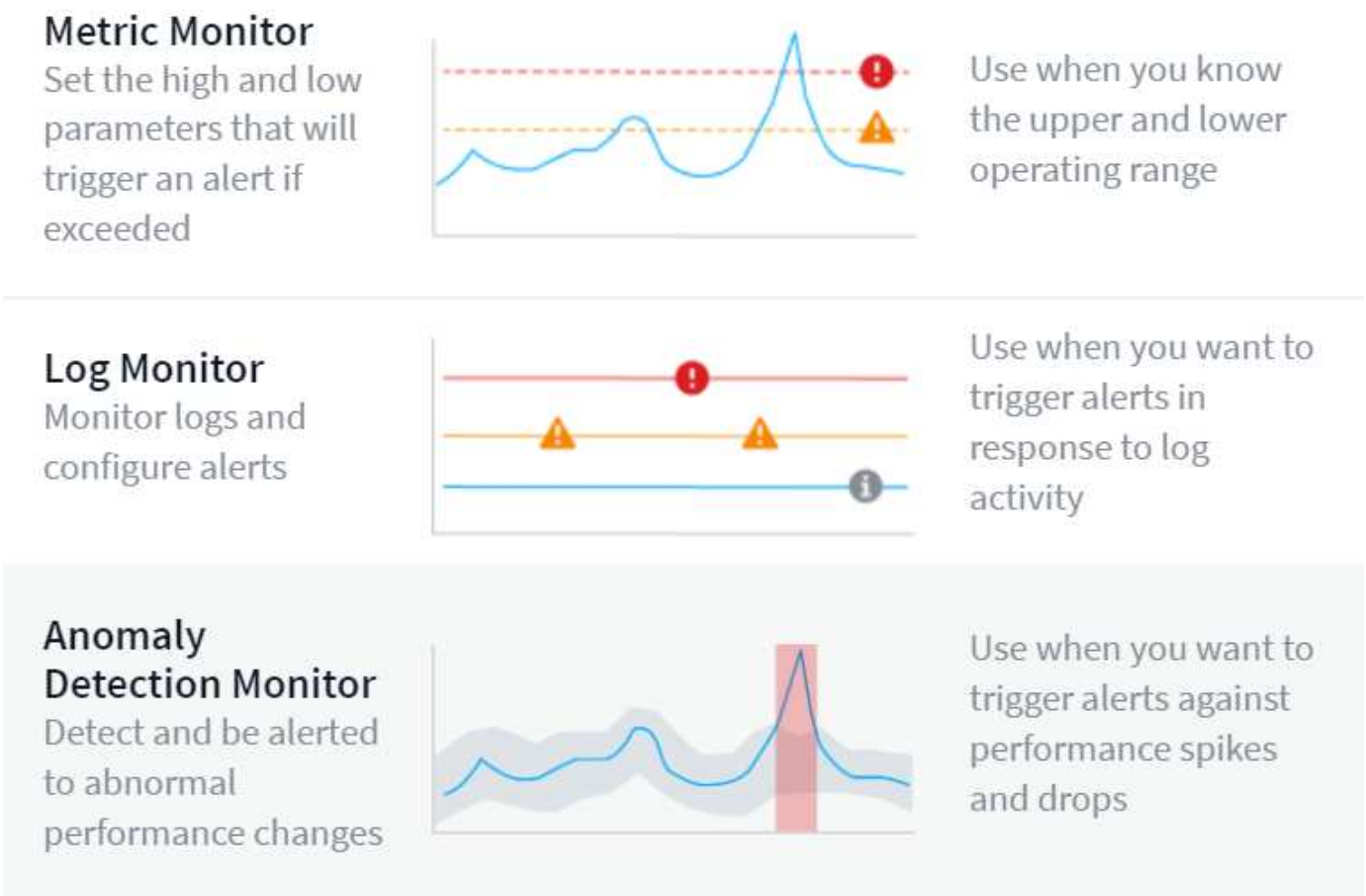
La surveillance de la détection des anomalies peut fournir des alertes utiles dans de nombreuses situations,

notamment les suivantes :

- Lorsque la définition de *normal* n'est pas claire. Par exemple, les taux d'erreur SAN peuvent être attendus à des niveaux variables selon le port. Alerter sur une erreur est bruyant et inutile, mais une augmentation soudaine ou significative pourrait indiquer un problème généralisé.
- Là où il y a des changements au fil du temps. Charges de travail qui présentent une saisonnalité (c'est-à-dire qu'elles sont occupées ou calmes à certains moments). Cela peut inclure des périodes de silence inattendues qui peuvent indiquer un blocage du lot.
- Travailler avec de grandes quantités de données où la définition et le réglage manuels des seuils ne sont pas pratiques. Par exemple, un locataire avec un grand nombre d'hôtes et/ou de volumes avec des charges de travail variables. Chacun peut avoir des SLA différents, il est donc important de comprendre ceux qui dépassent la norme.

Création d'un moniteur de détection d'anomalies

Pour alerter sur les anomalies, créez un moniteur en accédant à **Observabilité > Alertes > +Moniteur**. Sélectionnez *Anomaly Detection Monitor* comme type de moniteur.

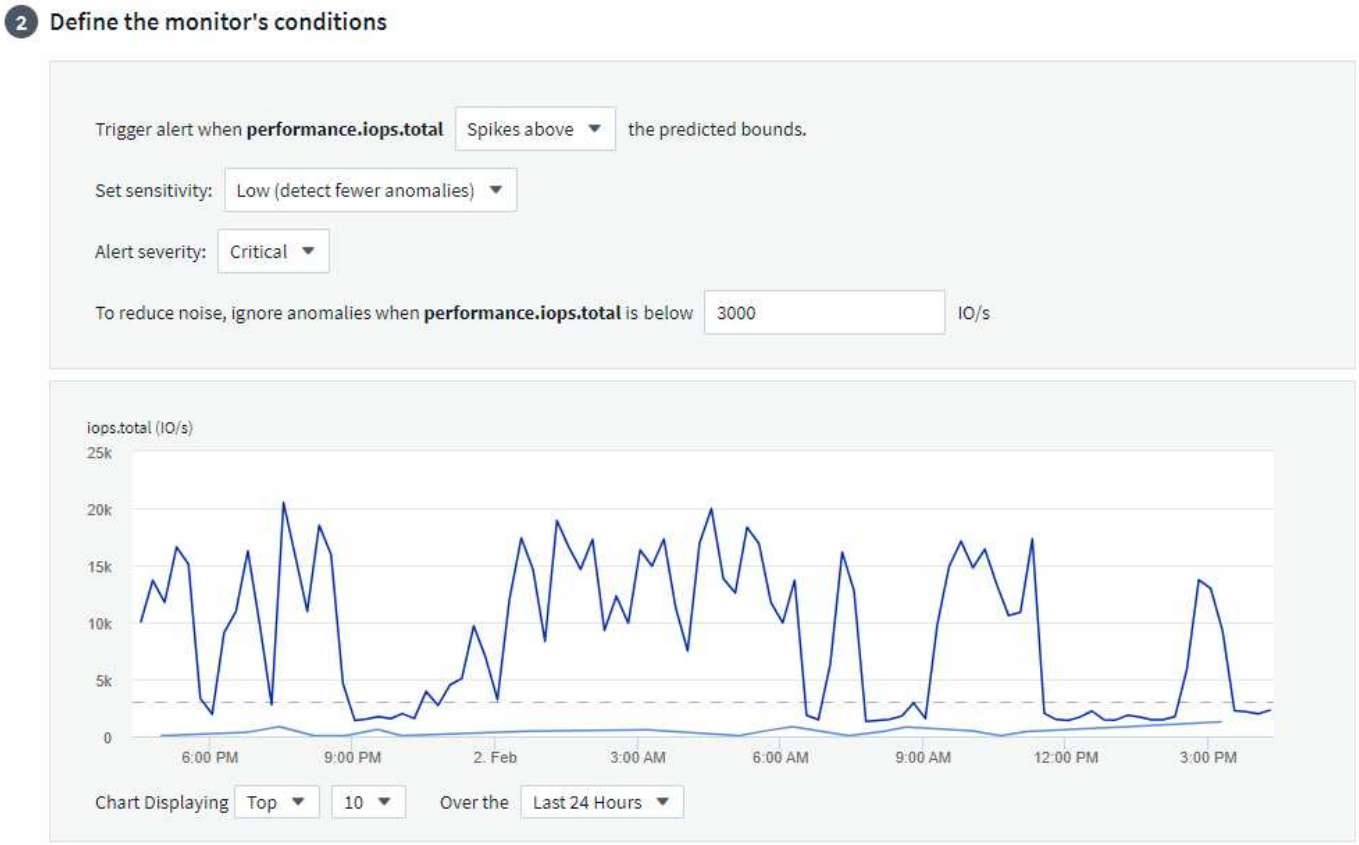


Choisissez l'objet et la métrique que vous souhaitez surveiller. Vous pouvez définir des filtres et des regroupements comme avec d'autres types de moniteurs.

Ensuite, définissez les conditions du moniteur.

- Déclenchez une alerte lorsque la métrique sélectionnée dépasse les limites prévues, chute en dessous de ces limites ou les deux.

- Définissez la sensibilité sur *Moyenne*, *Faible* (moins d'anomalies sont détectées) ou *Élevée* (plus d'anomalies sont détectées).
- Déterminez si le niveau d'alerte est *Critique* ou *Avertissement*.
- Vous pouvez également définir une valeur en dessous de laquelle les anomalies sont *ignorées*. Cela peut aider à réduire le bruit. Cette valeur est affichée sous forme de ligne pointillée sur l'exemple de graphique.



Enfin, vous pouvez configurer une méthode de livraison pour les alertes (e-mail, webhook ou les deux), donner au moniteur une description facultative ou des actions correctives et ajouter le moniteur à un groupe personnalisé, si vous le souhaitez.

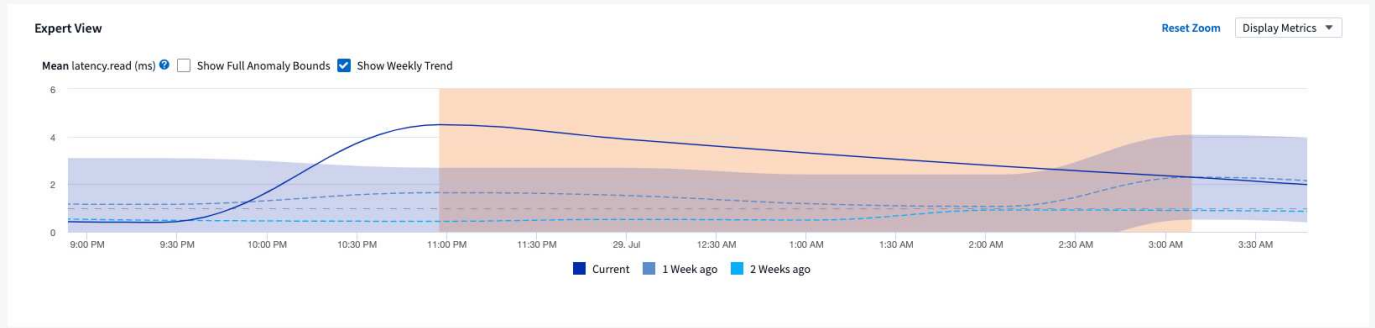
Enregistrez le moniteur avec un nom significatif et vous avez terminé.

Lors de sa création, le moniteur analyse les données de la semaine précédente pour établir une base de référence initiale. La détection des anomalies devient plus précise à mesure que le temps passe et que l'historique se déroule.

> Lorsqu'un moniteur est créé, DII examine toutes les données existantes de la semaine précédente pour détecter des pics ou des baisses de données significatifs ; ceux-ci sont considérés comme des anomalies. Au cours de la première semaine suivant la création du moniteur (la phase « d'apprentissage »), il existe un risque d'augmentation du « bruit » dans les alertes. Pour atténuer ce bruit, seuls les pics ou les chutes durant plus de 30 minutes sont considérés comme des anomalies et génèrent des alertes. Au cours de la semaine suivante, à mesure que davantage de données sont analysées, le bruit diminue généralement et un pic ou une baisse significative durant une certaine période sera considéré comme une anomalie.

Visualisation des anomalies

Sur une page de destination d'alerte, les alertes déclenchées lorsque des anomalies sont détectées afficheront une bande en surbrillance dans le graphique, à partir du moment où la métrique a dépassé les limites prévues jusqu'au moment où elle est revenue à l'intérieur de ces limites.



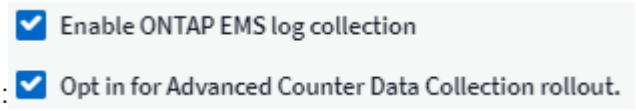
Lorsque vous consultez un graphique d'anomalie sur une page de destination d'alerte, vous pouvez choisir les options suivantes :

- Tendance hebdomadaire : comparez les valeurs à la même heure, au même jour des semaines précédentes, jusqu'à 5 semaines précédentes.
- Limites d'anomalie complètes : par défaut, le graphique se concentre sur la valeur de la métrique afin que vous puissiez mieux analyser le comportement de la métrique. Sélectionnez pour afficher les limites complètes de l'anomalie (valeur maximale, etc.)

Vous pouvez également afficher les objets qui ont contribué à l'anomalie en les sélectionnant dans la section des performances de la page de destination. Le graphique montrera le comportement des objets sélectionnés.

Moniteurs système

Data Infrastructure Insights comprend un certain nombre de moniteurs définis par le système pour les métriques et les journaux. Les moniteurs système disponibles dépendent des collecteurs de données présents sur votre locataire. De ce fait, les moniteurs disponibles dans Data Infrastructure Insights peuvent changer à mesure que des collecteurs de données sont ajoutés ou que leurs configurations sont modifiées.

De nombreux moniteurs système sont dans l'état *Paused* par défaut. Vous pouvez activer un moniteur système en sélectionnant l'option *Reprendre* pour le moniteur. Assurez-vous que *Collecte de données de compteur avancée* et *Activer la collecte de journaux ONTAP EMS* sont activés dans le collecteur de données ONTAP sous *Configuration avancée* : 

toc:[]

Descriptions des moniteurs

Les moniteurs définis par le système sont composés de mesures et de conditions prédéfinies, ainsi que de descriptions par défaut et d'actions correctives, qui ne peuvent pas être modifiées. Vous *pouvez* modifier la liste des destinataires des notifications pour les moniteurs définis par le système. Pour afficher les métriques, les conditions, la description et les actions correctives, ou pour modifier la liste des destinataires, ouvrez un groupe de moniteurs défini par le système et cliquez sur le nom du moniteur dans la liste.

Les groupes de moniteurs définis par le système ne peuvent pas être modifiés ou supprimés.

Les moniteurs définis par le système suivants sont disponibles, dans les groupes indiqués.

- * ONTAP Infrastructure* inclut des moniteurs pour les problèmes liés à l'infrastructure dans les clusters ONTAP .
- * Exemples de charge de travail ONTAP * inclut des moniteurs pour les problèmes liés à la charge de travail.
- Les moniteurs des deux groupes sont par défaut à l'état *Paused*.

Vous trouverez ci-dessous les moniteurs système actuellement inclus avec Data Infrastructure Insights:

Moniteurs métriques

Nom du moniteur	Gravité	Description du moniteur	Action corrective

Utilisation élevée des ports Fibre Channel	CRITIQUE	Les ports du protocole Fibre Channel sont utilisés pour recevoir et transférer le trafic SAN entre le système hôte client et les LUN ONTAP . Si l'utilisation du port est élevée, elle deviendra un goulot d'étranglement et affectera à terme les performances des charges de travail sensibles du protocole Fibre Channel. Une alerte d'avertissement indique qu'une action planifiée doit être prise pour équilibrer le trafic réseau. Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour équilibrer le trafic réseau afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Déplacez les charges de travail vers un autre port FCP moins utilisé. 2. Limitez le trafic de certains LUN uniquement aux travaux essentiels, soit via des politiques QoS dans ONTAP , soit via une configuration côté hôte pour alléger l'utilisation des ports FCP.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Configurez davantage de ports FCP pour gérer le trafic de données afin que l'utilisation du port soit répartie entre davantage de ports. 2. Déplacez les charges de travail vers un autre port FCP moins utilisé. 3. Limitez le trafic de certains LUN uniquement aux travaux essentiels, soit via des politiques QoS dans ONTAP , soit via une configuration côté hôte pour alléger l'utilisation des ports FCP.

Latence Lun élevée	CRITIQUE	Les LUN sont des objets qui servent au trafic d'E/S souvent généré par des applications sensibles aux performances telles que les bases de données. Des latences LUN élevées signifient que les applications elles-mêmes peuvent souffrir et être incapables d'accomplir leurs tâches.…Une alerte d'avertissement indique qu'une action planifiée doit être entreprise pour déplacer le LUN vers le nœud ou l'agrégat approprié.…Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour assurer la continuité du service. Voici les latences attendues en fonction du type de support : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et disque dur SATA 17 à 20 millisecondes	Si le seuil critique est dépassé, envisagez les actions suivantes pour minimiser les interruptions de service : si le LUN ou son volume est associé à une politique de qualité de service (QoS), évaluez ses limites de seuil et vérifiez si elles entraînent une limitation de la charge de travail du LUN. Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures suivantes : 1. Si l'agrégat connaît également une utilisation élevée, déplacez le LUN vers un autre agrégat. 2. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si le LUN ou son volume est associé à une stratégie QoS, évaluez ses limites de seuil et vérifiez si elles entraînent une limitation de la charge de travail du LUN.

Utilisation élevée des ports réseau	CRITIQUE	Les ports réseau sont utilisés pour recevoir et transférer le trafic des protocoles NFS, CIFS et iSCSI entre les systèmes hôtes clients et les volumes ONTAP . Si l'utilisation du port est élevée, cela devient un goulot d'étranglement et cela affectera à terme les performances des charges de travail NFS, CIFS et iSCSI.…Une alerte d'avertissement indique qu'une action planifiée doit être prise pour équilibrer le trafic réseau.…Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour équilibrer le trafic réseau afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Limitez le trafic de certains volumes uniquement aux travaux essentiels, soit via des politiques QoS dans ONTAP , soit via une analyse côté hôte pour réduire l'utilisation des ports réseau. 2. Configurez un ou plusieurs volumes pour utiliser un autre port réseau moins utilisé.… Si le seuil d'avertissement est dépassé, envisagez les actions immédiates suivantes : 1. Configurez davantage de ports réseau pour gérer le trafic de données afin que l'utilisation du port soit répartie entre davantage de ports. 2. Configurez un ou plusieurs volumes pour utiliser un autre port réseau moins utilisé.

Latence de l’espace de noms NVMe élevée	CRITIQUE	Les espaces de noms NVMe sont des objets qui servent au trafic d’E/S généré par des applications sensibles aux performances telles que les bases de données. Une latence élevée des espaces de noms NVMe signifie que les applications elles-mêmes peuvent souffrir et être incapables d’accomplir leurs tâches.…Une alerte d’avertissement indique qu’une action planifiée doit être entreprise pour déplacer le LUN vers le nœud ou l’agrégat approprié.…Une alerte critique indique qu’une interruption de service est imminente et que des mesures d’urgence doivent être prises pour assurer la continuité du service.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : si l’espace de noms NVMe ou son volume dispose d’une politique de qualité de service qui lui est attribuée, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail de l’espace de noms NVMe. Si le seuil d’avertissement est dépassé, envisagez de prendre les mesures suivantes : 1. Si l’agrégat connaît également une utilisation élevée, déplacez le LUN vers un autre agrégat. 2. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud. 3. Si l’espace de noms NVMe ou son volume dispose d’une politique QoS qui lui est attribuée, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail de l’espace de noms NVMe.

Capacité QTree complète	CRITIQUE	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota d'espace par défaut ou d'un quota défini par une politique de quota pour limiter la quantité de données stockées dans l'arbre dans la capacité du volume.…Une alerte d'avertissement indique qu'une action planifiée doit être entreprise pour augmenter l'espace.…Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité du service.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Augmentez l'espace du qtree afin de s'adapter à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace du qtree afin de s'adapter à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.

Limite stricte de capacité de QTree	CRITIQUE	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota d'espace mesuré en Ko qui est utilisé pour stocker des données afin de contrôler la croissance du volume de données utilisateur et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui fournit une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de quota de capacité totale dans le qtree et de ne plus pouvoir stocker de données. La surveillance de la quantité de données stockées dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmenter le quota d'espace des arbres afin de s'adapter à la croissance 2. Demandez à l'utilisateur de supprimer les données indésirables dans l'arborescence pour libérer de l'espace

Limite souple de capacité QTree	AVERTISSEMENT	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota d'espace mesuré en Ko qu'il peut utiliser pour stocker des données afin de contrôler la croissance du volume de données utilisateur et de ne pas dépasser sa capacité totale.…Un qtree maintient un quota de capacité de stockage souple qui fournit une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de quota de capacité totale dans le qtree et de ne plus pouvoir stocker de données. La surveillance de la quantité de données stockées dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, envisagez les actions immédiates suivantes : 1. Augmenter le quota d'espace des arbres pour s'adapter à la croissance. 2. Demandez à l'utilisateur de supprimer les données indésirables dans l'arborescence pour libérer de l'espace.

Limite stricte des fichiers QTree	CRITIQUE	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota du nombre de fichiers qu'il peut contenir pour maintenir une taille de système de fichiers gérable au sein du volume.…Un qtree maintient un quota de nombre de fichiers fixe au-delà duquel les nouveaux fichiers de l'arbre sont refusés. La surveillance du nombre de fichiers dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Augmentez le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers indésirables du système de fichiers qtree.
Limite souple des fichiers QTree	AVERTISSEMENT	Un qtree est un système de fichiers défini logiquement qui peut exister en tant que sous-répertoire spécial du répertoire racine dans un volume. Chaque qtree dispose d'un quota du nombre de fichiers qu'il peut contenir afin de maintenir une taille de système de fichiers gérable au sein du volume. Un qtree maintient un quota de nombre de fichiers souple pour fournir une alerte à l'utilisateur de manière proactive avant d'atteindre la limite de fichiers dans le qtree et de ne pas pouvoir stocker de fichiers supplémentaires. La surveillance du nombre de fichiers dans un qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez le quota de nombre de fichiers pour le qtree. 2. Supprimez les fichiers indésirables du système de fichiers qtree.

Instantané Réserve Espace Plein	CRITIQUE	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Une partie de cet espace, appelée espace réservé aux instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données nouvelles et mises à jour sont stockées dans le volume ONTAP , plus la capacité de snapshot est utilisée et moins la capacité de stockage de snapshot est disponible pour les données nouvelles ou mises à jour futures. Si la capacité des données de snapshot dans un volume atteint l'espace de réserve total de snapshot, le client peut être incapable de stocker de nouvelles données de snapshot et le niveau de protection des données dans le volume peut être réduit. La surveillance de la capacité de snapshot du volume utilisé garantit la continuité des services de données.	Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine. 2. Supprimez quelques anciens instantanés indésirables pour libérer de l'espace.… Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace de réserve d'instantanés dans le volume pour s'adapter à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine.

Limite de capacité de stockage	CRITIQUE	Lorsqu'un pool de stockage (agrégat) se remplit, les opérations d'E/S ralentissent et finissent par s'arrêter, ce qui entraîne un incident de panne de stockage. Une alerte d'avertissement indique qu'une action planifiée doit être entreprise prochainement pour restaurer l'espace libre minimum. Une alerte critique indique qu'une interruption de service est imminente et que des mesures d'urgence doivent être prises pour libérer de l'espace afin d'assurer la continuité du service.	Si le seuil critique est dépassé, envisagez immédiatement les actions suivantes pour minimiser les interruptions de service : 1. Supprimer les instantanés sur les volumes non critiques. 2. Supprimez les volumes ou les LUN qui sont des charges de travail non essentielles et qui peuvent être restaurés à partir de copies hors stockage. Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Déplacez un ou plusieurs volumes vers un autre emplacement de stockage. 2. Ajoutez plus de capacité de stockage. 3. Modifiez les paramètres d'efficacité du stockage ou hiérarchisez les données inactives vers le stockage cloud.

Limite de performance de stockage	CRITIQUE	Lorsqu'un système de stockage atteint sa limite de performances, les opérations ralentissent, la latence augmente et les charges de travail et les applications peuvent commencer à échouer. ONTAP évalue l'utilisation du pool de stockage pour les charges de travail et estime le pourcentage de performances consommé.…Une alerte d'avertissement indique qu'une action planifiée doit être prise pour réduire la charge du pool de stockage afin de garantir qu'il restera suffisamment de performances du pool de stockage pour répondre aux pics de charge de travail.…Une alerte critique indique qu'une baisse de performances est imminente et que des mesures d'urgence doivent être prises pour réduire la charge du pool de stockage afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Suspendez les tâches planifiées telles que les instantanés ou la réplication SnapMirror . 2. Charges de travail non essentielles inactives.… Si le seuil d'avertissement est dépassé, prenez immédiatement les mesures suivantes : 1. Déplacez une ou plusieurs charges de travail vers un autre emplacement de stockage. 2. Ajoutez davantage de nœuds de stockage (AFF) ou d'étagères de disques (FAS) et redistribuez les charges de travail 3. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications).

Limite stricte de capacité de quota utilisateur	CRITIQUE	ONTAP reconnaît les utilisateurs de systèmes Unix ou Windows qui ont le droit d'accéder aux volumes, fichiers ou répertoires d'un volume. Par conséquent, ONTAP permet aux clients de configurer la capacité de stockage pour leurs utilisateurs ou groupes d'utilisateurs de leurs systèmes Linux ou Windows. Le quota de stratégie d'utilisateur ou de groupe limite la quantité d'espace que l'utilisateur peut utiliser pour ses propres données. Une limite stricte de ce quota permet de notifier l'utilisateur lorsque la quantité de capacité utilisée dans le volume est juste avant d'atteindre le quota de capacité totale. La surveillance de la quantité de données stockées dans un quota d'utilisateur ou de groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmentez l'espace du quota utilisateur ou groupe afin de s'adapter à la croissance. 2. Demandez à l'utilisateur ou au groupe de supprimer les données indésirables pour libérer de l'espace.

Limite souple de capacité de quota utilisateur	AVERTISSEMENT	ONTAP reconnaît les utilisateurs de systèmes Unix ou Windows qui ont le droit d'accéder aux volumes, fichiers ou répertoires d'un volume. Par conséquent, ONTAP permet aux clients de configurer la capacité de stockage pour leurs utilisateurs ou groupes d'utilisateurs de leurs systèmes Linux ou Windows. Le quota de stratégie d'utilisateur ou de groupe limite la quantité d'espace que l'utilisateur peut utiliser pour ses propres données. Une limite souple de ce quota permet une notification proactive à l'utilisateur lorsque la quantité de capacité utilisée dans le volume atteint le quota de capacité totale. La surveillance de la quantité de données stockées dans un quota d'utilisateur ou de groupe garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace du quota utilisateur ou groupe afin de s'adapter à la croissance. 2. Supprimez les données indésirables pour libérer de l'espace.

Volume Capacité Plein	CRITIQUE	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Plus les données stockées dans le volume ONTAP sont nombreuses, moins il y a de disponibilité de stockage pour les données futures. Si la capacité de stockage des données dans un volume atteint la capacité de stockage totale, le client peut être incapable de stocker des données en raison d'un manque de capacité de stockage. La surveillance du volume de capacité de stockage utilisé garantit la continuité des services de données.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmentez l'espace du volume pour accueillir la croissance. 2. Supprimez les données indésirables pour libérer de l'espace. 3. Si les copies d'instantanés occupent plus d'espace que la réserve d'instantanés, supprimez les anciens instantanés ou activez la suppression automatique des instantanés de volume.…Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmenter l'espace du volume afin d'accueillir la croissance 2. Si les copies d'instantanés occupent plus d'espace que la réserve d'instantanés, supprimez les anciens instantanés ou activez la suppression automatique des instantanés de volume.……

Limite de volume d’inodes	CRITIQUE	Les volumes qui stockent des fichiers utilisent des nœuds d’index (inode) pour stocker les métadonnées des fichiers. Lorsqu’un volume épuise son allocation d’inodes, aucun fichier supplémentaire ne peut y être ajouté. Une alerte d’avertissement indique qu’une action planifiée doit être entreprise pour augmenter le nombre d’inodes disponibles. Une alerte critique indique que l’épuisement de la limite de fichiers est imminent et que des mesures d’urgence doivent être prises pour libérer des inodes afin de garantir la continuité du service.	Si le seuil critique est dépassé, envisagez les actions immédiates suivantes pour minimiser les interruptions de service : 1. Augmentez la valeur des inodes pour le volume. Si la valeur des inodes est déjà à la valeur maximale, divisez le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale. 2. Utilisez FlexGroup car il permet de prendre en charge des systèmes de fichiers volumineux.… Si le seuil d’avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez la valeur des inodes pour le volume. Si la valeur des inodes est déjà au maximum, divisez le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale. 2. Utilisez FlexGroup car il permet de prendre en charge des systèmes de fichiers volumineux

Volume Latence élevée	CRITIQUE	Les volumes sont des objets qui servent le trafic d'E/S souvent généré par des applications sensibles aux performances, notamment les applications DevOps, les répertoires personnels et les bases de données. Des latences de volume élevées signifient que les applications elles-mêmes peuvent en souffrir et être incapables d'accomplir leurs tâches. La surveillance des latences de volume est essentielle pour maintenir des performances cohérentes des applications. Les latences suivantes sont attendues en fonction du type de support : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et disque dur SATA 17 à 20 millisecondes.	Si le seuil critique est dépassé, envisagez de suivre les actions immédiates pour minimiser les interruptions de service : si une politique de qualité de service (QoS) est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. Si le seuil d'avertissement est dépassé, envisagez les actions immédiates suivantes : 1. Si l'agrégat connaît également une utilisation élevée, déplacez le volume vers un autre agrégat. 2. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. 3. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud.
Nom du moniteur	Gravité	Description du moniteur	Action corrective

Nœud à latence élevée	AVERTISSEMENT / CRITIQUE	La latence du nœud a atteint des niveaux où elle pourrait affecter les performances des applications sur le nœud. Une latence de nœud plus faible garantit des performances constantes des applications. Les latences attendues en fonction du type de support sont : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et HDD SATA 17 à 20 millisecondes.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Suspendre les tâches planifiées, les instantanés ou la réplication SnapMirror 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Désactiver les charges de travail non essentielles Envisagez des actions immédiates lorsque le seuil d'avertissement est dépassé : 1. Déplacer une ou plusieurs charges de travail vers un autre emplacement de stockage 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Ajoutez davantage de nœuds de stockage (AFF) ou d'étagères de disques (FAS) et redistribuez les charges de travail 4. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Limite de performance du nœud	AVERTISSEMENT / CRITIQUE	L'utilisation des performances du nœud a atteint des niveaux où elle pourrait affecter les performances des E/S et des applications prises en charge par le nœud. Une faible utilisation des performances des nœuds garantit des performances constantes des applications.	Des mesures immédiates doivent être prises pour minimiser les interruptions de service si le seuil critique est dépassé : 1. Suspendre les tâches planifiées, les instantanés ou la réplication SnapMirror 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Désactiver les charges de travail non essentielles Envisagez les actions suivantes si le seuil d'avertissement est dépassé : 1. Déplacer une ou plusieurs charges de travail vers un autre emplacement de stockage 2. Réduisez la demande de charges de travail de moindre priorité via des limites de QoS 3. Ajoutez davantage de nœuds de stockage (AFF) ou d'étagères de disques (FAS) et redistribuez les charges de travail 4. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Machine virtuelle de stockage à latence élevée	AVERTISSEMENT / CRITIQUE	La latence de la machine virtuelle de stockage (SVM) a atteint des niveaux où elle pourrait affecter les performances des applications sur la machine virtuelle de stockage. La faible latence des machines virtuelles de stockage garantit des performances constantes des applications. Les latences attendues en fonction du type de support sont : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et HDD SATA 17 à 20 millisecondes.	Si le seuil critique est dépassé, évaluez immédiatement les limites de seuil pour les volumes de la machine virtuelle de stockage avec une politique QoS attribuée, afin de vérifier si elles entraînent une limitation des charges de travail du volume. Envisagez les actions immédiates suivantes lorsque le seuil d'avertissement est dépassé : 1. Si l'agrégat connaît également une utilisation élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre agrégat. 2. Pour les volumes de la machine virtuelle de stockage avec une politique QoS attribuée, évaluez les limites de seuil si elles entraînent une limitation des charges de travail du volume 3. Si le nœud connaît une utilisation élevée, déplacez certains volumes de la machine virtuelle de stockage vers un autre nœud ou réduisez la charge de travail totale du nœud.
Limite stricte des fichiers de quotas utilisateur	CRITIQUE	Le nombre de fichiers créés dans le volume a atteint la limite critique et des fichiers supplémentaires ne peuvent pas être créés. La surveillance du nombre de fichiers stockés garantit que l'utilisateur reçoit un service de données ininterrompu.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé.…Envisagez de prendre les mesures suivantes : 1. Augmenter le quota de nombre de fichiers pour l'utilisateur spécifique 2. Supprimez les fichiers indésirables pour réduire la pression sur le quota de fichiers pour l'utilisateur spécifique

Limite souple des fichiers de quotas utilisateur	AVERTISSEMENT	Le nombre de fichiers créés dans le volume a atteint la limite du quota et est proche de la limite critique. Vous ne pouvez pas créer de fichiers supplémentaires si le quota atteint la limite critique. La surveillance du nombre de fichiers stockés par un utilisateur garantit que l'utilisateur reçoit un service de données ininterrompu.	Envisagez des actions immédiates si le seuil d'alerte est dépassé : 1. Augmenter le quota de nombre de fichiers pour le quota utilisateur spécifique 2. Supprimez les fichiers indésirables pour réduire la pression sur le quota de fichiers pour l'utilisateur spécifique

Taux d’échec du cache de volume	AVERTISSEMENT / CRITIQUE	Le ratio de manque de cache de volume est le pourcentage de demandes de lecture provenant des applications clientes qui sont renvoyées depuis le disque au lieu d’être renvoyées depuis le cache. Cela signifie que le volume a atteint le seuil défini.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d’E/S 2. S’il n’est pas déjà présent sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un Flash Cache 3. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites de QoS. Envisagez des actions immédiates lorsque le seuil d’avertissement est dépassé : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d’E/S 2. S’il n’est pas déjà présent sur le nœud du volume, augmentez le cache WAFL en achetant et en ajoutant un Flash Cache 3. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites QoS 4. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Surengagement de quota de volume Qtree	AVERTISSEMENT / CRITIQUE	Volume Qtree Quota Overcommit spécifie le pourcentage auquel un volume est considéré comme surengagé par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du dépassement de quota du volume qtree garantit que l'utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Augmenter l'espace du volume 2. Supprimer les données indésirables Lorsque le seuil d'avertissement est dépassé, envisagez d'augmenter l'espace du volume.

Retour en haut

Moniteurs de journaux

Nom du moniteur	Gravité	Description	Action corrective
Informations d'identification AWS non initialisées	INFO	Cet événement se produit lorsqu'un module tente d'accéder aux informations d'identification basées sur les rôles Amazon Web Services (AWS) Identity and Access Management (IAM) à partir du thread d'informations d'identification cloud avant leur initialisation.	Attendez que le thread d'informations d'identification cloud, ainsi que le système, terminent l'initialisation.

Niveau Cloud inaccessible	CRITIQUE	Un nœud de stockage ne peut pas se connecter à l'API du magasin d'objets Cloud Tier. Certaines données seront inaccessibles.	Si vous utilisez des produits sur site, effectuez les actions correctives suivantes : …Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show ». …Vérifiez la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le LIF intercluster du nœud de destination. …Assurez-vous des points suivants : …La configuration de votre magasin d'objets n'a pas changé. …Les informations de connexion et de connectivité sont toujours valides. …Contactez le support technique NetApp si le problème persiste. Si vous utilisez Cloud Volumes ONTAP, effectuez les actions correctives suivantes : …Assurez-vous que la configuration de votre magasin d'objets n'a pas changé.… Assurez-vous que les informations de connexion et de connectivité sont toujours valides. Contactez le support technique NetApp si le problème persiste.
Disque hors service	INFO	Cet événement se produit lorsqu'un disque est retiré du service parce qu'il a été marqué comme défectueux, est en cours de nettoyage ou est entré dans le centre de maintenance.	Aucun.

FlexGroup Constituent Full	CRITIQUE	Un constituant d'un volume FlexGroup est plein, ce qui peut entraîner une interruption potentielle du service. Vous pouvez toujours créer ou développer des fichiers sur le volume FlexGroup . Cependant, aucun des fichiers stockés sur le constituant ne peut être modifié. Par conséquent, vous risquez de voir des erreurs aléatoires de manque d'espace lorsque vous essayez d'effectuer des opérations d'écriture sur le volume FlexGroup .	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.
Le constituant de Flexgroup est presque plein	AVERTISSEMENT	Un constituant d'un volume FlexGroup est presque à court d'espace, ce qui peut entraîner une interruption potentielle du service. Les fichiers peuvent être créés et développés. Cependant, si le constituant manque d'espace, vous ne pourrez peut-être pas ajouter ou modifier les fichiers sur le constituant.	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.
Le constituant de FlexGroup est presque à court d'inodes	AVERTISSEMENT	Un constituant d'un volume FlexGroup est presque à court d'inodes, ce qui peut entraîner une interruption potentielle du service. Le constituant reçoit moins de demandes de création que la moyenne. Cela peut avoir un impact sur les performances globales du volume FlexGroup , car les demandes sont acheminées vers les composants avec plus d'inodes.	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.

Constituant FlexGroup hors des inodes	CRITIQUE	Un constituant d'un volume FlexGroup est à court d'inodes, ce qui peut entraîner une interruption potentielle du service. Vous ne pouvez pas créer de nouveaux fichiers sur ce constituant. Cela pourrait conduire à une distribution globalement déséquilibrée du contenu sur le volume FlexGroup .	Il est recommandé d'ajouter de la capacité au volume FlexGroup en utilisant la commande « volume modify -files +X ». Vous pouvez également supprimer les fichiers du volume FlexGroup . Il est toutefois difficile de déterminer quels dossiers ont atterri chez le mandant.
LUN hors ligne	INFO	Cet événement se produit lorsqu'un LUN est mis hors ligne manuellement.	Remettez le LUN en ligne.
Panne du ventilateur de l'unité principale	AVERTISSEMENT	Un ou plusieurs ventilateurs de l'unité principale sont en panne. Le système reste opérationnel.…Cependant , si la condition persiste trop longtemps, la surchauffe peut déclencher un arrêt automatique.	Réinstallez les ventilateurs défectueux. Si l'erreur persiste, remplacez-les.
Ventilateur de l'unité principale en état d'avertissement	INFO	Cet événement se produit lorsqu'un ou plusieurs ventilateurs de l'unité principale sont dans un état d'avertissement.	Remplacez les ventilateurs indiqués pour éviter la surchauffe.

Batterie NVRAM faible	AVERTISSEMENT	La capacité de la batterie NVRAM est extrêmement faible. Il peut y avoir une perte de données potentielle si la batterie est déchargée. Votre système génère et transmet un message AutoSupport ou « appel à domicile » au support technique NetApp et aux destinations configurées s'il est configuré pour le faire. La livraison réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Effectuez les actions correctives suivantes :…Affichez l'état actuel de la batterie, sa capacité et son état de charge à l'aide de la commande « system node environment sensors show »….Si la batterie a été remplacée récemment ou si le système n'a pas été opérationnel pendant une période prolongée, surveillez la batterie pour vérifier qu'elle se charge correctement.…Contactez le support technique NetApp si l'autonomie de la batterie continue de diminuer en dessous des niveaux critiques et que le système de stockage s'arrête automatiquement.
Processeur de service non configuré	AVERTISSEMENT	Cet événement se produit chaque semaine pour vous rappeler de configurer le processeur de service (SP). Le SP est un périphérique physique intégré à votre système pour fournir des capacités d'accès à distance et de gestion à distance. Vous devez configurer le SP pour utiliser toutes ses fonctionnalités.	Effectuez les actions correctives suivantes :…Configurez le SP à l'aide de la commande « system service-processor network modify ».…Vous pouvez également obtenir l'adresse MAC du SP à l'aide de la commande « system service-processor network show ».…Vérifiez la configuration réseau du SP à l'aide de la commande « system service-processor network show ».…Vérifiez que le SP peut envoyer un e-mail AutoSupport à l'aide de la commande « system service-processor autosupport invoke ». REMARQUE : les hôtes et les destinataires de messagerie AutoSupport doivent être configurés dans ONTAP avant d'émettre cette commande.

Processeur de service hors ligne	CRITIQUE	ONTAP ne reçoit plus de pulsations du processeur de service (SP), même si toutes les actions de récupération du SP ont été effectuées. ONTAP ne peut pas surveiller l'état du matériel sans le SP… Le système s'arrêtera pour éviter tout dommage matériel et toute perte de données. Configurez une alerte panique pour être averti immédiatement si le SP se déconnecte.	Redémarrez le système en effectuant les actions suivantes :…Retirez le contrôleur du châssis.…Remettez le contrôleur en place.…Rallumez le contrôleur.…Si le problème persiste, remplacez le module du contrôleur.
Les ventilateurs d'étagère sont en panne	CRITIQUE	Le ventilateur de refroidissement ou le module de ventilateur indiqué de l'étagère est en panne. Il est possible que les disques de l'étagère ne reçoivent pas suffisamment de flux d'air de refroidissement, ce qui peut entraîner une panne du disque.	Effectuez les actions correctives suivantes :…Vérifiez que le module du ventilateur est bien en place et fixé. REMARQUE : le ventilateur est intégré au module d'alimentation de certaines étagères de disques. Si le problème persiste, remplacez le module de ventilateur. Si le problème persiste, contactez le support technique NetApp pour obtenir de l'aide.
Le système ne peut pas fonctionner en raison d'une panne du ventilateur de l'unité principale	CRITIQUE	Un ou plusieurs ventilateurs de l'unité principale sont tombés en panne, perturbant le fonctionnement du système. Cela pourrait entraîner une perte potentielle de données.	Remplacez les ventilateurs défectueux.
Disques non attribués	INFO	Le système possède des disques non attribués : la capacité est gaspillée et votre système peut être soumis à une mauvaise configuration ou à une modification partielle de la configuration.	Effectuez les actions correctives suivantes :…Déterminez quels disques ne sont pas attribués à l'aide de la commande « disk show -n ».…Attribuez les disques à un système à l'aide de la commande « disk assign ».

Serveur antivirus occupé	AVERTISSEMENT	Le serveur antivirus est trop occupé pour accepter de nouvelles demandes d'analyse.	Si ce message apparaît fréquemment, assurez-vous qu'il existe suffisamment de serveurs antivirus pour gérer la charge d'analyse antivirus générée par le SVM.
Les informations d'identification AWS pour le rôle IAM ont expiré	CRITIQUE	Cloud Volume ONTAP est devenu inaccessible. Les informations d'identification basées sur les rôles de gestion des identités et des accès (IAM) ont expiré. Les informations d'identification sont acquises auprès du serveur de métadonnées Amazon Web Services (AWS) à l'aide du rôle IAM et sont utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3).	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.
Informations d'identification AWS pour le rôle IAM introuvables	CRITIQUE	Le thread d'informations d'identification cloud ne peut pas acquérir les informations d'identification basées sur les rôles Amazon Web Services (AWS) Identity and Access Management (IAM) à partir du serveur de métadonnées AWS. Les informations d'identification sont utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.

Les informations d'identification AWS pour le rôle IAM ne sont pas valides	CRITIQUE	Les informations d'identification basées sur les rôles de gestion des identités et des accès (IAM) ne sont pas valides. Les informations d'identification sont acquises auprès du serveur de métadonnées Amazon Web Services (AWS) à l'aide du rôle IAM et sont utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.
Rôle AWS IAM introuvable	CRITIQUE	Le thread des rôles de gestion des identités et des accès (IAM) ne trouve pas de rôle IAM Amazon Web Services (AWS) sur le serveur de métadonnées AWS. Le rôle IAM est requis pour acquérir les informations d'identification basées sur les rôles utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide.
Rôle AWS IAM non valide	CRITIQUE	Le rôle Amazon Web Services (AWS) Identity and Access Management (IAM) sur le serveur de métadonnées AWS n'est pas valide. Le Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…Vérifiez que le rôle AWS IAM associé à l'instance est valide et que les privilèges appropriés lui ont été accordés.

Échec de la connexion au serveur de métadonnées AWS	CRITIQUE	Le thread des rôles de gestion des identités et des accès (IAM) ne peut pas établir de lien de communication avec le serveur de métadonnées Amazon Web Services (AWS). Une communication doit être établie pour acquérir les informations d'identification basées sur les rôles AWS IAM nécessaires utilisées pour signer les demandes d'API à Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP est devenu inaccessible.…	Procédez comme suit :…Connectez-vous à la console de gestion AWS EC2.…Accédez à la page Instances.…Recherchez l'instance pour le déploiement Cloud Volumes ONTAP et vérifiez son état.…
La limite d'utilisation de l'espace FabricPool est presque atteinte	AVERTISSEMENT	L'utilisation totale de l'espace FabricPool à l'échelle du cluster des magasins d'objets provenant de fournisseurs sous licence de capacité a presque atteint la limite sous licence.	Effectuez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque niveau de stockage FabricPool à l'aide de la commande « storage aggregate object-store show-space ».…Supprimez les copies Snapshot des volumes avec la stratégie de hiérarchisation « snapshot » ou « backup » à l'aide de la commande « volume snapshot delete » pour libérer de l'espace.…Installez une nouvelle licence sur le cluster pour augmenter la capacité sous licence.

Limite d’utilisation de l’espace FabricPool atteinte	CRITIQUE	L’utilisation totale de l’espace FabricPool à l’échelle du cluster des magasins d’objets provenant de fournisseurs sous licence de capacité a atteint la limite de licence.	Effectuez les actions correctives suivantes :…Vérifiez le pourcentage de la capacité sous licence utilisée par chaque niveau de stockage FabricPool à l’aide de la commande « storage aggregate object-store show-space ».…Supprimez les copies Snapshot des volumes avec la stratégie de hiérarchisation « snapshot » ou « backup » à l’aide de la commande « volume snapshot delete » pour libérer de l’espace.…Installez une nouvelle licence sur le cluster pour augmenter la capacité sous licence.

Échec de la restitution des agrégats	CRITIQUE	Cet événement se produit lors de la migration d'un agrégat dans le cadre d'un basculement de stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes :… Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show »…. Vérifiez la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le LIF intercluster du nœud de destination. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show »….Vous pouvez également remplacer l'erreur en spécifiant false pour le paramètre « require-partner-waiting » de la commande giveback.…Contactez le support technique NetApp pour obtenir plus d'informations ou une assistance.

Interconnexion HA en panne	AVERTISSEMENT	L'interconnexion haute disponibilité (HA) est en panne. Risque d'interruption de service lorsque le basculement n'est pas disponible.	Les actions correctives dépendent du nombre et du type de liens d'interconnexion HA pris en charge par la plate-forme, ainsi que de la raison pour laquelle l'interconnexion est en panne. …Si les liaisons sont interrompues :…Vérifiez que les deux contrôleurs de la paire HA sont opérationnels.…Pour les liaisons connectées en externe, assurez-vous que les câbles d'interconnexion sont correctement connectés et que les modules enfichables à petit facteur de forme (SFP), le cas échéant, sont correctement installés sur les deux contrôleurs.…Pour les liaisons connectées en interne, désactivez et réactivez les liaisons, l'une après l'autre, en utilisant les commandes « ic link off » et « ic link on ». …Si les liens sont désactivés, activez-les en utilisant la commande « ic link on ». …Si un homologue n'est pas connecté, désactivez et réactivez les liens, l'un après l'autre, en utilisant les commandes « ic link off » et « ic link on ».…Contactez le support technique NetApp si le problème persiste.

Nombre maximal de sessions par utilisateur dépassé	AVERTISSEMENT	Vous avez dépassé le nombre maximal de sessions autorisées par utilisateur sur une connexion TCP. Toute demande d'établissement d'une session sera refusée jusqu'à ce que certaines sessions soient libérées. …	Effectuez les actions correctives suivantes : …Inspectez toutes les applications qui s'exécutent sur le client et fermez celles qui ne fonctionnent pas correctement. …Redémarrez le client. …Vérifiez si le problème est causé par une application nouvelle ou existante : …Si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande « cifs option modify -max -opens-same-file-per -tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer de privilèges avancés pour définir un seuil plus élevé pour le client. …Si le problème est causé par une application existante, il peut y avoir un problème avec le client. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Nombre maximal de fois par fichier ouvert dépassé	AVERTISSEMENT	Vous avez dépassé le nombre maximal de fois que vous pouvez ouvrir le fichier via une connexion TCP. Toute demande d'ouverture de ce fichier sera refusée jusqu'à ce que vous fermiez certaines instances ouvertes du fichier. Cela indique généralement un comportement anormal de l'application.	Effectuez les actions correctives suivantes :…Inspectez les applications qui s'exécutent sur le client à l'aide de cette connexion TCP. Le client peut fonctionner de manière incorrecte en raison de l'application qui s'exécute dessus. Redémarrez le client. Vérifiez si le problème est causé par une application nouvelle ou existante : Si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande « cifs option modify -max -opens-same-file-per -tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer de privilèges avancés pour définir un seuil plus élevé pour le client. …Si le problème est causé par une application existante, il peut y avoir un problème avec le client. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Conflit de nom NetBIOS	CRITIQUE	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom, provenant d'une machine distante. Cela est généralement dû à un conflit dans le nom NetBIOS ou dans un alias. Par conséquent, les clients risquent de ne pas pouvoir accéder aux données ou de se connecter au bon nœud de service de données dans le cluster.	Effectuez l'une des actions correctives suivantes :…En cas de conflit dans le nom NetBIOS ou dans un alias, effectuez l'une des opérations suivantes :…Supprimez l'alias NetBIOS en double à l'aide de la commande « vserver cifs delete -aliases alias -vserver vserver »….Renommez un alias NetBIOS en supprimant le nom en double et en ajoutant un alias avec un nouveau nom à l'aide de la commande « vserver cifs create -aliases alias -vserver vserver ». …S'il n'y a pas d'alias configuré et qu'il y a un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver vserver » et « vserver cifs create -cifs-server netbiosname ». REMARQUE : la suppression d'un serveur CIFS peut rendre les données inaccessibles. …Supprimez le nom NetBIOS ou renommez le NetBIOS sur la machine distante.
Pool de stockage NFSv4 épuisé	CRITIQUE	Un pool de stockage NFSv4 a été épuisé.	Si le serveur NFS ne répond pas pendant plus de 10 minutes après cet événement, contactez le support technique NetApp .

Aucun moteur d’analyse enregistré	CRITIQUE	Le connecteur antivirus a notifié à ONTAP qu’il ne dispose pas d’un moteur d’analyse enregistré. Cela peut entraîner l’indisponibilité des données si l’option « scan-mandatory » est activée.	Effectuez les actions correctives suivantes :…Assurez-vous que le logiciel du moteur d’analyse installé sur le serveur antivirus est compatible avec ONTAP.…Assurez-vous que le logiciel du moteur d’analyse est en cours d’exécution et configuré pour se connecter au connecteur antivirus via une boucle de rappel locale.
Pas de connexion Vscan	CRITIQUE	ONTAP n’a pas de connexion Vscan pour répondre aux demandes d’analyse antivirus. Cela peut entraîner l’indisponibilité des données si l’option « scan-mandatory » est activée.	Assurez-vous que le pool de scanners est correctement configuré et que les serveurs antivirus sont actifs et connectés à ONTAP.
Espace de volume racine du nœud faible	CRITIQUE	Le système a détecté que le volume racine est dangereusement bas en termes d’espace. Le nœud n’est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé au sein du cluster, ce qui limite l’accès NFS et CIFS sur le nœud. La capacité administrative est limitée aux procédures de récupération locales permettant au nœud de libérer de l’espace sur le volume racine.	Effectuez les actions correctives suivantes :… Libérez de l’espace sur le volume racine en supprimant les anciennes copies Snapshot, en supprimant les fichiers dont vous n’avez plus besoin du répertoire /mroot ou en augmentant la capacité du volume racine.… Redémarrez le contrôleur.… Contactez le support technique NetApp pour plus d’informations ou d’assistance.
Partage administrateur inexistant	CRITIQUE	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	Assurez-vous que Vscan est activé pour l’ID SVM mentionné. L’activation de Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour le SVM.

Espace de noms NVMe insuffisant	CRITIQUE	Un espace de noms NVMe a été mis hors ligne en raison d'une erreur d'écriture causée par un manque d'espace.	Ajoutez de l'espace au volume, puis mettez l'espace de noms NVMe en ligne à l'aide de la commande « vserver nvme namespace modify ».
Période de grâce NVMe-oF active	AVERTISSEMENT	Cet événement se produit quotidiennement lorsque le protocole NVMe over Fabrics (NVMe-oF) est utilisé et que la période de grâce de la licence est active. La fonctionnalité NVMe-oF nécessite une licence après l'expiration de la période de grâce de la licence. La fonctionnalité NVMe-oF est désactivée lorsque la période de grâce de la licence est terminée.	Contactez votre représentant commercial pour obtenir une licence NVMe-oF et l'ajouter au cluster, ou supprimez toutes les instances de configuration NVMe-oF du cluster.
Période de grâce NVMe-oF expirée	AVERTISSEMENT	La période de grâce de la licence NVMe over Fabrics (NVMe-oF) est terminée et la fonctionnalité NVMe-oF est désactivée.	Contactez votre représentant commercial pour obtenir une licence NVMe-oF et l'ajouter au cluster.
Début de la période de grâce NVMe-oF	AVERTISSEMENT	La configuration NVMe over Fabrics (NVMe-oF) a été détectée lors de la mise à niveau vers le logiciel ONTAP 9.5. La fonctionnalité NVMe-oF nécessite une licence après l'expiration de la période de grâce de la licence.	Contactez votre représentant commercial pour obtenir une licence NVMe-oF et l'ajouter au cluster.
Hôte du magasin d'objets non résoluble	CRITIQUE	Le nom d'hôte du serveur de magasin d'objets ne peut pas être résolu en une adresse IP. Le client du magasin d'objets ne peut pas communiquer avec le serveur du magasin d'objets sans résoudre une adresse IP. Par conséquent, les données peuvent être inaccessibles.	Vérifiez la configuration DNS pour vérifier que le nom d'hôte est correctement configuré avec une adresse IP.

LIF intercluster du magasin d'objets en panne	CRITIQUE	Le client du magasin d'objets ne trouve pas de LIF opérationnel pour communiquer avec le serveur du magasin d'objets. Le nœud n'autorisera pas le trafic client du magasin d'objets tant que le LIF intercluster ne sera pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuez les actions correctives suivantes :…Vérifiez l'état du LIF intercluster à l'aide de la commande « network interface show -role intercluster ».…Vérifiez que le LIF intercluster est configuré correctement et opérationnel.…Si un LIF intercluster n'est pas configuré, ajoutez-le à l'aide de la commande « network interface create -role intercluster ».
Non-concordance des signatures du magasin d'objets	CRITIQUE	La signature de la demande envoyée au serveur de magasin d'objets ne correspond pas à la signature calculée par le client. Par conséquent, les données peuvent être inaccessibles.	Vérifiez que la clé d'accès secrète est correctement configurée. S'il est configuré correctement, contactez le support technique NetApp pour obtenir de l'aide.

Délai d’expiration de READDIR	CRITIQUE	Une opération de fichier READDIR a dépassé le délai d’exécution autorisé dans WAFL. Cela peut être dû à des répertoires très volumineux ou peu nombreux. Des mesures correctives sont recommandées.	Effectuez les actions correctives suivantes :…Recherchez des informations spécifiques aux répertoires récents dont les opérations de fichier READDIR ont expiré en utilisant la commande CLI nodeshell de privilège « diag » suivante : wafl readdir notice show.…Vérifiez si les répertoires sont indiqués comme clairsemés ou non :…Si un répertoire est indiqué comme clairsemé, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer la clairsemée du fichier de répertoire. …Si un répertoire n’est pas indiqué comme étant clairsemé et que le répertoire est volumineux, il est recommandé de réduire la taille du fichier de répertoire en réduisant le nombre d’entrées de fichier dans le répertoire.

Échec de la relocalisation des agrégats	CRITIQUE	Cet événement se produit lors du déplacement d'un agrégat, lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes :… Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show »…. Vérifiez la connectivité réseau au serveur de magasin d'objets à l'aide de la commande « ping » sur le LIF intercluster du nœud de destination. …Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show »….Vous pouvez également contourner l'erreur en utilisant le paramètre « override-destination-checks » de la commande de relocation.…Contactez le support technique NetApp pour obtenir plus d'informations ou une assistance.
Échec de la copie fantôme	CRITIQUE	Une opération de service de sauvegarde et de restauration de Volume Shadow Copy Service (VSS) de Microsoft Server a échoué.	Vérifiez les éléments suivants à l'aide des informations fournies dans le message d'événement :… La configuration de la copie fantôme est-elle activée ?… Les licences appropriées sont-elles installées ? …Sur quels partages l'opération de cliché instantané est-elle effectuée ?…Le nom du partage est-il correct ?…Le chemin du partage existe-t-il ?…Quels sont les états de l'ensemble de clichés instantanés et de ses clichés instantanés ?

Panne d’alimentation du commutateur de stockage	AVERTISSEMENT	Il manque une alimentation dans le commutateur du cluster. La redondance est réduite, le risque de panne en cas de nouvelle panne de courant est réduit.	Effectuez les actions correctives suivantes :… Assurez-vous que le bloc d’alimentation secteur, qui alimente le commutateur de cluster, est sous tension.… Assurez-vous que le cordon d’alimentation est connecté au bloc d’alimentation.… Contactez le support technique NetApp si le problème persiste.
Trop d’authentifications CIFS	AVERTISSEMENT	De nombreuses négociations d’authentification ont eu lieu simultanément. Il y a 256 demandes de nouvelles sessions incomplètes de ce client.	Recherchez pourquoi le client a créé 256 nouvelles demandes de connexion ou plus. Vous devrez peut-être contacter le fournisseur du client ou de l’application pour déterminer pourquoi l’erreur s’est produite.
Accès utilisateur non autorisé au partage administrateur	AVERTISSEMENT	Un client a tenté de se connecter au partage privilégié ONTAP_ADMIN$ même si son utilisateur connecté n’est pas un utilisateur autorisé.	Effectuez les actions correctives suivantes :… Assurez-vous que le nom d’utilisateur et l’adresse IP mentionnés sont configurés dans l’un des pools de scanners Vscan actifs.… Vérifiez la configuration du pool de scanners actuellement actif à l’aide de la commande « vserver vscan scanner pool show-active ».

Virus détecté	AVERTISSEMENT	Un serveur Vscan a signalé une erreur au système de stockage. Cela indique généralement qu'un virus a été détecté. Cependant, d'autres erreurs sur le serveur Vscan peuvent provoquer cet événement.…L'accès client au fichier est refusé. Le serveur Vscan peut, selon ses paramètres et sa configuration, nettoyer le fichier, le mettre en quarantaine ou le supprimer.	Vérifiez le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il a réussi à nettoyer, mettre en quarantaine ou supprimer le fichier infecté. Si cela n'est pas possible, un administrateur système devra peut-être supprimer manuellement le fichier.
Volume hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettez le volume en ligne.
Volume restreint	INFO	Cet événement indique qu'un volume flexible est rendu restreint.	Remettez le volume en ligne.
L'arrêt de la machine virtuelle de stockage a réussi	INFO	Ce message s'affiche lorsqu'une opération « vserver stop » réussit.	Utilisez la commande « vserver start » pour démarrer l'accès aux données sur une machine virtuelle de stockage.
Panique du nœud	AVERTISSEMENT	Cet événement est émis lorsqu'une panique se produit	Contactez le support client NetApp .

Retour en haut

Moniteurs de journaux anti-ransomware

Nom du moniteur	Gravité	Description	Action corrective
Surveillance anti-ransomware de la machine virtuelle de stockage désactivée	AVERTISSEMENT	La surveillance anti-ransomware pour la VM de stockage est désactivée. Activez l'anti-ransomware pour protéger la machine virtuelle de stockage.	Aucune
Surveillance anti-ransomware des machines virtuelles de stockage activée (mode d'apprentissage)	INFO	La surveillance anti-ransomware pour la VM de stockage est activée en mode apprentissage.	Aucune

Surveillance anti-ransomware du volume activée	INFO	La surveillance anti-ransomware du volume est activée.	Aucune
Surveillance anti-ransomware du volume désactivée	AVERTISSEMENT	La surveillance anti-ransomware du volume est désactivée. Activez l'anti-ransomware pour protéger le volume.	Aucune
Surveillance anti-ransomware du volume activée (mode d'apprentissage)	INFO	La surveillance anti-ransomware du volume est activée en mode apprentissage.	Aucune
Surveillance anti-ransomware du volume interrompue (mode d'apprentissage)	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue en mode apprentissage.	Aucune
Surveillance anti-ransomware du volume suspendue	AVERTISSEMENT	La surveillance anti-ransomware du volume est suspendue.	Aucune
Désactivation de la surveillance anti-ransomware du volume	AVERTISSEMENT	La surveillance anti-ransomware du volume est désactivée.	Aucune
Activité de ransomware détectée	CRITIQUE	Pour protéger les données du ransomware détecté, une copie instantanée a été prise et peut être utilisée pour restaurer les données d'origine. Votre système génère et transmet un message AutoSupport ou « appel à domicile » au support technique NetApp et à toutes les destinations configurées. Le message AutoSupport améliore la détermination et la résolution des problèmes.	Reportez-vous au « NOM DU DOCUMENT FINAL » pour prendre des mesures correctives en cas d'activité de ransomware.

Retour en haut

Moniteurs FSx pour NetApp ONTAP

Nom du moniteur	Seuils	Description du moniteur	Action corrective

La capacité du volume FSx est pleine	Avertissement à > 85 %…Critique à > 95 %	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Plus les données stockées dans le volume ONTAP sont nombreuses, moins il y a de disponibilité de stockage pour les données futures. Si la capacité de stockage des données dans un volume atteint la capacité de stockage totale, le client peut être incapable de stocker des données en raison d'un manque de capacité de stockage. La surveillance du volume de capacité de stockage utilisé garantit la continuité des services de données.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Envisagez de supprimer les données qui ne sont plus nécessaires pour libérer de l'espace
FSx Volume Latence élevée	Avertissement à > 1 000 µs… Critique à > 2 000 µs	Les volumes sont des objets qui servent le trafic d'E/S souvent généré par des applications sensibles aux performances, notamment les applications DevOps, les répertoires personnels et les bases de données. Des latences de volume élevées signifient que les applications elles-mêmes peuvent en souffrir et être incapables d'accomplir leurs tâches. La surveillance des latences de volume est essentielle pour maintenir des performances cohérentes des applications.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume… Prévoyez de prendre prochainement les mesures suivantes si le seuil d'avertissement est dépassé :…1. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume.…2. Si le nœud subit également une utilisation élevée, déplacez le volume vers un autre nœud ou réduisez la charge de travail totale du nœud.

Limite d’inodes de volume FSx	Avertissement à > 85 %…Critique à > 95 %	Les volumes qui stockent des fichiers utilisent des nœuds d’index (inode) pour stocker les métadonnées des fichiers. Lorsqu’un volume épuise son allocation d’inode, aucun fichier supplémentaire ne peut y être ajouté. Une alerte d’avertissement indique qu’une action planifiée doit être entreprise pour augmenter le nombre d’inodes disponibles. Une alerte critique indique que l’épuisement de la limite de fichier est imminent et que des mesures d’urgence doivent être prises pour libérer des inodes afin d’assurer la continuité du service	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Envisagez d’augmenter la valeur des inodes pour le volume. Si la valeur des inodes est déjà au maximum, envisagez de diviser le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale… Prévoyez de prendre prochainement les mesures suivantes si le seuil d’avertissement est dépassé :…1. Envisagez d’augmenter la valeur des inodes pour le volume. Si la valeur des inodes est déjà au maximum, envisagez de diviser le volume en deux volumes ou plus, car le système de fichiers a dépassé la taille maximale.
Surcharge de quota Qtree du volume FSx	Avertissement à > 95 %…Critique à > 100 %	Volume Qtree Quota Overcommit spécifie le pourcentage auquel un volume est considéré comme surengagé par les quotas qtree. Le seuil défini pour le quota qtree est atteint pour le volume. La surveillance du dépassement de quota du volume qtree garantit que l’utilisateur reçoit un service de données ininterrompu.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Supprimez les données indésirables… Lorsque le seuil d’avertissement est dépassé, envisagez d’augmenter l’espace du volume.

L’espace de réserve des instantanés FSx est plein	Avertissement à > 90 %…Critique à > 95 %	La capacité de stockage d’un volume est nécessaire pour stocker les données d’application et de client. Une partie de cet espace, appelée espace réservé aux instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données nouvelles et mises à jour sont stockées dans le volume ONTAP , plus la capacité de snapshot est utilisée et moins la capacité de stockage de snapshot sera disponible pour les données nouvelles ou mises à jour futures. Si la capacité des données d’instantané dans un volume atteint l’espace de réserve total d’instantané, le client peut être incapable de stocker de nouvelles données d’instantané et le niveau de protection des données dans le volume peut être réduit. La surveillance de la capacité de snapshot du volume utilisé garantit la continuité des services de données.	Des mesures immédiates sont nécessaires pour minimiser les interruptions de service si le seuil critique est dépassé :…1. Envisagez de configurer des instantanés pour utiliser l’espace de données dans le volume lorsque la réserve d’instantanés est pleine…2. Envisagez de supprimer certains anciens instantanés qui ne sont peut-être plus nécessaires pour libérer de l’espace… Prévoyez de prendre prochainement les mesures suivantes si le seuil d’avertissement est dépassé :…1. Envisagez d’augmenter l’espace de réserve d’instantanés dans le volume pour s’adapter à la croissance…2. Envisagez de configurer des instantanés pour utiliser l’espace de données dans le volume lorsque la réserve d’instantanés est pleine.

Taux d'échec du cache de volume FSx	Avertissement à > 95 %…Critique à > 100 %	Le ratio de manque de cache de volume est le pourcentage de demandes de lecture provenant des applications clientes qui sont renvoyées depuis le disque au lieu d'être renvoyées depuis le cache. Cela signifie que le volume a atteint le seuil défini.	Si le seuil critique est dépassé, des mesures immédiates doivent être prises pour minimiser les interruptions de service : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d'E/S 2. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites de QoS… Envisagez des actions immédiates lorsque le seuil d'avertissement est dépassé : 1. Déplacez certaines charges de travail hors du nœud du volume pour réduire la charge d'E/S 2. Réduisez la demande de charges de travail de priorité inférieure sur le même nœud via des limites QoS 3. Modifier les caractéristiques de la charge de travail (taille des blocs, mise en cache des applications, etc.)

Retour en haut

Moniteurs K8s

Nom du moniteur	Description	Mesures correctives	Gravité/Seuil

Latence de volume persistante élevée	Des latences de volume persistantes élevées signifient que les applications elles-mêmes peuvent en souffrir et être incapables d'accomplir leurs tâches. La surveillance des latences de volume persistantes est essentielle pour maintenir des performances cohérentes des applications. Les latences suivantes sont attendues en fonction du type de support : SSD jusqu'à 1 à 2 millisecondes ; SAS jusqu'à 8 à 10 millisecondes et disque dur SATA 17 à 20 millisecondes.	**Actions immédiates** Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : si une politique de qualité de service (QoS) est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Si le pool de stockage connaît également une utilisation élevée, déplacez le volume vers un autre pool de stockage. 2. Si une politique QoS est attribuée au volume, évaluez ses seuils de limite au cas où ils entraîneraient une limitation de la charge de travail du volume. 3. Si le contrôleur subit également une utilisation élevée, déplacez le volume vers un autre contrôleur ou réduisez la charge de travail totale du contrôleur.	Avertissement à > 6 000 µs Critique à > 12 000 µs
Saturation élevée de la mémoire du cluster	La saturation de la mémoire allouable du cluster est élevée. La saturation du processeur du cluster est calculée comme la somme de l'utilisation de la mémoire divisée par la somme de la mémoire allouable sur tous les nœuds K8.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer de la mémoire sur les nœuds.	Avertissement à > 80 % Critique à > 90 %
Échec de la connexion du POD	Cette alerte se produit lorsqu'une pièce jointe de volume avec POD échoue.		Avertissement

Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifiez la congestion du réseau - Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifiez les performances du réseau matériel.	Avertissement à > 10 % Critique à > 25 %
Capacité élevée du système de fichiers du nœud	Capacité élevée du système de fichiers du nœud	- Augmentez la taille des disques de nœuds pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire l'utilisation des fichiers d'application.	Avertissement à > 80 % Critique à > 90 %
Gigue élevée du réseau de charge de travail	Gigue TCP élevée (variations élevées de latence/temps de réponse)	Vérifiez la congestion du réseau. Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifier les performances du réseau matériel	Avertissement à > 30 ms Critique à > 50 ms

Débit de volume persistant	Les seuils MBPS sur les volumes persistants peuvent être utilisés pour alerter un administrateur lorsque les volumes persistants dépassent les attentes de performances prédéfinies, ce qui peut avoir un impact sur d'autres volumes persistants. L'activation de ce moniteur générera des alertes adaptées au profil de débit typique des volumes persistants sur SSD. Ce moniteur couvrira tous les volumes persistants de votre locataire. Les valeurs de seuil d'avertissement et de critique peuvent être ajustées en fonction de vos objectifs de surveillance en dupliquant ce moniteur et en définissant des seuils adaptés à votre classe de stockage. Un moniteur dupliqué peut être davantage ciblé sur un sous-ensemble des volumes persistants de votre locataire.	**Actions immédiates** Si le seuil critique est dépassé, planifiez des actions immédiates pour minimiser les interruptions de service : 1. Introduisez les limites QoS MBPS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Introduisez les limites QoS MBPS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies.	Avertissement à > 10 000 Mo/s Critique à > 15 000 Mo/s
Conteneur menacé de rupture de stock	Les limites de mémoire du conteneur sont définies trop bas. Le conteneur risque d'être expulsé (Out of Memory Kill).	Augmenter les limites de mémoire du conteneur.	Avertissement à > 95 %
Réduction de la charge de travail	La charge de travail n'a pas de pods sains.		Critique à < 1
Échec de la liaison de la réclamation de volume persistant	Cette alerte se produit lorsqu'une liaison échoue sur un PVC.		Avertissement
Les limites de mémoire de ResourceQuota sont sur le point d'être dépassées	Les limites de mémoire pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %
Demandes de mémoire ResourceQuota sur le point d'être dépassées	Les demandes de mémoire pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %

Échec de la création du nœud	Le nœud n'a pas pu être planifié en raison d'une erreur de configuration.	Consultez le journal des événements Kubernetes pour connaître la cause de l'échec de la configuration.	Primordial
Échec de la récupération du volume persistant	Le volume n'a pas réussi sa récupération automatique.		Avertissement @ > 0 B
Limitation du processeur du conteneur	Les limites du processeur du conteneur sont définies trop bas. Les processus de conteneurs sont ralentis.	Augmenter les limites du processeur du conteneur.	Avertissement à > 95 % Critique à > 98 %
Échec de la suppression de l'équilibreur de charge de service			Avertissement
IOPS de volume persistant	Les seuils IOPS sur les volumes persistants peuvent être utilisés pour alerter un administrateur lorsque les volumes persistants dépassent les attentes de performances prédéfinies. L'activation de ce moniteur générera des alertes adaptées au profil IOPS typique des volumes de persistance. Ce moniteur couvrira tous les volumes persistants de votre locataire. Les valeurs de seuil d'avertissement et de critique peuvent être ajustées en fonction de vos objectifs de surveillance en dupliquant ce moniteur et en définissant des seuils adaptés à votre charge de travail.	**Actions immédiates** Si le seuil critique est dépassé, planifiez des actions immédiates pour minimiser les interruptions de service : 1. Introduisez les limites IOPS QoS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, planifiez les actions immédiates suivantes : 1. Introduisez les limites IOPS QoS pour le volume. 2. Vérifiez l'application qui pilote la charge de travail sur le volume pour détecter d'éventuelles anomalies.	Avertissement à > 20 000 E/S Critique à > 25 000 E/S
Échec de la mise à jour de l'équilibreur de charge de service			Avertissement
Échec du montage du POD	Cette alerte se produit lorsqu'un montage échoue sur un POD.		Avertissement

Pression PID du nœud	Les identifiants de processus disponibles sur le nœud (Linux) sont tombés en dessous d'un seuil d'éviction.	Recherchez et corrigez les pods qui génèrent de nombreux processus et privent le nœud d'ID de processus disponibles. Configurez PodPidsLimit pour protéger votre nœud contre les pods ou les conteneurs qui génèrent trop de processus.	Critique @ > 0
Échec de l'extraction de l'image du pod	Kubernetes n'a pas réussi à extraire l'image du conteneur de pod.	- Assurez-vous que l'image du pod est correctement orthographiée dans la configuration du pod. - Vérifiez que la balise d'image existe dans votre registre. - Vérifiez les informations d'identification du registre d'images. - Vérifiez les problèmes de connectivité du registre. - Vérifiez que vous n'atteignez pas les limites de débit imposées par les fournisseurs de registre public.	Avertissement
Le travail dure trop longtemps	Le travail dure trop longtemps		Avertissement à > 1 h Critique à > 5 h
Mémoire de nœud élevée	L'utilisation de la mémoire du nœud est élevée	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer de la mémoire sur les nœuds.	Avertissement à > 85 % Critique à > 90 %
Les limites du processeur ResourceQuota sont sur le point d'être dépassées	Les limites du processeur pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %
Boucle de crash de pod arrière	Le Pod s'est écrasé et a tenté de redémarrer plusieurs fois.		Critique @ > 3
CPU du nœud élevé	L'utilisation du processeur du nœud est élevée.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer du CPU sur les nœuds.	Avertissement à > 80 % Critique à > 90 %

Latence du réseau de charge de travail RTT élevée	Latence TCP RTT (Round Trip Time) élevée	Vérifiez la congestion du réseau ▒ Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifiez les performances du réseau matériel.	Avertissement à > 150 ms Critique à > 300 ms
Échec du travail	La tâche n'a pas été terminée avec succès en raison d'une panne ou d'un redémarrage du nœud, d'un épuisement des ressources, d'un délai d'expiration de la tâche ou d'un échec de planification du pod.	Vérifiez les journaux d'événements Kubernetes pour connaître les causes d'échec.	Avertissement @ > 1
Volume persistant plein en quelques jours	Le volume persistant manquera d'espace dans quelques jours	-Augmentez la taille du volume pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. -Réduire la quantité de données stockées dans les applications.	Avertissement à < 8 jours Critique à < 3 jours
Pression de la mémoire des nœuds	Le nœud manque de mémoire. La mémoire disponible a atteint le seuil d'expulsion.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer de la mémoire sur les nœuds.	Critique @ > 0
Nœud non prêt	Le nœud n'est pas prêt depuis 5 minutes	Vérifiez que le nœud dispose de suffisamment de ressources CPU, mémoire et disque. Vérifiez la connectivité du réseau du nœud. Vérifiez les journaux d'événements Kubernetes pour connaître les causes d'échec.	Critique à < 1
Capacité de volume persistante élevée	La capacité utilisée par le backend de volume persistant est élevée.	- Augmentez la taille du volume pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire la quantité de données stockées dans les applications.	Avertissement à > 80 % Critique à > 90 %

Échec de la création de l'équilibreur de charge de service	Échec de la création de l'équilibreur de charge de service		Primordial
Incompatibilité de réplication de charge de travail	Certains pods ne sont actuellement pas disponibles pour un déploiement ou un DaemonSet.		Avertissement @ > 1
Les requêtes CPU ResourceQuota sont sur le point d'être dépassées	Les demandes CPU pour l'espace de noms sont sur le point de dépasser ResourceQuota		Avertissement à > 80 % Critique à > 90 %
Taux de retransmission élevé	Taux de retransmission TCP élevé	Vérifiez la congestion du réseau - Identifiez les charges de travail qui consomment beaucoup de bande passante réseau. Vérifiez l'utilisation élevée du processeur Pod. Vérifiez les performances du réseau matériel.	Avertissement à > 10 % Critique à > 25 %
Pression du disque du nœud	L'espace disque disponible et les inodes sur le système de fichiers racine ou le système de fichiers image du nœud ont satisfait un seuil d'expulsion.	- Augmentez la taille des disques de nœuds pour garantir qu'il y a suffisamment d'espace pour les fichiers d'application. - Réduire l'utilisation des fichiers d'application.	Critique @ > 0
Saturation élevée du processeur du cluster	La saturation du processeur allouable au cluster est élevée. La saturation du processeur du cluster est calculée comme la somme de l'utilisation du processeur divisée par la somme du processeur allouable sur tous les nœuds K8.	Ajouter des nœuds. Corrigez tous les nœuds non planifiés. Ajustez la taille des pods pour libérer du CPU sur les nœuds.	Avertissement à > 80 % Critique à > 90 %

Retour en haut

Moniteurs de journaux de modifications

Nom du moniteur	Gravité	Description du moniteur
Volume interne découvert	Informatif	Ce message s'affiche lorsqu'un volume interne est découvert.
Volume interne modifié	Informatif	Ce message s'affiche lorsqu'un volume interne est modifié.

Nœud de stockage découvert	Informatif	Ce message s'affiche lorsqu'un nœud de stockage est découvert.
Nœud de stockage supprimé	Informatif	Ce message s'affiche lorsqu'un nœud de stockage est supprimé.
Pool de stockage découvert	Informatif	Ce message s'affiche lorsqu'un pool de stockage est découvert.
Machine virtuelle de stockage découverte	Informatif	Ce message s'affiche lorsqu'une machine virtuelle de stockage est découverte.
Machine virtuelle de stockage modifiée	Informatif	Ce message s'affiche lorsqu'une machine virtuelle de stockage est modifiée.

Retour en haut

Moniteurs de collecte de données

Nom du moniteur	Description	Action corrective
Arrêt de l'unité d'acquisition	Les unités d'acquisition Data Infrastructure Insights redémarrent périodiquement dans le cadre de mises à niveau pour introduire de nouvelles fonctionnalités. Cela se produit une fois par mois ou moins dans un environnement typique. Une alerte d'avertissement indiquant qu'une unité d'acquisition s'est arrêtée doit être suivie peu de temps après par une résolution indiquant que l'unité d'acquisition nouvellement redémarrée a terminé un enregistrement auprès de Data Infrastructure Insights. En général, ce cycle d'arrêt à enregistrement prend entre 5 et 15 minutes.	Si l'alerte se produit fréquemment ou dure plus de 15 minutes, vérifiez le fonctionnement du système hébergeant l'unité d'acquisition, le réseau et tout proxy connectant l'AU à Internet.
Échec du collecteur	L'enquête d'un collecteur de données a rencontré une situation d'échec inattendue.	Visitez la page du collecteur de données dans Data Infrastructure Insights pour en savoir plus sur la situation.

Avertissement aux collectionneurs	Cette alerte peut généralement survenir en raison d'une configuration erronée du collecteur de données ou du système cible. Revoyez les configurations pour éviter de futures alertes. Cela peut également être dû à une récupération de données incomplètes alors que le collecteur de données a rassemblé toutes les données qu'il pouvait. Cela peut se produire lorsque les situations changent pendant la collecte de données (par exemple, une machine virtuelle présente au début de la collecte de données est supprimée pendant la collecte de données et avant que ses données ne soient capturées).	Vérifiez la configuration du collecteur de données ou du système cible. Notez que le moniteur pour Collector Warning peut envoyer plus d'alertes que les autres types de moniteurs. Il est donc recommandé de ne définir aucun destinataire d'alerte, sauf si vous effectuez un dépannage.

Retour en haut

Moniteurs de sécurité

Nom du moniteur	Seuil	Description du moniteur	Action corrective
Transport HTTPS AutoSupport désactivé	Avertissement @ < 1	AutoSupport prend en charge HTTPS, HTTP et SMTP pour les protocoles de transport. En raison de la nature sensible des messages AutoSupport , NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi de messages AutoSupport au support NetApp .	Pour définir HTTPS comme protocole de transport pour les messages AutoSupport , exécutez la commande ONTAP suivante :…system node autosupport modify -transport https
Chiffres non sécurisés en cluster pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Pour supprimer les chiffrements CBC, exécutez la commande ONTAP suivante :…security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc

Bannière de connexion au cluster désactivée	Avertissement @ < 1	Indique que la bannière de connexion est désactivée pour les utilisateurs accédant au système ONTAP . L'affichage d'une bannière de connexion est utile pour établir les attentes en matière d'accès et d'utilisation du système.	Pour configurer la bannière de connexion d'un cluster, exécutez la commande ONTAP suivante :…security login banner modify -vserver <admin svm> -message "Accès restreint aux utilisateurs autorisés"
Communication entre pairs du cluster non chiffrée	Avertissement @ < 1	Lors de la réplication de données pour la reprise après sinistre, la mise en cache ou la sauvegarde, vous devez protéger ces données pendant le transport sur le réseau d'un cluster ONTAP à un autre. Le chiffrement doit être configuré sur les clusters source et de destination.	Pour activer le chiffrement sur les relations homologues de cluster créées avant ONTAP 9.6, le cluster source et de destination doivent être mis à niveau vers la version 9.6. Utilisez ensuite la commande « cluster peer modify » pour modifier les homologues du cluster source et de destination afin d'utiliser le chiffrement de peering de cluster. Consultez le Guide de renforcement de la sécurité NetApp pour ONTAP 9 pour plus de détails.
Utilisateur administrateur local par défaut activé	Avertissement @ > 0	NetApp recommande de verrouiller (désactiver) tous les comptes d'utilisateur administrateur par défaut (intégrés) inutiles avec la commande lock. Il s'agit principalement de comptes par défaut pour lesquels les mots de passe n'ont jamais été mis à jour ou modifiés.	Pour verrouiller le compte « admin » intégré, exécutez la commande ONTAP suivante :…security login lock -username admin
Mode FIPS désactivé	Avertissement @ < 1	Lorsque la conformité FIPS 140-2 est activée, TLSv1 et SSLv3 sont désactivés et seuls TLSv1.1 et TLSv1.2 restent activés. ONTAP vous empêche d'activer TLSv1 et SSLv3 lorsque la conformité FIPS 140-2 est activée.	Pour activer la conformité FIPS 140-2 sur un cluster, exécutez la commande ONTAP suivante en mode privilège avancé :…security config modify -interface SSL -is -fips-enabled true

Transfert de journaux non chiffré	Avertissement @ < 1	Le déchargement des informations syslog est nécessaire pour limiter la portée ou l'empreinte d'une violation à un seul système ou à une seule solution. Par conséquent, NetApp recommande de décharger en toute sécurité les informations syslog vers un emplacement de stockage ou de conservation sécurisé.	Une fois qu'une destination de transfert de journal est créée, son protocole ne peut pas être modifié. Pour passer à un protocole chiffré, supprimez et recréez la destination de transfert de journal à l'aide de la commande ONTAP suivante :…cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
Mot de passe haché MD5	Avertissement @ > 0	NetApp recommande fortement d'utiliser la fonction de hachage SHA-512 plus sécurisée pour les mots de passe des comptes utilisateurs ONTAP . Les comptes utilisant la fonction de hachage MD5 moins sécurisée doivent migrer vers la fonction de hachage SHA-512.	NetApp recommande fortement aux comptes utilisateurs de migrer vers la solution SHA-512 plus sécurisée en demandant aux utilisateurs de modifier leurs mots de passe.…pour verrouiller les comptes avec des mots de passe qui utilisent la fonction de hachage MD5, exécutez la commande ONTAP suivante :…security login lock -vserver * -username * -hash-function md5
Aucun serveur NTP n'est configuré	Avertissement @ < 1	Indique que le cluster n'a pas de serveurs NTP configurés. Pour la redondance et un service optimal, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	Pour associer un serveur NTP au cluster, exécutez la commande ONTAP suivante : cluster time-service ntp server create -server <ntp server host name or IP address>
Le nombre de serveurs NTP est faible	Avertissement @ < 3	Indique que le cluster possède moins de 3 serveurs NTP configurés. Pour la redondance et un service optimal, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	Pour associer un serveur NTP au cluster, exécutez la commande ONTAP suivante :…cluster time-service ntp server create -server <nom d'hôte ou adresse IP du serveur NTP>

Shell distant activé	Avertissement @ > 0	Remote Shell n'est pas une méthode sécurisée pour établir un accès en ligne de commande à la solution ONTAP . Le shell distant doit être désactivé pour un accès distant sécurisé.	NetApp recommande Secure Shell (SSH) pour un accès distant sécurisé.…Pour désactiver le shell distant sur un cluster, exécutez la commande ONTAP suivante en mode de privilège avancé :…security protocol modify -application rsh- enabled false
Journal d'audit de la machine virtuelle de stockage désactivé	Avertissement @ < 1	Indique que la journalisation d'audit est désactivée pour SVM.	Pour configurer le journal d'audit d'un serveur virtuel, exécutez la commande ONTAP suivante :…vserver audit enable -vserver <svm>
Chiffres non sécurisés de la machine virtuelle de stockage pour SSH	Avertissement @ < 1	Indique que SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Pour supprimer les chiffrements CBC, exécutez la commande ONTAP suivante :…security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Bannière de connexion à la machine virtuelle de stockage désactivée	Avertissement @ < 1	Indique que la bannière de connexion est désactivée pour les utilisateurs accédant aux SVM sur le système. L'affichage d'une bannière de connexion est utile pour établir les attentes en matière d'accès et d'utilisation du système.	Pour configurer la bannière de connexion d'un cluster, exécutez la commande ONTAP suivante :…security login banner modify -vserver <svm> -message "Accès restreint aux utilisateurs autorisés"
Protocole Telnet activé	Avertissement @ > 0	Telnet n'est pas une méthode sécurisée pour établir un accès en ligne de commande à la solution ONTAP . Telnet doit être désactivé pour un accès distant sécurisé.	NetApp recommande Secure Shell (SSH) pour un accès à distance sécurisé. Pour désactiver Telnet sur un cluster, exécutez la commande ONTAP suivante en mode privilège avancé :…security protocol modify -application telnet -enabled false

Retour en haut

Contrôleurs de la protection des données

Nom du moniteur	Seuils	Description du moniteur	Action corrective
Espace insuffisant pour la copie de l'instantané Lun	(Filtre contains_luns = Oui) Avertissement à > 95 %…Critique à > 100 %	La capacité de stockage d'un volume est nécessaire pour stocker les données d'application et de client. Une partie de cet espace, appelée espace réservé aux instantanés, est utilisée pour stocker des instantanés qui permettent de protéger les données localement. Plus les données nouvelles et mises à jour sont stockées dans le volume ONTAP , plus la capacité de snapshot est utilisée et moins la capacité de stockage de snapshot sera disponible pour les données nouvelles ou mises à jour futures. Si la capacité des données de snapshot dans un volume atteint l'espace de réserve total de snapshot, le client peut être incapable de stocker de nouvelles données de snapshot et réduire le niveau de protection des données dans les LUN du volume. La surveillance de la capacité de snapshot du volume utilisé garantit la continuité des services de données.	**Actions immédiates** Si le seuil critique est dépassé, envisagez des actions immédiates pour minimiser les interruptions de service : 1. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine. 2. Supprimez certains anciens instantanés indésirables pour libérer de l'espace. **Actions à effectuer prochainement** Si le seuil d'avertissement est dépassé, prévoyez de prendre les mesures immédiates suivantes : 1. Augmentez l'espace de réserve d'instantanés dans le volume pour s'adapter à la croissance. 2. Configurez les instantanés pour utiliser l'espace de données dans le volume lorsque la réserve d'instantanés est pleine.

Décalage relationnel SnapMirror	Avertissement à > 150 %… Critique à > 300 %	Le décalage de relation SnapMirror est la différence entre l'horodatage de l'instantané et l'heure sur le système de destination. Lag_time_percent est le rapport entre le temps de latence et l'intervalle de planification de la politique SnapMirror . Si le temps de latence est égal à l'intervalle de planification, lag_time_percent sera de 100 %. Si la politique SnapMirror n'a pas de planification, lag_time_percent ne sera pas calculé.	Surveillez l'état de SnapMirror à l'aide de la commande « snapmirror show ». Vérifiez l'historique des transferts SnapMirror à l'aide de la commande « snapmirror show-history »

Retour en haut

Moniteurs de volume de nuages (CVO)

Nom du moniteur	Gravité de l'IC	Description du moniteur	Action corrective
Disque CVO hors service	INFO	Cet événement se produit lorsqu'un disque est retiré du service parce qu'il a été marqué comme défectueux, est en cours de nettoyage ou est entré dans le centre de maintenance.	Aucune

Échec de la restitution du pool de stockage par CVO	CRITIQUE	Cet événement se produit lors de la migration d'un agrégat dans le cadre d'un basculement de stockage (SFO), lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes : Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show ». Vérifiez la connectivité réseau au serveur de magasin d'objets en utilisant la commande « ping » sur le LIF intercluster du nœud de destination. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show ». Alternativement, vous pouvez remplacer l'erreur en spécifiant false pour le paramètre « require-partner-waiting » de la commande giveback. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Interconnexion CVO HA en panne	AVERTISSEMENT	L'interconnexion haute disponibilité (HA) est en panne. Risque d'interruption de service lorsque le basculement n'est pas disponible.	Les actions correctives dépendent du nombre et du type de liens d'interconnexion HA pris en charge par la plate-forme, ainsi que de la raison pour laquelle l'interconnexion est en panne. Si les liens sont interrompus : vérifiez que les deux contrôleurs de la paire HA sont opérationnels. Pour les liaisons connectées en externe, assurez-vous que les câbles d'interconnexion sont correctement connectés et que les connecteurs à petit facteur de forme (SFP), le cas échéant, sont correctement installés sur les deux contrôleurs. Pour les liens connectés en interne, désactivez et réactivez les liens, l'un après l'autre, en utilisant les commandes « ic link off » et « ic link on ». Si les liens sont désactivés, activez-les en utilisant la commande « ic link on ». Si un pair n'est pas connecté, désactivez et réactivez les liens, l'un après l'autre, en utilisant les commandes « ic link off » et « ic link on ». Contactez le support technique NetApp si le problème persiste.

Nombre maximal de sessions CVO par utilisateur dépassé	AVERTISSEMENT	Vous avez dépassé le nombre maximal de sessions autorisées par utilisateur sur une connexion TCP. Toute demande d'établissement d'une session sera refusée jusqu'à ce que certaines sessions soient libérées.	Effectuez les actions correctives suivantes : inspectez toutes les applications qui s'exécutent sur le client et fermez celles qui ne fonctionnent pas correctement. Redémarrez le client. Vérifiez si le problème est causé par une application nouvelle ou existante : si l'application est nouvelle, définissez un seuil plus élevé pour le client en utilisant la commande « cifs option modify -max -opens-same-file-per -tree ». Dans certains cas, les clients fonctionnent comme prévu, mais nécessitent un seuil plus élevé. Vous devez disposer de privilèges avancés pour définir un seuil plus élevé pour le client. Si le problème est causé par une application existante, il peut y avoir un problème avec le client. Contactez le support technique NetApp pour plus d'informations ou d'assistance.

Conflit de nom NetBIOS CVO	CRITIQUE	Le service de noms NetBIOS a reçu une réponse négative à une demande d'enregistrement de nom, provenant d'une machine distante. Cela est généralement dû à un conflit dans le nom NetBIOS ou dans un alias. Par conséquent, les clients risquent de ne pas pouvoir accéder aux données ou de se connecter au bon nœud de service de données dans le cluster.	Effectuez l'une des actions correctives suivantes : S'il existe un conflit dans le nom NetBIOS ou un alias, effectuez l'une des opérations suivantes : Supprimez l'alias NetBIOS en double à l'aide de la commande « vserver cifs delete -aliases alias -vserver vserver ». Renommez un alias NetBIOS en supprimant le nom en double et en ajoutant un alias avec un nouveau nom à l'aide de la commande « vserver cifs create -aliases alias -vserver vserver ». S'il n'y a pas d'alias configuré et qu'il y a un conflit dans le nom NetBIOS, renommez le serveur CIFS en utilisant les commandes « vserver cifs delete -vserver vserver » et « vserver cifs create -cifs -server netbiosname ». REMARQUE : la suppression d'un serveur CIFS peut rendre les données inaccessibles. Supprimez le nom NetBIOS ou renommez le NetBIOS sur la machine distante.
Pool de stockage CVO NFSv4 épuisé	CRITIQUE	Un pool de stockage NFSv4 a été épuisé.	Si le serveur NFS ne répond pas pendant plus de 10 minutes après cet événement, contactez le support technique NetApp .
Panique du nœud CVO	AVERTISSEMENT	Cet événement est émis lorsqu'une panique se produit	Contactez le support client NetApp .

Faible volume d’espace racine du nœud CVO	CRITIQUE	Le système a détecté que le volume racine est dangereusement bas en termes d’espace. Le nœud n’est pas entièrement opérationnel. Les LIF de données peuvent avoir basculé au sein du cluster, ce qui limite l’accès NFS et CIFS sur le nœud. La capacité administrative est limitée aux procédures de récupération locales permettant au nœud de libérer de l’espace sur le volume racine.	Effectuez les actions correctives suivantes : libérez de l’espace sur le volume racine en supprimant les anciennes copies Snapshot, en supprimant les fichiers dont vous n’avez plus besoin du répertoire /mroot ou en augmentant la capacité du volume racine. Redémarrez le contrôleur. Contactez le support technique NetApp pour plus d’informations ou d’assistance.
Partage administratif inexistant du CVO	CRITIQUE	Problème Vscan : un client a tenté de se connecter à un partage ONTAP_ADMIN$ inexistant.	Assurez-vous que Vscan est activé pour l’ID SVM mentionné. L’activation de Vscan sur un SVM entraîne la création automatique du partage ONTAP_ADMIN$ pour le SVM.
Hôte du magasin d’objets CVO non résoluble	CRITIQUE	Le nom d’hôte du serveur de magasin d’objets ne peut pas être résolu en une adresse IP. Le client du magasin d’objets ne peut pas communiquer avec le serveur du magasin d’objets sans résoudre une adresse IP. Par conséquent, les données peuvent être inaccessibles.	Vérifiez la configuration DNS pour vérifier que le nom d’hôte est correctement configuré avec une adresse IP.
LIF intercluster du magasin d’objets CVO en panne	CRITIQUE	Le client du magasin d’objets ne trouve pas de LIF opérationnel pour communiquer avec le serveur du magasin d’objets. Le nœud n’autorisera pas le trafic client du magasin d’objets tant que le LIF intercluster ne sera pas opérationnel. Par conséquent, les données peuvent être inaccessibles.	Effectuez les actions correctives suivantes : Vérifiez l’état LIF intercluster à l’aide de la commande « network interface show -role intercluster ». Vérifiez que le LIF intercluster est correctement configuré et opérationnel. Si un LIF intercluster n’est pas configuré, ajoutez-le à l’aide de la commande « network interface create -role intercluster ».

Non-concordance des signatures du magasin d'objets CVO	CRITIQUE	La signature de la demande envoyée au serveur de magasin d'objets ne correspond pas à la signature calculée par le client. Par conséquent, les données peuvent être inaccessibles.	Vérifiez que la clé d'accès secrète est correctement configurée. S'il est configuré correctement, contactez le support technique NetApp pour obtenir de l'aide.
Mémoire du moniteur QoS CVO au maximum	CRITIQUE	La mémoire dynamique du sous-système QoS a atteint sa limite pour le matériel de la plate-forme actuelle. Certaines fonctionnalités QoS peuvent fonctionner avec une capacité limitée.	Supprimez certaines charges de travail ou flux actifs pour libérer de la mémoire. Utilisez la commande « statistics show -object workload -counter ops » pour déterminer quelles charges de travail sont actives. Les charges de travail actives affichent des opérations non nulles. Utilisez ensuite la commande « workload delete <workload_name> » plusieurs fois pour supprimer des charges de travail spécifiques. Vous pouvez également utiliser la commande « stream delete -workload <nom de la charge de travail> * » pour supprimer les flux associés de la charge de travail active.

Délai d’expiration de CVO READDIR	CRITIQUE	Une opération de fichier READDIR a dépassé le délai d’exécution autorisé dans WAFL. Cela peut être dû à des répertoires très volumineux ou peu nombreux. Des mesures correctives sont recommandées.	Effectuez les actions correctives suivantes : recherchez des informations spécifiques aux répertoires récents dont les opérations de fichier READDIR ont expiré en utilisant la commande CLI nodeshell de privilège « diag » suivante : wafl readdir notice show. Vérifiez si les répertoires sont indiqués comme clairsemés ou non : si un répertoire est indiqué comme clairsemé, il est recommandé de copier le contenu du répertoire dans un nouveau répertoire pour supprimer la clairsemée du fichier de répertoire. Si un répertoire n’est pas indiqué comme clairsemé et que le répertoire est volumineux, il est recommandé de réduire la taille du fichier de répertoire en réduisant le nombre d’entrées de fichier dans le répertoire.

Échec de la relocalisation du pool de stockage CVO	CRITIQUE	Cet événement se produit lors du déplacement d'un agrégat, lorsque le nœud de destination ne peut pas atteindre les magasins d'objets.	Effectuez les actions correctives suivantes : Vérifiez que votre LIF intercluster est en ligne et fonctionnel à l'aide de la commande « network interface show ». Vérifiez la connectivité réseau au serveur de magasin d'objets en utilisant la commande « ping » sur le LIF intercluster du nœud de destination. Vérifiez que la configuration de votre magasin d'objets n'a pas changé et que les informations de connexion et de connectivité sont toujours exactes à l'aide de la commande « aggregate object-store config show ». Vous pouvez également remplacer l'erreur en utilisant le paramètre « override-destination-checks » de la commande de relocalisation. Contactez le support technique NetApp pour plus d'informations ou d'assistance.
Échec de la copie fantôme CVO	CRITIQUE	Une opération de service de sauvegarde et de restauration de Volume Shadow Copy Service (VSS) de Microsoft Server a échoué.	Vérifiez les éléments suivants à l'aide des informations fournies dans le message d'événement : la configuration de la copie fantôme est-elle activée ? Les licences appropriées sont-elles installées ? Sur quelles actions l'opération de cliché instantané est-elle effectuée ? Le nom de l'action est-il correct ? Le chemin de partage existe-t-il ? Quels sont les états de l'ensemble de copies fantômes et de ses copies fantômes ?

L’arrêt de la machine virtuelle de stockage CVO a réussi	INFO	Ce message s’affiche lorsqu’une opération « vserver stop » réussit.	Utilisez la commande « vserver start » pour démarrer l’accès aux données sur une machine virtuelle de stockage.
CVO Trop d’authentification CIFS	AVERTISSEMENT	De nombreuses négociations d’authentification ont eu lieu simultanément. Il y a 256 demandes de nouvelles sessions incomplètes de ce client.	Recherchez pourquoi le client a créé 256 nouvelles demandes de connexion ou plus. Vous devrez peut-être contacter le fournisseur du client ou de l’application pour déterminer pourquoi l’erreur s’est produite.
Disques non attribués CVO	INFO	Le système possède des disques non attribués : la capacité est gaspillée et votre système peut être soumis à une mauvaise configuration ou à une modification partielle de la configuration.	Effectuez les actions correctives suivantes : déterminez quels disques ne sont pas attribués à l’aide de la commande « disk show -n ». Affectez les disques à un système en utilisant la commande « disk assign ».
Accès utilisateur non autorisé CVO au partage administrateur	AVERTISSEMENT	Un client a tenté de se connecter au partage privilégié ONTAP_ADMIN$ même si son utilisateur connecté n’est pas un utilisateur autorisé.	Effectuez les actions correctives suivantes : assurez-vous que le nom d’utilisateur et l’adresse IP mentionnés sont configurés dans l’un des pools de scanners Vscan actifs. Vérifiez la configuration du pool de scanners actuellement active à l’aide de la commande « vserver vscan scanner pool show-active ».

Virus CVO détecté	AVERTISSEMENT	Un serveur Vscan a signalé une erreur au système de stockage. Cela indique généralement qu'un virus a été détecté. Cependant, d'autres erreurs sur le serveur Vscan peuvent provoquer cet événement. L'accès du client au fichier est refusé. Le serveur Vscan peut, selon ses paramètres et sa configuration, nettoyer le fichier, le mettre en quarantaine ou le supprimer.	Vérifiez le journal du serveur Vscan signalé dans l'événement « syslog » pour voir s'il a réussi à nettoyer, mettre en quarantaine ou supprimer le fichier infecté. Si cela n'est pas possible, un administrateur système devra peut-être supprimer manuellement le fichier.
Volume CVO hors ligne	INFO	Ce message indique qu'un volume est mis hors ligne.	Remettez le volume en ligne.
Volume CVO restreint	INFO	Cet événement indique qu'un volume flexible est rendu restreint.	Remettez le volume en ligne.

Retour en haut

Moniteurs de journaux médiateurs SnapMirror for Business Continuity (SMBC)

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Ajout du médiateur ONTAP	INFO	Ce message s'affiche lorsque ONTAP Mediator est ajouté avec succès sur un cluster.	Aucune
Médiateur ONTAP non accessible	CRITIQUE	Ce message s'affiche lorsque le médiateur ONTAP est réutilisé ou que le package Médiateur n'est plus installé sur le serveur Médiateur. Par conséquent, le basculement de SnapMirror n'est pas possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Suppression du médiateur ONTAP	INFO	Ce message s'affiche lorsque ONTAP Mediator est supprimé avec succès d'un cluster.	Aucune

Médiateur ONTAP inaccessible	AVERTISSEMENT	Ce message s'affiche lorsque le médiateur ONTAP est inaccessible sur un cluster. Par conséquent, le basculement de SnapMirror n'est pas possible.	Vérifiez la connectivité réseau au médiateur ONTAP en utilisant les commandes « network ping » et « network traceroute ». Si le problème persiste, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Le certificat SMBC CA a expiré	CRITIQUE	Ce message s'affiche lorsque le certificat de l'autorité de certification (CA) ONTAP Mediator a expiré. Par conséquent, toute communication ultérieure avec le médiateur de ONTAP ne sera plus possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat CA sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Expiration du certificat SMBC CA	AVERTISSEMENT	Ce message s'affiche lorsque le certificat de l'autorité de certification (CA) ONTAP Mediator doit expirer dans les 30 prochains jours.	Avant l'expiration de ce certificat, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat CA sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».

Certificat client SMBC expiré	CRITIQUE	Ce message s'affiche lorsque le certificat client ONTAP Mediator a expiré. Par conséquent, toute communication ultérieure avec le médiateur de ONTAP ne sera plus possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Expiration du certificat client SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat client ONTAP Mediator doit expirer dans les 30 prochains jours.	Avant l'expiration de ce certificat, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Relation SMBC désynchronisée Remarque : UM n'a pas celui-ci	CRITIQUE	Ce message s'affiche lorsqu'une relation SnapMirror for Business Continuity (SMBC) change de statut de « synchronisé » à « désynchronisé ». En raison de ce RPO=0, la protection des données sera perturbée.	Vérifiez la connexion réseau entre les volumes source et de destination. Surveillez l'état de la relation SMBC en utilisant la commande « snapmirror show » sur la destination et en utilisant la commande « snapmirror list-destinations » sur la source. La resynchronisation automatique tentera de ramener la relation à l'état « synchronisé ». Si la resynchronisation échoue, vérifiez que tous les nœuds du cluster sont en quorum et sont sains.

Certificat du serveur SMBC expiré	CRITIQUE	Ce message s'affiche lorsque le certificat du serveur ONTAP Mediator a expiré. Par conséquent, toute communication ultérieure avec le médiateur de ONTAP ne sera plus possible.	Supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat de serveur sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».
Expiration du certificat du serveur SMBC	AVERTISSEMENT	Ce message s'affiche lorsque le certificat du serveur ONTAP Mediator doit expirer dans les 30 prochains jours.	Avant l'expiration de ce certificat, supprimez la configuration du médiateur ONTAP actuel à l'aide de la commande « snapmirror mediator remove ». Mettre à jour un nouveau certificat de serveur sur le serveur ONTAP Mediator. Reconfigurez l'accès au médiateur ONTAP à l'aide de la commande « snapmirror mediator add ».

Retour en haut

Moniteurs d'alimentation, de pulsation et de système divers supplémentaires

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Découverte d'une alimentation pour étagère à disques	INFORMATIF	Ce message s'affiche lorsqu'un bloc d'alimentation est ajouté à l'étagère de disques.	AUCUN
Étagères de disques Alimentation retirée	INFORMATIF	Ce message s'affiche lorsqu'un bloc d'alimentation est retiré de l'étagère de disque.	AUCUN
Commutation automatique non planifiée de MetroCluster désactivée	CRITIQUE	Ce message s'affiche lorsque la fonction de basculement automatique non planifié est désactivée.	Exécutez la commande « metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true » pour chaque nœud du cluster pour activer le basculement automatique.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Pont de stockage MetroCluster inaccessible	CRITIQUE	Le pont de stockage n'est pas accessible via le réseau de gestion	1) Si le pont est surveillé par SNMP, vérifiez que le LIF de gestion des nœuds est actif à l'aide de la commande « network interface show ». Vérifiez que le pont est actif en utilisant la commande « network ping ». 2) Si le pont est surveillé en bande, vérifiez le câblage de la structure vers le pont, puis vérifiez que le pont est sous tension.
Température anormale du pont MetroCluster (en dessous du seuil critique)	CRITIQUE	Le capteur sur le pont Fibre Channel signale une température inférieure au seuil critique.	1) Vérifiez l'état de fonctionnement des ventilateurs sur le pont de stockage. 2) Vérifiez que le pont fonctionne dans les conditions de température recommandées.
Température anormale du pont MetroCluster (supérieure au seuil critique)	CRITIQUE	Le capteur sur le pont Fibre Channel signale une température supérieure au seuil critique.	1) Vérifiez l'état de fonctionnement du capteur de température du châssis sur le pont de stockage à l'aide de la commande « storage bridge show -cooling ». 2) Vérifiez que le pont de stockage fonctionne dans les conditions de température recommandées.
L'agrégat MetroCluster laissé pour compte	AVERTISSEMENT	L'agrégat a été laissé sur place lors du virage.	1) Vérifiez l'état agrégé en utilisant la commande « aggr show ». 2) Si l'agrégat est en ligne, restituez-le à son propriétaire d'origine en utilisant la commande « metrocluster switchback ».

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Tous les liens entre les partenaires du Metrocluster sont interrompus	CRITIQUE	Les adaptateurs d'interconnexion RDMA et les LIF intercluster ont des connexions rompues avec le cluster appairé ou le cluster appairé est en panne.	1) Assurez-vous que les LIF interclusters sont opérationnels. Réparez les LIF interclusters s'ils sont en panne. 2) Vérifiez que le cluster appairé est opérationnel à l'aide de la commande « cluster peer ping ». Consultez le Guide de récupération après sinistre de MetroCluster si le cluster appairé est en panne. 3) Pour le fabric MetroCluster, vérifiez que les ISL du fabric back-end sont opérationnels. Réparez les ISL du tissu back-end s'ils sont en panne. 4) Pour les configurations MetroCluster non fabric, vérifiez que le câblage est correct entre les adaptateurs d'interconnexion RDMA. Reconfigurez le câblage si les liaisons sont coupées.
Les partenaires de MetroCluster ne sont pas joignables via le réseau de peering	CRITIQUE	La connectivité au cluster homologue est interrompue.	1) Assurez-vous que le port est connecté au bon réseau/commutateur. 2) Assurez-vous que le LIF intercluster est connecté au cluster homologue. 3) Assurez-vous que le cluster appairé est opérationnel en utilisant la commande « cluster peer ping ». Consultez le Guide de récupération après sinistre de MetroCluster si le cluster appairé est en panne.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Toutes les liaisons du commutateur MetroCluster Inter sont interrompues	CRITIQUE	Toutes les liaisons inter-commutateurs (ISL) sur le commutateur de stockage sont hors service.	1) Réparez les ISL de la structure principale sur le commutateur de stockage. 2) Assurez-vous que le commutateur partenaire est activé et que ses ISL sont opérationnels. 3) Assurez-vous que les équipements intermédiaires, tels que les périphériques xWDM, sont opérationnels.
Liaison SAS entre le nœud MetroCluster et la pile de stockage interrompue	AVERTISSEMENT	L'adaptateur SAS ou son câble connecté peut être en cause.	1. Vérifiez que l'adaptateur SAS est en ligne et en cours d'exécution. 2. Vérifiez que la connexion du câble physique est sécurisée et fonctionnelle, et remplacez le câble si nécessaire. 3. Si l'adaptateur SAS est connecté à des étagères de disques, assurez-vous que les IOM et les disques sont correctement installés.
Les liens initiateurs de MetroClusterFC sont hors service	CRITIQUE	L'adaptateur initiateur FC est en cause.	1. Assurez-vous que le lien initiateur FC n'a pas été altéré. 2. Vérifiez l'état opérationnel de l'adaptateur initiateur FC à l'aide de la commande « system node run -node local -command storage show adapter ».
Liaison d'interconnexion FC-VI interrompue	CRITIQUE	Le lien physique sur le port FC-VI est hors ligne.	1. Assurez-vous que la liaison FC-VI n'a pas été altéré. 2. Vérifiez que l'état physique de l'adaptateur FC-VI est « Up » en utilisant la commande « metrocluster interconnect adapter show ». 3. Si la configuration inclut des commutateurs fabric, assurez-vous qu'ils sont correctement câblés et configurés.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Disques de rechange MetroCluster abandonnés	AVERTISSEMENT	Le disque de rechange a été laissé sur place lors du changement de direction.	Si le disque n'est pas défectueux, restituez-le à son propriétaire d'origine en utilisant la commande « metrocluster switchback ».
Port du pont de stockage MetroCluster en panne	CRITIQUE	Le port sur le pont de stockage est hors ligne.	1) Vérifiez l'état opérationnel des ports sur le pont de stockage en utilisant la commande « storage bridge show -ports ». 2) Vérifiez la connectivité logique et physique au port.
Panne des ventilateurs du commutateur de stockage MetroCluster	CRITIQUE	Le ventilateur du commutateur de stockage est tombé en panne.	1) Assurez-vous que les ventilateurs du commutateur fonctionnent correctement en utilisant la commande « storage switch show -cooling ». 2) Assurez-vous que les FRU du ventilateur sont correctement insérés et opérationnels.
Commutateur de stockage MetroCluster inaccessible	CRITIQUE	Le commutateur de stockage n'est pas accessible via le réseau de gestion.	1) Assurez-vous que le LIF de gestion des nœuds est actif en utilisant la commande « network interface show ». 2) Assurez-vous que le commutateur est actif en utilisant la commande « network ping ». 3) Assurez-vous que le commutateur est accessible via SNMP en vérifiant ses paramètres SNMP après vous être connecté au commutateur.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Panne d'alimentation du commutateur MetroCluster	CRITIQUE	Un bloc d'alimentation sur le commutateur de stockage n'est pas opérationnel.	1) Vérifiez les détails de l'erreur en utilisant la commande « storage switch show -error -switch -name <swtich name> ». 2) Identifiez le bloc d'alimentation défectueux en utilisant la commande « storage switch show -power -switch-name <switch name> ». 3) Assurez-vous que le bloc d'alimentation est correctement inséré dans le châssis du commutateur de stockage et qu'il est entièrement opérationnel.
Défaillance des capteurs de température du commutateur MetroCluster	CRITIQUE	Le capteur du commutateur Fibre Channel est tombé en panne.	1) Vérifiez l'état de fonctionnement des capteurs de température sur le commutateur de stockage en utilisant la commande « storage switch show -cooling ». 2) Vérifiez que le commutateur fonctionne dans les conditions de température recommandées.
Température anormale du commutateur MetroCluster	CRITIQUE	Le capteur de température du commutateur Fibre Channel a signalé une température anormale.	1) Vérifiez l'état de fonctionnement des capteurs de température sur le commutateur de stockage en utilisant la commande « storage switch show -cooling ». 2) Vérifiez que le commutateur fonctionne dans les conditions de température recommandées.

Nom du moniteur	Gravité	Description du moniteur	Action corrective
Battement de cœur du processeur de service manqué	INFORMATIF	Ce message s'affiche lorsque ONTAP ne reçoit pas le signal « pulsation » attendu du processeur de service (SP). Parallèlement à ce message, les fichiers journaux du SP seront envoyés pour débogage. ONTAP réinitialisera le SP pour tenter de restaurer la communication. Le SP sera indisponible pendant deux minutes maximum pendant son redémarrage.	Contactez le support technique NetApp .
Arrêt du battement de cœur du processeur de service	AVERTISSEMENT	Ce message s'affiche lorsque ONTAP ne reçoit plus de pulsations du processeur de service (SP). Selon la conception matérielle, le système peut continuer à fournir des données ou décider de s'arrêter pour éviter toute perte de données ou tout dommage matériel. Le système continue de fournir des données, mais comme le SP ne fonctionne peut-être pas, le système ne peut pas envoyer de notifications d'appareils en panne, d'erreurs de démarrage ou d'erreurs de test automatique de mise sous tension (POST) du micrologiciel ouvert (OFW). Si votre système est configuré pour le faire, il génère et transmet un message AutoSupport (ou « appel à domicile ») au support technique NetApp et aux destinations configurées. La livraison réussie d'un message AutoSupport améliore considérablement la détermination et la résolution des problèmes.	Si le système s'est arrêté, essayez un cycle d'alimentation dur : retirez le contrôleur du châssis, remettez-le en place, puis rallumez le système. Contactez le support technique NetApp si le problème persiste après le cycle d'alimentation ou pour toute autre condition pouvant nécessiter une attention particulière.

Retour en haut

Plus d'informations

- "Affichage et suppression des alertes"

Notifications Webhook

Notification à l'aide de Webhooks

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé.

De nombreuses applications commerciales prennent en charge les webhooks comme interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et Discord prennent tous en charge les webhooks. En prenant en charge un canal webhook générique et personnalisable, Data Infrastructure Insights peut prendre en charge bon nombre de ces canaux de diffusion. Des informations sur les webhooks peuvent être trouvées sur ces sites Web d'application. Par exemple, Slack fournit"ce guide utile" .

Vous pouvez créer plusieurs canaux webhook, chaque canal ciblant un objectif différent ; applications distinctes, destinataires différents, etc.

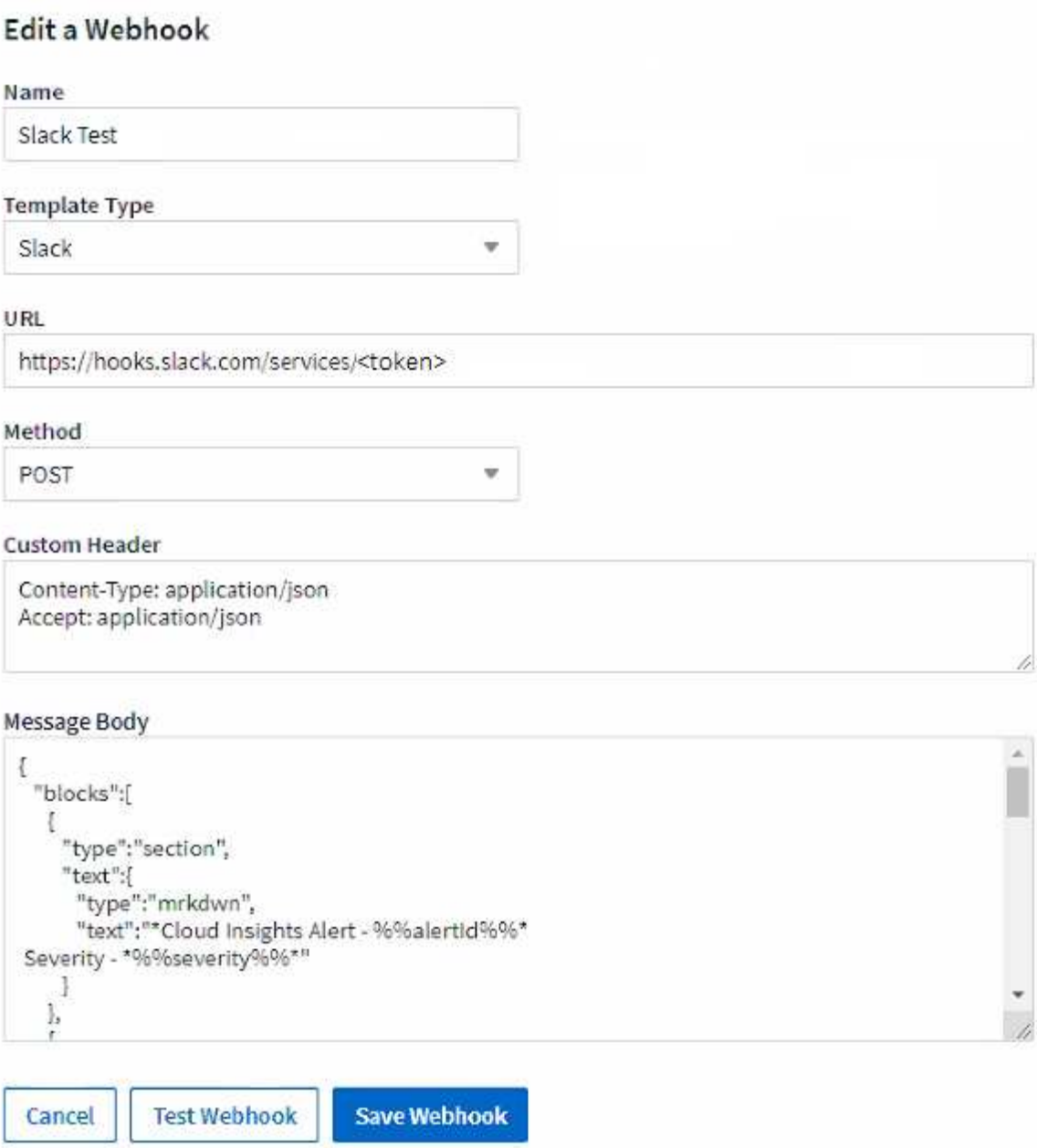
L'instance de canal webhook est composée des éléments suivants :

Nom	Nom unique
URL	URL cible du webhook, y compris le préfixe *http://* ou *https://* ainsi que les paramètres d'URL
Méthode	GET, POST - La valeur par défaut est POST
En-tête personnalisé	Spécifiez ici toutes les lignes d'en-tête personnalisées
Corps du message	Mettez le corps de votre message ici
Paramètres d'alerte par défaut	Répertorie les paramètres par défaut du webhook
Paramètres et secrets personnalisés	Les paramètres et secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Créer un Webhook

Pour créer un webhook Data Infrastructure Insights , accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**.

L'image suivante montre un exemple de webhook configuré pour Slack :



Saisissez les informations appropriées pour chacun des champs et cliquez sur « Enregistrer » lorsque vous avez terminé.

Vous pouvez également cliquer sur le bouton « Tester le Webhook » pour tester la connexion. Notez que cela enverra le « Corps du message » (sans substitutions) à l'URL définie selon la méthode sélectionnée.

Les webhooks Data Infrastructure Insights comprennent un certain nombre de paramètres par défaut. De plus, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Paramètres : que sont-ils et comment les utiliser ?

Les paramètres d'alerte sont des valeurs dynamiques renseignées par alerte. Par exemple, le paramètre *%%TriggeredOn%%* sera remplacé par l'objet sur lequel l'alerte a été déclenchée.

Vous pouvez ajouter n'importe quel attribut d'objet (par exemple, le nom de stockage) en tant que paramètre à un webhook. Par exemple, vous pouvez définir des paramètres pour le nom du volume et le nom du stockage dans une description de webhook comme : « Latence élevée pour le volume : *%%relatedObject.volume.name%%*, Stockage : *%%relatedObject.storage.name%%* ».

Notez que dans cette section, les substitutions ne sont *pas* effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le bouton envoie une charge utile qui affiche les *%%* substitutions mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

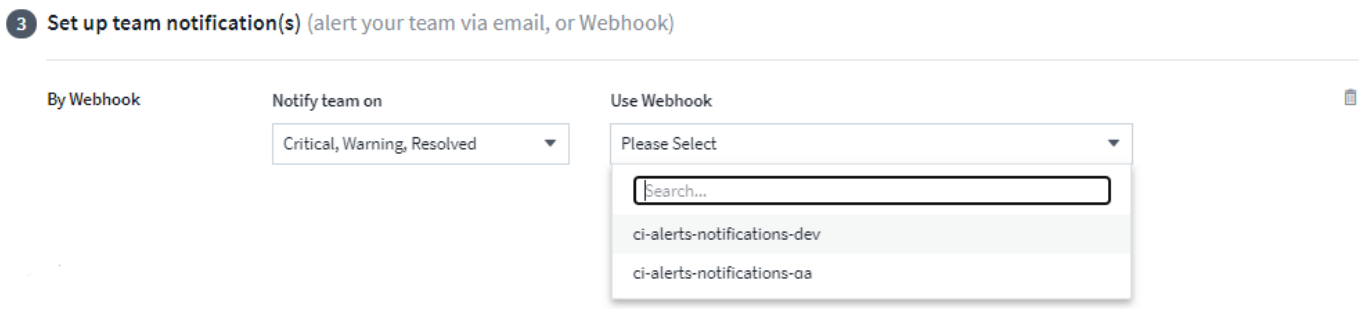
Dans cette section, vous pouvez ajouter tous les paramètres personnalisés et/ou secrets que vous souhaitez. Pour des raisons de sécurité, si un secret est défini, seul le créateur du webhook peut modifier ce canal de webhook. Il est en lecture seule pour les autres. Vous pouvez utiliser des secrets dans les URL/en-têtes comme *%%<secret_name>%%*.

Page de liste des Webhooks

Sur la page de liste des Webhooks, les champs Nom, Créé par, Créé le, Statut, Sécurisé et Dernier signalement sont affichés.

Choisir une notification Webhook dans un moniteur

Pour choisir la notification webhook dans un"moniteur" , allez dans **Alertes > Gérer les moniteurs** et sélectionnez le moniteur souhaité ou ajoutez un nouveau moniteur. Dans la section *Configurer les notifications d'équipe*, choisissez *Webhook* comme méthode de livraison. Sélectionnez les niveaux d'alerte (Critique, Avertissement, Résolu), puis choisissez le webhook souhaité.



Exemples de webhooks :

Webhooks pour"Mou" Webhooks pour"PagerDuty" Webhooks pour"Équipes" Webhooks pour"Discorde"

Exemple de webhook pour Discord

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Discord.

Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation Discord" pour les informations les plus récentes.

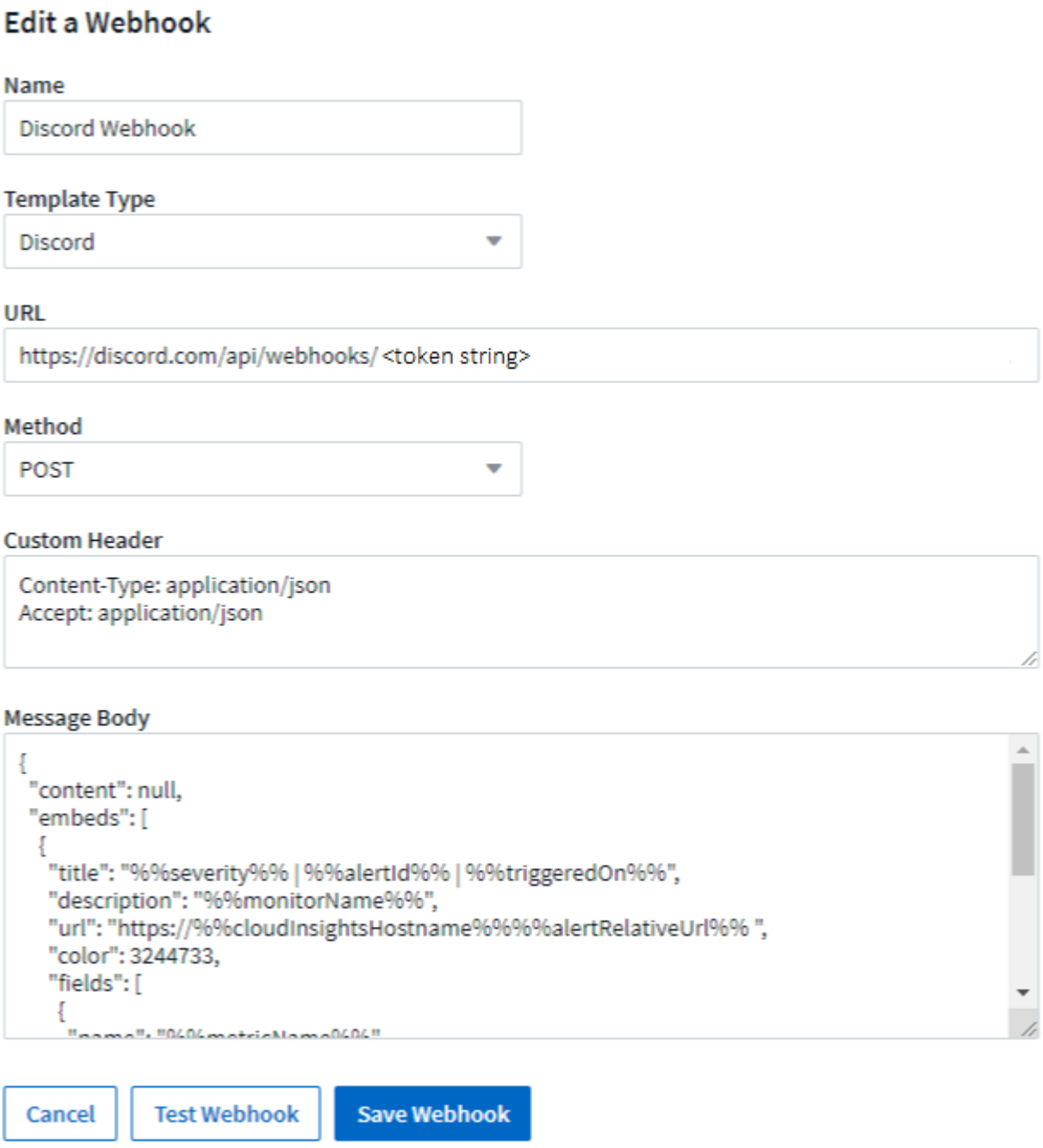
Configuration de Discord :

- Dans Discord, sélectionnez le serveur, sous Canaux texte, sélectionnez Modifier le canal (icône en forme d'engrenage)
- Sélectionnez **Intégrations > Afficher les webhooks** et cliquez sur **Nouveau webhook**

- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Data Infrastructure Insights .

Créer un webhook Data Infrastructure Insights :

1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Discord ».
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Discord**.
4. Collez l'URL ci-dessus dans le champ *URL*.

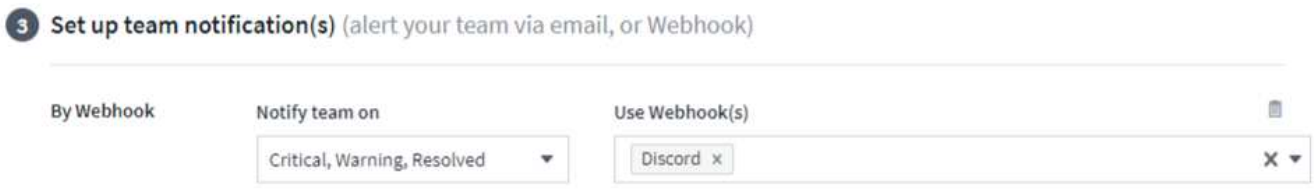


Afin de tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par n'importe quelle URL valide (telle que *https://netapp.com*), puis cliquez sur le bouton *Tester le Webhook*. Assurez-vous de réinitialiser le corps du message une fois le test terminé.

Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « Discord » pour les événements souhaités (Critique, Avertissement, Résolu)



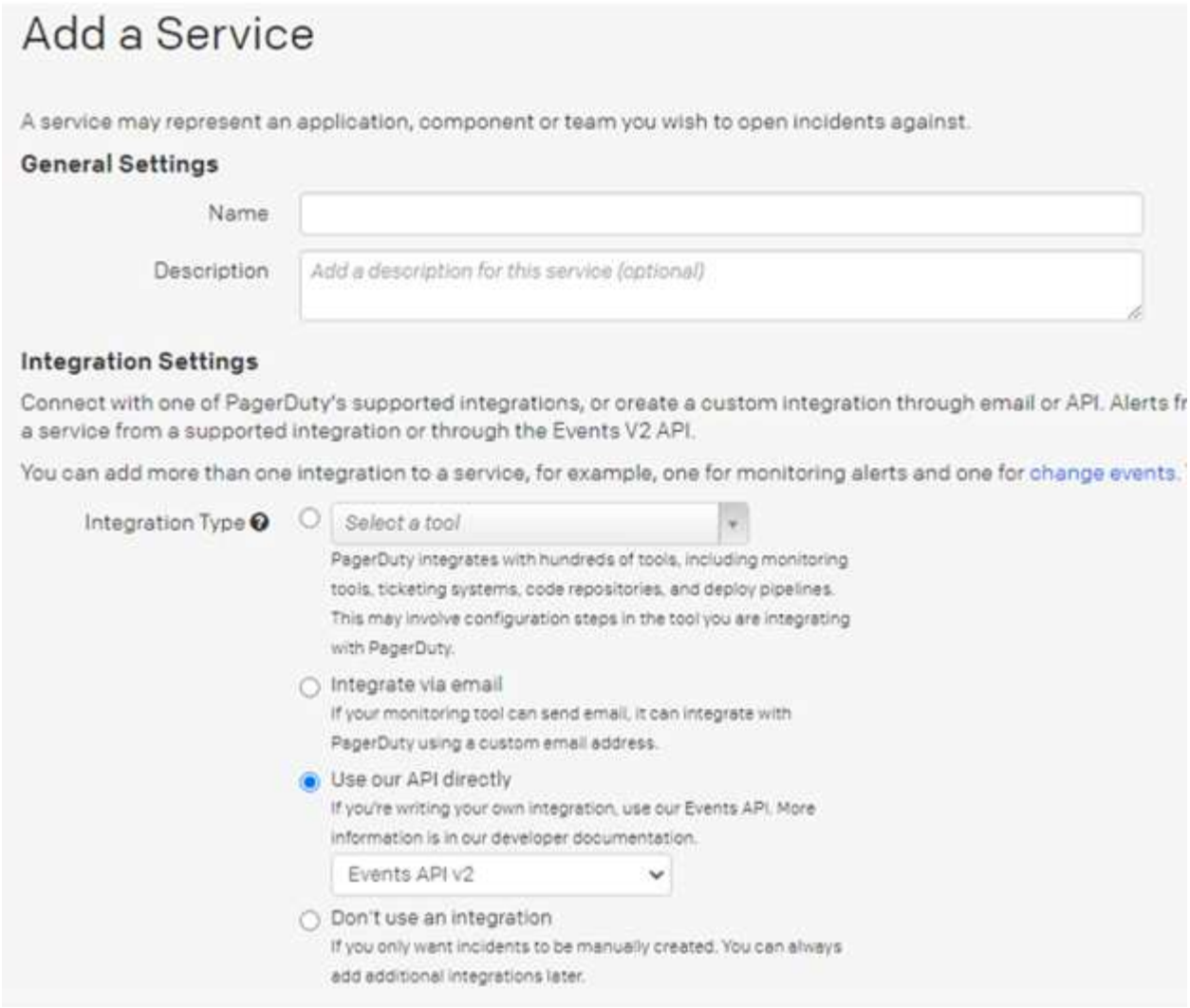
Exemple de webhook pour PagerDuty

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour PagerDuty.

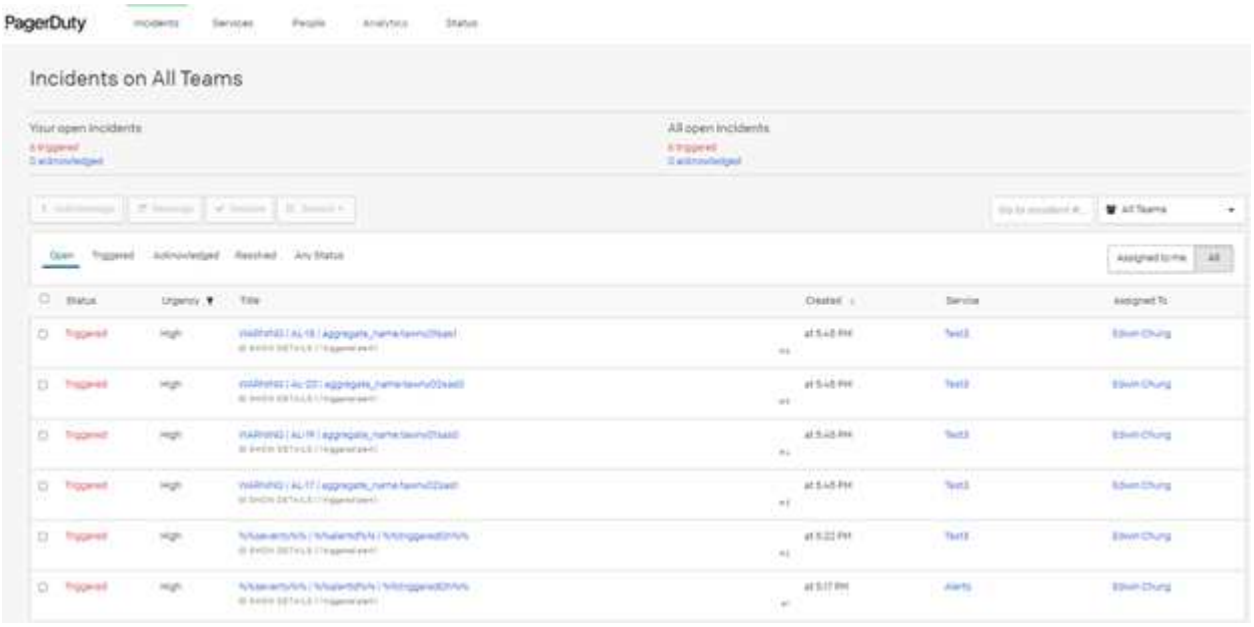
Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation de PagerDuty" pour les informations les plus récentes.

Configuration de PagerDuty :

1. Dans PagerDuty, accédez à **Services > Répertoire des services** et cliquez sur le bouton **+Nouveau service**
2. Saisissez un *Nom* et sélectionnez *Utiliser directement notre API*. Cliquez sur *Ajouter un service*.

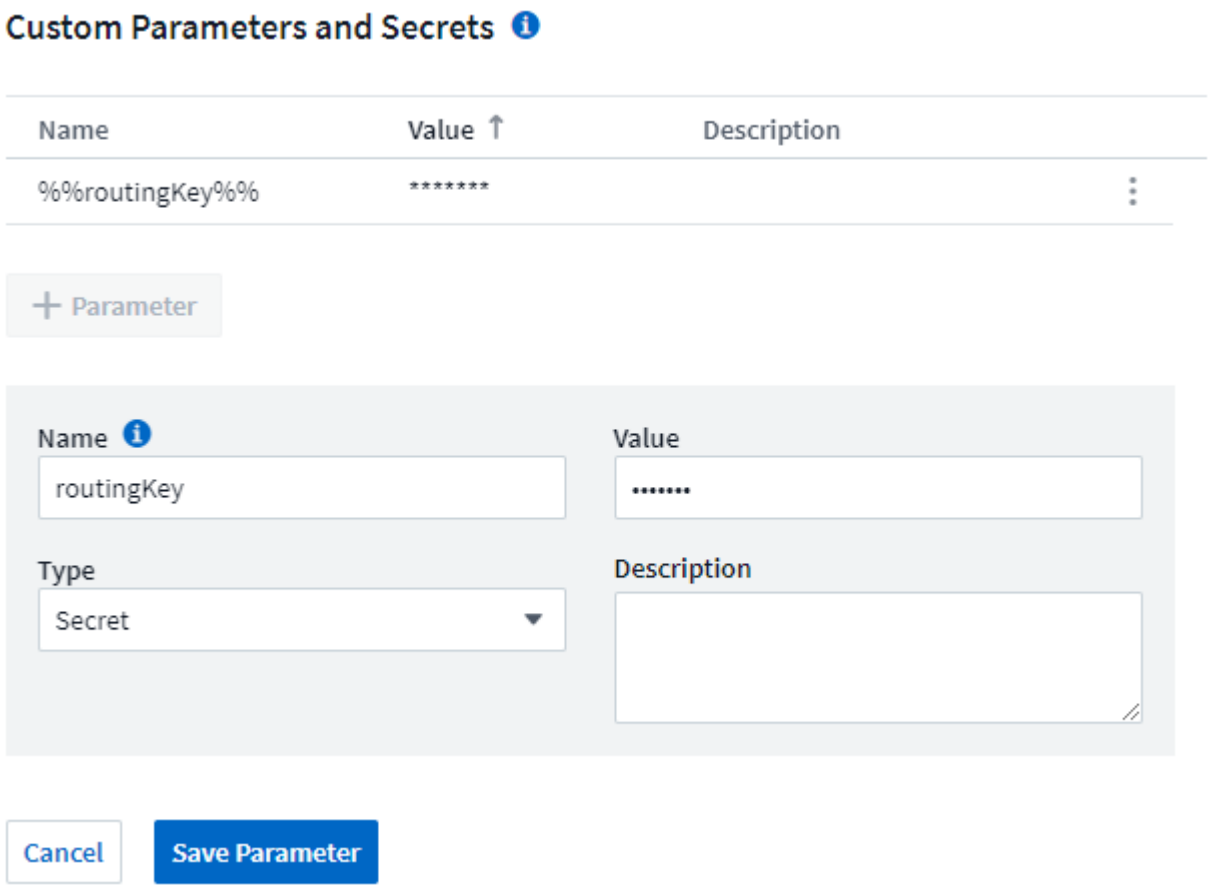


3. Cliquez sur l'onglet *Intégrations* pour voir la **Clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créerez le webhook Data Infrastructure Insights ci-dessous.
4. Accédez à **Incidents** ou **Services** pour afficher les alertes.



Créer un webhook Data Infrastructure Insights :

1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Déclencheur PagerDuty ». Vous utiliserez ce webhook pour les événements de niveau critique et d'avertissement.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **PagerDuty**.
4. Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur la valeur PagerDuty *Integration Key* ci-dessus.



Répétez ces étapes pour créer un webhook « PagerDuty Resolve » pour les événements résolus.

PagerDuty vers les Data Infrastructure Insights, cartographie des champs

Le tableau et l'image suivants montrent le mappage des champs entre PagerDuty et Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Touche d'alerte	ID d'alerte
Source	Déclenché sur
Composant	Nom métrique
Groupe	Type d'objet

PagerDuty	Data Infrastructure Insights
Classe	Nom du moniteur

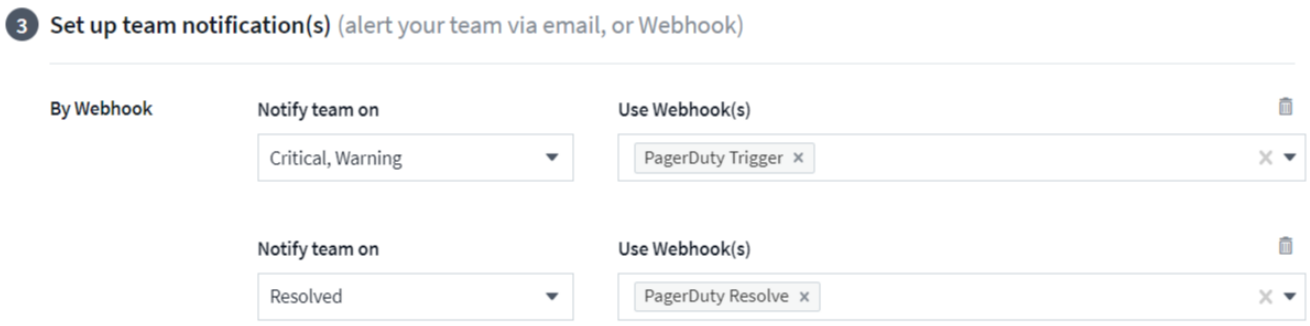
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « PagerDuty Trigger » pour les événements de niveau critique et d'avertissement.
- Choisissez « PagerDuty Resolve » pour les événements résolus.



La définition de notifications distinctes pour les événements déclencheurs et les événements résolus est une bonne pratique, car PagerDuty gère les événements déclencheurs différemment des événements résolus.

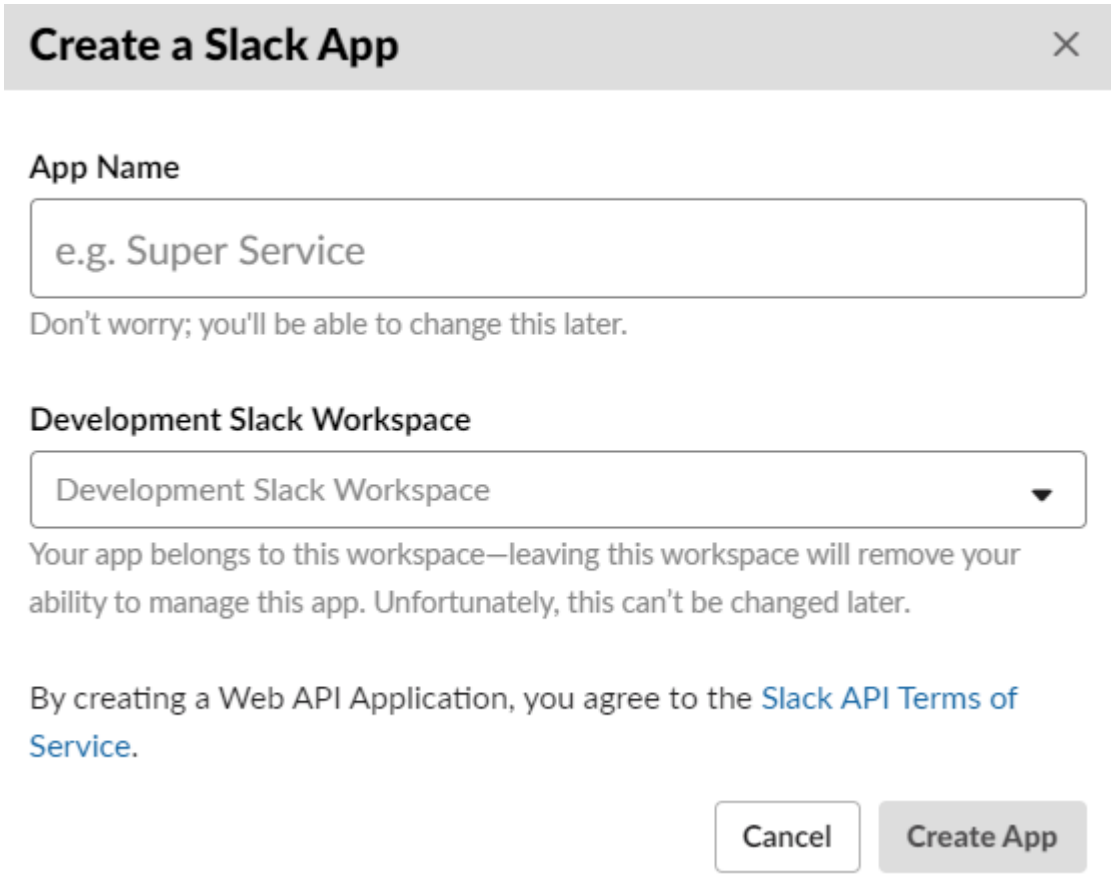
Exemple de webhook pour Slack

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Slack.

Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation Slack" pour les informations les plus récentes.

Exemple de Slack :

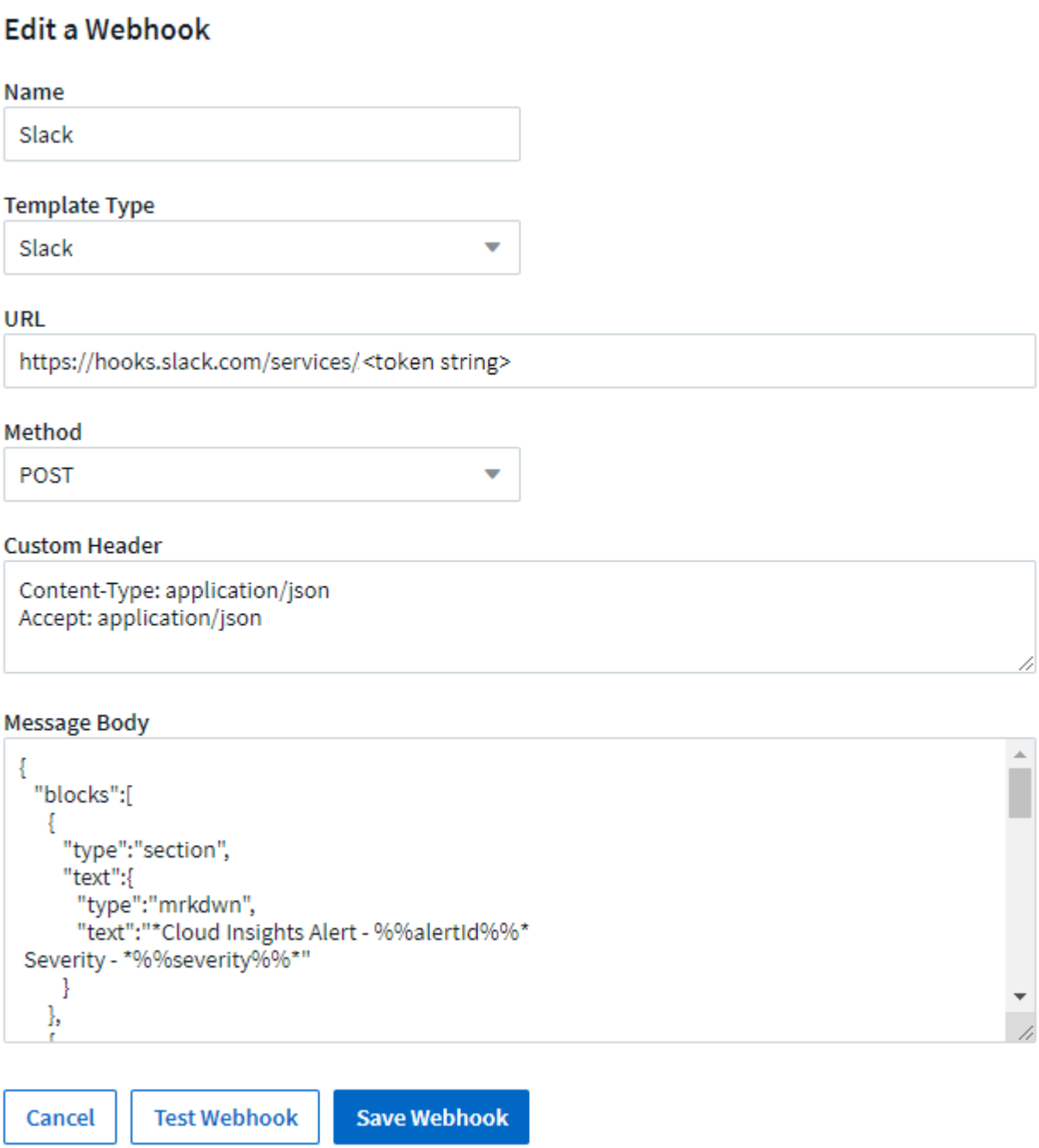
- Aller à https://api.slack.com/apps et créez une nouvelle application. Donnez-lui un nom significatif et sélectionnez l'espace de travail Slack.



- Accédez à Webhooks entrants, cliquez sur *Activer les Webhooks entrants*, Demander à *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel publier.
- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Data Infrastructure Insights .

Créer un webhook Data Infrastructure Insights :

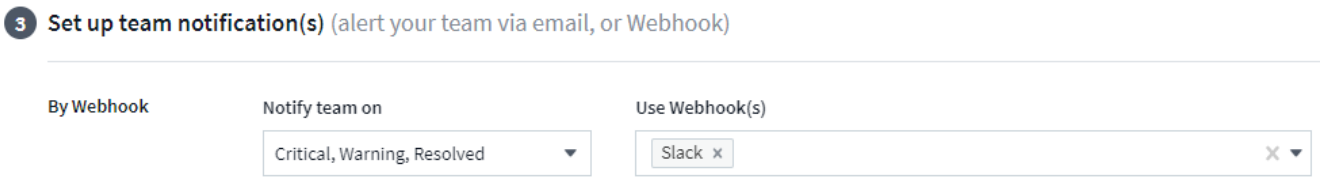
1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Slack Webhook ».
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Slack**.
4. Collez l'URL ci-dessus dans le champ *URL*.



Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « Slack » pour les événements souhaités (Critique, Avertissement, Résolu)



Plus d'informations :

- Pour modifier le format et la mise en page du message, voir https://api.slack.com/messaging/composing
- Gestion des erreurs : https://api.slack.com/messaging/webhooks#handling_errors

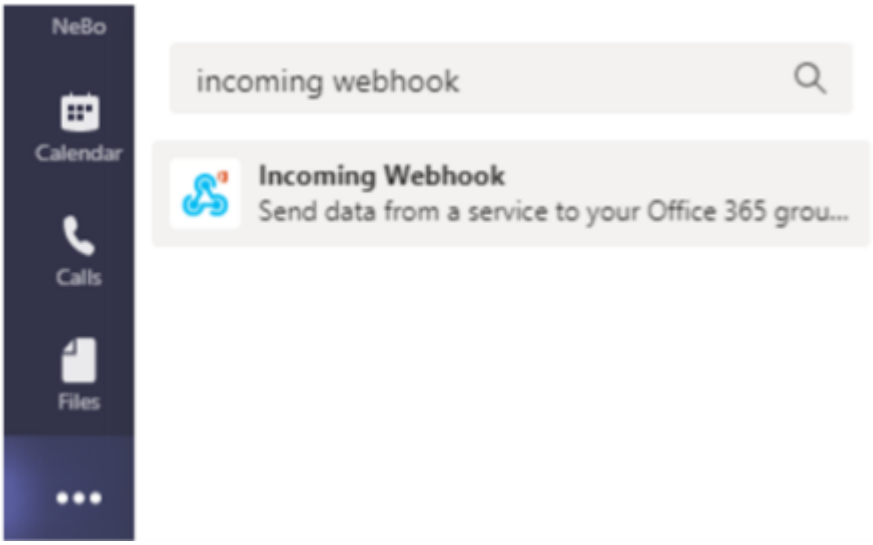
Exemple de webhook pour Microsoft Teams

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Teams.

Cette page fait référence à des instructions de tiers, qui peuvent être sujettes à modification. Reportez-vous à la"Documentation des équipes" pour les informations les plus récentes.

Configuration des équipes :

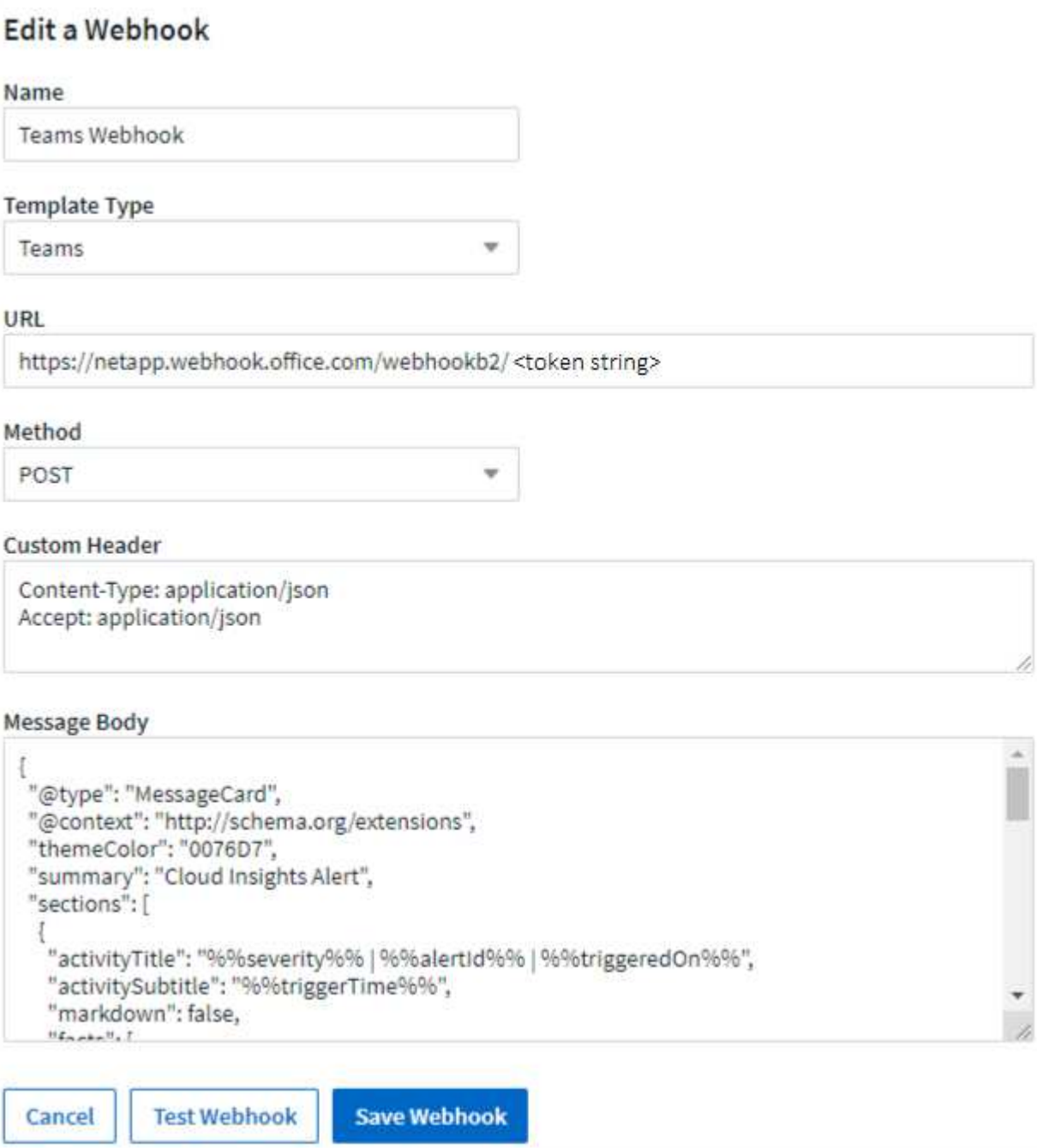
1. Dans Teams, sélectionnez le kebab et recherchez Webhook entrant.



2. Sélectionnez **Ajouter à une équipe > Sélectionner une équipe > Configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Data Infrastructure Insights .

Créer un webhook Data Infrastructure Insights :

1. Dans Data Infrastructure Insights, accédez à **Admin > Notifications** et sélectionnez l'onglet **Webhooks**. Cliquez sur **+Webhook** pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif, tel que « Webhook Équipes ».
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Équipes**.

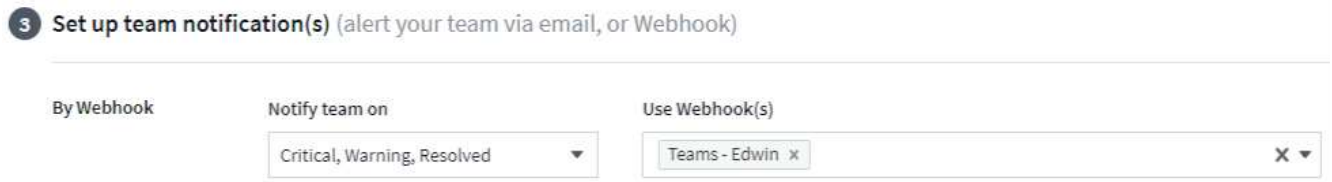


1. Collez l'URL ci-dessus dans le champ *URL*.

Notifications via Webhook

Pour notifier des événements via un webhook, dans Data Infrastructure Insights, accédez à **Alertes > Moniteurs** et cliquez sur **+Moniteur** pour créer un nouveau"moniteur" .

- Sélectionnez une métrique et définissez les conditions du moniteur.
- Sous *Configurer les notifications d'équipe*, choisissez la méthode de livraison **Webhook**.
- Choisissez le webhook « Équipes » pour les événements souhaités (Critique, Avertissement, Résolu)



Travailler avec des annotations

Définition des annotations

Lors de la personnalisation de Data Infrastructure Insights pour suivre les données en fonction des besoins de votre entreprise, vous pouvez définir des notes spécialisées, appelées annotations, et les attribuer à vos ressources.

Vous pouvez attribuer des annotations aux actifs avec des informations telles que la fin de vie de l'actif, le centre de données, l'emplacement du bâtiment, le niveau de stockage ou le niveau de service du volume.

L'utilisation d'annotations pour vous aider à surveiller votre environnement comprend les tâches de haut niveau suivantes :

- Création ou modification de définitions pour tous les types d'annotations.
- Affichage des pages d'actifs et association de chaque actif à une ou plusieurs annotations.

  Par exemple, si un actif est loué et que le bail expire dans les deux mois, vous souhaiterez peut-être appliquer une annotation de fin de vie à l'actif. Cela permet d'empêcher d'autres personnes d'utiliser cet actif pendant une période prolongée.

- Création de règles pour appliquer automatiquement des annotations à plusieurs ressources du même type.
- Filtrer les ressources par leurs annotations.

Types d'annotations par défaut

Data Infrastructure Insights fournit certains types d'annotations par défaut. Ces annotations peuvent être utilisées pour filtrer ou regrouper des données.

Vous pouvez associer des ressources à des types d'annotation par défaut tels que les suivants :

- Cycle de vie des actifs, comme l'anniversaire, le coucher du soleil ou la fin de vie
- Informations de localisation sur un appareil, telles qu'un centre de données, un bâtiment ou un étage
- Classification des actifs, par exemple par qualité (niveaux), par appareils connectés (niveau de commutation) ou par niveau de service
- Statut, tel que chaud (utilisation élevée)

Le tableau suivant répertorie les types d'annotations fournis par Data Infrastructure Insights.

Types d'annotations	Description	Type
Alias	Nom convivial pour une ressource	Texte
Groupe de ressources informatiques	Affectation de groupe utilisée par le collecteur de données des systèmes de fichiers hôte et VM	Liste
Centre de données	Localisation physique	Liste
Chaud	Appareils soumis à une utilisation intensive de manière régulière ou au seuil de capacité	Booléen
Remarque	Commentaires associés à une ressource	Test
Niveau de service	Un ensemble de niveaux de service pris en charge que vous pouvez attribuer aux ressources. Fournit une liste d'options ordonnées pour les volumes internes, qtree et les volumes. Modifiez les niveaux de service pour définir des politiques de performances pour différents niveaux.	Liste
Coucher de soleil	Seuil défini après lequel aucune nouvelle allocation ne peut être effectuée sur ce périphérique. Utile pour les migrations planifiées et autres modifications de réseau en attente.	Date
Niveau de commutation	Options prédéfinies pour la configuration des catégories pour les commutateurs. En règle générale, ces désignations restent valables pendant toute la durée de vie de l'appareil, même si vous pouvez les modifier. Disponible uniquement pour les commutateurs.	Liste
Étage	Peut être utilisé pour définir différents niveaux de service au sein de votre environnement. Les niveaux peuvent définir le type de niveau, comme la vitesse nécessaire (par exemple, or ou argent). Cette fonctionnalité est disponible uniquement sur les volumes internes, les qtrees, les baies de stockage, les pools de stockage et les volumes.	Liste
Gravité de la violation	Rang (par exemple, majeur) d'une violation (par exemple, ports hôtes manquants ou redondance manquante), dans une hiérarchie de l'importance la plus élevée à la plus faible.	Liste

Alias, Centre de données, Chaud, Niveau de service, Coucher de soleil, Niveau de commutateur, Niveau et Gravité de la violation sont des annotations au niveau du système, que vous ne pouvez pas supprimer ou renommer ; vous ne pouvez modifier que leurs valeurs attribuées.

Créer des annotations personnalisées

À l'aide d'annotations, vous pouvez ajouter des données personnalisées spécifiques à votre entreprise qui correspondent aux besoins de votre entreprise aux actifs. Bien que Data Infrastructure Insights fournisse un ensemble d'annotations par défaut, vous souhaiterez peut-être afficher les données d'autres manières. Les données des annotations personnalisées complètent les données de l'appareil déjà collectées, telles que le fabricant de stockage, les volumes numériques et les statistiques de performances. Les données que vous ajoutez à l'aide d'annotations ne sont pas découvertes par Data Infrastructure Insights.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Gérer > Annotations**.

   La page Annotations affiche la liste des annotations.

2. Cliquez sur **+Ajouter**
3. Saisissez un **Nom** et une **Description** de l'annotation.

   Vous pouvez saisir jusqu'à 255 caractères dans ces champs.

4. Cliquez sur **Type**, puis sélectionnez l'une des options suivantes qui représente le type de données autorisées dans cette annotation :

Types d'annotations

- Booléen : Crée une liste déroulante avec les options « oui » et « non ». Par exemple, l'annotation « Rattaché directement » est booléenne.
- Date : cela crée un champ qui contient une date. Par exemple, si l'annotation est une date, sélectionnez cette option.
- Liste : crée l'un des éléments suivants :
  - Une liste déroulante fixe

    Lorsque d'autres attribuent ce type d'annotation sur un appareil, ils ne peuvent pas ajouter plus de valeurs à la liste.

  - Une liste déroulante flexible

    Si vous sélectionnez l'option Ajouter de nouvelles valeurs à la volée lorsque vous créez cette liste, lorsque d'autres personnes attribuent ce type d'annotation sur un appareil, elles peuvent ajouter davantage de valeurs à la liste.

- Numéro : crée un champ dans lequel l'utilisateur attribuant l'annotation peut saisir un numéro. Par exemple, si le type d'annotation est « Étage », l'utilisateur peut sélectionner le type de valeur « numéro » et saisir le numéro de l'étage.
- Texte : crée un champ qui autorise le texte libre. Par exemple, vous pouvez saisir « Langue » comme type d'annotation, sélectionner « Texte » comme type de valeur et saisir une langue comme valeur.

> Après avoir défini le type et enregistré vos modifications, vous ne pouvez pas modifier le type de l'annotation. Si vous devez modifier le type, vous devez supprimer l'annotation et en créer une nouvelle.

1. Si vous sélectionnez Liste comme type d'annotation, procédez comme suit :
   a. Sélectionnez **Ajouter de nouvelles valeurs à la volée** si vous souhaitez pouvoir ajouter davantage de valeurs à l'annotation lorsque vous êtes sur une page d'actif, ce qui crée une liste flexible.

      Par exemple, supposons que vous êtes sur une page d'actif et que l'actif comporte l'annotation Ville avec les valeurs Détroit, Tampa et Boston. Si vous avez sélectionné l'option **Ajouter de nouvelles valeurs à la volée**, vous pouvez ajouter des valeurs supplémentaires à la ville comme San Francisco et Chicago directement sur la page de l'actif au lieu de devoir accéder à la page Annotations pour les ajouter. Si vous ne choisissez pas cette option, vous ne pouvez pas ajouter de nouvelles valeurs d'annotation lors de l'application de l'annotation ; cela crée une liste fixe.

b. Saisissez une valeur et une description dans les champs **Valeur** et **Description**.

c. Cliquez sur **Ajouter** pour ajouter des valeurs supplémentaires.

d. Cliquez sur l'icône Corbeille pour supprimer une valeur.

2. Cliquez sur **Enregistrer**

Vos annotations apparaissent dans la liste sur la page Annotations.

Remarque sur les annotations booléennes

Lors du filtrage sur une annotation booléenne, les valeurs suivantes peuvent vous être présentées sur lesquelles filtrer :

- **Tout** : cela renverra *tous* les résultats, y compris les résultats définis sur « Oui », « Non » ou pas définis du tout.
- **Oui** : renvoie uniquement les résultats « Oui ». Notez que DII affiche « Oui » comme coche dans la plupart des tableaux. Les valeurs peuvent être définies sur « Vrai », « Activé », etc. DII traite toutes ces valeurs comme « Oui ».
- **Non** : renvoie uniquement les résultats « Non ». Notez que DII affiche « Non » sous la forme d'un « X » dans la plupart des tableaux. Les valeurs peuvent être définies sur « Faux », « Désactivé », etc. DII traite toutes ces valeurs comme « Non ».
- **Aucun** : renvoie uniquement les résultats pour lesquels l'annotation n'a pas été définie du tout. Également appelées valeurs « nulles ».

Après avoir terminé

Dans l'interface utilisateur, l'annotation est immédiatement disponible pour utilisation.

Utilisation des annotations

Vous créez des annotations et les attribuez aux ressources que vous surveillez. Les annotations sont des notes qui fournissent des informations sur un actif, telles que l'emplacement physique, la fin de vie, le niveau de stockage ou les niveaux de service de volume.

Définition des annotations

À l'aide d'annotations, vous pouvez ajouter des données personnalisées spécifiques à votre entreprise qui correspondent aux besoins de votre entreprise aux actifs. Bien que Data Infrastructure Insights fournisse un ensemble d'annotations par défaut, telles que le cycle de vie de l'actif (anniversaire ou fin de vie), l'emplacement du bâtiment ou du centre de données et le niveau, vous souhaiterez peut-être afficher les données d'autres manières.

Les données des annotations personnalisées complètent les données de l'appareil déjà collectées, telles que le fabricant du commutateur, le nombre de ports et les statistiques de performances. Les données que vous ajoutez à l'aide d'annotations ne sont pas découvertes par Data Infrastructure Insights.

Avant de commencer

- Énumérez toute terminologie industrielle à laquelle les données environnementales doivent être associées.
- Lister la terminologie de l'entreprise à laquelle les données d'environnement doivent être associées.
- Identifiez tous les types d'annotations par défaut que vous pourriez être en mesure d'utiliser.

- Identifiez les annotations personnalisées que vous devez créer. Vous devez créer l'annotation avant de pouvoir l'attribuer à un actif.

Utilisez les étapes suivantes pour créer une annotation.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Enrichir > Annotations**
2. Cliquez sur **+ Annotation** pour créer une nouvelle annotation.
3. Saisissez un nom, une description et un type pour la nouvelle annotation.

   Par exemple, saisissez ce qui suit pour créer une annotation de texte qui définit l'emplacement physique d'un actif dans le centre de données 4 :

   - Saisissez un nom pour l'annotation, par exemple « Emplacement »
   - Saisissez une description de ce que décrit l'annotation, par exemple « L'emplacement physique est le centre de données 4 »
   - Saisissez le « type » d'annotation, par exemple « Texte ».

Attribution manuelle d'annotations aux ressources

L'attribution d'annotations aux ressources vous aide à trier, regrouper et générer des rapports sur les ressources de manière pertinente pour votre entreprise. Bien que vous puissiez attribuer automatiquement des annotations à des ressources d'un type particulier à l'aide de règles d'annotation, vous pouvez attribuer des annotations à une ressource individuelle à l'aide de sa page de ressource.

Avant de commencer

- Vous devez avoir créé l'annotation que vous souhaitez attribuer.

Étapes

1. Connectez-vous à votre environnement Data Infrastructure Insights .
2. Localisez l'actif auquel vous souhaitez appliquer l'annotation.
   - Vous pouvez localiser des actifs en effectuant une requête, en choisissant parmi un widget de tableau de bord ou en effectuant une recherche. Lorsque vous avez localisé l'actif souhaité, cliquez sur le lien pour ouvrir la page de destination de l'actif.
3. Sur la page de l'actif, dans la section Données utilisateur, cliquez sur **+ Annotation**.
4. La boîte de dialogue Ajouter une annotation s'affiche.
5. Sélectionnez une annotation dans la liste.
6. Cliquez sur Valeur et effectuez l'une des opérations suivantes, selon le type d'annotation que vous avez sélectionné :
   - Si le type d'annotation est liste, date ou booléen, sélectionnez une valeur dans la liste.
   - Si le type d'annotation est du texte, saisissez une valeur.
7. Cliquez sur **Enregistrer**.

Si vous souhaitez modifier la valeur de l'annotation après l'avoir attribuée, cliquez sur le champ d'annotation et sélectionnez une valeur différente. Si l'annotation est de type liste pour laquelle l'option *Ajouter de nouvelles valeurs à la volée* est sélectionnée, vous pouvez saisir une nouvelle valeur en plus de sélectionner une valeur existante.

Attribution d’annotations à l’aide de règles d’annotation

Pour attribuer automatiquement des annotations aux ressources en fonction de critères que vous définissez, vous configurez des règles d’annotation. Data Infrastructure Insights attribue les annotations aux ressources en fonction de ces règles. Data Infrastructure Insights fournit également deux règles d’annotation par défaut, que vous pouvez modifier selon vos besoins ou supprimer si vous ne souhaitez pas les utiliser.

Création de règles d’annotation

Au lieu d’appliquer manuellement des annotations à des ressources individuelles, vous pouvez appliquer automatiquement des annotations à plusieurs ressources à l’aide de règles d’annotation. Les annotations définies manuellement sur les pages d’actifs individuelles ont priorité sur les annotations basées sur des règles lorsque Insight évalue les règles d’annotation.

Avant de commencer

Vous devez avoir créé une requête pour la règle d’annotation.

À propos de cette tâche

Bien que vous puissiez modifier les types d’annotations pendant que vous créez les règles, vous devez avoir défini les types à l’avance.

Étapes

1. Cliquez sur **Gérer > Règles d’annotation**

   La page Règles d’annotation affiche la liste des règles d’annotation existantes.

2. Cliquez sur **+ Ajouter**.
3. Procédez comme suit :
   a. Dans la case **Nom**, saisissez un nom unique qui décrit la règle.

      Ce nom apparaîtra dans la page Règles d’annotation.

   b. Cliquez sur **Requête** et sélectionnez la requête utilisée pour appliquer l’annotation aux ressources.
   c. Cliquez sur **Annotation** et sélectionnez l’annotation que vous souhaitez appliquer.
   d. Cliquez sur **Valeur** et sélectionnez une valeur pour l’annotation.

      Par exemple, si vous choisissez Anniversaire comme annotation, vous spécifiez une date pour la valeur.

   e. Cliquez sur **Enregistrer**
   f. Cliquez sur **Exécuter toutes les règles** si vous souhaitez exécuter toutes les règles immédiatement ; sinon, les règles sont exécutées à un intervalle régulier.

Création de règles d’annotation

Vous pouvez utiliser des règles d’annotation pour appliquer automatiquement des annotations à plusieurs ressources en fonction de critères que vous définissez. Data Infrastructure Insights attribue les annotations aux ressources en fonction de ces règles. Les annotations définies manuellement sur les pages d’actifs individuelles ont priorité sur les annotations basées sur des règles lorsque Cloud Insight évalue les règles d’annotation.

Avant de commencer

Vous devez avoir créé une requête pour la règle d'annotation.

Étapes

1. Dans le menu Data Infrastructure Insights, cliquez sur **Gérer > Règles d'annotation**.
2. Cliquez sur **+ Règle** pour ajouter une nouvelle règle d'annotation.

   La boîte de dialogue Ajouter une règle s'affiche.

3. Procédez comme suit :
   a. Dans la case **Nom**, saisissez un nom unique qui décrit la règle.

      Le nom apparaît dans la page Règles d'annotation.

   b. Cliquez sur **Requête** et sélectionnez la requête que Data Infrastructure Insights utilise pour identifier les ressources auxquelles l'annotation s'applique.
   c. Cliquez sur **Annotation** et sélectionnez l'annotation que vous souhaitez appliquer.
   d. Cliquez sur **Valeur** et sélectionnez une valeur pour l'annotation.

      Par exemple, si vous choisissez Anniversaire comme annotation, vous spécifiez une date pour la valeur.

   e. Cliquez sur **Enregistrer**
   f. Cliquez sur **Exécuter toutes les règles** si vous souhaitez exécuter toutes les règles immédiatement ; sinon, les règles sont exécutées à un intervalle régulier.

> Dans un environnement Data Infrastructure Insights de grande taille, vous remarquerez peut-être que l'exécution des règles d'annotation semble prendre un certain temps. Cela est dû au fait que l'indexeur s'exécute en premier et doit se terminer avant d'exécuter les règles. L'indexeur est ce qui donne à Data Infrastructure Insights la possibilité de rechercher ou de filtrer des objets et des compteurs nouveaux ou mis à jour dans vos données. Le moteur de règles attend que l'indexeur termine sa mise à jour avant d'appliquer les règles.

Modification des règles d'annotation

Vous pouvez modifier une règle d'annotation pour changer le nom de la règle, son annotation, la valeur de l'annotation ou la requête associée à la règle.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Gérer > Règles d'annotation**.

   La page Règles d'annotation affiche la liste des règles d'annotation existantes.

2. Localisez la règle d'annotation que vous souhaitez modifier.

   Vous pouvez filtrer les règles d'annotation en saisissant une valeur dans la zone de filtre ou en cliquant sur un numéro de page pour parcourir les règles d'annotation par page.

3. Cliquez sur l'icône de menu de la règle que vous souhaitez modifier.

4. Cliquez sur **Modifier**

   La boîte de dialogue Modifier la règle s'affiche.

5. Modifiez le nom, l'annotation, la valeur ou la requête de la règle d'annotation.

Modification de l'ordre des règles

Les règles d'annotation sont traitées du haut de la liste des règles vers le bas. Pour modifier l'ordre dans lequel une règle est traitée, procédez comme suit :

Étapes

1. Cliquez sur l'icône de menu de la règle que vous souhaitez déplacer.
2. Cliquez sur **Déplacer vers le haut** ou **Déplacer vers le bas** selon vos besoins jusqu'à ce que la règle apparaisse à l'emplacement souhaité.

Notez que lors de l'exécution de plusieurs règles qui mettent à jour la même annotation sur un actif, la première règle (exécutée de haut en bas) applique l'annotation et met à jour l'actif, puis la deuxième règle s'applique mais ne modifie aucune annotation déjà définie par la règle précédente.

Suppression des règles d'annotation

Vous souhaiterez peut-être supprimer les règles d'annotation qui ne sont plus utilisées.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Gérer > Règles d'annotation**.

   La page Règles d'annotation affiche la liste des règles d'annotation existantes.

2. Localisez la règle d'annotation que vous souhaitez supprimer.

   Vous pouvez filtrer les règles d'annotation en saisissant une valeur dans la zone de filtre ou en cliquant sur un numéro de page pour parcourir les règles d'annotation par page.

3. Cliquez sur l'icône de menu de la règle que vous souhaitez supprimer.
4. Cliquez sur **Supprimer**

   Un message de confirmation s'affiche, vous demandant si vous souhaitez supprimer la règle.

5. Cliquez sur **OK**

Importation d'annotations

Data Infrastructure Insights inclut une API permettant d'importer des annotations ou des applications à partir d'un fichier CSV et de les attribuer aux objets que vous spécifiez.

L'API Data Infrastructure Insights est disponible dans * Data Infrastructure Insights Premium Edition*.

Importation

Les liens **Admin > Accès API** contiennent"documentation" pour l'API **Assets/Import**. Cette documentation

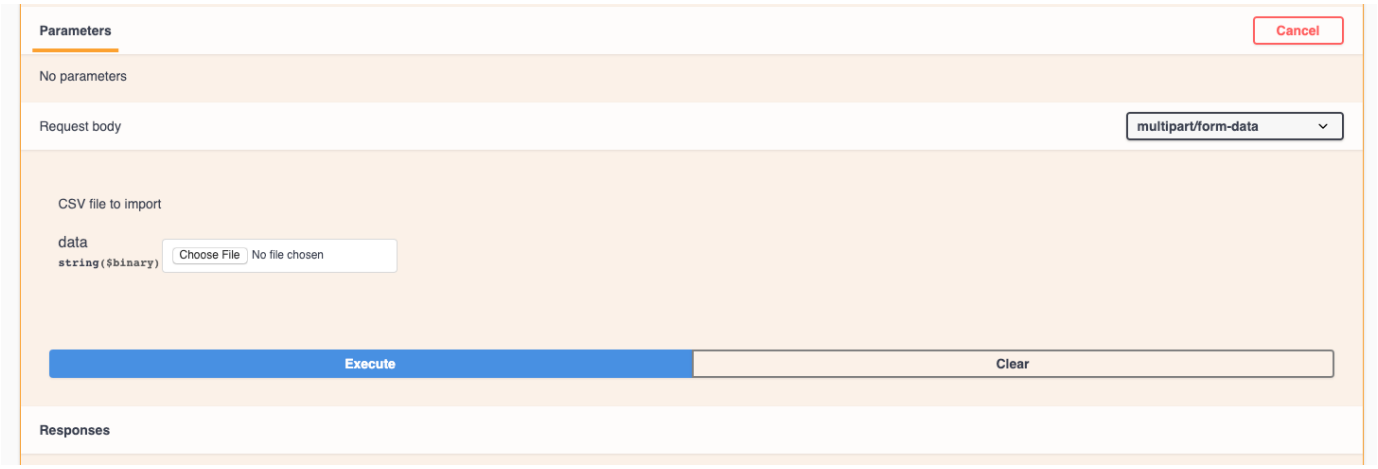
contient des informations sur le format de fichier .CSV.

Format de fichier .CSV

Le format général du fichier CSV est le suivant. La première ligne du fichier définit les champs d'importation et spécifie l'ordre des champs. Ceci est suivi de lignes séparées pour chaque annotation ou application. Vous n'avez pas besoin de définir tous les champs. Cependant, les lignes d'annotation suivantes doivent suivre le même ordre que la ligne de définition.

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
Consultez la documentation de l'API pour des exemples de fichiers .CSV.
```

Vous pouvez importer et attribuer des annotations à partir d'un fichier .CSV depuis l'API Swagger elle-même. Choisissez simplement le fichier à utiliser et cliquez sur le bouton *Exécuter* :



Comportement d'importation

Lors de l'opération d'importation, les données sont ajoutées, fusionnées ou remplacées, en fonction des objets et des types d'objets importés. Lors de l'importation, gardez à l'esprit les comportements suivants.

- Ajoute une annotation ou une application si aucune n'existe avec le même nom dans le système cible.
- Fusionne une annotation si le type d'annotation est une liste et qu'une annotation portant le même nom existe dans le système cible.
- Remplace une annotation si le type d'annotation est autre qu'une liste et qu'une annotation portant le

même nom existe dans le système cible.

Remarque : si une annotation portant le même nom mais un type différent existe dans le système cible, l'importation échoue. Si les objets dépendent de l'annotation ayant échoué, ces objets peuvent afficher des informations incorrectes ou indésirables. Vous devez vérifier toutes les dépendances d'annotation une fois l'opération d'importation terminée.

- Si une valeur d'annotation est vide, cette annotation est supprimée de l'objet. Les annotations héritées ne sont pas affectées.
- Les valeurs d'annotation de type date doivent être transmises sous forme d'heure Unix en millisecondes.
- Lors de l'annotation de volumes ou de volumes internes, le nom de l'objet est une combinaison du nom de stockage et du nom de volume utilisant le séparateur « -> ». Par exemple : *<Nom de stockage>-><Nom du volume>*
- Si un nom d'objet contient une virgule, le nom entier doit être entre guillemets. Par exemple : *"NetApp1,NetApp2"->023F*
- Lors de l'ajout d'annotations aux stockages, aux commutateurs et aux ports, la colonne « Application » sera ignorée.
- Le locataire, le secteur d'activité, l'unité commerciale et/ou le projet constituent une entité commerciale. Comme pour toutes les entités commerciales, n'importe laquelle des valeurs peut être vide.

Les types d'objets suivants peuvent être annotés.

TYPE D'OBJET	NOM OU CLÉ
Hôte	id-><id> ou <Nom> ou <IP>
Machine virtuelle	id-><id> ou <Nom>
Pool de stockage	id-><id> ou <Nom de stockage>-><Nom du pool de stockage>
Volume interne	id-><id> ou <Nom de stockage>-><Nom du volume interne>
Volume	id-><id> ou <Nom de stockage>-><Nom du volume>
Stockage	id-><id> ou <Nom> ou <IP>
Changer	id-><id> ou <Nom> ou <IP>
Port	id-><id> ou <WWN>
Qtree	id-><id> ou <Nom de stockage>-><Nom du volume interne>-><Nom Qtree>
Partager	id-><id> ou <Nom de stockage>-><Nom du volume interne>-><Nom de partage>-><Protocole>[-><Nom Qtree (facultatif en cas de Qtree par défaut)>]

Travailler avec des applications

Suivi de l'utilisation des actifs par application

Comprendre les applications utilisées dans l'environnement de votre entreprise vous aide à suivre l'utilisation et le coût des actifs.

Avant de pouvoir suivre les données associées aux applications exécutées sur votre locataire, vous devez d'abord définir ces applications et les associer aux ressources appropriées. Vous pouvez associer des applications aux ressources suivantes : hôtes, machines virtuelles, volumes, volumes internes, qtrees, partages et hyperviseurs.

Cette rubrique fournit un exemple de suivi de l'utilisation des machines virtuelles que l'équipe marketing utilise pour sa messagerie Exchange.

Vous souhaiterez peut-être créer un tableau similaire au suivant pour identifier les applications utilisées sur votre locataire et noter le groupe ou l'unité commerciale utilisant chaque application.

Locataire	Secteur d'activité	Unité commerciale	Projet	Applications
NetApp	Stockage de données	Légal	Brevets	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Stockage de données	Commercialisation	Événements de vente	Exchange, base de données partagée Oracle, planificateur d'événements BlastOff

Le tableau montre que l'équipe marketing utilise l'application Exchange. Nous souhaitons suivre leur utilisation de la machine virtuelle pour Exchange, afin de pouvoir prédire quand nous devrons ajouter plus de stockage. Nous pouvons associer l'application Exchange à toutes les machines virtuelles de Marketing :

1. Créer une application nommée *Exchange*
2. Accédez à **Requêtes > +Nouvelle requête** pour créer une nouvelle requête pour les machines virtuelles (ou sélectionnez une requête de machine virtuelle existante, le cas échéant).

   En supposant que toutes les machines virtuelles de l'équipe marketing aient un nom contenant la chaîne « **mkt** », créez votre requête pour filtrer le nom de la machine virtuelle pour « mkt ».
3. Sélectionnez les machines virtuelles.
4. Associez les machines virtuelles à l'application *Exchange* à l'aide de **Actions en masse > Ajouter des applications**.
5. Sélectionnez l'application souhaitée et cliquez sur **Enregistrer**.
6. Une fois terminé, **Enregistrez** la requête.

Création d'applications

Pour suivre les données associées à des applications spécifiques exécutées sur votre locataire, vous pouvez définir les applications dans Data Infrastructure Insights.

À propos de cette tâche

Data Infrastructure Insights vous permet de suivre les données des actifs associés aux applications pour des éléments tels que l'utilisation ou les rapports de coûts.

Étapes

1. Dans le menu Data Infrastructure Insights , cliquez sur **Observabilité > Enrichir > Applications**. Sélectionner

La boîte de dialogue Ajouter une application s'affiche.

2. Entrez un nom unique pour l'application.
3. Sélectionnez une priorité pour l'application.
4. Cliquez sur **Enregistrer**.

Après avoir défini une application, elle peut être affectée à des actifs.

Affectation d'applications à des actifs

Cette procédure attribue l'application à un hôte à titre d'exemple. Vous pouvez attribuer un hôte, une machine virtuelle, un volume ou des volumes internes à une application.

Étapes

1. Localisez l'actif auquel vous souhaitez affecter l'application :
2. Cliquez sur **Requêtes > +Nouvelle requête** et recherchez Hôte.
3. Cliquez sur la case à cocher à gauche de l'hôte que vous souhaitez associer à l'application.
4. Cliquez sur **Actions en masse > Ajouter une application**.
5. Sélectionnez l'application à laquelle vous attribuez l'actif.

Toutes les nouvelles applications que vous attribuez remplacent toutes les applications de l'actif dérivées d'un autre actif. Par exemple, les volumes héritent des applications des hôtes et lorsque de nouvelles applications sont attribuées à un volume, la nouvelle application a la priorité sur l'application dérivée.

Pour les environnements comportant de grandes quantités d'actifs associés, l'héritage des affectations d'application à ces actifs peut prendre plusieurs minutes. Veuillez prévoir plus de temps pour que l'héritage se produise si vous avez de nombreux biens liés.

Après avoir terminé

Après avoir attribué l'hôte à l'application, vous pouvez attribuer les ressources restantes à l'application. Pour accéder à la page de destination de l'application, cliquez sur **Gérer > Application** et sélectionnez l'application que vous avez créée.

Résolution automatique des appareils

Présentation de la résolution automatique des appareils

Vous devez identifier tous les appareils que vous souhaitez surveiller avec Data Infrastructure Insights. L'identification est nécessaire afin de suivre avec précision les performances et l'inventaire de votre locataire. En règle générale, la majorité des appareils détectés sur votre locataire sont identifiés via la *Résolution automatique des appareils*.

Une fois les collecteurs de données configurés, les périphériques de votre locataire, y compris les commutateurs, les baies de stockage et votre infrastructure virtuelle d'hyperviseurs et de machines virtuelles, sont identifiés. Cependant, cela n'identifie normalement pas 100 % des appareils de votre locataire.

Une fois les périphériques de type collecteur de données configurés, la meilleure pratique consiste à exploiter les règles de résolution de périphérique pour aider à identifier les périphériques inconnus restants sur votre

locataire. La résolution des appareils peut vous aider à résoudre les appareils inconnus tels que les types d'appareils suivants :

- Hôtes physiques
- Baies de stockage
- bandes

Les appareils restant inconnus après la résolution de l'appareil sont considérés comme des appareils génériques, que vous pouvez également afficher dans les requêtes et sur les tableaux de bord.

Les règles créées à leur tour identifieront automatiquement les nouveaux appareils avec des attributs similaires à mesure qu'ils sont ajoutés à votre environnement. Dans certains cas, la résolution des appareils permet également une identification manuelle en contournant les règles de résolution des appareils pour les appareils non détectés dans Data Infrastructure Insights.

Une identification incomplète des appareils peut entraîner des problèmes, notamment :

- Chemins incomplets
- Connexions multi-chemins non identifiées
- L'impossibilité de regrouper les applications
- Vues topologiques inexactes
- Données inexactes dans l'entrepôt de données et les rapports

La fonctionnalité de résolution de l'appareil (Gérer > Résolution de l'appareil) comprend les onglets suivants, chacun jouant un rôle dans la planification de la résolution de l'appareil et l'affichage des résultats :

- **Fibre Channel Identify** contient une liste de WWN et d'informations de port des périphériques Fibre Channel qui n'ont pas été résolus via la résolution automatique des périphériques. L'onglet identifie également le pourcentage d'appareils qui ont été identifiés.
- **Identification de l'adresse IP** contient une liste des périphériques accédant aux partages CIFS et aux partages NFS qui n'ont pas été identifiés via la résolution automatique des périphériques. L'onglet identifie également le pourcentage d'appareils qui ont été identifiés.
- **Règles de résolution automatique** contient la liste des règles exécutées lors de la résolution des périphériques Fibre Channel. Il s'agit de règles que vous créez pour résoudre les problèmes de périphériques Fibre Channel non identifiés.
- **Préférences** fournit des options de configuration que vous utilisez pour personnaliser la résolution de l'appareil pour votre environnement.

Avant de commencer

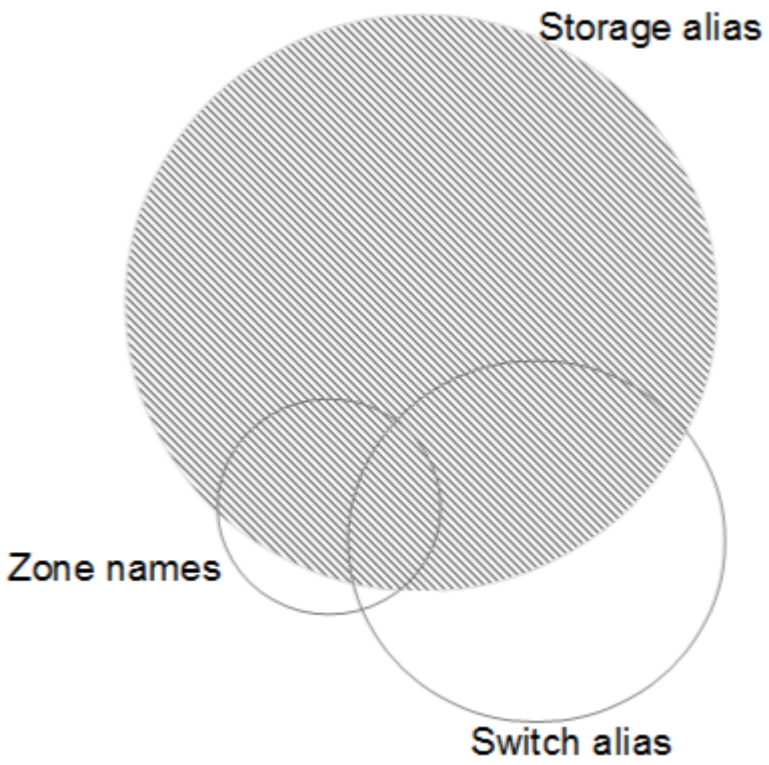
Vous devez savoir comment votre environnement est configuré avant de définir les règles d'identification des périphériques. Plus vous en savez sur votre environnement, plus il sera facile d'identifier les appareils.

Vous devez répondre à des questions similaires aux suivantes pour vous aider à créer des règles précises :

- Votre environnement dispose-t-il de normes de dénomination pour les zones ou les hôtes et quel pourcentage d'entre elles sont exactes ?
- Votre environnement utilise-t-il un alias de commutateur ou un alias de stockage et correspondent-ils au nom d'hôte ?
- À quelle fréquence les schémas de dénomination changent-ils sur votre locataire ?

- Y a-t-il eu des acquisitions ou des fusions qui ont introduit des schémas de dénomination différents ?

Après avoir analysé votre environnement, vous devriez être en mesure d'identifier les normes de dénomination existantes que vous pouvez vous attendre à rencontrer de manière fiable. Les informations que vous avez recueillies peuvent être représentées graphiquement dans une figure similaire à la suivante :



Dans cet exemple, le plus grand nombre de périphériques est représenté de manière fiable par des alias de stockage. Les règles qui identifient les hôtes à l'aide d'alias de stockage doivent être écrites en premier, les règles utilisant des alias de commutateur doivent être écrites ensuite et les dernières règles créées doivent utiliser des alias de zone. En raison du chevauchement de l'utilisation des alias de zone et des alias de commutateur, certaines règles d'alias de stockage peuvent identifier des périphériques supplémentaires, laissant moins de règles requises pour les alias de zone et les alias de commutateur.

Étapes pour identifier les appareils

En règle générale, vous utiliseriez un flux de travail similaire à celui suivant pour identifier les appareils sur votre locataire. L'identification est un processus itératif et peut nécessiter plusieurs étapes de planification et d'affinement des règles.

- Environnement de recherche
- Règles du plan
- Créer/Réviser les règles
- Résultats de l'examen
- Créer des règles supplémentaires ou identifier manuellement les appareils
- Fait

Si vous avez des périphériques non identifiés (également appelés périphériques inconnus ou génériques) sur votre locataire et que vous configurez ensuite une source de données qui identifie ces périphériques lors de l'interrogation, ils ne seront plus affichés ni comptés comme des périphériques génériques.

En rapport:"Création de règles de résolution de périphérique" "Résolution du périphérique Fibre Channel" "Résolution du périphérique IP" "Définition des préférences de résolution de l'appareil"

Règles de résolution des appareils

Vous créez des règles de résolution de périphérique pour identifier les hôtes, le stockage et les bandes qui ne sont pas automatiquement identifiés actuellement par Data Infrastructure Insights. Les règles que vous créez identifient les périphériques actuellement présents dans votre environnement et identifient également les périphériques similaires lorsqu'ils sont ajoutés à votre environnement.

Création de règles de résolution de périphérique

Lorsque vous créez des règles, vous commencez par identifier la source d'informations sur laquelle la règle s'exécute, la méthode utilisée pour extraire les informations et si la recherche DNS est appliquée aux résultats de la règle.

Source utilisée pour identifier l'appareil	* Alias SRM pour les hôtes * Alias de stockage contenant un nom d'hôte ou de bande intégré * Alias de commutateur contenant un nom d'hôte ou de bande intégré * Noms de zone contenant un nom d'hôte intégré
Méthode utilisée pour extraire le nom du périphérique de la source	* Tel quel (extraire un nom d'un SRM) * Délimiteurs * Expressions régulières
Recherche DNS	Spécifie si vous utilisez DNS pour vérifier le nom d'hôte

Vous créez des règles dans l'onglet Règles de résolution automatique. Les étapes suivantes décrivent le processus de création de règles.

Procédure

1. Cliquez sur **Gérer > Résolution du périphérique**
2. Dans l'onglet **Règles de résolution automatique**, cliquez sur **+ Règle d'hôte** ou **+ Règle de bande**.

   L'écran **Règle de résolution** s'affiche.

   Cliquez sur le lien *Afficher les critères de correspondance* pour obtenir de l'aide et des exemples de création d'expressions régulières.

3. Dans la liste **Type**, sélectionnez l'appareil que vous souhaitez identifier.

   Vous pouvez sélectionner *Hôte* ou *Bande*.

4. Dans la liste **Source**, sélectionnez la source que vous souhaitez utiliser pour identifier l'hôte.

Selon la source choisie, Data Infrastructure Insights affiche la réponse suivante :

a. **Zones** répertorie les zones et WWN qui doivent être identifiés par Data Infrastructure Insights.
b. **SRM** répertorie les alias non identifiés qui doivent être identifiés par Data Infrastructure Insights
c. **Alias de stockage** répertorie les alias de stockage et les WWN qui doivent être identifiés par Data Infrastructure Insights
d. **Alias de commutateur** répertorie les alias de commutateur qui doivent être identifiés par Data Infrastructure Insights

5. Dans la liste **Méthode**, sélectionnez la méthode que vous souhaitez utiliser pour identifier l'hôte.

Source	Méthode
SRM	Tel quel, délimiteurs, expressions régulières
Alias de stockage	Délimiteurs, expressions régulières
Changer d'alias	Délimiteurs, expressions régulières
Zones	Délimiteurs, expressions régulières

◦ Les règles utilisant des délimiteurs nécessitent les délimiteurs et la longueur minimale du nom d'hôte. La longueur minimale du nom d'hôte est le nombre de caractères que Data Infrastructure Insights doit utiliser pour identifier un hôte. Data Infrastructure Insights effectue des recherches DNS uniquement pour les noms d'hôtes d'une longueur égale ou supérieure.

Pour les règles utilisant des délimiteurs, la chaîne d'entrée est tokenisée par le délimiteur et une liste de candidats au nom d'hôte est créée en effectuant plusieurs combinaisons du jeton adjacent. La liste est ensuite triée, du plus grand au plus petit. Par exemple, pour une entrée sring de *vipsnq03_hba3_emc3_12ep0*, la liste donnerait le résultat suivant :

▪ vipsnq03_hba3_emc3_12ep0
▪ vipsnq03_hba3_emc3
▪ hba3 emc3_12ep0
▪ vipsnq03_hba3
▪ emc3_12ep0
▪ hba3_emc3
▪ vipsnq03
▪ 12ep0
▪ emc3
▪ hba3

◦ Les règles utilisant des expressions régulières nécessitent une expression régulière, le format et la sélection de la sensibilité à la casse.

6. Cliquez sur **Exécuter AR** pour exécuter toutes les règles, ou cliquez sur la flèche vers le bas du bouton pour exécuter la règle que vous avez créée (et toutes les autres règles créées depuis la dernière exécution complète d'AR).

Les résultats de l'exécution de la règle sont affichés dans l'onglet **FC identify**.

Démarrage d'une mise à jour automatique de la résolution de l'appareil

Une mise à jour de résolution de périphérique valide les modifications manuelles qui ont été ajoutées depuis la dernière exécution de résolution automatique complète du périphérique. L'exécution d'une mise à jour peut être utilisée pour valider et exécuter uniquement les nouvelles entrées manuelles apportées à la configuration de résolution du périphérique. Aucune exécution de résolution complète de l'appareil n'est effectuée.

Procédure

1. Connectez-vous à l'interface Web de Data Infrastructure Insights .
2. Cliquez sur **Gérer > Résolution du périphérique**
3. Dans l'écran **Résolution de l'appareil**, cliquez sur la flèche vers le bas du bouton **Exécuter AR**.
4. Cliquez sur **Mettre à jour** pour démarrer la mise à jour.

Identification manuelle assistée par des règles

Cette fonctionnalité est utilisée pour les cas particuliers où vous souhaitez exécuter une règle spécifique ou une liste de règles (avec ou sans réorganisation unique) pour résoudre les hôtes, les périphériques de stockage et les périphériques de bande inconnus.

Avant de commencer

Vous disposez d'un certain nombre d'appareils qui n'ont pas été identifiés et vous disposez également de plusieurs règles qui ont identifié avec succès d'autres appareils.

> Si votre source ne contient qu'une partie d'un nom d'hôte ou de périphérique, utilisez une règle d'expression régulière et formatez-la pour ajouter le texte manquant.

Procédure

1. Connectez-vous à l'interface Web de Data Infrastructure Insights .
2. Cliquez sur **Gérer > Résolution du périphérique**
3. Cliquez sur l'onglet **Identification Fibre Channel**.

   Le système affiche les périphériques ainsi que leur état de résolution.

4. Sélectionnez plusieurs appareils non identifiés.
5. Cliquez sur **Actions en masse** et sélectionnez **Définir la résolution de l'hôte** ou **Définir la résolution de la bande**.

   Le système affiche l'écran Identifier qui contient une liste de toutes les règles qui ont identifié avec succès les périphériques.

6. Modifiez l'ordre des règles pour un ordre qui répond à vos besoins.

   L'ordre des règles est modifié dans l'écran Identifier, mais n'est pas modifié globalement.

7. Sélectionnez la méthode qui répond à vos besoins.

Data Infrastructure Insights exécute le processus de résolution de l'hôte dans l'ordre dans lequel les méthodes apparaissent, en commençant par celles du haut.

Lorsque des règles applicables sont rencontrées, les noms des règles sont affichés dans la colonne Règles et identifiés comme manuels.

En rapport:"Résolution du périphérique Fibre Channel" "Résolution du périphérique IP" "Définition des préférences de résolution de l'appareil"

Résolution du périphérique Fibre Channel

L'écran d'identification Fibre Channel affiche le WWN et le WWPN des périphériques Fibre Channel dont les hôtes n'ont pas été identifiés par la résolution automatique des périphériques. L'écran affiche également tous les périphériques qui ont été résolus par résolution manuelle.

Les périphériques qui ont été résolus par résolution manuelle contiennent un statut *OK* et identifient la règle utilisée pour identifier le périphérique. Les appareils manquants ont le statut *Non identifié*. Les appareils spécifiquement exclus de l'identification ont le statut *Exclus*. La couverture totale pour l'identification des appareils est répertoriée sur cette page.

Vous effectuez des actions groupées en sélectionnant plusieurs périphériques sur le côté gauche de l'écran d'identification Fibre Channel. Les actions peuvent être effectuées sur un seul appareil en survolant un appareil et en sélectionnant les boutons *Identifier* ou *Désidentifier* à l'extrême droite de la liste.

Le lien *Couverture totale* affiche une liste du nombre d'appareils identifiés/nombre d'appareils disponibles pour votre configuration :

- Alias SRM
- Alias de stockage
- Changer d'alias
- Zones
- Défini par l'utilisateur

Ajout manuel d'un périphérique Fibre Channel

Vous pouvez ajouter manuellement un périphérique Fibre Channel à Data Infrastructure Insights à l'aide de la fonctionnalité *Ajout manuel* disponible dans l'onglet Identification Fibre Channel de résolution de périphérique. Ce processus peut être utilisé pour la pré-identification d'un dispositif qui devrait être découvert dans le futur.

Avant de commencer

Pour ajouter avec succès une identification de périphérique au système, vous devez connaître l'adresse WWN ou IP et le nom de l'appareil.

À propos de cette tâche

Vous pouvez ajouter manuellement un hôte, un stockage, une bande ou un périphérique Fibre Channel inconnu.

Procédure

1. Connectez-vous à l'interface Web de Data Infrastructure Insights
2. Cliquez sur **Gérer > Résolution du périphérique**
3. Cliquez sur l'onglet **Identification Fibre Channel**.
4. Cliquez sur le bouton **Ajouter**.

   La boîte de dialogue **Ajouter un périphérique** s'affiche

5. Saisissez l'adresse WWN ou IP, le nom de l'appareil et sélectionnez le type d'appareil.

   Le périphérique que vous saisissez est ajouté à la liste des périphériques dans l'onglet Identification Fibre Channel. La règle est identifiée comme *Manuel*.

Importation de l'identification du périphérique Fibre Channel à partir d'un fichier .CSV

Vous pouvez importer manuellement l'identification du périphérique Fibre Channel dans la résolution de périphérique Data Infrastructure Insights à l'aide d'une liste de périphériques dans un fichier .CSV.

1. Avant de commencer

Vous devez disposer d'un fichier .CSV correctement formaté pour pouvoir importer les identifications des appareils directement dans la résolution de l'appareil. Le fichier .CSV pour les périphériques Fibre Channel nécessite les informations suivantes :

WWN	propriété intellectuelle	Nom	Type

Les champs de données doivent être placés entre guillemets, comme indiqué dans l'exemple ci-dessous.

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

> En tant que meilleure pratique, il est recommandé d'exporter d'abord les informations d'identification de Fibre Channel vers un fichier .CSV, d'apporter les modifications souhaitées dans ce fichier, puis de réimporter le fichier dans Fibre Channel Identify. Cela garantit que les colonnes attendues sont présentes et dans le bon ordre.

Pour importer les informations d'identification Fibre Channel :

1. Connectez-vous à l'interface Web de Data Infrastructure Insights .
2. Cliquez sur **Gérer > Résolution du périphérique**
3. Sélectionnez l'onglet **Identification Fibre Channel**.
4. Cliquez sur le bouton **Identifier > Identifier à partir du fichier**.
5. Accédez au dossier contenant vos fichiers .CSV à importer et sélectionnez le fichier souhaité.

   Les périphériques que vous saisissez sont ajoutés à la liste des périphériques dans l'onglet Identification Fibre Channel. La « Règle » est identifiée comme Manuel.

Exportation des identifications de périphériques Fibre Channel vers un fichier .CSV

Vous pouvez exporter les identifications de périphériques Fibre Channel existantes vers un fichier .CSV à partir de la fonctionnalité de résolution de périphériques Data Infrastructure Insights . Vous souhaiterez peut-être exporter une identification d'appareil afin de pouvoir la modifier, puis la réimporter dans Data Infrastructure Insights où elle sera ensuite utilisée pour identifier les appareils similaires à ceux correspondant à l'origine à l'identification exportée.

À propos de cette tâche

Ce scénario peut être utilisé lorsque les appareils ont des attributs similaires qui peuvent être facilement modifiés dans le fichier .CSV, puis réimportés dans le système.

Lorsque vous exportez une identification de périphérique Fibre Channel vers un fichier .CSV, le fichier contient les informations suivantes dans l'ordre indiqué :

WWN	propriété intellectuelle	Nom	Type

Procédure

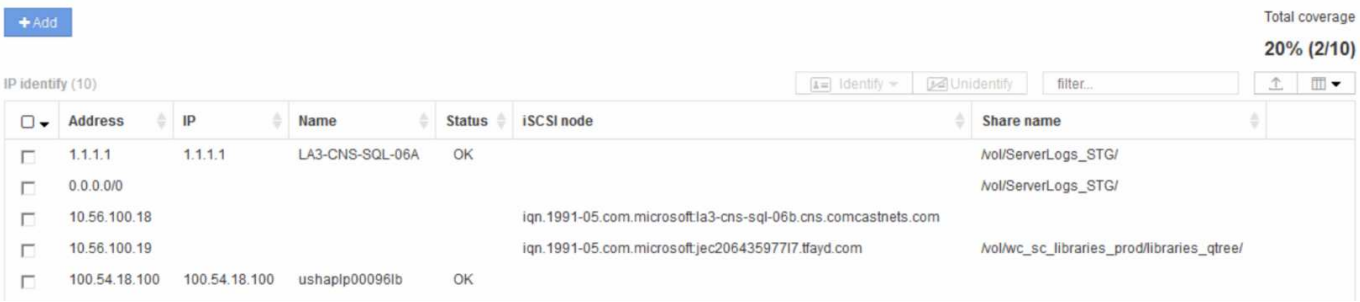
1. Connectez-vous à l'interface Web de Data Infrastructure Insights .
2. Cliquez sur **Gérer > Résolution du périphérique**
3. Sélectionnez l'onglet **Identification Fibre Channel**.
4. Sélectionnez le ou les périphériques Fibre Channel dont vous souhaitez exporter l'identification.
5. Cliquez sur *Exporter* bouton.

   Sélectionnez si vous souhaitez ouvrir le fichier .CSV ou enregistrer le fichier.

En rapport:"Résolution du périphérique IP" "Création de règles de résolution de périphérique" "Définition des préférences de résolution de l'appareil"

Résolution du périphérique IP

L'écran d'identification IP affiche tous les partages iSCSI et CIFS ou NFS qui ont été identifiés par une résolution automatique ou manuelle du périphérique. Des appareils non identifiés sont également affichés. L'écran inclut l'adresse IP, le nom, l'état, le nœud iSCSI et le nom de partage des périphériques. Le pourcentage d'appareils qui ont été identifiés avec succès est également affiché.



Ajout manuel de périphériques IP

Vous pouvez ajouter manuellement un périphérique IP à Data Infrastructure Insights à l'aide de la fonction d'ajout manuel disponible dans l'écran Identification IP.

Procédure

1. Connectez-vous à l'interface Web de Data Infrastructure Insights .
2. Cliquez sur **Gérer > Résolution de l'appareil**
3. Cliquez sur l'onglet **Identification de l'adresse IP**.

4. Cliquez sur le bouton **Ajouter**.

   La boîte de dialogue Ajouter un périphérique s'affiche

5. Saisissez l'adresse, l'adresse IP et un nom d'appareil unique.

Résultat

L'appareil que vous saisissez est ajouté à la liste des appareils dans l'onglet Identification de l'adresse IP.

Importation de l'identification du périphérique IP à partir d'un fichier .CSV

Vous pouvez importer manuellement les identifications de périphériques IP dans la fonction Résolution de périphérique à l'aide d'une liste d'identifications de périphériques dans un fichier .CSV.

1. Avant de commencer

Vous devez disposer d'un fichier .CSV correctement formaté pour pouvoir importer les identifications des appareils directement dans la fonction Résolution des appareils. Le fichier .CSV pour les périphériques IP nécessite les informations suivantes :

Adresse	propriété intellectuelle	Nom

Les champs de données doivent être placés entre guillemets, comme indiqué dans l'exemple ci-dessous.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

En tant que meilleure pratique, il est recommandé d'exporter d'abord les informations d'identification de l'adresse IP vers un fichier .CSV, d'apporter les modifications souhaitées dans ce fichier, puis de réimporter le fichier dans l'identification de l'adresse IP. Cela garantit que les colonnes attendues sont présentes et dans le bon ordre.

Exportation de l'identification du périphérique IP vers un fichier .CSV

Vous pouvez exporter les identifications de périphériques IP existantes vers un fichier .CSV à partir de la fonctionnalité de résolution de périphérique de Data Infrastructure Insights . Vous souhaiterez peut-être exporter une identification d'appareil afin de pouvoir la modifier, puis la réimporter dans Data Infrastructure Insights où elle sera ensuite utilisée pour identifier les appareils similaires à ceux correspondant à l'origine à l'identification exportée.

À propos de cette tâche

1. Ce scénario peut être utilisé lorsque les appareils ont des attributs similaires qui peuvent être facilement modifiés dans le fichier .CSV, puis réimportés dans le système.

Lorsque vous exportez une identification de périphérique IP vers un fichier .CSV, le fichier contient les informations suivantes dans l'ordre indiqué :

Adresse	propriété intellectuelle	Nom

Procédure

1. Connectez-vous à l'interface Web de Data Infrastructure Insights .
2. Cliquez sur **Gérer > Résolution du périphérique**
3. Sélectionnez l'onglet **Identification de l'adresse IP**.
4. Sélectionnez le ou les périphériques IP dont vous souhaitez exporter l'identification.
5. Cliquez sur *Exporter* bouton.

   Sélectionnez si vous souhaitez ouvrir le fichier .CSV ou enregistrer le fichier.

En rapport:"Résolution du périphérique Fibre Channel" "Création de règles de résolution de périphérique" "Définition des préférences de résolution de l'appareil"

Options de paramétrage dans l'onglet Préférences

L'onglet des préférences de résolution de périphérique vous permet de créer une planification de résolution automatique, de spécifier les fournisseurs de stockage et de bande à inclure ou à exclure de l'identification et de définir les options de recherche DNS.

Planification de résolution automatique

Un programme de résolution automatique peut spécifier quand la résolution automatique du périphérique est exécutée :

Option	Description
Chaque	Utilisez cette option pour exécuter la résolution automatique du périphérique à des intervalles de jours, d'heures ou de minutes.
Tous les jours	Utilisez cette option pour exécuter la résolution automatique de l'appareil quotidiennement à une heure précise.
Manuellement	Utilisez cette option pour exécuter uniquement la résolution automatique du périphérique manuellement.
À chaque changement d'environnement	Utilisez cette option pour exécuter la résolution automatique du périphérique chaque fois qu'un changement se produit dans l'environnement.

Si vous spécifiez *Manuellement*, la résolution automatique nocturne du périphérique est désactivée.

Options de traitement DNS

Les options de traitement DNS vous permettent de sélectionner les fonctionnalités suivantes :

- Lorsque le traitement des résultats de recherche DNS est activé, vous pouvez ajouter une liste de noms DNS à ajouter aux périphériques résolus.
- Vous pouvez sélectionner Résolution automatique des IP : pour activer la résolution automatique de l'hôte pour les initiateurs iSCSI et les hôtes accédant aux partages NFS à l'aide de la recherche DNS. Si cela n'est pas spécifié, seule la résolution basée sur FC est effectuée.

- Vous pouvez choisir d'autoriser les traits de soulignement dans les noms d'hôtes et d'utiliser un alias « connecté à » au lieu de l'alias de port standard dans les résultats.

Inclure ou exclure des fournisseurs spécifiques de stockage et de bandes

Vous pouvez inclure ou exclure des fournisseurs de stockage et de bande spécifiques pour une résolution automatique. Vous souhaiterez peut-être exclure des fournisseurs spécifiques si vous savez, par exemple, qu'un hôte spécifique deviendra un hôte hérité et devra être exclu de votre nouvel environnement. Vous pouvez également rajouter des fournisseurs que vous avez précédemment exclus mais que vous ne souhaitez plus exclure.

> Les règles de résolution de périphérique pour la bande fonctionnent uniquement pour les WWN où le fournisseur de ce WWN est défini sur *Inclus en tant que bande uniquement* dans les préférences des fournisseurs.

Voir aussi :"Exemples d'expressions régulières"

Exemples d'expressions régulières

Si vous avez sélectionné l'approche d'expression régulière comme stratégie de dénomination de source, vous pouvez utiliser les exemples d'expression régulière comme guides pour vos propres expressions utilisées dans les méthodes de résolution automatique de Data Infrastructure Insights .

Formatage des expressions régulières

Lors de la création d'expressions régulières pour la résolution automatique de Data Infrastructure Insights , vous pouvez configurer le format de sortie en saisissant des valeurs dans un champ nommé *FORMAT*.

Le paramètre par défaut est \1, ce qui signifie qu'un nom de zone correspondant à l'expression régulière est remplacé par le contenu de la première variable créée par l'expression régulière. Dans une expression régulière, les valeurs des variables sont créées par des instructions entre parenthèses. Si plusieurs instructions entre parenthèses se produisent, les variables sont référencées numériquement, de gauche à droite. Les variables peuvent être utilisées dans le format de sortie dans n'importe quel ordre. Un texte constant peut également être inséré dans la sortie, en l'ajoutant au champ FORMAT.

Par exemple, vous pouvez avoir les noms de zone suivants pour cette convention de dénomination de zone :

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_Miami_hostname1_filer_FC1
* S14_Tampa_hostname2_switch_FC4
* S3991_Boston_hostname3_windows2K_FC0
* S44_Raleigh_hostname4_solaris_FC1
```

Et vous souhaiterez peut-être que la sortie soit au format suivant :

```
 [hostname]-[data center]-[device type]
Pour ce faire, vous devez capturer les champs nom d'hôte, centre de
données et type de périphérique dans des variables et les utiliser dans la
sortie.  L'expression régulière suivante ferait cela :
```

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Comme il y a trois ensembles de parenthèses, les variables \1, \2 et \3
seraient renseignées.
```

Vous pouvez ensuite utiliser le format suivant pour recevoir une sortie dans votre format préféré :

```
 \2-\1-\3
Votre résultat serait le suivant :
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Les traits d'union entre les variables fournissent un exemple de texte constant qui est inséré dans la sortie formatée.

Exemples

Exemple 1 montrant les noms de zone

Dans cet exemple, vous utilisez l'expression régulière pour extraire un nom d'hôte du nom de zone. Vous pouvez créer une expression régulière si vous avez quelque chose de similaire aux noms de zone suivants :

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

L'expression régulière que vous pourriez utiliser pour capturer le nom d'hôte serait :

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
Le résultat est une correspondance de toutes les zones commençant par S
qui sont suivies de n'importe quelle combinaison de chiffres, suivis d'un
trait de soulignement, du nom d'hôte alphanumérique (myComputer1Name),
d'un trait de soulignement ou d'un trait d'union, des lettres majuscules
HBA et d'un seul chiffre (0-9).  Le nom d'hôte seul est stocké dans la
variable *\1*.
```

L’expression régulière peut être décomposée en ses composants :

- « S » représente le nom de la zone et commence l’expression. Cela correspond uniquement à un « S » au début du nom de la zone.
- Les caractères [0-9] entre parenthèses indiquent que ce qui suit « S » doit être un chiffre compris entre 0 et 9 inclus.
- Le signe + indique que l’occurrence de l’information dans les parenthèses précédentes doit exister 1 ou plusieurs fois.
- Le _ (trait de soulignement) signifie que les chiffres après S doivent être suivis immédiatement par un seul caractère de soulignement dans le nom de la zone. Dans cet exemple, la convention de dénomination de zone utilise le trait de soulignement pour séparer le nom de zone du nom d’hôte.
- Après le trait de soulignement requis, les parenthèses indiquent que le modèle contenu à l’intérieur sera stocké dans la variable \1.
- Les caractères entre crochets [a-zA-Z0-9] indiquent que les caractères correspondants sont tous des lettres (quelle que soit la casse) et des chiffres.
- Le * (astérisque) suivant les parenthèses indique que les caractères entre parenthèses apparaissent 0 fois ou plus.
- Les caractères entre crochets [_-] (trait de soulignement et tiret) indiquent que le motif alphanumérique doit être suivi d’un trait de soulignement ou d’un tiret.
- Les lettres HBA dans l’expression régulière indiquent que cette séquence exacte de caractères doit apparaître dans le nom de la zone.
- L’ensemble final de caractères entre crochets [0-9] correspond à un seul chiffre compris entre 0 et 9 inclus.

Exemple 2

Dans cet exemple, passez au premier trait de soulignement « _ », puis faites correspondre E et tout ce qui suit jusqu’au deuxième « _ », puis ignorez tout ce qui suit.

Zone: Z_E2FHDBS01_E1NETAPP

Nom d’hôte : E2FHDBS01

Expr. régulière : .***?(E.?)***.*?

Exemple 3

Les parenthèses « ( ) » autour de la dernière section de l’expression régulière (ci-dessous) identifient quelle partie est le nom d’hôte. Si vous vouliez que VSAN3 soit le nom d’hôte, ce serait : _([a-zA-Z0-9]).*

Zone : A_VSAN3_SR48KENT_A_CX2578_SPA0

Nom d’hôte : SR48KENT

RegExp : _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

Exemple 4 montrant un modèle de dénomination plus complexe

Vous pouvez créer une expression régulière si vous avez quelque chose de similaire aux noms de zone suivants :

- monNomOrdinateur123-HBA1_Symm1_FA3

- monNomOrdinateur123-HBA2_Symm1_FA5
- monNomOrdinateur123-HBA3_Symm1_FA7

L'expression régulière que vous pourriez utiliser pour les capturer serait :

```
 ([a-zA-Z0-9]*)_.*
La variable \1 ne contiendrait que _myComputerName123_ après avoir été
évaluée par cette expression.
```

L'expression régulière peut être décomposée en ses composants :

- Les parenthèses indiquent que le modèle contenu à l'intérieur sera stocké dans la variable \1.
- Les caractères entre crochets [a-zA-Z0-9] signifient que n'importe quelle lettre (quelle que soit la casse) ou chiffre correspondra.
- Le * (astérisque) suivant les parenthèses indique que les caractères entre parenthèses apparaissent 0 fois ou plus.
- Le caractère _ (trait de soulignement) dans l'expression régulière signifie que le nom de la zone doit avoir un trait de soulignement immédiatement après la chaîne alphanumérique correspondant aux crochets précédents.
- Le . (point) correspond à n'importe quel caractère (un caractère générique).
- L'astérisque * indique que le caractère générique du point précédent peut apparaître 0 fois ou plus.

  En d'autres termes, la combinaison .* indique n'importe quel caractère, n'importe quel nombre de fois.

Exemple 5 montrant des noms de zone sans modèle

Vous pouvez créer une expression régulière si vous avez quelque chose de similaire aux noms de zone suivants :

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

L'expression régulière que vous pourriez utiliser pour les capturer serait :

```
 (.*?)_.*
La variable \1 contiendrait _myComputerName_ (dans le premier exemple de
nom de zone) ou _myComputerName123_ (dans le deuxième exemple de nom de
zone).  Cette expression régulière correspondrait donc à tout ce qui
précède le premier trait de soulignement.
```

L'expression régulière peut être décomposée en ses composants :

- Les parenthèses indiquent que le modèle contenu à l'intérieur sera stocké dans la variable \1.
- Le .* (point astérisque) correspond à n'importe quel caractère, n'importe quel nombre de fois.
- Le * (astérisque) suivant les parenthèses indique que les caractères entre parenthèses apparaissent 0 fois ou plus.

- Le caractère ? rend le match non gourmand. Cela l'oblige à arrêter la correspondance au premier trait de soulignement, plutôt qu'au dernier.
- Les caractères _.* correspondent au premier trait de soulignement trouvé et à tous les caractères qui le suivent.

Exemple 6 montrant des noms d'ordinateurs avec un modèle

Vous pouvez créer une expression régulière si vous avez quelque chose de similaire aux noms de zone suivants :

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

L'expression régulière que vous pourriez utiliser pour les capturer serait :

```
 .*?_.*?_([a-zA-Z0-9]*[ABT])_.*
Étant donné que la convention de dénomination de zone présente davantage
un modèle, nous pourrions utiliser l'expression ci-dessus, qui
correspondra à toutes les instances d'un nom d'hôte (myComputerName dans
l'exemple) qui se termine par un A, un B ou un T, en plaçant ce nom d'hôte
dans la variable \1.
```

L'expression régulière peut être décomposée en ses composants :

- Le .* (point astérisque) correspond à n'importe quel caractère, n'importe quel nombre de fois.
- Le caractère ? rend le match non gourmand. Cela l'oblige à arrêter la correspondance au premier trait de soulignement, plutôt qu'au dernier.
- Le caractère de soulignement correspond au premier trait de soulignement du nom de la zone.
- Ainsi, la première combinaison .*?_ correspond aux caractères Storage1_ dans le premier exemple de nom de zone.
- La deuxième combinaison .*?_ se comporte comme la première, mais correspond à Switch1_ dans le premier exemple de nom de zone.
- Les parenthèses indiquent que le modèle contenu à l'intérieur sera stocké dans la variable \1.
- Les caractères entre crochets [a-zA-Z0-9] signifient que n'importe quelle lettre (quelle que soit la casse) ou chiffre correspondra.
- Le * (astérisque) suivant les parenthèses indique que les caractères entre parenthèses apparaissent 0 fois ou plus.
- Les caractères entre crochets dans l'expression régulière [ABT] correspondent à un seul caractère dans le nom de la zone qui doit être A, B ou T.
- Le _ (trait de soulignement) suivant les parenthèses indique que la correspondance du caractère [ABT] doit être suivie d'un trait de soulignement.
- Le .* (point astérisque) correspond à n'importe quel caractère, n'importe quel nombre de fois.

Le résultat de ceci amènerait donc la variable \1 à contenir n'importe quelle chaîne alphanumérique qui :

- était précédé d'un certain nombre de caractères alphanumériques et de deux traits de soulignement
- était suivi d'un trait de soulignement (puis de n'importe quel nombre de caractères alphanumériques)
- avait un caractère final A, B ou T, avant le troisième trait de soulignement.

Exemple 7

Zone : monNomOrdinateur123_HBA1_Symm1_FA1

Nom d'hôte : monNomOrdinateur123

Expr. régulière : ([a-zA-Z0-9]+)_.*

Exemple 8

Cet exemple trouve tout ce qui se trouve avant le premier _.

Zone : MonOrdinateur_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Nom d'hôte : MyComputerName

Exp régulière : (.**?)_.**

Exemple 9

Cet exemple trouve tout ce qui se trouve après le 1er _ et jusqu'au deuxième _.

Zone : Z_NomDeMonOrdinateur_NomDeStockage

Nom d'hôte : NomMonOrdinateur

Expr. régulière : .***?(.?)***.*?

Exemple 10

Cet exemple extrait « MyComputerName123 » des exemples de zone.

Zone : Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Nom d'hôte : MyComputerName123

RegExp : .**?.?**([a-zA-Z0-9]+)**[ABT]_.**

Exemple 11

Zone : Storage1_Switch1_MyComputerName123A_A1_FC1

Nom d'hôte : MyComputerName123A

RegExp : .**?.?**([a-zA-z0-9]+).*?

Exemple 12

Le ^ (circonflexe ou caret) **à l'intérieur des crochets** nie l'expression, par exemple, [^Ff] signifie tout sauf F majuscule ou minuscule, et [^az] signifie tout sauf les minuscules a à z, et dans le cas ci-dessus, tout sauf le _. L'instruction de format ajoute le « - » au nom de l'hôte de sortie.

Zone: mhs_apps44_d_A_10a0_0429

Nom d'hôte : mhs-apps44-d

RegExp: ()_([AB]).*Format dans Data Infrastructure Insights: \1-\2 ([^_])_ ()_([^_]).*Format dans Data Infrastructure Insights: \1-\2-\3

Exemple 13

Dans cet exemple, l'alias de stockage est délimité par « \" et l'expression doit utiliser « \\" pour définir qu'il y a réellement des « \" utilisés dans la chaîne, et qu'ils ne font pas partie de l'expression elle-même.

Alias de stockage : \Hosts\E2DOC01C1\E2DOC01N1

Nom d'hôte : E2DOC01N1

RegExp: \\.**?\\.**?\\(.*?)

Exemple 14

Cet exemple extrait « PD-RV-W-AD-2 » des exemples de zone.

Zone: PD_D-PD-RV-W-AD-2_01

Nom d'hôte : PD-RV-W-AD-2

Expr. régulière : -(.*-\d).*

Exemple 15

Le paramètre de format dans ce cas ajoute le « US-BV- » au nom d'hôte.

Zone: SRV_USBVM11_F1

Nom d'hôte : US-BV-M11

Expr. régulière : SRV_USBV([A-Za-z0-9]+)_F[12]

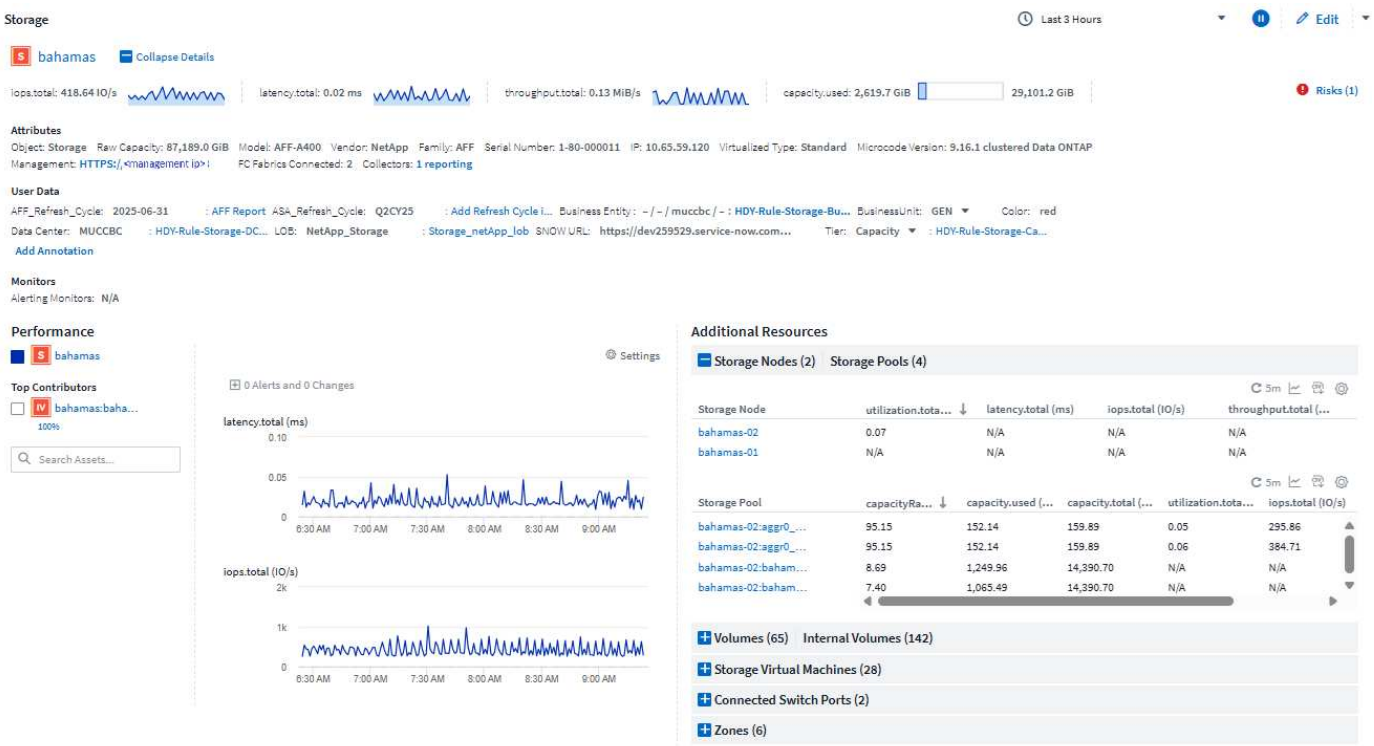
Format : US-BV-\1

Informations sur la page des actifs

Présentation de la page des ressources

Les pages de destination des actifs résument l'état actuel d'un actif et contiennent des liens vers des informations supplémentaires sur l'actif et ses actifs associés.

Les pages de destination vous offrent une vue d'une seule page de l'objet, avec des informations sur le résumé, les performances et les ressources associées.



Section Sommaire

En haut d'une page de destination se trouve la section Résumé extensible, qui comprend plusieurs graphiques sparkline affichant les tendances récentes des données pour des éléments tels que le débit ou la latence, ainsi que les informations et les attributs de l'objet, et tous les moniteurs pouvant alerter pour l'objet.

La section Résumé s'affiche également et vous permet de modifier les annotations attribuées à l'actif.

Section Performance

La section Performances affiche les données de performances de l'objet. Sélectionnez *Paramètres* pour ajouter des graphiques supplémentaires à l'affichage comme Débit ou Capacité, ou sélectionnez des ressources corrélées ou contributives pour représenter leurs données avec celles de l'objet. Les périphériques susceptibles de provoquer des conflits seront également répertoriés dans la section Performances. Les données des graphiques s'actualisent automatiquement à mesure que les collecteurs de données interrogent et que les données mises à jour sont acquises.

Vous pouvez sélectionner lemétrique vous souhaitez afficher le graphique des performances pour la période sélectionnée. Cliquez sur le menu déroulant *Paramètres* et choisissez parmi les mesures répertoriées.

En plus des données de performances, toutes les alertes qui sont ou étaient actives dans la plage horaire de la page sélectionnée seront également affichées.

Vous pouvez choisir parmi les appareils suivants qui peuvent être répertoriés dans la section Performances :

- Corrélation supérieure

  Affiche les actifs qui ont une forte corrélation (pourcentage) avec une ou plusieurs mesures de performance par rapport à l'actif de base.

- Principaux contributeurs

  Affiche les actifs qui contribuent (en pourcentage) à l'actif de base.

- Principaux changements

  Actifs liés aux changements récents.

- Conflits de charge de travail

  Affiche les ressources qui ont un impact ou sont impactées par d'autres ressources partagées, telles que les hôtes, les réseaux et le stockage. On les appelle parfois ressources *gourmandes* et *dégradées*.

Section Ressources supplémentaires

La section Ressources supplémentaires affiche des tableaux de données pour les ressources liées au type d'objet actuel. Vous pouvez développer et réduire ces tableaux afin de vous concentrer sur des ressources spécifiques. Sélectionnez l'icône d'engrenage pour afficher temporairement des mesures ou des attributs supplémentaires dans un tableau.

Ajouter des widgets personnalisés

Vous pouvez ajouter vos propres widgets à n'importe quelle page d'actif. Les widgets que vous ajoutez apparaîtront sur les pages d'actifs pour tous les objets de ce type. Par exemple, l'ajout d'un widget personnalisé à une page de ressource de stockage affichera ce widget sur les pages de ressources pour toutes les ressources de stockage.

Les widgets personnalisés sont placés au bas d'une page de destination, sous les sections Performances et Ressources.

Types de pages d'actifs

Data Infrastructure Insights fournit des pages d'actifs pour les actifs suivants :

- Machine virtuelle
- Machine virtuelle de stockage (SVM)
- Volume
- Volume interne
- Hôte (y compris l'hyperviseur)
- Piscine de stockage
- Stockage
- Magasin de données
- Application
- Nœud de stockage
- Qtree
- Disque
- VMDK
- Port
- Changer
- Tissu
- Hôte
- Zone

Modification de la plage horaire des données affichées

Par défaut, une page d'actif affiche les 3 dernières heures de données ; cependant, vous pouvez modifier le segment temporel des données affichées en utilisant une option située sur chaque page d'actif, quel que soit le type d'actif. Pour modifier la plage horaire, cliquez sur la plage horaire affichée dans la barre supérieure et choisissez parmi les segments horaires suivants :

- Les 15 dernières minutes
- Les 30 dernières minutes
- Les 60 dernières minutes
- Les 2 dernières heures
- 3 dernières heures (c'est la valeur par défaut)
- Les 6 dernières heures
- Les 12 dernières heures
- Dernières 24 heures
- Les 2 derniers jours

- Les 3 derniers jours
- Les 7 derniers jours
- Les 14 derniers jours
- Les 30 derniers jours
- Plage horaire personnalisée

La plage horaire personnalisée vous permet de sélectionner jusqu'à 31 jours consécutifs. Vous pouvez également définir l'heure de début et l'heure de fin de la journée pour cette plage. L'heure de début par défaut est 00h00 le premier jour sélectionné et l'heure de fin par défaut est 23h59 le dernier jour sélectionné. Cliquez sur Appliquer pour appliquer la plage horaire personnalisée à la page de l'actif.

Les informations sur la page s'actualisent automatiquement en fonction de la plage horaire sélectionnée. Le taux de rafraîchissement actuel est affiché dans le coin supérieur droit de la section Résumé ainsi que sur tous les tableaux ou widgets pertinents de la page.

Définitions des mesures de performance

La section Performance peut afficher plusieurs mesures en fonction de la période sélectionnée pour l'actif. Chaque métrique est affichée dans son propre graphique de performances. Vous pouvez ajouter ou supprimer des métriques et des actifs associés des graphiques en fonction des données que vous souhaitez voir ; les métriques parmi lesquelles vous pouvez choisir varient en fonction du type d'actif.

Métrique	Description
Crédit BB zéro Rx, Tx	Nombre de fois où le nombre de crédits de tampon à tampon de réception/transmission est passé à zéro pendant la période d'échantillonnage. Cette mesure représente le nombre de fois où le port connecté a dû arrêter de transmettre parce que ce port n'avait plus de crédits à fournir.
Crédit BB à durée zéro Tx	Durée en millisecondes pendant laquelle le crédit BB de transmission était nul pendant l'intervalle d'échantillonnage.
Taux de réussite du cache (total, lecture, écriture) %	Pourcentage de requêtes aboutissant à des hits dans le cache. Plus le nombre de hits par rapport aux accès au volume est élevé, meilleures sont les performances. Cette colonne est vide pour les baies de stockage qui ne collectent pas d'informations sur les hits de cache.
Utilisation du cache (total) %	Pourcentage total de requêtes de cache aboutissant à des hits de cache
Rejets de classe 3	Nombre de rejets de transport de données Fibre Channel de classe 3.
Utilisation du processeur (total) %	Quantité de ressources CPU activement utilisées, en pourcentage du total disponible (sur tous les CPU virtuels).
Erreur CRC	Nombre de trames avec des contrôles de redondance cyclique (CRC) non valides détectées par le port pendant la période d'échantillonnage

Fréquence d’images	Fréquence d’images transmise en images par seconde (FPS)
Taille moyenne de la trame (Rx, Tx)	Rapport entre le trafic et la taille de la trame. Cette mesure vous permet d’identifier s’il existe des trames en surplomb dans la structure.
Taille du cadre trop longue	Nombre de trames de transmission de données Fibre Channel trop longues.
Taille du cadre trop courte	Nombre de trames de transmission de données Fibre Channel trop courtes.
Densité d’E/S (totale, lecture, écriture)	Nombre d’IOPS divisé par la capacité utilisée (telle qu’acquise à partir de l’inventaire le plus récent de la source de données) pour l’élément Volume, Volume interne ou Stockage. Mesuré en nombre d’opérations d’E/S par seconde par To.
IOPS (total, lecture, écriture)	Nombre de demandes de service d’E/S en lecture/écriture passant par le canal d’E/S ou une partie de ce canal par unité de temps (mesuré en E/S par seconde)
Débit IP (total, lecture, écriture)	Total : débit agrégé auquel les données IP ont été transmises et reçues en mégaoctets par seconde.
Lire : Débit IP (réception) :	Débit moyen auquel les données IP ont été reçues en mégaoctets par seconde.
Écriture : Débit IP (transmission) :	Débit moyen auquel les données IP ont été transmises en mégaoctets par seconde.
Latence (totale, lecture, écriture)	Latence (R&W) : taux auquel les données sont lues ou écrites sur les machines virtuelles dans un laps de temps fixe. La valeur est mesurée en mégaoctets par seconde.
Latence:	Temps de réponse moyen des machines virtuelles dans un magasin de données.
Latence maximale :	Le temps de réponse le plus élevé des machines virtuelles dans un magasin de données.
Échec de la liaison	Nombre de défaillances de liaison détectées par le port pendant la période d’échantillonnage.
Réinitialisation du lien Rx, Tx	Nombre de réinitialisations de liaison de réception ou de transmission pendant la période d’échantillonnage. Cette métrique représente le nombre de réinitialisations de lien émises par le port connecté à ce port.
Utilisation de la mémoire (totale) %	Seuil pour la mémoire utilisée par l’hôte.

R/W partiel (total) %	Nombre total de fois qu'une opération de lecture/écriture franchit une limite de bande sur n'importe quel module de disque dans un LUN RAID 5, RAID 1/0 ou RAID 0. En général, les croisements de bande ne sont pas bénéfiques, car chacun nécessite une E/S supplémentaire. Un faible pourcentage indique une taille d'élément de bande efficace et indique un alignement incorrect d'un volume (ou d'un LUN NetApp). Pour CLARiiON, cette valeur correspond au nombre de croisements de bandes divisé par le nombre total d'IOPS.
Erreurs de port	Rapport des erreurs de port sur la période d'échantillonnage/la durée donnée.
Nombre de pertes de signal	Nombre d'erreurs de perte de signal. Si une erreur de perte de signal se produit, il n'y a pas de connexion électrique et un problème physique existe.
Taux de swap (taux total, taux d'entrée, taux de sortie)	Taux auquel la mémoire est échangée vers l'intérieur, vers l'extérieur ou les deux du disque vers la mémoire active pendant la période d'échantillonnage. Ce compteur s'applique aux machines virtuelles.
Nombre de pertes de synchronisation	Nombre d'erreurs de perte de synchronisation. Si une erreur de perte de synchronisation se produit, le matériel ne peut pas comprendre le trafic ni s'y verrouiller. Il se peut que tous les équipements n'utilisent pas le même débit de données, ou que les connexions optiques ou physiques soient de mauvaise qualité. Le port doit se resynchroniser après chaque erreur de ce type, ce qui affecte les performances du système. Mesuré en Ko/sec.
Débit (total, lecture, écriture)	Débit auquel les données sont transmises, reçues ou les deux dans un laps de temps fixe en réponse aux demandes de service d'E/S (mesuré en Mo par seconde).
Délai d'expiration des trames de rejet - Tx	Nombre de trames de transmission rejetées en raison d'un dépassement de délai.
Taux de trafic (total, lecture, écriture)	Trafic transmis, reçu ou les deux reçus pendant la période d'échantillonnage, en mébioctets par seconde.
Utilisation du trafic (total, lecture, écriture)	Rapport entre le trafic reçu/transmis/total et la capacité reçue/transmise/totale, pendant la période d'échantillonnage.
Utilisation (totale, lecture, écriture) %	Pourcentage de bande passante disponible utilisée pour la transmission (Tx) et la réception (Rx).
Écriture en attente (total)	Nombre de demandes de service d'E/S d'écriture en attente.

Filtrage des objets en contexte

Lors de la configuration d'un widget sur la page de destination d'un actif, vous pouvez définir des filtres *in-context* pour afficher uniquement les objets directement liés à l'actif actuel. Par défaut, lorsque vous ajoutez un widget, *tous* les objets du type sélectionné sur votre locataire sont affichés. Les filtres contextuels vous permettent d'afficher uniquement les données pertinentes pour votre actif actuel.

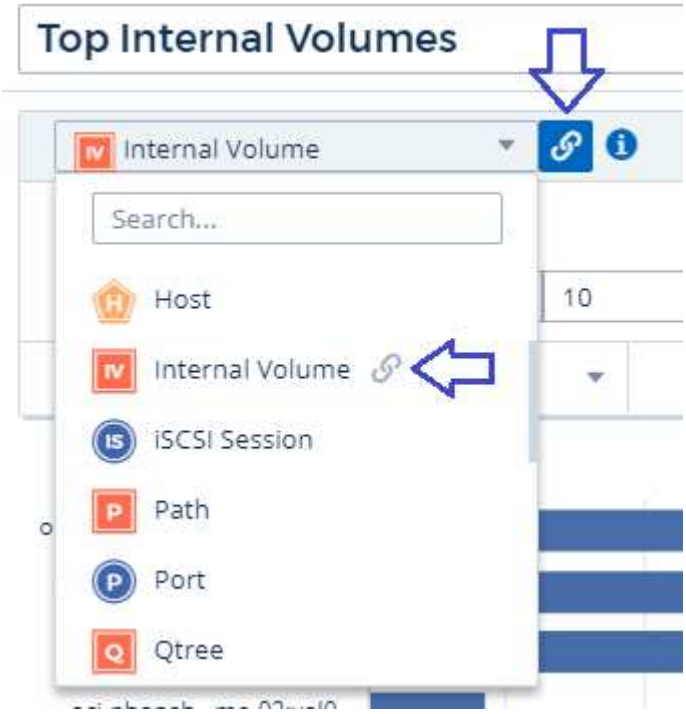
Sur la plupart des pages de destination des ressources, les widgets vous permettent de filtrer les objets liés à la ressource actuelle. Dans les listes déroulantes de filtre, les types d'objets qui affichent une icône de lien peuvent être filtrés dans le contexte de l'actif actuel.

Par exemple, sur une page d'actif de stockage, vous pouvez ajouter un widget de graphique à barres pour afficher les IOPS les plus élevées sur les volumes internes uniquement sur ce stockage. Par défaut, lorsque vous ajoutez un widget, *tous* les volumes internes de votre locataire sont affichés.

Pour afficher uniquement les volumes internes sur la ressource de stockage actuelle, procédez comme suit :

Étapes

1. Ouvrez une page d'actif pour n'importe quel actif **Stockage**.
2. Cliquez sur **Modifier** pour ouvrir la page de l'actif en mode Édition.
3. Cliquez sur **Ajouter un widget** et sélectionnez *Graphique à barres*.
4. Sélectionnez **Volume interne** comme type d'objet à afficher sur le graphique à barres. Notez que le type d'objet de volume interne possède une icône de lien à côté de lui. L'icône « lié » est activée par défaut.



5. Choisissez *IOPS - Total* et définissez les filtres supplémentaires que vous souhaitez.
6. Réduisez le champ **Roll Up** en cliquant sur le [X] à côté de celui-ci. Le champ **Afficher** s'affiche.
7. Choisissez d'afficher le Top 10.

8. Enregistrez le widget.

   Le graphique à barres affiche uniquement les volumes internes qui résident sur la ressource de stockage actuelle.

Le widget sera affiché sur les pages d'actifs pour tous les objets de stockage. Lorsque le lien contextuel est activé dans le widget, le graphique à barres affiche les données des volumes internes liés uniquement à la ressource de stockage actuellement affichée.

Pour dissocier les données de l'objet, modifiez le widget et cliquez sur l'icône de lien à côté du type d'objet. Le lien est désactivé et le graphique affiche les données de *tous* les objets de votre locataire.

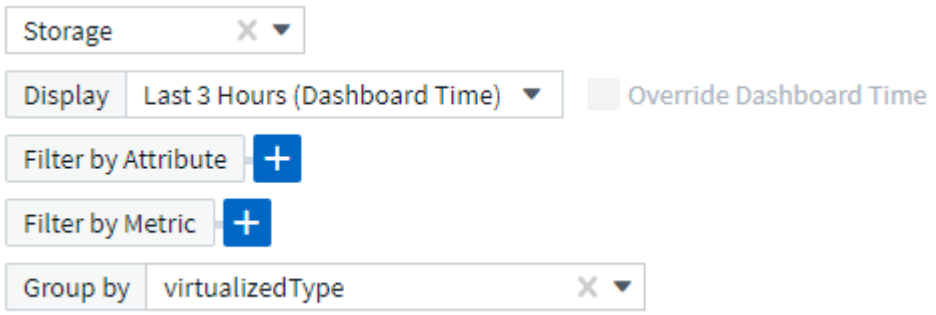
Vous pouvez également utiliser**"variables spéciales dans les widgets"** pour afficher des informations relatives aux actifs sur les pages de destination.

Virtualisation du stockage

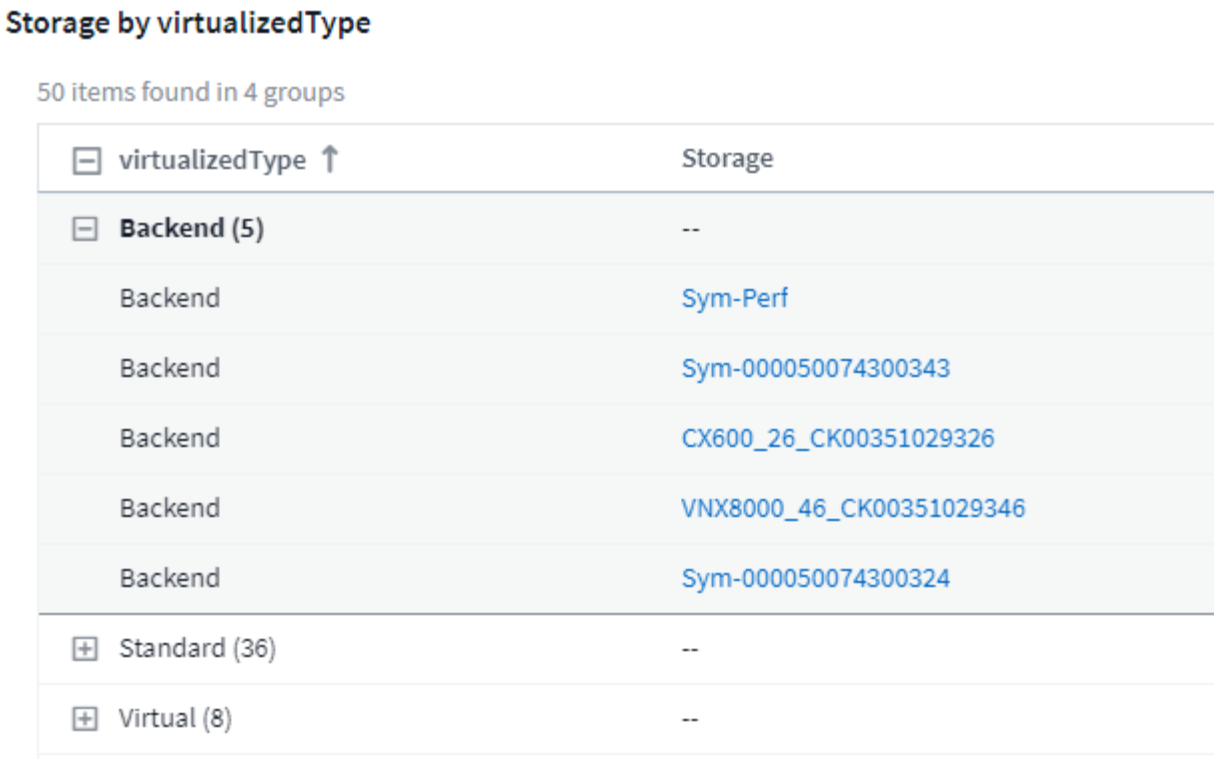
Data Infrastructure Insights peut faire la différence entre une baie de stockage disposant d'un stockage local ou d'une virtualisation d'autres baies de stockage. Cela vous donne la possibilité de relier les coûts et de distinguer les performances du front-end jusqu'au back-end de votre infrastructure.

Virtualisation dans un widget de table

L'un des moyens les plus simples de commencer à examiner votre virtualisation de stockage est de créer un widget de tableau de bord affichant le type virtualisé. Lors de la création de la requête pour le widget, ajoutez simplement « virtualizedType » à votre regroupement ou filtre.

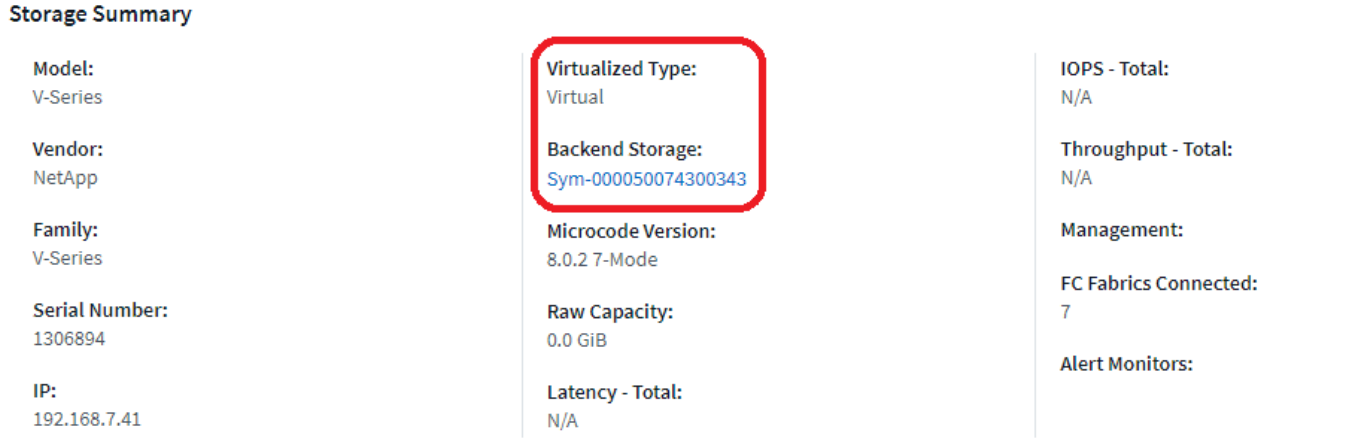


Le widget de tableau résultant vous montre les stockages *Standard*, *Backend* et *Virtual* sur votre locataire.



Les pages de destination affichent des informations virtualisées

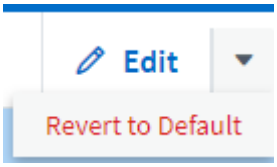
Sur une page de destination de stockage, de volume, de volume interne ou de disque, vous pouvez voir les informations de virtualisation pertinentes. Par exemple, en regardant la page de destination de stockage ci-dessous, vous pouvez voir qu'il s'agit d'un stockage virtuel et quel système de stockage backend s'applique. Tous les tableaux pertinents sur les pages de destination afficheront également des informations de virtualisation, le cas échéant.



Pages de destination et tableaux de bord existants

Sachez que si vous disposez actuellement de pages de destination ou de tableaux de bord personnalisés sur votre locataire, ceux-ci n'afficheront pas automatiquement toutes les informations de virtualisation par défaut. Cependant, vous pouvez *revenir aux valeurs par défaut* de n'importe quel tableau de bord ou page de destination personnalisé (vous devrez réimplémenter vos personnalisations) ou modifier les widgets concernés pour inclure les attributs ou les mesures de virtualisation souhaités.

Revenir à la valeur par défaut est disponible dans le coin supérieur droit d'un tableau de bord personnalisé ou d'un écran de page de destination.



Conseils et astuces pour rechercher des actifs et des alertes

Plusieurs techniques de recherche peuvent être utilisées pour rechercher des données ou des objets dans votre environnement surveillé.

- **Recherche générique**

  Vous pouvez effectuer une recherche avec plusieurs caractères génériques à l'aide du caractère *. Par exemple, *applic*n* renverrait *application*.

- **Phrases utilisées dans la recherche**

  Une phrase est un groupe de mots entourés de guillemets doubles ; par exemple, « VNX LUN 5 ». Vous pouvez utiliser des guillemets doubles pour rechercher des documents contenant des espaces dans leurs noms ou leurs attributs.

- **Opérateurs booléens**

  En utilisant les opérateurs booléens OU, ET et NON, vous pouvez combiner plusieurs termes pour former une requête plus complexe.

  OU

  L'opérateur OR est l'opérateur de conjonction par défaut.

  S'il n'y a pas d'opérateur booléen entre deux termes, l'opérateur OU est utilisé.

  L'opérateur OR relie deux termes et trouve un document correspondant si l'un des termes existe dans un document.

  Par exemple, *storage OR netapp* recherche les documents qui contiennent *storage* ou *netapp*.

  Des notes élevées sont attribuées aux documents qui correspondent à la plupart des termes.

  ET

  Vous pouvez utiliser l'opérateur AND pour rechercher des documents dans lesquels les deux termes de recherche existent dans un seul document. Par exemple, *storage AND netapp* recherche les documents qui contiennent à la fois *storage* et *netapp*.

  Vous pouvez utiliser le symbole **&&** à la place du mot AND.

  PAS

  Lorsque vous utilisez l'opérateur NOT, tous les documents contenant le terme après NOT sont exclus des résultats de la recherche. Par exemple, *storage NOT netapp* recherche les documents qui contiennent

uniquement *storage* et non *netapp*.

Vous pouvez utiliser le symbole **!** à la place du mot NOT.

La recherche n’est pas sensible à la casse.

Rechercher à l’aide de termes indexés

Les recherches qui correspondent à davantage de termes indexés génèrent des scores plus élevés.

La chaîne de recherche est divisée en termes de recherche distincts par un espace. Par exemple, la chaîne de recherche « storage aurora netapp » est divisée en trois mots-clés : « storage », « aurora » et « netapp ». La recherche est effectuée en utilisant les trois termes. Les documents qui correspondent à la plupart de ces termes auront le score le plus élevé. Plus vous fournissez d’informations, meilleurs seront les résultats de recherche. Par exemple, vous pouvez rechercher un stockage par son nom et son modèle.

L’interface utilisateur affiche les résultats de la recherche par catégories, avec les trois premiers résultats par catégorie. Si vous n’avez pas trouvé l’objet que vous attendiez, vous pouvez inclure plus de termes dans la chaîne de recherche pour améliorer les résultats de la recherche.

Le tableau suivant fournit une liste de termes indexés qui peuvent être ajoutés à la chaîne de recherche.

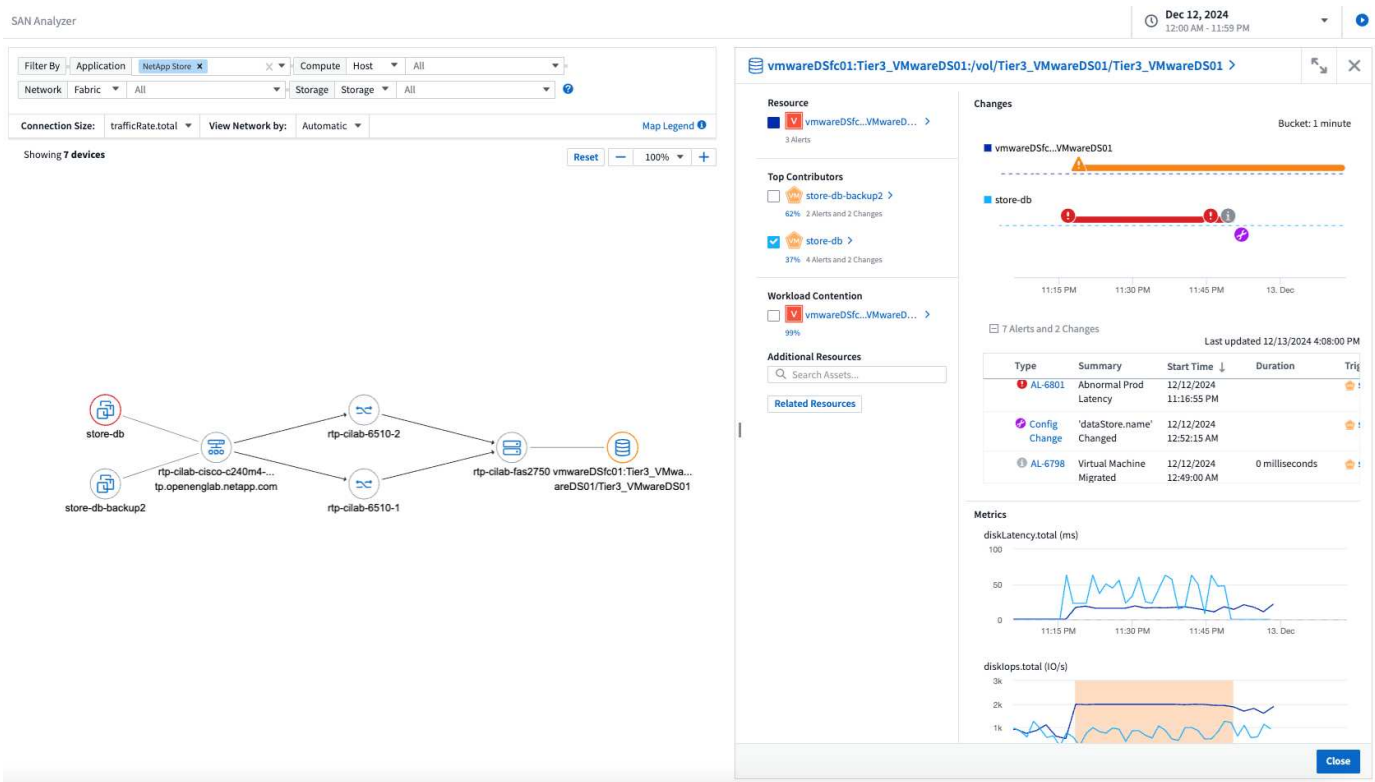
Catégorie	Termes indexés
Stockage	modèle de fournisseur de nom de « stockage »
Pool de stockage	nom du pool de stockage nom du stockage adresses IP du stockage numéro de série du stockage fournisseur de stockage modèle de stockage noms de tous les volumes internes associés noms de tous les disques associés
Volume interne	"internalvolume" nom nom du stockage adresses IP du stockage numéro de série du stockage fournisseur de stockage modèle de stockage nom du pool de stockage noms de tous les partages associés noms de toutes les applications associées
Volume	nom de « volume » nom de l’étiquette noms de tous les volumes internes nom du pool de stockage nom du stockage adresses IP du stockage numéro de série du stockage fournisseur de stockage modèle de stockage
Nœud de stockage	"storagenode" nom nom du stockage adresses IP du stockage numéro de série du stockage fournisseur de stockage modèle de stockage
Hôte	nom d'« hôte » adresses IP noms de toutes les applications associées
Magasin de données	nom du « datastore » nom du centre virtuel noms IP de tous les volumes noms de tous les volumes internes

Catégorie	Termes indexés
Machines virtuelles	nom de « machine virtuelle » nom DNS adresses IP nom de l'hôte adresses IP de l'hôte noms de tous les magasins de données noms de toutes les applications associées
Commutateurs (réguliers et NPV)	"switch" adresse IP nom wwn numéro de série modèle identifiant de domaine nom de la structure wwn de la structure
Application	« application » nom locataire secteur d'activité unité commerciale projet
Ruban adhésif	"bande" adresse IP nom numéro de série fournisseur
Port	nom WWN « port »
Tissu	nom wwn « tissu »
Machine virtuelle de stockage (SVM)	UUID du nom « storagevirtualmachine »

Analyse des données

Présentation de SAN Analyzer

Le SAN joue un rôle crucial dans la gestion des charges de travail vitales, mais sa complexité peut entraîner des pannes importantes et des perturbations pour les clients. Avec **SAN Analyzer** de DII, la gestion du SAN devient plus simple et plus efficace. Cet outil puissant offre une visibilité de bout en bout, mappant les dépendances de la VM/hôte au réseau, au LUN et au stockage. En fournissant une carte topologique interactive, SAN Analyzer vous permet d'identifier les problèmes, de comprendre les changements et d'améliorer la compréhension du flux de données. Optimisez la gestion SAN dans les environnements informatiques complexes avec SAN Analyzer et augmentez votre visibilité sur les charges de travail en bloc.



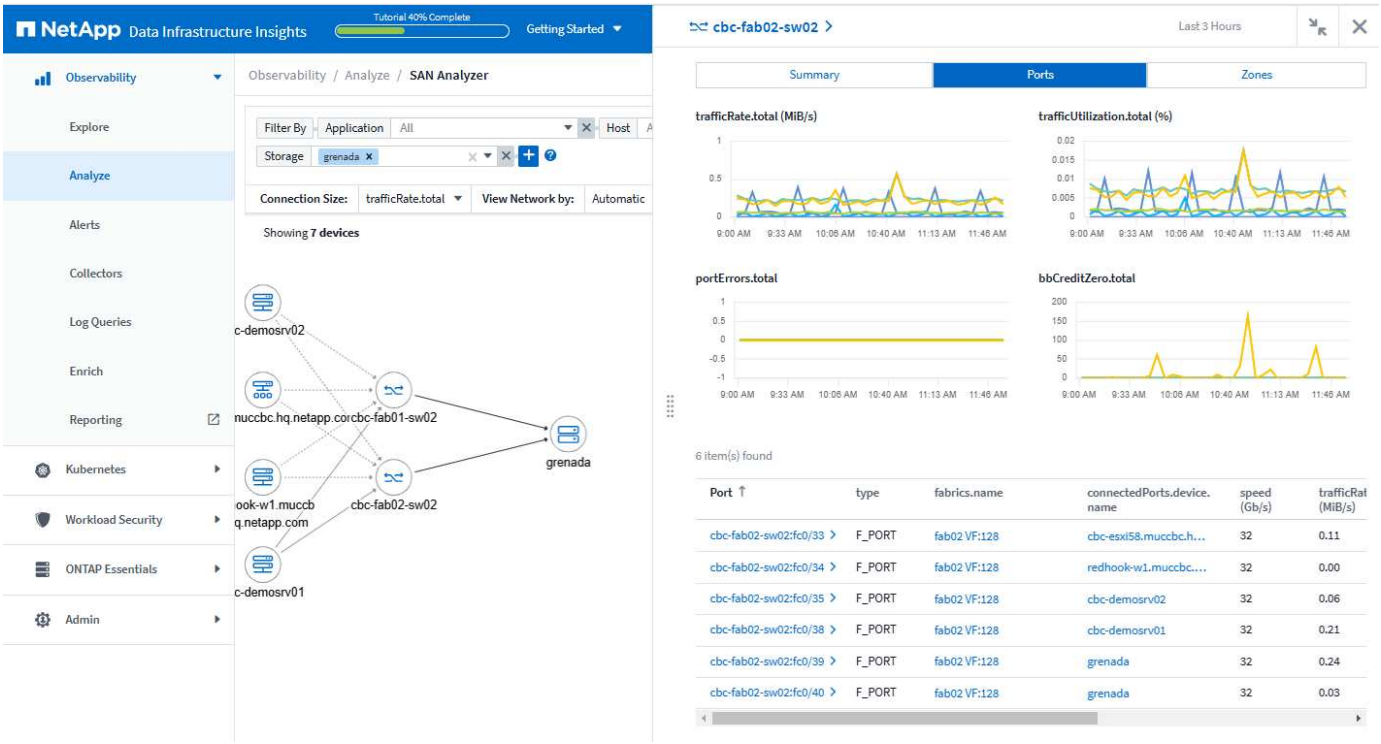
Explorez les connexions entre vos actifs

Sélectionnez **Observabilité > Analyser > Analyseur SAN** pour afficher l'analyseur SAN. Définissez un filtre pour l'application, l'hôte, la structure et/ou le stockage. La carte des objets s'affiche, montrant les objets connectés. Passez la souris sur un objet pour afficher les mesures de trafic pour ces connexions.

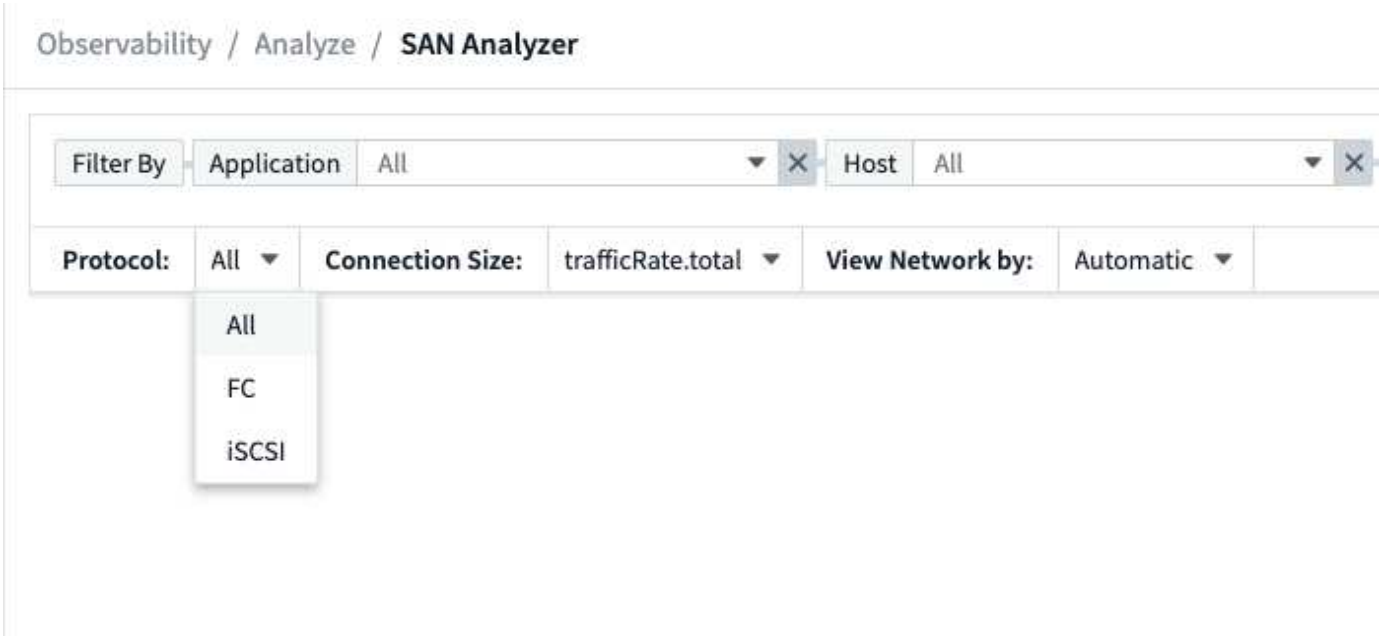
> La plupart des filtres SAN Analyzer (y compris ceux que vous pouvez ajouter) sont contextuels ; lorsque vous sélectionnez un objet dans l'un de ces filtres, les choix présentés dans les autres listes déroulantes de filtres sont actualisés en fonction de l'objet ou des objets sélectionnés. Les seules exceptions à cette règle sont Application, Port et Switch ; ces filtres ne sont pas contextuels.

Cliquer sur un objet ou un groupe ouvre un panneau coulissant fournissant des détails supplémentaires sur l'objet et ses connexions. Le panneau coulissant affiche un résumé, qui fournit des détails sur l'objet sélectionné (par exemple, IP, hyperviseur, Connected Fabrics, etc., selon le type d'objet), ainsi que des graphiques affichant des métriques pour l'objet telles que la latence ou les IOPS, et les modifications et alertes si nécessaire. Vous pouvez également choisir d'afficher les mesures des objets les plus corrélés sur les graphiques, si vous le souhaitez.

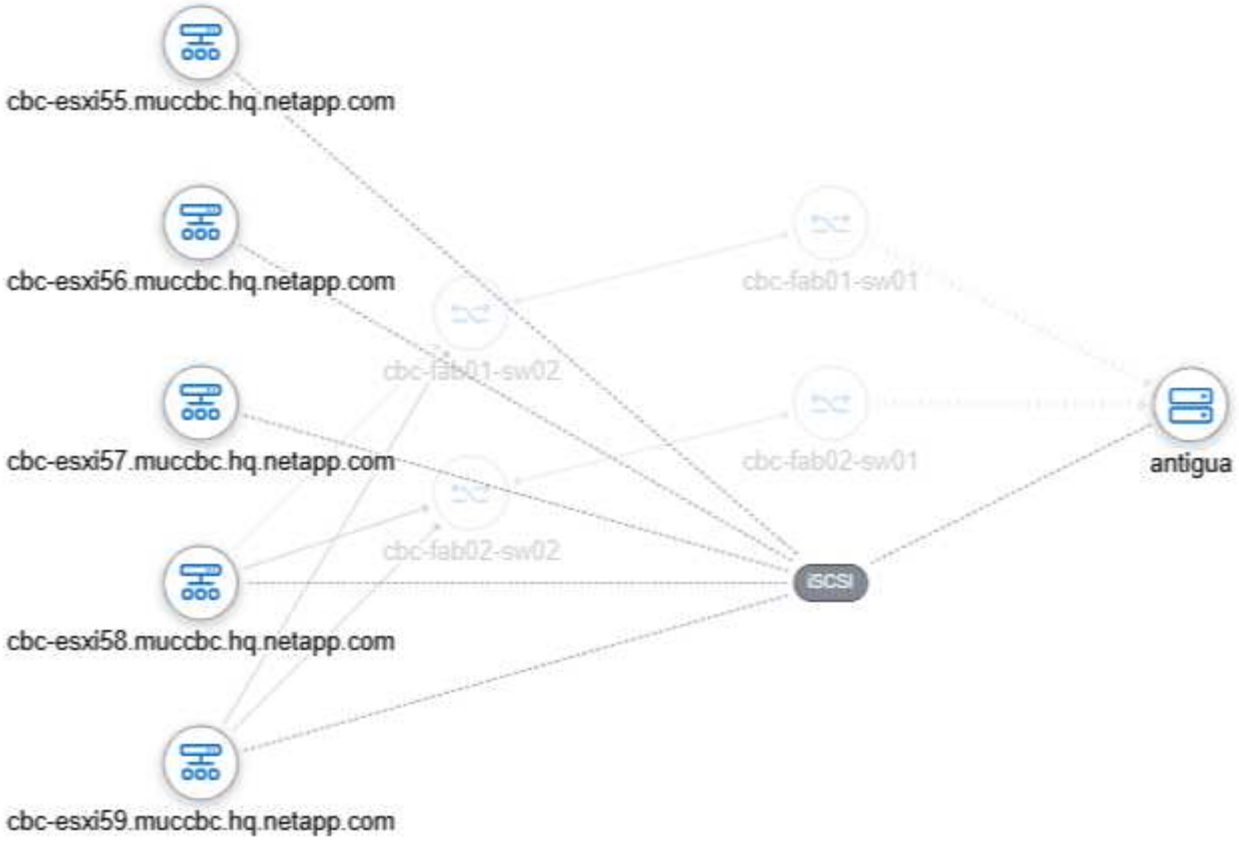
En plus de l'onglet Résumé, le panneau coulissant affiche des onglets pour des éléments tels que les détails du port ou les informations de zone, selon l'objet choisi.



Si votre environnement possède des protocoles différents, vous pouvez filtrer par iSCSI ou FC :



Si votre environnement inclut des périphériques iSCSI, le survol de l'objet *iSCSI* met en évidence les connexions liées à ces périphériques iSCSI concernés.



Conseils de dépannage

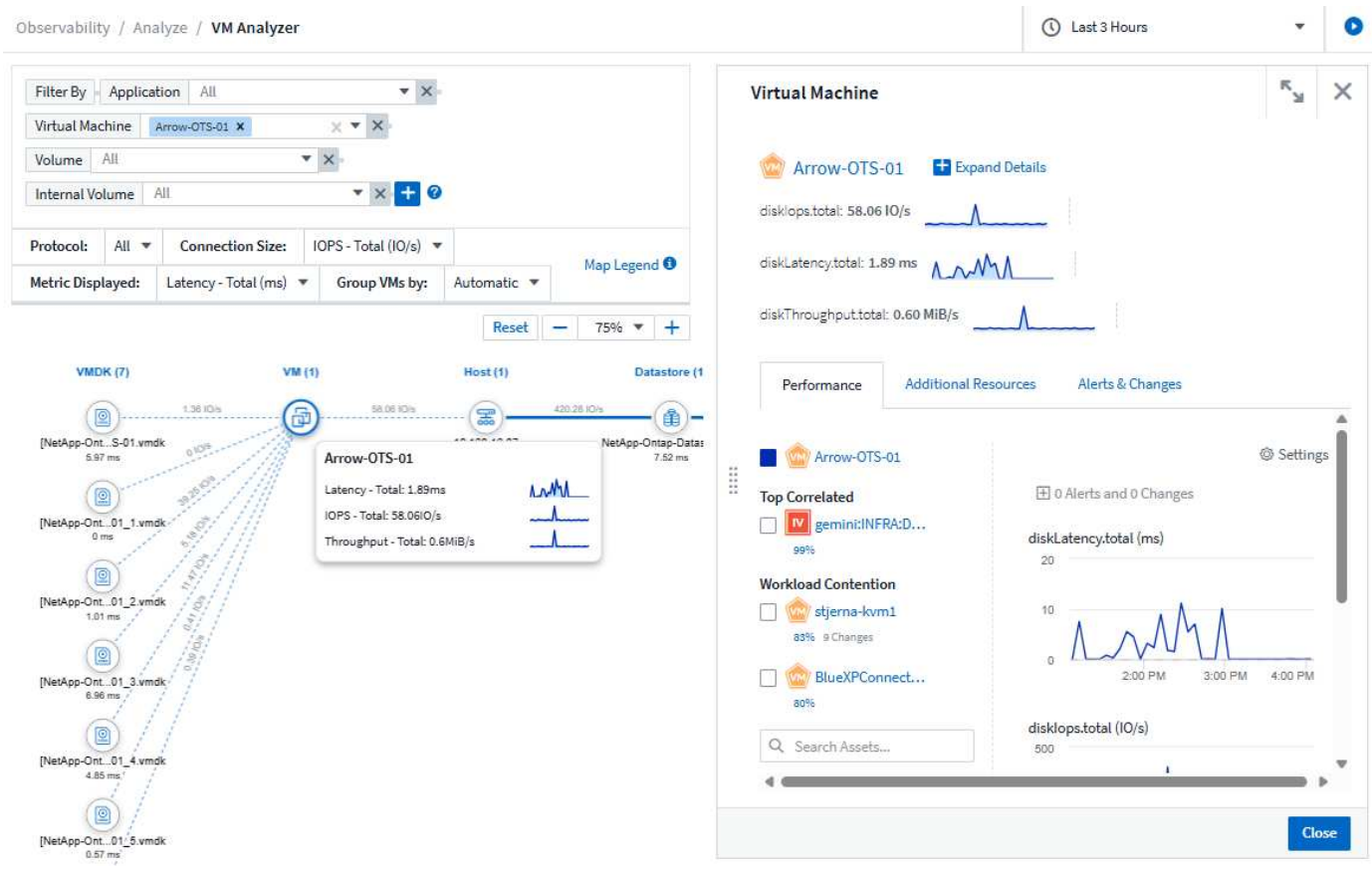
Quelques solutions à essayer si vous rencontrez des problèmes :

Problème:	Essayez ceci :
Je vois <0, =0 ou >0 dans la légende pour des métriques telles que *trafficUtilization* ou *trafficRate*.	Cela peut se produire dans de très rares cas où les valeurs métriques sont inférieures à deux décimales, comme 0,000123. L'élargissement de la fenêtre temporelle pourrait aider à analyser la métrique plus efficacement.

Présentation de VM Analyzer

Avec **VM Analyzer** de DII, la gestion de vos actifs virtuels devient plus simple et plus efficace. Cet outil puissant offre une visibilité de bout en bout, mappant les dépendances de VMDK/VM à l'hôte, au magasin de données, au volume interne/volume au stockage.

En fournissant une carte topologique interactive, VM Analyzer vous permet d'identifier les problèmes, de comprendre les changements et d'améliorer la compréhension du flux de données. Rationalisez la gestion des machines virtuelles et augmentez votre visibilité sur les charges de travail virtuelles.



Explorez les connexions entre vos actifs

Sélectionnez **Observabilité > Analyser > Analyseur de VM** pour afficher l'analyseur de VM. Définissez un filtre pour l'application, la machine virtuelle, le volume, le volume interne ou ajoutez vos propres filtres. La carte des objets s'affiche, montrant les objets connectés. Passez la souris sur un objet pour afficher les mesures de trafic pour ces connexions.

La plupart des filtres VM Analyzer (y compris ceux que vous pouvez ajouter) sont contextuels ; lorsque vous sélectionnez un objet dans l'un de ces filtres, les choix présentés dans les autres listes déroulantes de filtres sont actualisés en contexte avec l'objet ou les objets sélectionnés.

Cliquer sur un objet ou un groupe ouvre un panneau coulissant fournissant des détails supplémentaires sur l'objet et ses connexions. Le panneau coulissant affiche un résumé, qui fournit des détails sur l'objet sélectionné (par exemple, le débit ou l'utilisation, selon le type d'objet), et des graphiques affichant des métriques pour l'objet telles que la latence ou les IOPS. Des onglets supplémentaires vous permettent d'explorer des ressources supplémentaires ou des modifications et des alertes associées. Vous pouvez

également choisir d'afficher les mesures des objets les plus corrélés ou les plus concurrents sur les graphiques, si vous le souhaitez.

Voyez-le en action

Dépannage simplifié avec VM Analyzer (vidéo), window=read-later

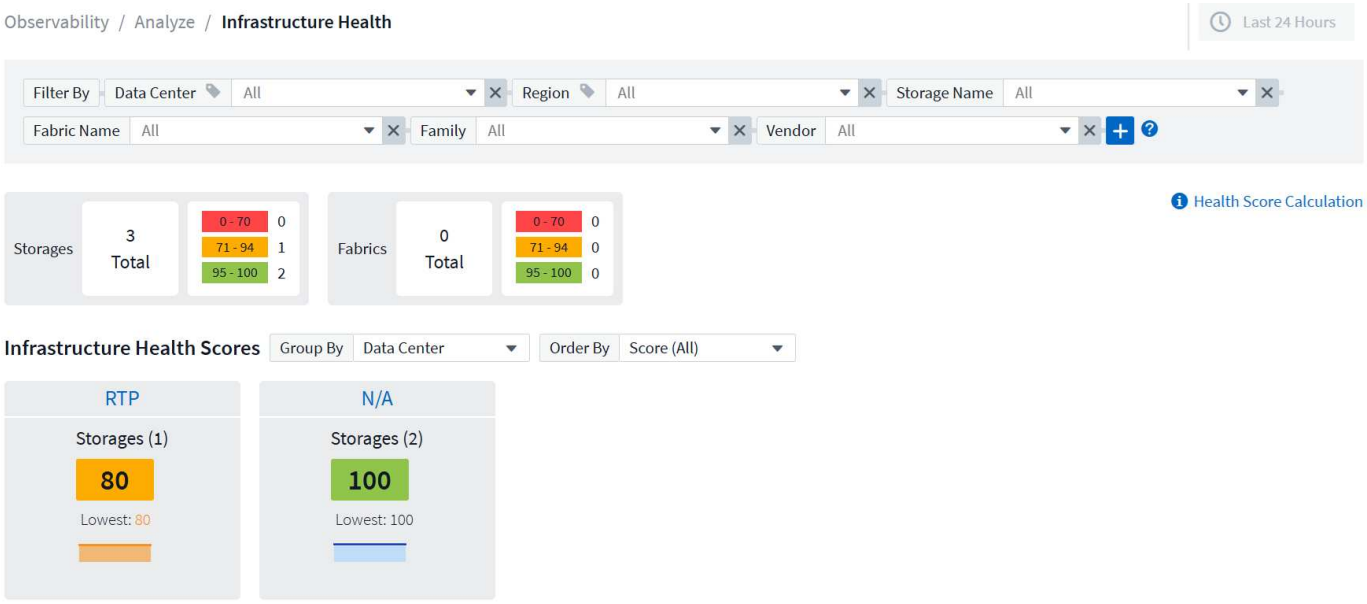
Surveiller la santé de l'infrastructure

Data Infrastructure Insights fournit une surveillance complète de l'état de l'infrastructure qui suit les performances, la capacité, la configuration et l'état des composants de votre environnement de stockage. Les scores de santé sont calculés en fonction des alertes de surveillance dans ces catégories, vous offrant une vue unifiée de la santé du système et permettant une résolution proactive des problèmes.

Le tableau de bord de l'état de santé des infrastructures

La surveillance de la santé des infrastructures est une"Aperçu" fonctionnalité et est sujette à changement.

Accédez à **Observabilité > Analyser** et sélectionnez **Santé de l'infrastructure**. Le tableau de bord fournit un aperçu de l'état de votre système, en fonction des catégories d'alertes et des scores du moniteur, comme expliqué ci-dessous. Définissez des filtres en haut pour affiner le champ de votre enquête.



Par défaut, les scores de santé sont regroupés par centre de données ; vous pouvez sélectionner le regroupement qui convient le mieux à votre session.

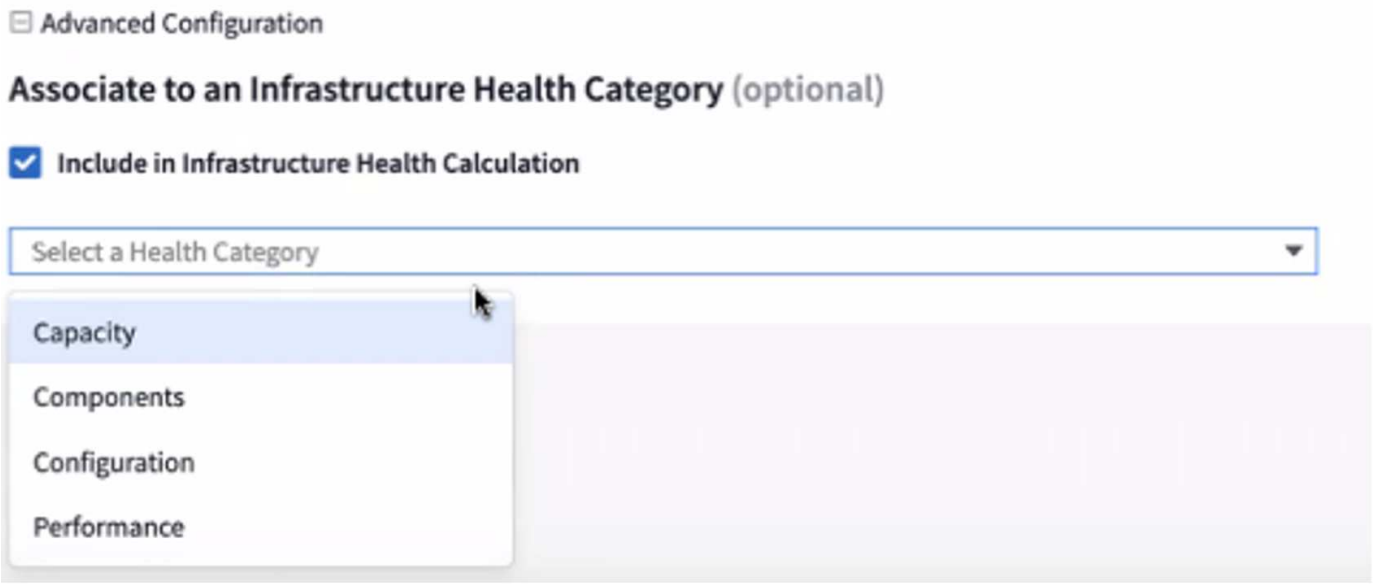
Configurer les moniteurs à utiliser pour la santé de l'infrastructure

Les scores de santé sont déterminés par des alertes configurées pour être incluses dans les calculs de santé du système.

Lors de la création d'un moniteur pour un objet d'infrastructure, vous pouvez choisir d'inclure ou non les alertes du moniteur dans les calculs. Au bas de l'écran, développez la Configuration avancée et sélectionnez *Inclure*

dans le calcul de l'état de l'infrastructure. Sélectionnez une catégorie à laquelle appliquer le calcul pour le moniteur :

- **Santé des composants** - panne de ventilateur, processeur de service hors ligne, etc.
- **Santé des performances** - utilisation élevée des nœuds de stockage, pic anormal de latence des nœuds, etc.
- **Capacité Santé** - La capacité du pool de stockage approche de sa pleine capacité, espace insuffisant pour l'instantané LUN, etc.
- **Santé de la configuration** - niveau cloud inaccessible, relation SnapMirror désynchronisée, etc.



Les scores de santé expliqués

Les scores sont présentés sur une échelle de 0 à 100, 100 correspondant à une santé complète. Les objets d'infrastructure surveillés qui rencontrent actuellement ou récemment des problèmes réduiront ce score en fonction des moyennes pondérées suivantes :

- Composants, performances ou capacité : 30 % chacun
- Configuration : 10%

Les scores de santé sont affectés par les alertes générées par les moniteurs que vous avez configurés pour être inclus dans les calculs de santé de l'infrastructure des manières suivantes :

- Les alertes critiques réduisent le score de santé du poids de la catégorie *complète*
- Les alertes d'avertissement réduisent le score de *la moitié* du poids de la catégorie.

Si certaines catégories ne sont pas déclarées, la moyenne pondérée sera ajustée en conséquence.

Par exemple : 1 alerte critique sur les composants (-30) et 1 alerte d'avertissement sur les performances (50 % de 30 = -15) donnent un score de santé de 55 (100 moins 45).

Lorsque les alertes sont résolues, ces réductions de score de santé s'estompent progressivement et le score se rétablit complètement dans les 2 heures.

Rapports

Présentation des rapports sur Data Infrastructure Insights

Le reporting Data Infrastructure Insights est un outil de veille économique qui vous permet d'afficher des rapports prédéfinis ou de créer des rapports personnalisés.

La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" . La disponibilité de la fonctionnalité de reporting est soumise à une exigence d'empreinte minimale. "Contactez votre représentant commercial NetApp" pour plus d'informations.

Avec les rapports Data Infrastructure Insights, vous pouvez effectuer les tâches suivantes :

- Exécuter un rapport prédéfini
- Créer un rapport personnalisé
- Personnaliser le format et le mode de livraison d'un rapport
- Planifier l'exécution automatique des rapports
- Rapports par courrier électronique
- Utiliser des couleurs pour représenter les seuils sur les données

Data Infrastructure Insights Reporting peut générer des rapports personnalisés pour des domaines tels que la rétrofacturation, l'analyse de la consommation et les prévisions, et peut aider à répondre à des questions telles que les suivantes :

- Quel est mon inventaire?
- Où est mon inventaire?
- Qui utilise nos actifs ?
- Quelle est la rétrofacturation pour le stockage alloué à une unité commerciale ?
- Combien de temps faudra-t-il avant que j'aie besoin d'acquérir une capacité de stockage supplémentaire ?
- Les unités commerciales sont-elles alignées sur les niveaux de stockage appropriés ?
- Comment l'allocation de stockage évolue-t-elle au cours d'un mois, d'un trimestre ou d'une année ?

Accès aux rapports d' Data Infrastructure Insights

Vous pouvez accéder aux rapports Data Infrastructure Insights en cliquant sur le lien **Rapports** dans le menu.

Vous serez redirigé vers l'interface de rapport. Data Infrastructure Insights utilise IBM Cognos Analytics pour son moteur de reporting.

Qu'est-ce que ETL ?

Lorsque vous travaillez avec des rapports, vous entendrez les termes « Data Warehouse » et « ETL ». ETL signifie « Extraire, Transformer et Charger ». Le processus ETL récupère les données collectées dans Data Infrastructure Insights et transforme les données dans un format à utiliser dans les rapports. « Entrepôt de données » fait référence aux données collectées disponibles pour le reporting.

Le processus ETL comprend ces processus individuels :

- **Extrait** : Extrait des données de Data Infrastructure Insights.
- **Transformer** : applique des règles ou des fonctions de logique métier aux données telles qu'elles sont extraites de Data Infrastructure Insights.
- **Charger** : enregistre les données transformées dans l'entrepôt de données pour les utiliser dans les rapports.

Rôles des utilisateurs des rapports sur Data Infrastructure Insights

Si vous disposez de Data Infrastructure Insights Premium Edition avec Reporting, chaque utilisateur de Data Infrastructure Insights sur votre locataire dispose également d'une connexion Single Sign-On (SSO) à l'application Reporting (c'est-à-dire Cognos). Cliquez simplement sur le lien **Rapports** dans le menu et vous serez automatiquement connecté aux rapports.

Votre rôle d'utilisateur dans Data Infrastructure Insights détermine votre rôle d'utilisateur Reporting :

Rôle de Data Infrastructure Insights	Rôle de reporting	Autorisations de signalement
Invité	Consommateur	Peut afficher, planifier et exécuter des rapports et définir des préférences personnelles telles que celles concernant les langues et les fuseaux horaires. Les consommateurs ne peuvent pas créer de rapports ni effectuer de tâches administratives.
Utilisateur	Auteur	Peut exécuter toutes les fonctions du consommateur ainsi que créer et gérer des rapports et des tableaux de bord.
Administrateur	Administrateur	Peut exécuter toutes les fonctions d'auteur ainsi que toutes les tâches administratives telles que la configuration des rapports et l'arrêt et le redémarrage des tâches de reporting.

Le tableau suivant présente les fonctions disponibles pour chaque rôle de reporting.

Fonctionnalité	Consommateur	Auteur	Administrateur
Afficher les rapports dans l'onglet Contenu de l'équipe	Oui	Oui	Oui
Exécuter des rapports	Oui	Oui	Oui
Rapports de planification	Oui	Oui	Oui
Télécharger des fichiers externes	Non	Oui	Oui

Créer des emplois	Non	Oui	Oui
Créer des histoires	Non	Oui	Oui
Créer des rapports	Non	Oui	Oui
Créer des packages et des modules de données	Non	Oui	Oui
Effectuer des tâches administratives	Non	Non	Oui
Ajouter/modifier un élément HTML	Non	Non	Oui
Exécuter un rapport avec un élément HTML	Oui	Oui	Oui
Ajouter/Modifier SQL personnalisé	Non	Non	Oui
Exécuter des rapports avec SQL personnalisé	Oui	Oui	Oui

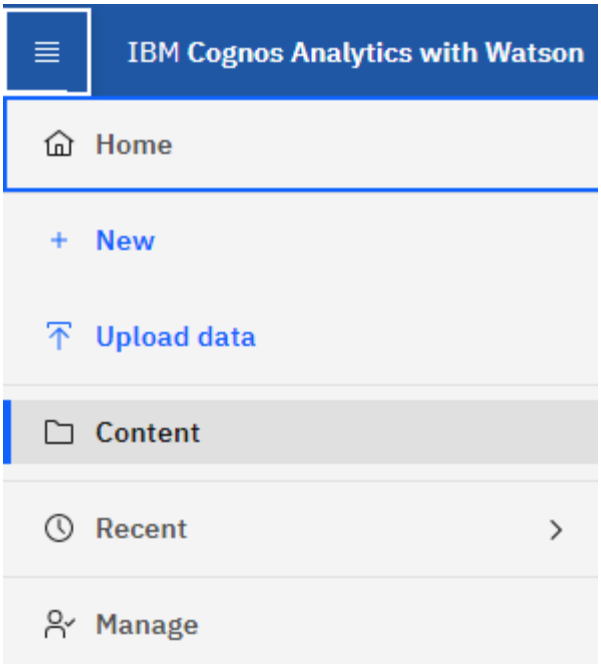
Définition des préférences de courrier électronique pour les rapports (Cognos)

Si vous modifiez vos préférences de messagerie utilisateur dans Data Infrastructure Insights Reporting (c'est-à-dire l'application Cognos), ces préférences sont actives *uniquement pour la session en cours*. La déconnexion et la reconnexion de Cognos réinitialiseront vos préférences de messagerie.

Quelles étapes dois-je suivre pour préparer mon environnement existant à l'activation de SSO ?

Pour garantir la conservation de vos rapports, migrez tous les rapports de *Mon contenu* vers *Contenu d'équipe* en suivant les étapes suivantes. Vous devez effectuer cette opération avant d'activer l'authentification unique sur votre locataire :

1. Accédez à **Menu > Contenu**



1. Créer un nouveau dossier dans ***Team Content***
   a. Si plusieurs utilisateurs ont été créés, veuillez créer un dossier distinct pour chaque utilisateur afin d'éviter d'écraser les rapports avec des noms en double.
2. Accédez à *Mon contenu*
3. Sélectionnez tous les rapports que vous souhaitez conserver.
4. Dans le coin supérieur droit du menu, sélectionnez « Copier ou déplacer »
5. Accédez au dossier nouvellement créé dans *Team Content*
6. Collez les rapports dans le dossier nouvellement créé à l'aide des boutons « Copier vers » ou « Déplacer vers »
7. Une fois SSO activé pour Cognos, connectez-vous à Data Infrastructure Insights avec l'adresse e-mail utilisée pour créer votre compte.
8. Accédez au dossier *Team Content* dans Cognos et copiez ou déplacez les rapports précédemment enregistrés vers *Mon contenu*.

Rapports prédéfinis simplifiés

Data Infrastructure Insights Reporting inclut des rapports prédéfinis qui répondent à un certain nombre d'exigences de reporting courantes, fournissant des informations essentielles dont les parties prenantes ont besoin pour prendre des décisions éclairées concernant leur infrastructure de stockage.

La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" .

Vous pouvez générer des rapports prédéfinis à partir du portail de création de rapports Data Infrastructure Insights , les envoyer par courrier électronique à d'autres utilisateurs et même les modifier. Plusieurs rapports vous permettent de filtrer par appareil, entité commerciale ou niveau. Les outils de reporting utilisent IBM Cognos comme base et vous offrent de nombreuses options de présentation des données.

Les rapports prédéfinis affichent votre inventaire, votre capacité de stockage, vos rétrofacturations, vos

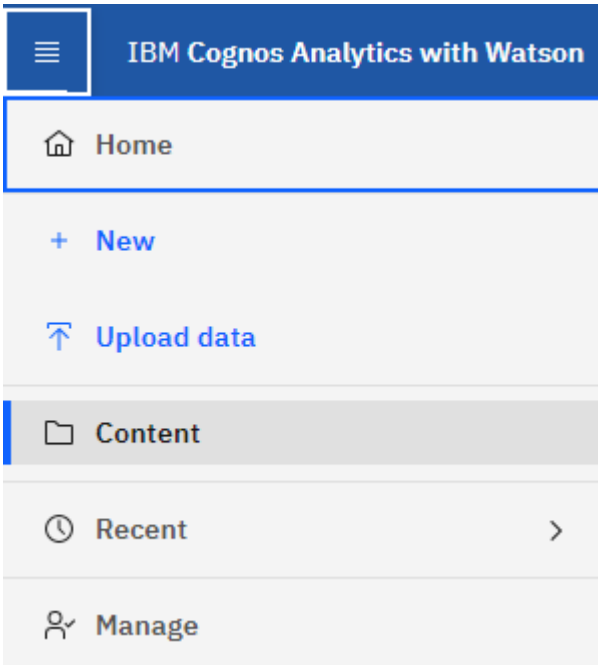
performances, votre efficacité de stockage et vos données de coût du cloud. Vous pouvez modifier ces rapports prédéfinis et enregistrer vos modifications.

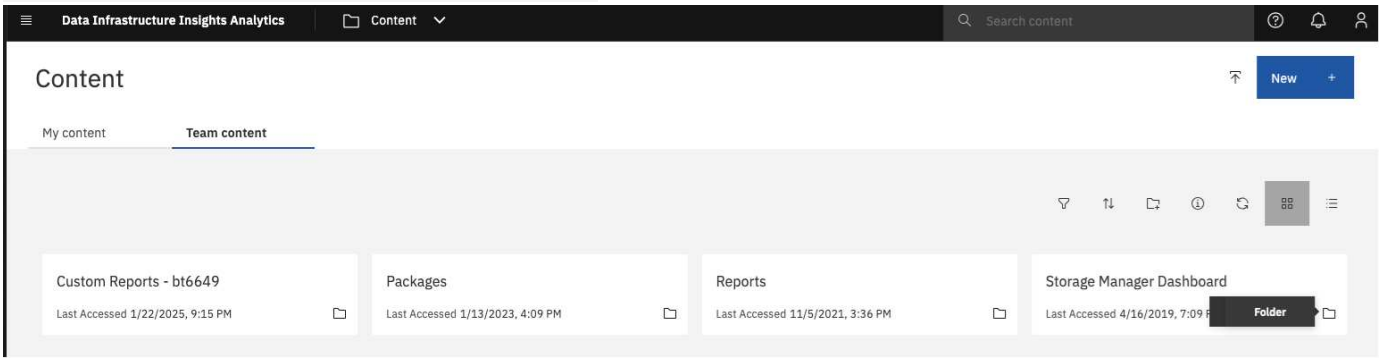
Vous pouvez générer des rapports dans différents formats, notamment HTML, PDF, CSV, XML et Excel.

Accéder aux rapports prédéfinis

Lorsque vous ouvrez le portail de rapports, le dossier *Team Content* est le point de départ pour sélectionner le type d'informations dont vous avez besoin dans les rapports Data Infrastructure Insights .

1. Dans le volet de navigation de gauche, sélectionnez **Contenu > Contenu de l'équipe**.
2. Sélectionnez **Rapports** pour accéder aux rapports prédéfinis.





Utiliser des rapports prédéfinis pour répondre aux questions courantes

Les rapports prédéfinis suivants sont disponibles dans **Contenu de l'équipe > Rapports**.

Capacité et performances du niveau de service des applications

Le rapport Capacité et performances du niveau de service des applications fournit un aperçu de haut niveau de vos applications. Vous pouvez utiliser ces informations pour la planification de la capacité ou pour un plan de migration.

Rétrofacturation

Le rapport de rétrofacturation fournit des informations sur la rétrofacturation et la responsabilité de la capacité de stockage par hôtes, applications et entités commerciales, et inclut des données actuelles et historiques.

Pour éviter le double comptage, n'incluez pas les serveurs ESX, surveillez uniquement les machines virtuelles.

Sources de données

Le rapport Sources de données affiche toutes les sources de données installées sur votre site, l'état de la source de données (succès/échec) et les messages d'état. Le rapport fournit des informations sur la manière de commencer à résoudre les problèmes liés aux sources de données. Les sources de données défaillantes ont un impact sur la précision des rapports et sur la convivialité générale du produit.

Performances ESX vs VM

Le rapport Performances ESX vs VM fournit une comparaison des serveurs et des machines virtuelles ESX, indiquant les IOP moyens et de pointe, le débit, la latence et les utilisations des serveurs et des machines virtuelles ESX. Pour éviter le double comptage, excluez les serveurs ESX ; incluez uniquement les machines virtuelles. Une version mise à jour de ce rapport est disponible sur le NetApp Storage Automation Store.

Résumé du tissu

Le rapport récapitulatif de la structure identifie les commutateurs et les informations sur les commutateurs, notamment le nombre de ports, les versions du micrologiciel et l'état de la licence. Le rapport n'inclut pas les ports de commutation NPV.

HBA hôtes

Le rapport HBA hôtes fournit une vue d'ensemble des hôtes de l'environnement et indique le fournisseur, le modèle et la version du micrologiciel des HBA, ainsi que le niveau du micrologiciel des commutateurs auxquels ils sont connectés. Ce rapport peut être utilisé pour analyser la compatibilité du micrologiciel lors de la planification d'une mise à niveau du micrologiciel pour un commutateur ou un HBA.

Capacité et performances du niveau de service de l'hôte

Le rapport Capacité et performances du niveau de service de l'hôte fournit un aperçu de l'utilisation du stockage par hôte pour les applications en mode bloc uniquement.

Résumé de l'hôte

Le rapport récapitulatif de l'hôte fournit un aperçu de l'utilisation du stockage par chaque hôte sélectionné avec des informations pour les hôtes Fibre Channel et iSCSI. Le rapport vous permet de comparer les ports et les chemins, la capacité Fibre Channel et ISCSI, ainsi que le nombre de violations.

Détails de la licence

Le rapport Détails de la licence indique la quantité de ressources pour lesquelles vous disposez d'une licence sur tous les sites disposant de licences actives. Le rapport montre également une somme de la quantité réelle sur tous les sites avec des licences actives. La sommation peut inclure des chevauchements de baies de stockage gérées par plusieurs serveurs.

Volumes cartographiés mais non masqués

Le rapport Volumes mappés mais non masqués répertorie les volumes dont le numéro d'unité logique (LUN) a été mappé pour être utilisé par un hôte particulier, mais n'est pas masqué pour cet hôte. Dans certains cas, il

peut s’agir de LUN mis hors service qui ont été démasqués. Les volumes non masqués sont accessibles par n’importe quel hôte, ce qui les rend vulnérables à la corruption des données.

Capacité et performances de NetApp

Le rapport Capacité et performances NetApp fournit des données globales sur la capacité allouée, utilisée et engagée avec des données de tendance et de performances pour la capacité NetApp .

Tableau de bord

Le rapport Scorecard fournit un résumé et un état général de tous les actifs acquis par Data Infrastructure Insights. Le statut est indiqué par des drapeaux verts, jaunes et rouges :

- Le vert indique un état normal
- Le jaune indique un problème potentiel dans l’environnement
- Le rouge indique un problème qui nécessite une attention particulière

Tous les champs du rapport sont décrits dans le dictionnaire de données fourni avec le rapport.

Résumé du stockage

Le rapport Résumé du stockage fournit un résumé global des données de capacité utilisées et inutilisées pour les pools de stockage bruts, alloués et les volumes. Ce rapport fournit un aperçu de tout le stockage découvert.

Capacité et performances des machines virtuelles

Décrit l’environnement de la machine virtuelle (VM) et son utilisation de la capacité. Les outils VM doivent être activés pour afficher certaines données, par exemple lorsque les VM ont été mises hors tension.

Chemins de VM

Le rapport Chemins d’accès VM fournit des données sur la capacité du magasin de données et des mesures de performances pour savoir quelle machine virtuelle s’exécute sur quel hôte, quels hôtes accèdent à quels volumes partagés, quel est le chemin d’accès actif et ce qui comprend l’allocation et l’utilisation de la capacité.

Capacité HDS par Thin Pool

Le rapport Capacité HDS par pool mince indique la quantité de capacité utilisable sur un pool de stockage provisionné de manière dynamique.

Capacité NetApp par agrégat

Le rapport NetApp Capacity by Aggregate affiche l’espace total brut, total, utilisé, disponible et engagé des agrégats.

Capacité Symmetrix par réseau épais

Le rapport Capacité Symmetrix par réseau épais affiche la capacité brute, la capacité utilisable, la capacité libre, la capacité mappée, masquée et la capacité libre totale.

Capacité Symmetrix par Thin Pool

Le rapport Capacité Symmetrix par Thin Pool affiche la capacité brute, la capacité utilisable, la capacité utilisée, la capacité libre, le pourcentage utilisé, la capacité souscrite et le taux d’abonnement.

XIV Capacité par baie

Le rapport XIV Capacité par baie affiche la capacité utilisée et inutilisée de la baie.

XIV Capacité par piscine

Le rapport XIV Capacité par pool affiche la capacité utilisée et inutilisée des pools de stockage.

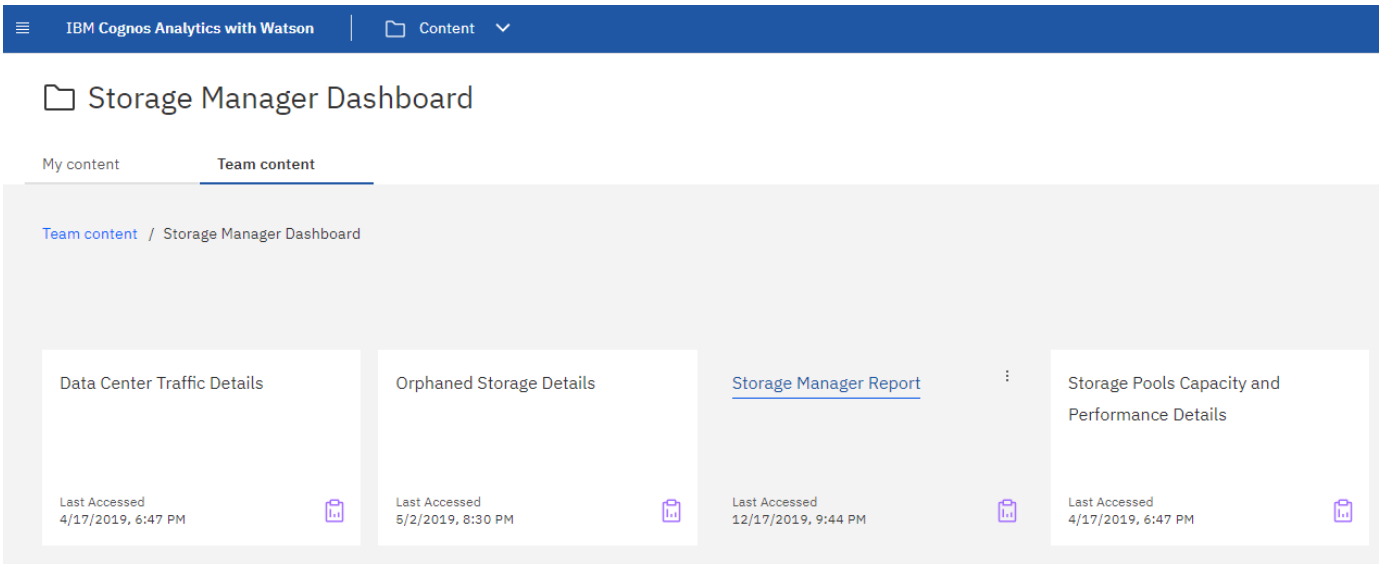
Tableau de bord du gestionnaire de stockage

Le tableau de bord du gestionnaire de stockage vous fournit une visualisation centralisée qui vous permet de comparer et de contraster l'utilisation des ressources au fil du temps par rapport aux plages acceptables et aux jours d'activité précédents. En affichant uniquement les indicateurs de performance clés de vos services de stockage, vous pouvez prendre des décisions sur la manière de maintenir vos centres de données.

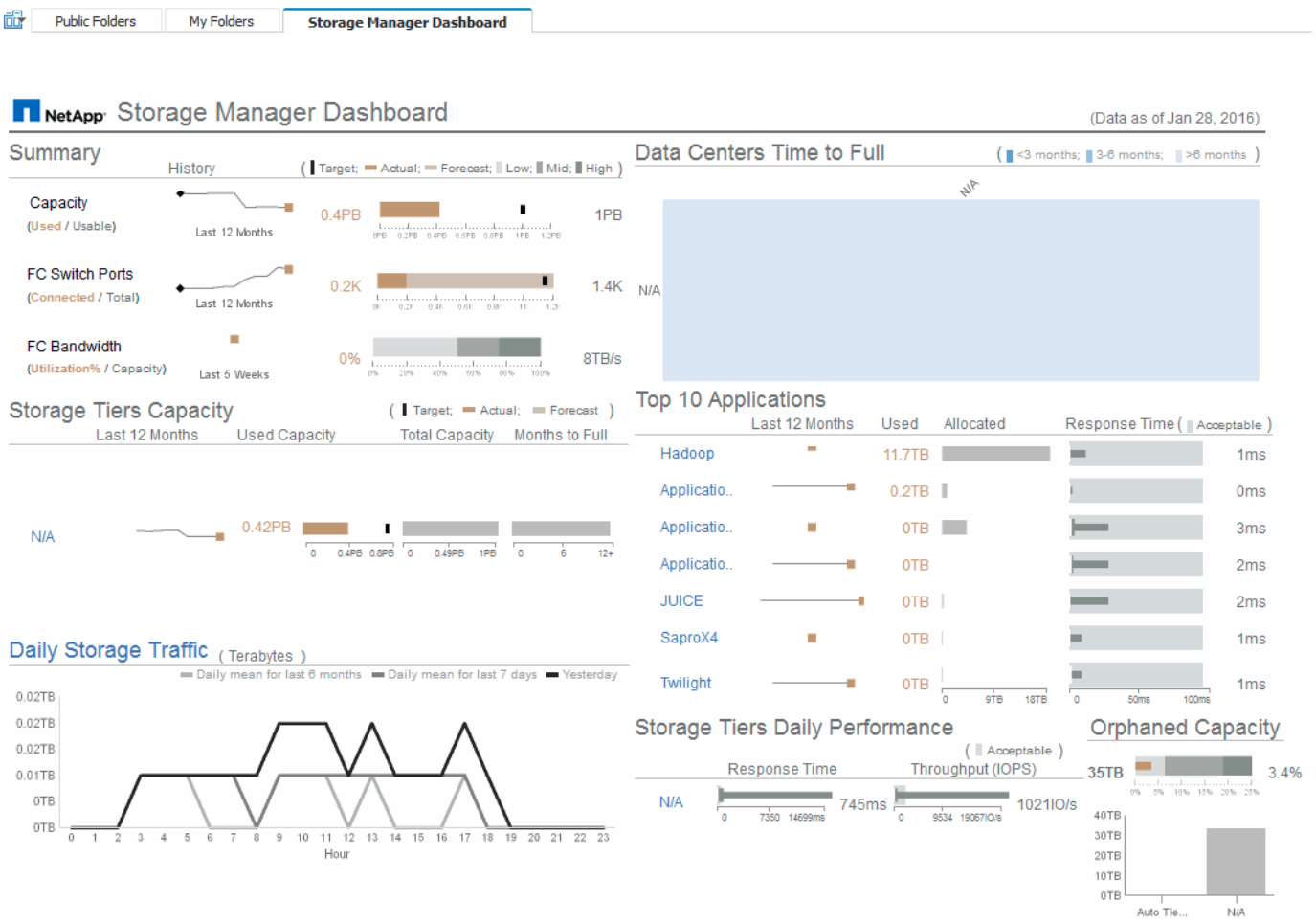
La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" .

Résumé

La sélection de **Tableau de bord du gestionnaire de stockage** dans le contenu de l'équipe vous fournit plusieurs rapports qui fournissent des informations sur votre trafic et votre stockage.



Pour une vue d'ensemble, le **Rapport du gestionnaire de stockage** comprend sept composants qui contiennent des informations contextuelles sur de nombreux aspects de votre environnement de stockage. Vous pouvez approfondir les aspects de vos services de stockage pour effectuer une analyse approfondie d'une section qui vous intéresse le plus.



Ce composant affiche la capacité de stockage utilisée par rapport à la capacité utilisable, le nombre total de ports de commutateur par rapport au nombre de ports de commutateur connectés et l'utilisation totale des ports de commutateur connectés par rapport à la bande passante totale, ainsi que l'évolution de chacun de ces éléments au fil du temps. Vous pouvez visualiser l'utilisation réelle par rapport aux plages basse, moyenne et haute, ce qui vous permet de comparer et de contraster l'utilisation entre les projections et vos valeurs réelles souhaitées, en fonction d'un objectif. Pour la capacité et les ports de commutation, vous pouvez configurer cette cible. La prévision est basée sur une extrapolation du taux de croissance actuel et de la date que vous avez définie. Lorsque la capacité utilisée prévue, basée sur la date de projection d'utilisation future, dépasse la cible, une alerte (cercle rouge continu) apparaît à côté de Capacité.

Capacité des niveaux de stockage

Ce composant affiche la capacité du niveau utilisée par rapport à la capacité allouée au niveau, ce qui indique comment la capacité utilisée augmente ou diminue sur une période de 12 mois et combien de mois restent avant la pleine capacité. L'utilisation de la capacité est affichée avec des valeurs fournies pour l'utilisation réelle, la prévision d'utilisation et un objectif de capacité, que vous pouvez configurer. Lorsque la capacité utilisée prévue, basée sur la date de projection d'utilisation future, dépasse la capacité cible, une alerte (cercle rouge continu) apparaît à côté d'un niveau.

Vous pouvez cliquer sur n'importe quel niveau pour afficher le rapport Détails de la capacité et des performances des pools de stockage, qui indique les capacités libres et utilisées, le nombre de jours avant le remplissage et les détails des performances (IOPS et temps de réponse) pour tous les pools du niveau sélectionné. Vous pouvez également cliquer sur n'importe quel nom de stockage ou de pool de stockage dans ce rapport pour afficher la page d'actif résumant l'état actuel de cette ressource.

Trafic de stockage quotidien

Ce composant montre les performances de l'environnement, s'il y a une croissance importante, des changements ou des problèmes potentiels par rapport aux six mois précédents. Il montre également le trafic moyen par rapport au trafic des sept jours précédents et du jour précédent. Vous pouvez visualiser toutes les anomalies dans la façon dont l'infrastructure fonctionne, car elle fournit des informations qui mettent en évidence les variations cycliques (sept jours précédents) et saisonnières (six mois précédents).

Vous pouvez cliquer sur le titre (Trafic de stockage quotidien) pour afficher le rapport Détails du trafic de stockage, qui affiche la carte thermique du trafic de stockage horaire pour le jour précédent pour chaque système de stockage. Cliquez sur n'importe quel nom de stockage dans ce rapport pour afficher la page d'actif résumant l'état actuel de cette ressource.

Les centres de données sont sur le point d'être saturés

Ce composant affiche tous les centres de données par rapport à tous les niveaux et la capacité restante dans chaque centre de données pour chaque niveau de stockage en fonction des taux de croissance prévus. Le niveau de capacité du niveau est indiqué en bleu ; plus la couleur est foncée, moins il reste de temps au niveau de l'emplacement avant d'être plein.

Vous pouvez cliquer sur une section d'un niveau pour afficher le rapport Détails des jours avant remplissage des pools de stockage, qui indique la capacité totale, la capacité libre et le nombre de jours avant remplissage de tous les pools du niveau sélectionné et du centre de données. Cliquez sur n'importe quel nom de stockage ou de pool de stockage dans ce rapport pour afficher la page d'actif résumant l'état actuel de cette ressource.

Top 10 des applications

Ce composant affiche les 10 principales applications en fonction de la capacité utilisée. Quelle que soit la manière dont le niveau organise les données, cette zone affiche la capacité actuellement utilisée et la part de l'infrastructure. Vous pouvez visualiser la gamme d'expériences utilisateur au cours des sept jours précédents pour voir si les consommateurs bénéficient de temps de réponse acceptables (ou, plus important encore, inacceptables).

Cette zone affiche également les tendances, qui indiquent si les applications atteignent leurs objectifs de niveau de service de performance (SLO). Vous pouvez afficher le temps de réponse minimum de la semaine précédente, le premier quartile, le troisième quartile et le temps de réponse maximum, avec une médiane affichée par rapport à un SLO acceptable, que vous pouvez configurer. Lorsque le temps de réponse médian d'une application est hors de la plage SLO acceptable, une alerte (cercle rouge continu) apparaît à côté de l'application. Vous pouvez cliquer sur une application pour afficher la page de ressource résumant l'état actuel de cette ressource.

Performances quotidiennes des niveaux de stockage

Ce composant affiche un résumé des performances du niveau en termes de temps de réponse et d'IOPS pour les sept jours précédents. Ces performances sont comparées à un SLO, que vous pouvez configurer, ce qui vous permet de voir s'il existe une opportunité de consolider les niveaux, de réaligner les charges de travail fournies à partir de ces niveaux ou d'identifier des problèmes avec des niveaux particuliers. Lorsque le temps de réponse médian ou le nombre d'IOPS médian est hors de la plage SLO acceptable, une alerte (cercle rouge continu) apparaît à côté d'un niveau.

Vous pouvez cliquer sur un nom de niveau pour afficher le rapport Détails de la capacité et des performances des pools de stockage, qui indique les capacités libres et utilisées, le nombre de jours avant le remplissage et les détails des performances (IOPS et temps de réponse) pour tous les pools du niveau sélectionné. Cliquez sur n'importe quel stockage ou pool de stockage dans ce rapport pour afficher la page d'actif résumant l'état actuel de cette ressource.

Capacité orpheline

Ce composant affiche la capacité orpheline totale et la capacité orpheline par niveau, en la comparant aux plages acceptables pour la capacité totale utilisable et en affichant la capacité réelle qui est orpheline. La capacité orpheline est définie par la configuration et par les performances. Le stockage orphelin par configuration décrit une situation dans laquelle un stockage est alloué à un hôte. Cependant, la configuration n'a pas été effectuée correctement et l'hôte ne peut pas accéder au stockage. Orphelin en raison des performances, c'est lorsque le stockage est correctement configuré pour être accessible par un hôte. Cependant, il n'y a eu aucun trafic de stockage.

La barre horizontale empilée indique les plages acceptables. Plus le gris est foncé, plus la situation est inacceptable. La situation réelle est illustrée par la barre étroite en bronze qui indique la capacité réelle qui est orpheline.

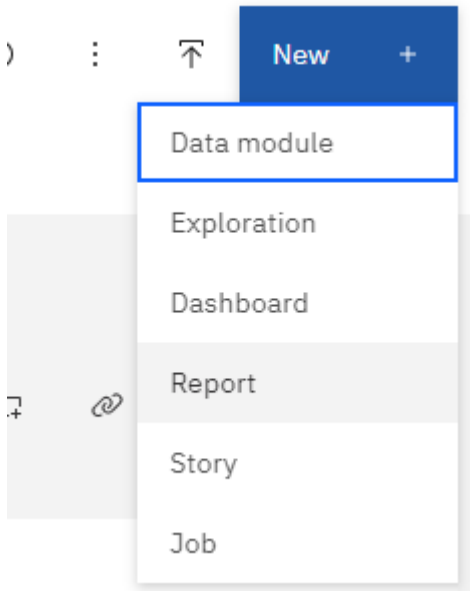
Vous pouvez cliquer sur un niveau pour afficher le rapport Détails du stockage orphelin, qui affiche tous les volumes identifiés comme orphelins par configuration et performances pour le niveau sélectionné. Cliquez sur n'importe quel stockage, pool de stockage ou volume dans ce rapport pour afficher la page d'actif résumant l'état actuel de cette ressource.

Création d'un rapport (exemple)

Utilisez les étapes de cet exemple pour générer un rapport simple sur la capacité physique du stockage et des pools de stockage dans un certain nombre de centres de données.

Étapes

1. Accédez à **Menu > Contenu > Contenu de l'équipe > Rapports**
2. En haut à droite de l'écran, sélectionnez **[Nouveau +]**
3. Sélectionnez **Signaler**



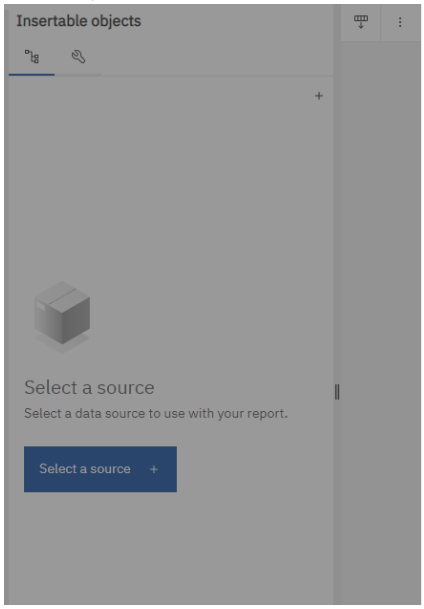
4. Dans l'onglet **Modèles**, sélectionnez *Vide*

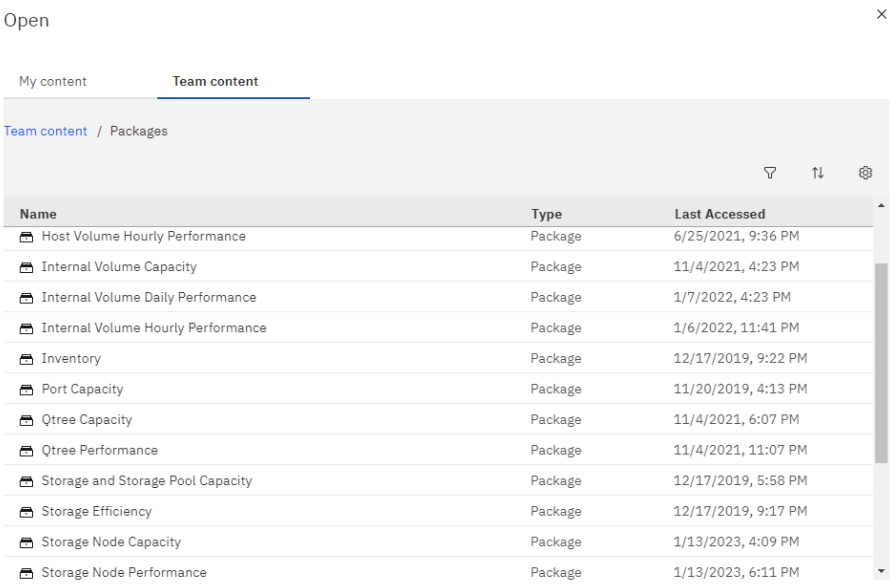
   Les onglets Source et Données s'affichent

5. Ouvrir **Sélectionner une source +**
6. Sous **Contenu de l'équipe**, ouvrez **Packages**

   Une liste des packages disponibles s'affiche.

7. Choisissez *Capacité de stockage et de pool de stockage*





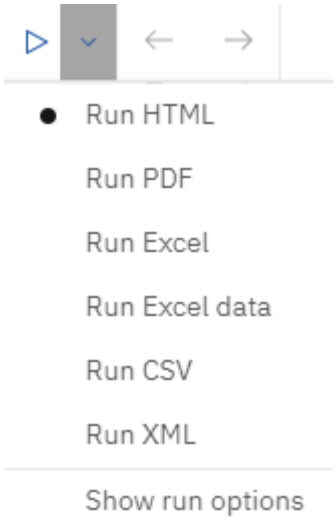
8. Sélectionnez **Ouvrir**

   Les styles disponibles pour votre rapport sont affichés.

9. Sélectionnez **Liste**

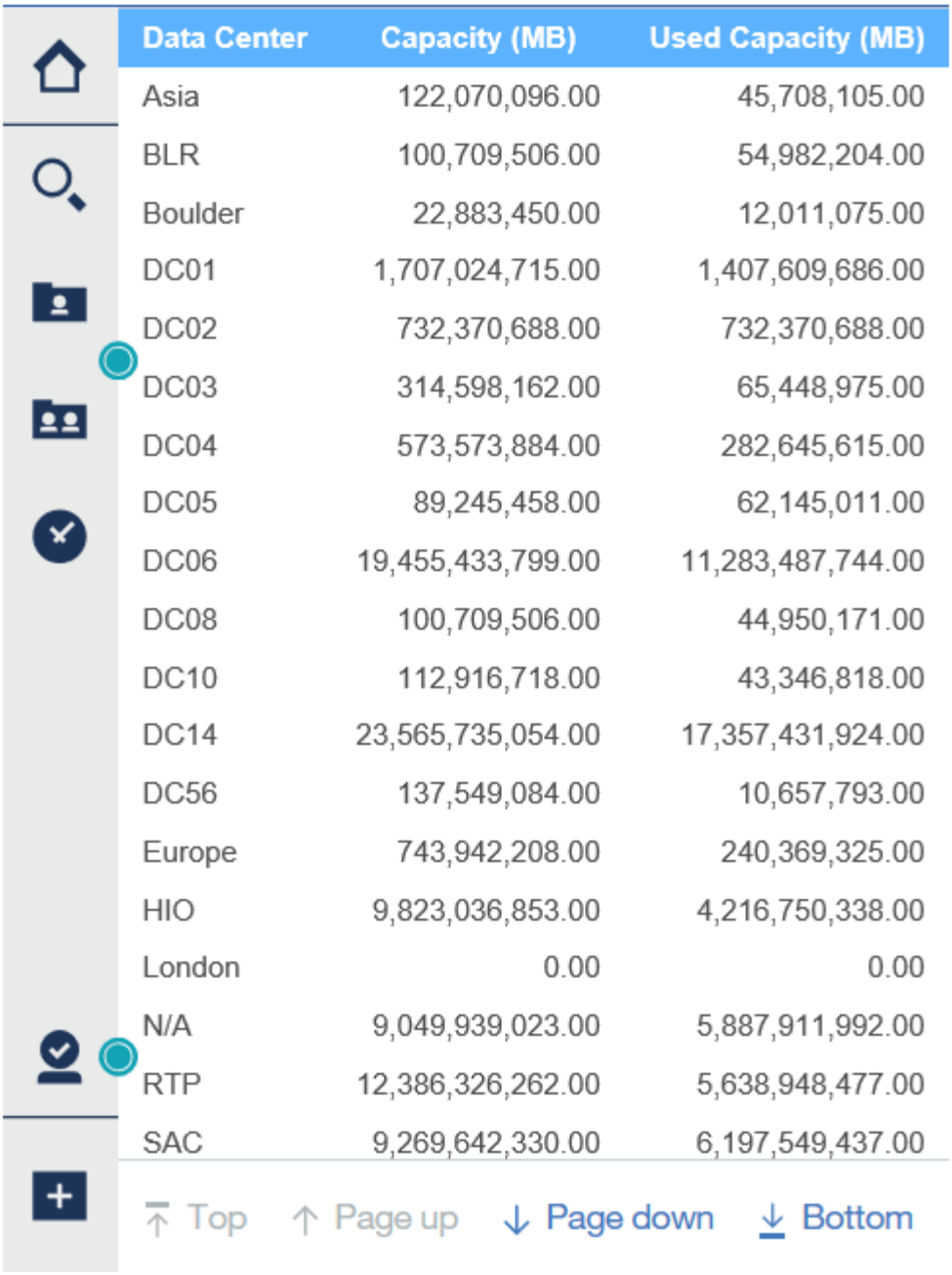
   Ajoutez des noms appropriés pour la liste et la requête

10. Sélectionnez **OK**
11. Développer la *capacité physique*
12. Développez jusqu'au niveau le plus bas du *Data Center*
13. Faites glisser *Data Center* vers la palette Rapports.
14. Augmenter la *Capacité (Mo)*
15. Faites glisser *Capacité (Mo)* vers la palette Rapports.
16. Faites glisser *Capacité utilisée (Mo)* vers la palette Rapports.
17. Exécutez le rapport en sélectionnant un type de sortie dans le menu **Exécuter**.



Résultat

Un rapport similaire au suivant est créé :



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Gestion des rapports

Vous pouvez personnaliser le format de sortie et la livraison d'un rapport, définir les propriétés ou les planifications du rapport et envoyer des rapports par courrier électronique.

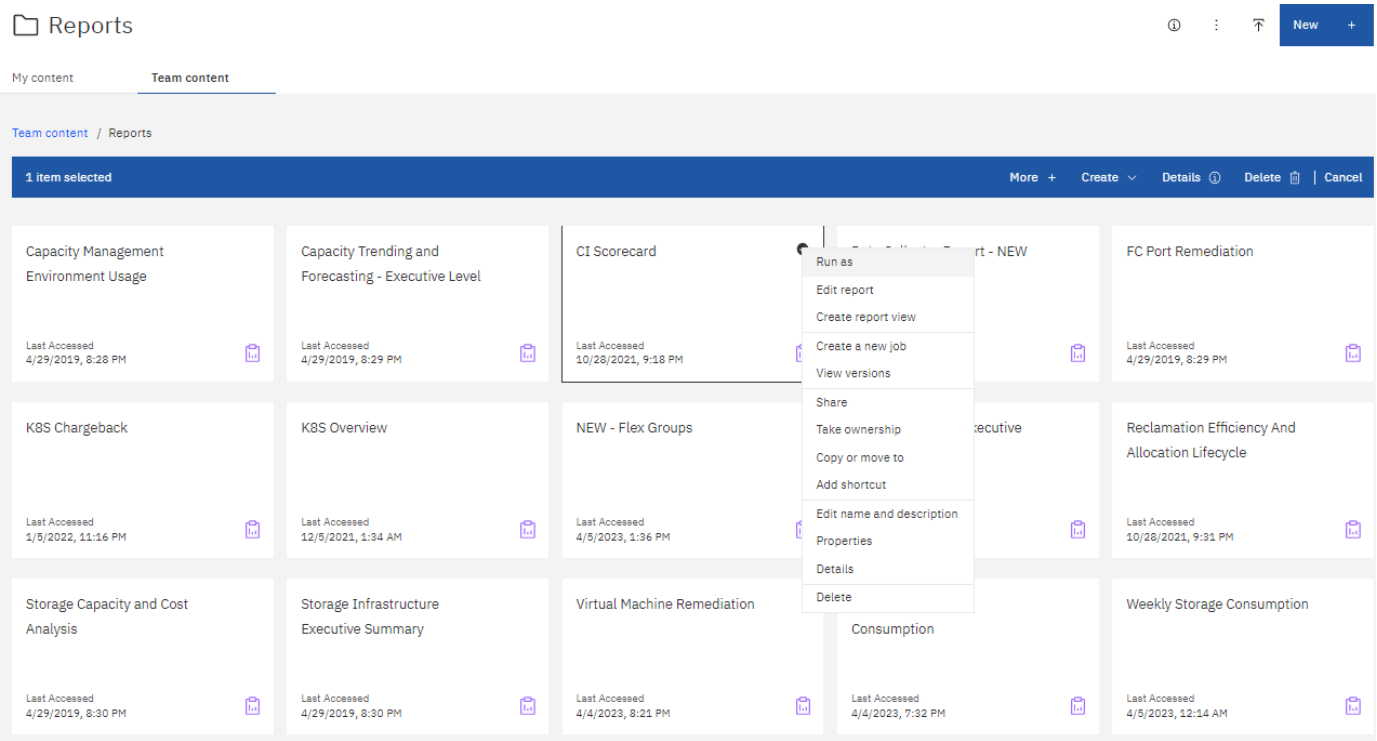
La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" .

Avant d'apporter des modifications aux autorisations de création de rapports ou à la sécurité, vous devez copier les rapports « Mon contenu » dans le dossier « Contenu de l'équipe » pour garantir que les rapports sont enregistrés.

Personnalisation du format de sortie et de la livraison d'un rapport

Vous pouvez personnaliser le format et le mode de livraison des rapports.

1. Dans le portail de rapports Data Infrastructure Insights , accédez à **Menu > Contenu > Mon contenu/Contenu de l'équipe**. Passez la souris sur le rapport que vous souhaitez personnaliser et ouvrez le menu « trois points ».

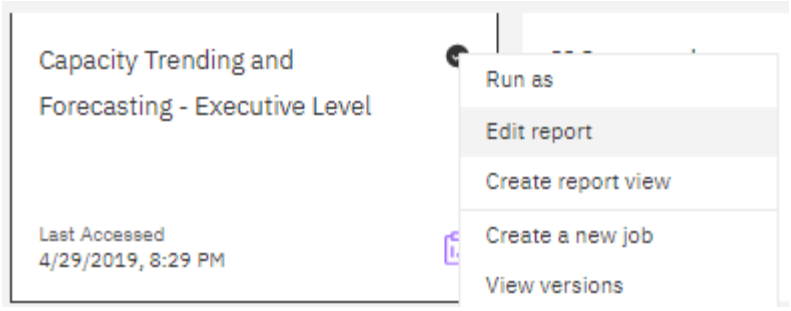


1. Cliquez sur **Propriétés > Planification**
2. Vous pouvez définir les options suivantes :
   - **Planifiez** quand vous souhaitez que les rapports s'exécutent.
   - Choisissez les **Options** pour le format et la livraison du rapport (Enregistrer, Imprimer, Envoyer par e-mail) et les langues du rapport.
3. Cliquez sur **Enregistrer** pour produire le rapport en utilisant les sélections que vous avez effectuées.

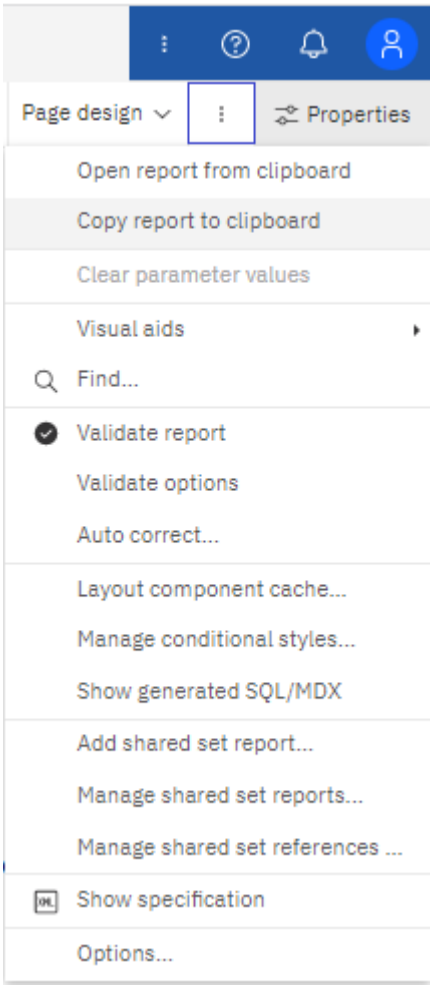
Copier un rapport dans le presse-papiers

Utilisez ce processus pour copier un rapport dans le presse-papiers.

1. Sélectionnez un rapport à copier (**Menu > Contenu > Mon contenu ou Contenu de l'équipe**)
2. Choisissez *Modifier le rapport* dans le menu déroulant du rapport



3. En haut à droite de l'écran, ouvrez le menu « trois points » à côté de « Propriétés ».
4. Sélectionnez **Copier le rapport dans le presse-papiers**.

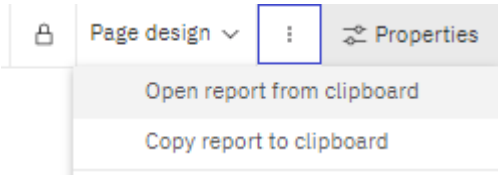


Ouvrir des rapports depuis le presse-papiers

Vous pouvez ouvrir une spécification de rapport qui a été précédemment copiée dans le presse-papiers.

À propos de cette tâche Commencez par créer un nouveau rapport ou ouvrir un rapport existant que vous souhaitez remplacer par le rapport copié. Les étapes ci-dessous concernent un nouveau rapport.

1. Sélectionnez **Menu > +Nouveau > Rapport** et créez un rapport vierge.
2. En haut à droite de l'écran, ouvrez le menu « trois points » à côté de « Propriétés ».
3. Sélectionnez **Ouvrir le rapport à partir du presse-papiers**.



1. Collez le code copié dans la fenêtre et sélectionnez **OK**.
2. Sélectionnez l'icône de la disquette pour enregistrer le rapport.
3. Choisissez où enregistrer le rapport (*Mon contenu*, *Contenu de l'équipe* ou créez un nouveau dossier).
4. Donnez au nouveau rapport un nom significatif et sélectionnez **Enregistrer**.

Modification d'un rapport existant

Gardez à l'esprit que la modification des fichiers dans leur emplacement par défaut entraîne le risque que ces rapports soient écrasés lors de la prochaine actualisation du catalogue de rapports. Il est recommandé d'enregistrer le rapport modifié sous un nouveau nom ou de le stocker dans un emplacement autre que celui par défaut.

Dépannage

Vous trouverez ici des suggestions pour résoudre les problèmes liés aux rapports.

Problème:	**Essayez ceci :**
Lors de la planification de l'envoi d'un rapport par e-mail, le nom de l'utilisateur connecté est pré-rempli dans le champ « À » de l'e-mail. Cependant, le nom est sous la forme « prénom nom » (prénom, espace, nom). Étant donné qu'il ne s'agit pas d'une adresse e-mail valide, l'e-mail ne sera pas envoyé lors de l'exécution du rapport planifié.	Lorsque vous planifiez l'envoi du rapport par courrier électronique, effacez le nom prérempli et saisissez une adresse électronique valide et correctement formatée dans le champ « À ».
Mon rapport planifié est envoyé par e-mail, mais le rapport n'est pas accessible si l'origine provient du dossier « Mon contenu ».	Afin d'éviter cela, le rapport ou la vue de rapport doit être enregistré dans le dossier « Contenu de l'équipe > Rapports personnalisés - xxxxxx » et le calendrier créé à partir de cette version enregistrée. Le dossier « Rapports personnalisés - xxxxxx » est visible par tous les utilisateurs du locataire.
lors de l'enregistrement d'un travail, le dossier peut afficher « Contenu de l'équipe » avec la liste du contenu de « Rapports personnalisés - xxxxxx », mais vous ne pouvez pas enregistrer le travail ici car Cognos pense qu'il s'agit du dossier « Contenu de l'équipe » dans lequel vous n'avez pas accès en écriture.	La solution consiste à créer un nouveau dossier avec un nom unique (par exemple « Nouveau dossier ») et à l'enregistrer à cet endroit, ou à l'enregistrer dans « Mon contenu », puis à le copier/déplacer vers « Rapports personnalisés - xxxxxx ».

Création de rapports personnalisés

Vous pouvez utiliser les outils de création de rapports pour créer des rapports personnalisés. Après avoir créé des rapports, vous pouvez les enregistrer et les exécuter selon un calendrier régulier. Les résultats des rapports peuvent être automatiquement

envoyés par courrier électronique à vous-même et à d'autres.

La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" .

Les exemples de cette section montrent le processus suivant, qui peut être utilisé pour n'importe lequel des modèles de données Data Infrastructure Insights Reporting :

- Identifier une question à laquelle il faut répondre avec un rapport
- Déterminer les données nécessaires pour étayer les résultats
- Sélection des éléments de données pour le rapport

Avant de concevoir votre rapport personnalisé, vous devez effectuer certaines tâches préalables. Si vous ne les remplissez pas, les rapports pourraient être inexacts ou incomplets.

Par exemple, si vous ne terminez pas le processus d'identification de l'appareil, vos rapports de capacité ne seront pas précis. Ou, si vous ne terminez pas la définition des annotations (telles que les niveaux, les unités commerciales et les centres de données), vos rapports personnalisés risquent de ne pas signaler avec précision les données de votre domaine ou d'afficher « N/A » pour certains points de données.

Avant de concevoir vos rapports, effectuez les tâches suivantes :

- Configurer tout"collecteurs de données" correctement.
- Saisissez des annotations (telles que les niveaux, les centres de données et les unités commerciales) sur les appareils et les ressources de votre locataire. Il est avantageux d'avoir des annotations stables avant de générer des rapports, car Data Infrastructure Insights Reporting collecte des informations historiques.

Processus de création de rapport

Le processus de création de rapports personnalisés (également appelés « ad hoc ») implique plusieurs tâches :

- Planifiez les résultats de votre rapport.
- Identifiez les données pour étayer vos résultats.
- Sélectionnez le modèle de données (par exemple, le modèle de données de rétrofacturation, le modèle de données d'inventaire, etc.) qui contient les données.
- Sélectionnez les éléments de données pour le rapport.
- Formatez, triez et filtrez éventuellement les résultats du rapport.

Planification des résultats de votre rapport personnalisé

Avant d'ouvrir les outils de création de rapport, vous souhaiterez peut-être planifier les résultats que vous souhaitez obtenir du rapport. Grâce aux outils de création de rapports, vous pouvez créer des rapports facilement et ne pas avoir besoin de beaucoup de planification. Cependant, il est judicieux d'obtenir une idée des exigences du demandeur du rapport.

- Identifiez la question exacte à laquelle vous souhaitez répondre. Par exemple:
  - Quelle est la capacité restante ?
  - Quels sont les coûts de rétrofacturation par unité commerciale ?
  - Quelle est la capacité par niveau pour garantir que les unités commerciales sont alignées sur le niveau de stockage approprié ?

    - Comment puis-je prévoir les besoins en énergie et en refroidissement ? (Ajoutez des métadonnées personnalisées en ajoutant des annotations aux ressources.)
- Identifiez les éléments de données dont vous avez besoin pour étayer la réponse.
- Identifiez les relations entre les données que vous souhaitez voir dans la réponse. N'incluez pas de relations illogiques dans votre question, par exemple : « Je veux voir les ports liés à la capacité. »
- Identifiez tous les calculs nécessaires sur les données.
- Déterminez quels types de filtrage sont nécessaires pour limiter les résultats.
- Déterminez si vous devez utiliser des données actuelles ou historiques.
- Déterminez si vous devez définir des privilèges d'accès sur les rapports pour limiter les données à des publics spécifiques.
- Déterminer comment le rapport sera distribué. Par exemple, doit-il être envoyé par courrier électronique selon un calendrier défini ou inclus dans la zone de dossier de contenu de l'équipe ?
- Déterminez qui tiendra à jour le rapport. Cela pourrait affecter la complexité de la conception.
- Créez une maquette du rapport.

Conseils pour la conception de rapports

Plusieurs conseils peuvent être utiles lorsque vous concevez des rapports.

- Déterminez si vous devez utiliser des données actuelles ou historiques.

  La plupart des rapports doivent uniquement rendre compte des dernières données disponibles dans Data Infrastructure Insights.

- Les rapports Data Infrastructure Insights fournissent des informations historiques sur la capacité et les performances, mais pas sur l'inventaire.
- Tout le monde voit toutes les données ; cependant, vous devrez peut-être limiter les données à des publics spécifiques.

  Pour segmenter les informations pour différents utilisateurs, vous pouvez créer des rapports et définir des autorisations d'accès sur ceux-ci.

Modèles de données de reporting

Data Infrastructure Insights comprend plusieurs modèles de données à partir desquels vous pouvez sélectionner des rapports prédéfinis ou créer votre propre rapport personnalisé.

Chaque modèle de données contient un datamart simple et un datamart avancé :

- Le datamart simple fournit un accès rapide aux éléments de données les plus couramment utilisés et inclut uniquement le dernier instantané des données de l'entrepôt de données ; il n'inclut pas les données historiques.
- Le datamart avancé fournit toutes les valeurs et tous les détails disponibles dans le datamart simple et inclut l'accès aux valeurs des données historiques.

Modèles de données de capacité

Vous permet de répondre à des questions sur la capacité de stockage, l'utilisation du système de fichiers, la capacité du volume interne, la capacité du port, la capacité du qtree et la capacité de la machine virtuelle (VM).

Le modèle de données de capacité est un conteneur pour plusieurs modèles de données de capacité. Vous pouvez créer des rapports répondant à différents types de questions à l'aide de ce modèle de données :

Modèle de données de capacité de stockage et de pool de stockage

Vous permet de répondre à des questions sur la planification des ressources de capacité de stockage, y compris le stockage et les pools de stockage, et inclut les données des pools de stockage physiques et virtuels. Ce modèle de données simple peut vous aider à répondre aux questions liées à la capacité de l'étage et à l'utilisation de la capacité des pools de stockage par niveau et par centre de données au fil du temps. Si vous débutez dans les rapports de capacité, vous devez commencer par ce modèle de données, car il s'agit d'un modèle de données plus simple et ciblé. Vous pouvez répondre à des questions similaires aux suivantes en utilisant ce modèle de données :

- Quelle est la date prévue pour atteindre le seuil de capacité de 80 % de mon stockage physique ?
- Quelle est la capacité de stockage physique sur une baie pour un niveau donné ?
- Quelle est ma capacité de stockage par fabricant et par famille ainsi que par centre de données ?
- Quelle est la tendance d'utilisation du stockage sur une baie pour tous les niveaux ?
- Quels sont mes 10 meilleurs systèmes de stockage avec la plus grande utilisation ?
- Quelle est la tendance d'utilisation du stockage des pools de stockage ?
- Quelle est la capacité déjà allouée ?
- Quelle capacité est disponible pour l'allocation ?

Modèle de données d'utilisation du système de fichiers

Ce modèle de données fournit une visibilité sur l'utilisation de la capacité par les hôtes au niveau du système de fichiers. Les administrateurs peuvent déterminer la capacité allouée et utilisée par système de fichiers, déterminer le type de système de fichiers et identifier les statistiques de tendance par type de système de fichiers. Vous pouvez répondre aux questions suivantes en utilisant ce modèle de données :

- Quelle est la taille du système de fichiers ?
- Où sont conservées les données et comment y accède-t-on, par exemple en local ou sur SAN ?
- Quelles sont les tendances historiques concernant la capacité du système de fichiers ? Alors, sur cette base, à quoi pouvons-nous nous attendre pour les besoins futurs ?

Modèle de données de capacité de volume interne

Vous permet de répondre à des questions sur la capacité interne utilisée, la capacité allouée et l'utilisation de la capacité au fil du temps :

- Quels volumes internes ont une utilisation supérieure à un seuil prédéfini ?
- Quels volumes internes risquent de manquer de capacité en fonction d'une tendance ? 8 Quelle est la capacité utilisée par rapport à la capacité allouée sur nos volumes internes ?

Modèle de données de capacité portuaire

Vous permet de répondre à des questions sur la connectivité du port du commutateur, l'état du port et la vitesse du port au fil du temps. Vous pouvez répondre à des questions similaires aux suivantes pour vous aider à planifier les achats de nouveaux commutateurs : Comment puis-je créer une prévision de consommation de ports qui prédit la disponibilité des ressources (ports) (en fonction du centre de données, du fournisseur de commutateurs et de la vitesse du port) ?

- Quels ports sont susceptibles de manquer de capacité, en fonction de la vitesse des données, du centre de données, du fournisseur et du nombre de ports hôtes et de stockage ?
- Quelles sont les tendances de la capacité des ports de commutation au fil du temps ?
- Quelles sont les vitesses des ports ?
- Quel type de capacité portuaire est nécessaire et quelle organisation est sur le point de manquer d'un certain type de port ou d'un certain fournisseur ?
- Quel est le moment optimal pour acheter cette capacité et la rendre disponible ?

Modèle de données Qtree Capacity

Vous permet de suivre l'utilisation de Qtree (avec des données telles que la capacité utilisée par rapport à la capacité allouée) au fil du temps. Vous pouvez afficher les informations selon différentes dimensions, par exemple par entité commerciale, application, niveau et niveau de service. Vous pouvez répondre aux questions suivantes en utilisant ce modèle de données :

- Quelle est la capacité utilisée pour les qtrees par rapport aux limites définies par application ou entité commerciale ?
- Quelles sont les tendances de notre capacité utilisée et libre afin que nous puissions faire une planification de capacité ?
- Quelles entités commerciales utilisent le plus de capacité ?
- Quelles applications consomment le plus de capacité ?

Modèle de données de capacité VM

Vous permet de signaler votre environnement virtuel et son utilisation de la capacité. Ce modèle de données vous permet de générer des rapports sur les changements d'utilisation de la capacité au fil du temps pour les machines virtuelles et les magasins de données. Le modèle de données fournit également des données de provisionnement dynamique et de rétrofacturation de machine virtuelle.

- Comment puis-je déterminer la rétrofacturation de capacité en fonction de la capacité provisionnée sur les machines virtuelles et les magasins de données ?
- Quelle capacité n'est pas utilisée par les machines virtuelles et quelle partie inutilisée est libre, orpheline ou autre ?
- Que devons-nous acheter en fonction des tendances de consommation ?
- Quelles économies d'efficacité de stockage puis-je réaliser en utilisant les technologies de provisionnement fin et de déduplication du stockage ?

Les capacités du modèle de données VM Capacity sont extraites des disques virtuels (VMDK). Cela signifie que la taille provisionnée d'une machine virtuelle utilisant le modèle de données VM Capacity correspond à la taille de ses disques virtuels. Ceci est différent de la capacité provisionnée dans la vue Machines virtuelles dans Data Infrastructure Insights, qui affiche la taille provisionnée pour la machine virtuelle elle-même.

Modèle de données de capacité de volume

Vous permet d'analyser tous les aspects des volumes de votre locataire et d'organiser les données par fournisseur, modèle, niveau, niveau de service et centre de données.

Vous pouvez afficher la capacité liée aux volumes orphelins, aux volumes inutilisés et aux volumes de protection (utilisés pour la réplication). Vous pouvez également voir différentes technologies de volume (iSCSI ou FC) et comparer les volumes virtuels aux volumes non virtuels pour les problèmes de virtualisation de

matrice.

Vous pouvez répondre à des questions similaires aux suivantes avec ce modèle de données :

- Quels volumes ont une utilisation supérieure à un seuil prédéfini ?
- Quelle est la tendance dans mon centre de données en matière de capacité de volume orphelin ?
- Quelle part de la capacité de mon centre de données est virtualisée ou provisionnée de manière dynamique ?
- Quelle part de la capacité de mon centre de données doit être réservée à la réplication ?

Modèle de données de rétrofacturation

Vous permet de répondre à des questions sur la capacité utilisée et la capacité allouée sur les ressources de stockage (volumes, volumes internes et qtrees). Ce modèle de données fournit des informations sur la rétrofacturation et la responsabilité de la capacité de stockage par hôtes, applications et entités commerciales, et inclut des données actuelles et historiques. Les données du rapport peuvent être classées par niveau de service et par niveau de stockage.

Vous pouvez utiliser ce modèle de données pour générer des rapports de rétrofacturation en recherchant la quantité de capacité utilisée par une entité commerciale. Ce modèle de données vous permet de créer des rapports unifiés de plusieurs protocoles (y compris NAS, SAN, FC et iSCSI).

- Pour le stockage sans volumes internes, les rapports de rétrofacturation affichent la rétrofacturation par volumes.
- Pour le stockage avec volumes internes :
  - Si des entités commerciales sont affectées à des volumes, les rapports de rétrofacturation affichent la rétrofacturation par volumes.
  - Si les entités commerciales ne sont pas affectées à des volumes mais affectées à des qtrees, les rapports de rétrofacturation affichent la rétrofacturation par qtrees.
  - Si les entités commerciales ne sont pas affectées à des volumes ni à des qtrees, les rapports de rétrofacturation affichent le volume interne.
  - La décision d’afficher la rétrofacturation par volume, qtree ou volume interne est prise pour chaque volume interne. Il est donc possible que différents volumes internes du même pool de stockage affichent la rétrofacturation à différents niveaux.

Les faits de capacité sont purgés après un intervalle de temps par défaut. Pour plus de détails, voir Processus de l’entrepôt de données.

Les rapports utilisant le modèle de données de rétrofacturation peuvent afficher des valeurs différentes de celles des rapports utilisant le modèle de données de capacité de stockage.

- Pour les baies de stockage qui ne sont pas des systèmes de stockage NetApp , les données des deux modèles de données sont les mêmes.
- Pour les systèmes de stockage NetApp et Celerra, le modèle de données de rétrofacturation utilise une seule couche (de volumes, de volumes internes ou de qtrees) pour baser ses frais, tandis que le modèle de données de capacité de stockage utilise plusieurs couches (de volumes et de volumes internes) pour baser ses frais.

Modèle de données d’inventaire

Vous permet de répondre à des questions sur les ressources d’inventaire, notamment les hôtes, les systèmes

de stockage, les commutateurs, les disques, les bandes, les qtrees, les quotas, les machines virtuelles et les serveurs, ainsi que les périphériques génériques. Le modèle de données d'inventaire comprend plusieurs sous-marchés qui vous permettent d'afficher des informations sur les réplications, les chemins FC, les chemins iSCSI, les chemins NFS et les violations. Le modèle de données d'inventaire n'inclut pas de données historiques. Questions auxquelles vous pouvez répondre avec ces données

- Quels sont mes actifs et où se trouvent-ils ?
- Qui utilise les actifs ?
- Quels types d'appareils possèdes-je et quels sont les composants de ces appareils ?
- Combien d'hôtes par système d'exploitation ai-je et combien de ports existent sur ces hôtes ?
- Quelles baies de stockage par fournisseur existent dans chaque centre de données ?
- Combien de commutateurs par fournisseur ai-je dans chaque centre de données ?
- Combien de ports ne sont pas autorisés ?
- Quelles bandes de fournisseurs utilisons-nous et combien de ports existent sur chaque bande ? Tous les périphériques génériques sont-ils identifiés avant de commencer à travailler sur les rapports ?
- Quels sont les chemins entre les hôtes et les volumes de stockage ou les bandes ?
- Quels sont les chemins entre les périphériques génériques et les volumes de stockage ou les bandes ?
- Combien de violations de chaque type ai-je par centre de données ?
- Pour chaque volume répliqué, quels sont les volumes source et cible ?
- Y a-t-il des incompatibilités de micrologiciel ou des décalages de vitesse de port entre les HBA hôtes Fibre Channel et les commutateurs ?

Modèle de données de performance

Vous permet de répondre à des questions sur les performances des volumes, des volumes d'application, des volumes internes, des commutateurs, des applications, des machines virtuelles, des VMDK, des ESX par rapport aux machines virtuelles, des hôtes et des nœuds d'application. La plupart d'entre eux rapportent des données horaires, quotidiennes ou les deux. À l'aide de ce modèle de données, vous pouvez créer des rapports qui répondent à plusieurs types de questions de gestion des performances :

- Quels volumes ou volumes internes n'ont pas été utilisés ou consultés pendant une période spécifique ?
- Pouvons-nous identifier une éventuelle mauvaise configuration du stockage d'une application (inutilisée) ?
- Quel était le modèle de comportement d'accès global pour une application ?
- Les volumes hiérarchisés sont-ils attribués de manière appropriée pour une application donnée ?
- Pourrions-nous utiliser un stockage moins cher pour une application en cours d'exécution sans impact sur les performances de l'application ?
- Quelles sont les applications qui génèrent le plus d'accès au stockage actuellement configuré ?

Lorsque vous utilisez les tableaux de performances des commutateurs, vous pouvez obtenir les informations suivantes :

- Le trafic de mon hôte via les ports connectés est-il équilibré ?
- Quels commutateurs ou ports présentent un nombre élevé d'erreurs ?
- Quels sont les commutateurs les plus utilisés en fonction des performances des ports ?
- Quels sont les commutateurs sous-utilisés en fonction des performances des ports ?

- Quelle est la tendance du débit de l'hôte en fonction des performances du port ?
- Quelle est l'utilisation des performances au cours des X derniers jours pour un hôte, un système de stockage, une bande ou un commutateur spécifié ?
- Quels périphériques produisent du trafic sur un commutateur spécifique (par exemple, quels périphériques sont responsables de l'utilisation d'un commutateur très utilisé) ?
- Quel est le débit d'une unité commerciale spécifique dans notre environnement ?

Lorsque vous utilisez les tableaux de performances du disque, vous pouvez obtenir les informations suivantes :

- Quel est le débit d'un pool de stockage spécifié en fonction des données de performances du disque ?
- Quel est le pool de stockage le plus utilisé ?
- Quelle est l'utilisation moyenne du disque pour un stockage spécifique ?
- Quelle est la tendance d'utilisation d'un système de stockage ou d'un pool de stockage en fonction des données de performances du disque ?
- Quelle est la tendance d'utilisation du disque pour un pool de stockage spécifique ?

Lorsque vous utilisez les tables de performances VM et VMDK, vous pouvez obtenir les informations suivantes :

- Mon environnement virtuel fonctionne-t-il de manière optimale ?
- Quels VMDK signalent les charges de travail les plus élevées ?
- Comment puis-je utiliser les performances signalées par les VMD mappés à différents magasins de données pour prendre des décisions concernant la hiérarchisation.

Le modèle de données de performances inclut des informations qui vous aident à déterminer la pertinence des niveaux, les erreurs de configuration de stockage pour les applications et les dernières heures d'accès des volumes et des volumes internes. Ce modèle de données fournit des données telles que les temps de réponse, les IOP, le débit, le nombre d'écritures en attente et l'état d'accès.

Modèle de données d'efficacité de stockage

Vous permet de suivre le score d'efficacité du stockage et le potentiel au fil du temps. Ce modèle de données stocke les mesures non seulement de la capacité provisionnée, mais également de la quantité utilisée ou consommée (la mesure physique). Par exemple, lorsque le provisionnement léger est activé, Data Infrastructure Insights indique la quantité de capacité extraite du périphérique. Vous pouvez également utiliser ce modèle pour déterminer l'efficacité lorsque la déduplication est activée. Vous pouvez répondre à diverses questions en utilisant le datamart Storage Efficiency :

- Quelles sont nos économies d'efficacité de stockage grâce à la mise en œuvre de technologies de provisionnement léger et de déduplication ?
- Quelles sont les économies de stockage réalisées dans les centres de données ?
- En fonction des tendances historiques en matière de capacité, quand devons-nous acheter du stockage supplémentaire ?
- Quel serait le gain de capacité si nous activions des technologies telles que le provisionnement léger et la déduplication ?
- En ce qui concerne la capacité de stockage, suis-je actuellement en danger ?

Tables de faits et de dimensions du modèle de données

Chaque modèle de données comprend à la fois des tables de faits et de dimensions.

- Tables de faits : contiennent des données mesurées, par exemple, la quantité, la capacité brute et utilisable. Contient des clés étrangères vers des tables de dimension.
- Tables de dimensions : contiennent des informations descriptives sur des faits, par exemple, le centre de données et les unités commerciales. Une dimension est une structure, souvent composée de hiérarchies, qui catégorise les données. Les attributs dimensionnels aident à décrire les valeurs dimensionnelles.

À l'aide d'attributs de dimension différents ou multiples (vus comme des colonnes dans les rapports), vous créez des rapports qui accèdent aux données de chaque dimension décrite dans le modèle de données.

Couleurs utilisées dans les éléments du modèle de données

Les couleurs sur les éléments du modèle de données ont des indications différentes.

- Actifs jaunes : représentent les mesures.
- Actifs non jaunes : représentent des attributs. Ces valeurs ne s'agrègent pas.

Utilisation de plusieurs modèles de données dans un seul rapport

En règle générale, vous utilisez un modèle de données par rapport. Cependant, vous pouvez rédiger un rapport qui combine des données provenant de plusieurs modèles de données.

Pour rédiger un rapport combinant des données provenant de plusieurs modèles de données, choisissez l'un des modèles de données à utiliser comme base, puis écrivez des requêtes SQL pour accéder aux données à partir des datamarts supplémentaires. Vous pouvez utiliser la fonction SQL Join pour combiner les données des différentes requêtes en une seule requête que vous pouvez utiliser pour rédiger le rapport.

Par exemple, supposons que vous souhaitiez connaître la capacité actuelle de chaque baie de stockage et que vous souhaitiez capturer des annotations personnalisées sur les baies. Vous pouvez créer le rapport à l'aide du modèle de données Capacité de stockage. Vous pouvez utiliser les éléments des tables Capacité actuelle et Dimensions et ajouter une requête SQL distincte pour accéder aux informations d'annotations dans le modèle de données d'inventaire. Enfin, vous pouvez combiner les données en liant les données de stockage d'inventaire à la table de dimension de stockage à l'aide du nom de stockage et des critères de jointure.

Accéder à la base de données de rapports via l'API

L'API puissante de Data Infrastructure Insights permet aux utilisateurs d'interroger directement la base de données Data Infrastructure Insights Reporting, sans passer par l'environnement Cognos Reporting.

Cette documentation fait référence à la fonctionnalité de création de rapports Data Infrastructure Insights , disponible dans Data Infrastructure Insights Premium Edition.

Odata

L'API de reporting Data Infrastructure Insights suit la"OData v4" (Open Data Protocol) norme pour l'interrogation de la base de données Reporting. Pour plus d'informations ou pour en savoir plus, consultez"ce tutoriel" sur OData.

Toutes les requêtes commenceront par l'URL *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata*

Générer une clé API

En savoir plus sur"API d' Data Infrastructure Insights" .

Pour générer une clé API, procédez comme suit :

- Connectez-vous à votre environnement Data Infrastructure Insights et sélectionnez **Admin > Accès API**.
- Cliquez sur « + Jeton d'accès API ».
- Entrez un nom et une description.
- Pour le type, choisissez *Data Warehouse*.
- Définissez les autorisations en lecture/écriture.
- Définissez une date d'expiration pour vos souhaits.
- Cliquez sur « Enregistrer », puis **copiez la clé et enregistrez-la** dans un endroit sûr. Vous ne pourrez pas accéder à la clé complète ultérieurement.

Les clés API sont utiles pour*Sync* ou *Async* .

Requête directe des tables

Avec la clé API en place, les requêtes directes sur la base de données de rapports sont désormais possibles. Les URL longues peuvent être simplifiées en https://…/odata/ à des fins d'affichage plutôt qu'en https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata/ complet

Essayez des requêtes simples comme

- https://< URL des Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_custom
- https://< URL des Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory
- https://< URL des Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/storage
- https://< URL des Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/disk
- https://…/odata/dwh_custom/requêtes_personnalisées

Exemples d'API REST

L'URL pour tous les appels est *https://< Data Infrastructure Insights URL>/rest/v1/dwh-management/odata*.

- GET /{schema}/** - Récupère les données de la base de données de rapports.

Format : *https://< URL Data Infrastructure Insights >/rest/v1/dwh-management/odata/<nom_schéma>/<requête>*

Exemple:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Résultat:
```

```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```


Conseils utiles

Gardez les points suivants à l'esprit lorsque vous travaillez avec des requêtes d'API de création de rapports.

- La charge utile de la requête doit être une chaîne JSON valide
- La charge utile de la requête doit être contenue dans une seule ligne
- Les guillemets doubles doivent être échappés, c'est-à-dire \"
- Les onglets sont pris en charge en tant que \t
- Évitez les commentaires
- Les noms de table en minuscules sont pris en charge

En plus:

- 2 en-têtes sont requis :
  - Nom « X-CloudInsights-ApiKey »
  - Valeur d'attribut « <apikey> »

Votre clé API sera spécifique à votre environnement Data Infrastructure Insights .

Synchrone ou asynchrone ?

Par défaut, une commande API fonctionnera en mode *synchrone*, ce qui signifie que vous envoyez la requête et la réponse est renvoyée immédiatement. Cependant, il arrive parfois qu'une requête prenne beaucoup de temps à s'exécuter, ce qui peut entraîner l'expiration de la requête. Pour contourner ce problème, vous pouvez exécuter une requête de manière *asynchrone*. En mode asynchrone, la requête renverra une URL via laquelle l'exécution pourra être surveillée. L'URL renverra le résultat lorsqu'il sera prêt.

Pour exécuter une requête en mode asynchrone, ajoutez l'en-tête **`Prefer: respond-async`** à la demande. Une fois l'exécution réussie, la réponse contiendra les en-têtes suivants :

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

L'interrogation de l'URL d'emplacement renverra les mêmes en-têtes si la réponse n'est pas encore prête, ou renverra le statut 200 si la réponse est prête. Le contenu de la réponse sera de type texte et contiendra l'état http de la requête d'origine et certaines métadonnées, suivis des résultats de la requête d'origine.

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

Pour voir une liste de toutes les requêtes asynchrones et lesquelles d'entre elles sont prêtes, utilisez la commande suivante :

```
 GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
La réponse a le format suivant :
```

```
{
   "queries" : [
       {
           "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
           "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
           "Finished": false
       }
   ]
}
```

Publication et dépublication d'annotations pour les rapports

Publication et dépublication d'annotations pour les rapports

Apprenez comment publier des annotations pour les utiliser dans les rapports et l'entrepôt de données, et comment les dépublier correctement lorsqu'elles ne sont plus nécessaires.

Publication d'annotations pour les rapports

Une fois que vous avez créé des annotations dans Data Infrastructure Insights, vous pouvez les publier pour les utiliser dans la génération de rapports.

Étapes pour publier des annotations

1. Accédez à la page **Observabilité > Enrichir > Annotations** et sélectionnez l'onglet *Annotations pour la génération de rapports*.
2. Repérez l'annotation que vous souhaitez publier.
3. Sélectionnez l'annotation et choisissez *Publier dans les rapports*. Vous pouvez également choisir de l'appliquer aux données historiques, ce qui permettra d'utiliser l'annotation lors de l'exécution de rapports d'historique.
4. Une fois publiée, l'annotation devient disponible pour être utilisée dans la création de rapports.
5. Les annotations sont publiées pour être utilisées dans les rapports après la prochaine exécution ETL.

> Tous les rapports faisant référence à cette annotation utiliseront les valeurs publiées. Si vous modifiez une annotation après sa publication, vous devrez peut-être la republier pour que ces modifications soient prises en compte dans les rapports.

Supprimer les annotations pour le rapport

Il peut arriver que vous ayez besoin de supprimer ou de dépublier des annotations, afin qu'elles ne soient plus utilisées dans la génération de rapports. Par exemple, une annotation peut ne plus être nécessaire, ou elle peut contenir des informations obsolètes qui ne devraient pas figurer dans les rapports.

Étapes pour dépublier les annotations

Avant de dépublier une annotation, sachez que cette action aura un impact sur tous les rapports existants qui utilisent cette annotation. Les rapports peuvent nécessiter une modification ou l'intervention de services professionnels pour supprimer les références aux annotations.

1. Dans l'interface utilisateur de Data Infrastructure Insights , accédez à l'onglet *Annotations pour la création de rapports*.
2. Repérez l'annotation que vous souhaitez dépublier.
3. Pour chaque objet sur lequel l'annotation est publiée, désélectionnez l'annotation et sélectionnez *Enregistrer*.
4. Supprimez toutes les requêtes ou règles qui font encore référence à l'annotation afin de vous assurer qu'elle n'est pas marquée comme « en cours d'utilisation ».
5. Les annotations ne seront pas publiées après la prochaine exécution ETL.
6. Une fois l'ETL terminé, l'annotation peut être supprimée de la liste des annotations si elle n'est plus nécessaire côté locataire.

> Les annotations continueront d'apparaître dans l'entrepôt de données jusqu'à ce qu'elles soient correctement dépubliées. Le simple fait de supprimer une annotation de la page Annotations sans la dépublier au préalable laissera des données obsolètes susceptibles d'apparaître dans les rapports existants. Suivez les étapes de dépublication ci-dessus pour garantir la suppression complète.

Impact sur les rapports existants

La suppression ou la dépublication d'annotations peut nécessiter des modifications des rapports existants qui font référence à ces annotations. Considérez ce qui suit :

- Les rapports qui utilisent l'annotation comme filtre ou dimension devront être mis à jour.
- Si une annotation est supprimée sans mettre à jour les rapports dépendants, ces rapports peuvent renvoyer des erreurs ou des résultats inattendus.
- Des services professionnels peuvent être nécessaires pour aider à la correction des rapports dans des situations complexes.

Il est recommandé de vérifier tous les rapports qui dépendent d'une annotation avant de la dépublier.

Comment les données historiques sont conservées pour les rapports

Data Infrastructure Insights conserve les données historiques à utiliser dans les rapports en fonction des entrepôts de données et de la granularité des données, comme indiqué dans le tableau suivant.

Datamart	Objet mesuré	Granularité	Période de conservation
Marchés de performance	Volumes et volumes internes	Toutes les heures	14 jours
Marchés de performance	Volumes et volumes internes	Tous les jours	13 mois
Marchés de performance	Application	Toutes les heures	13 mois

Marchés de performance	Hôte	Toutes les heures	13 mois
Marchés de performance	Performances du commutateur pour le port	Toutes les heures	35 jours
Marchés de performance	Performances du commutateur pour l'hôte, le stockage et la bande	Toutes les heures	13 mois
Marchés de performance	Nœud de stockage	Toutes les heures	14 jours
Marchés de performance	Nœud de stockage	Tous les jours	13 mois
Marchés de performance	Performances de la machine virtuelle	Toutes les heures	14 jours
Marchés de performance	Performances de la machine virtuelle	Tous les jours	13 mois
Marchés de performance	Performances de l'hyperviseur	Toutes les heures	35 jours
Marchés de performance	Performances de l'hyperviseur	Tous les jours	13 mois
Marchés de performance	Performances de VMDK	Toutes les heures	35 jours
Marchés de performance	Performances de VMDK	Tous les jours	13 mois
Marchés de performance	Performances du disque	Toutes les heures	14 jours
Marchés de performance	Performances du disque	Tous les jours	13 mois
Centres de capacité	Tous (sauf les volumes individuels)	Tous les jours	13 mois
Centres de capacité	Tous (sauf les volumes individuels)	Représentant mensuel	14 mois et plus
Magasins d'inventaire	Volumes individuels	État actuel	1 jour (ou jusqu'au prochain ETL)

Diagrammes de schéma de reporting des Data Infrastructure Insights

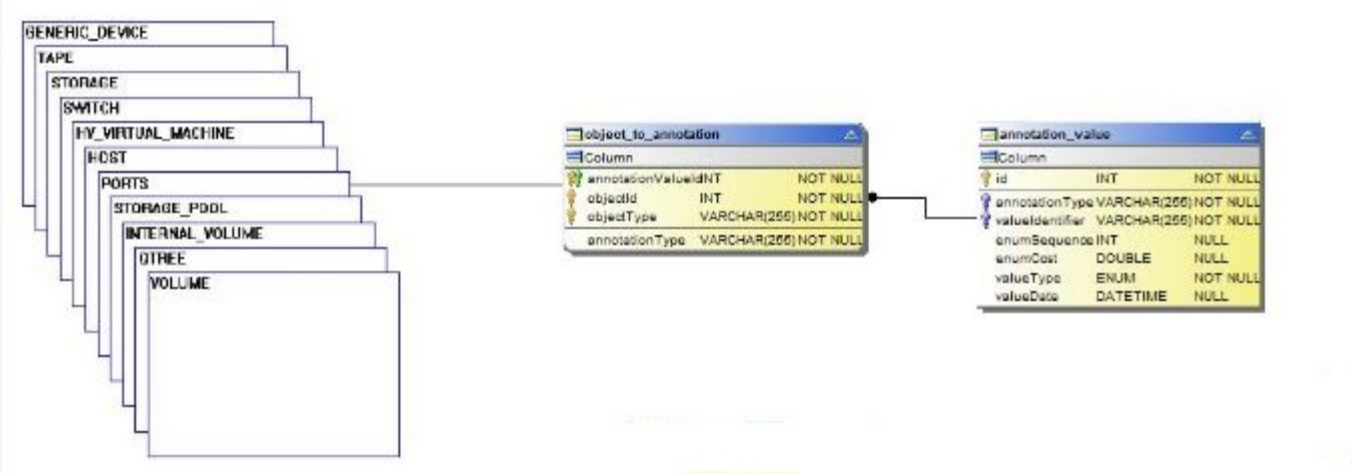
Ce document fournit des diagrammes de schéma pour la base de données de rapports.

La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" .

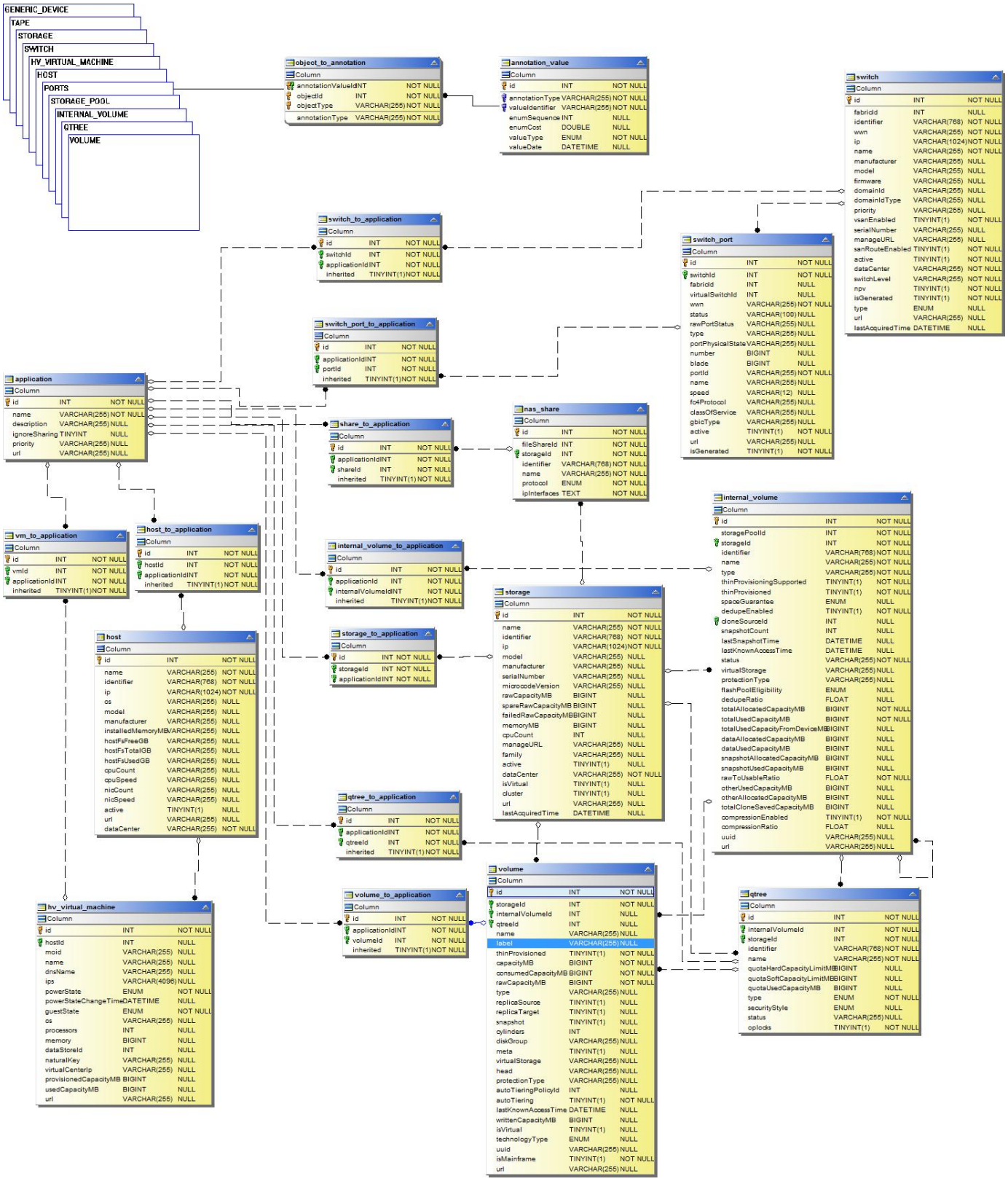
Datamart d'inventaire

Les images suivantes décrivent le datamart d'inventaire.

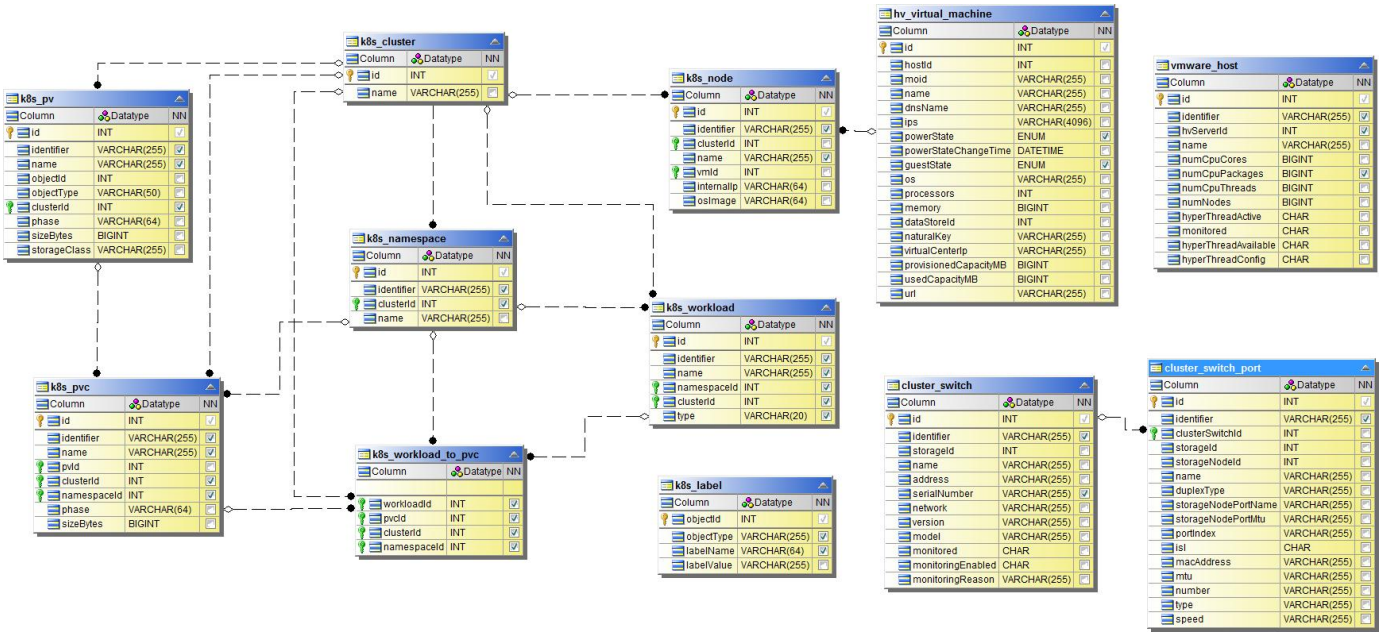
Annotations



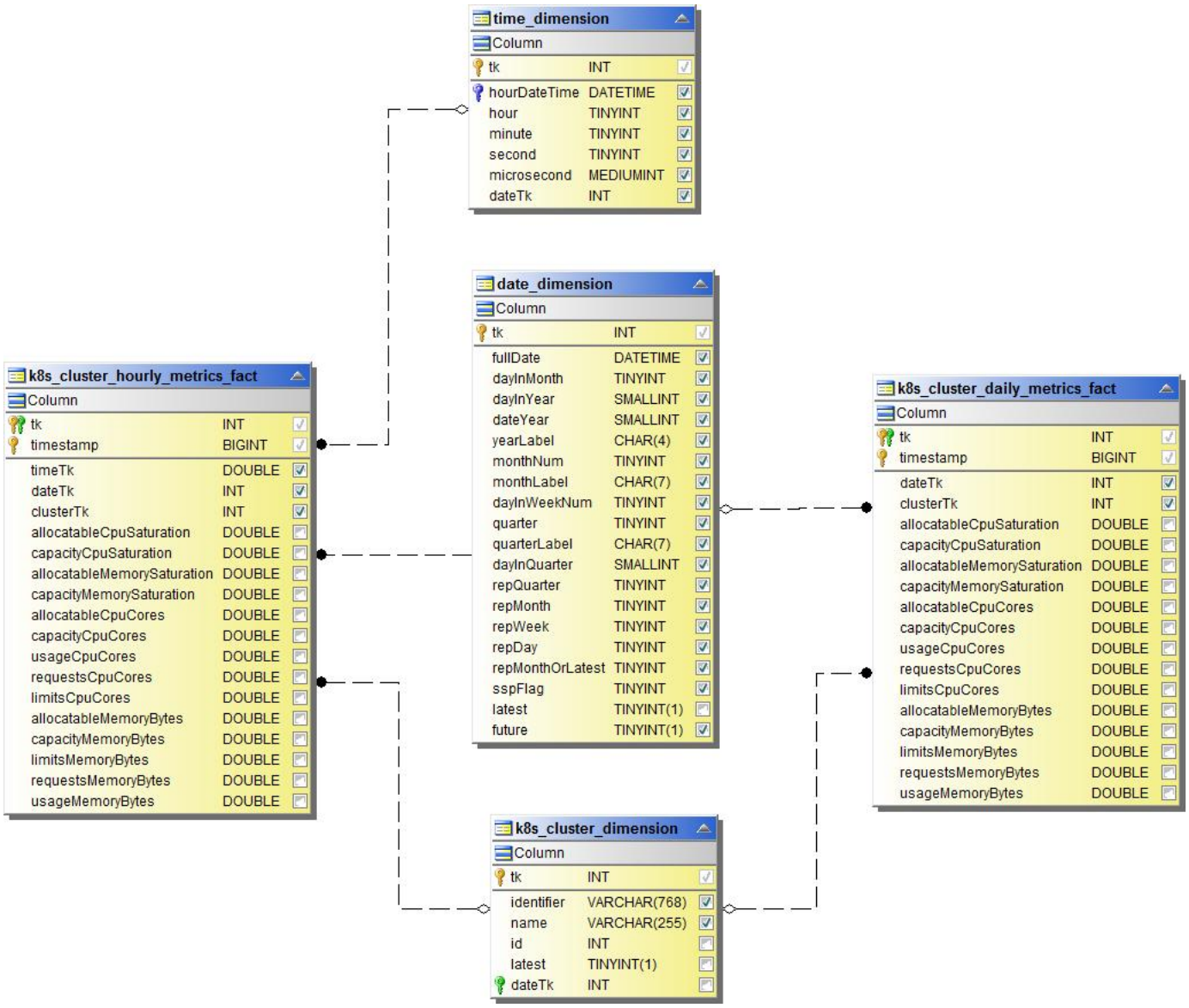
Applications



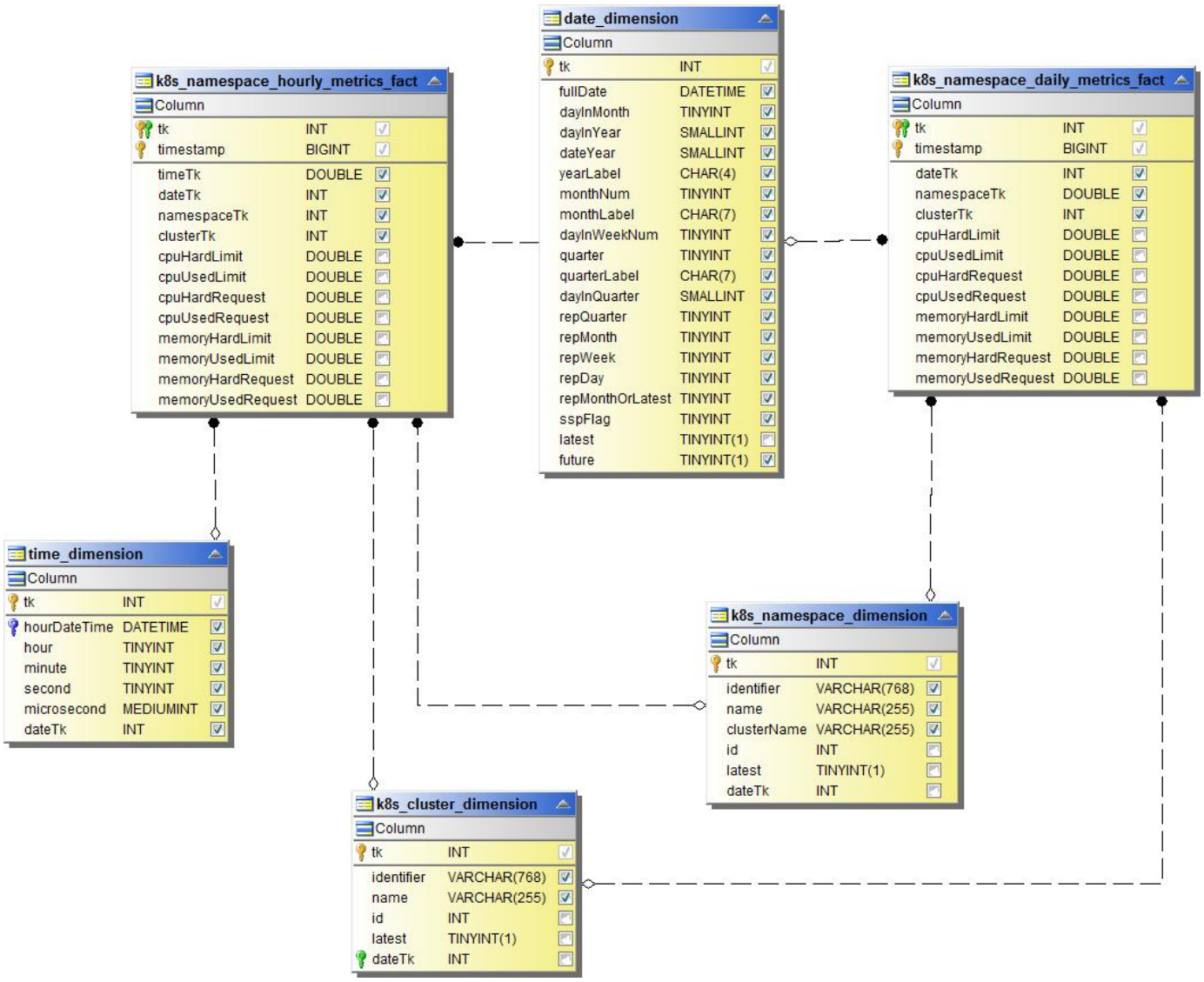
Métriques Kubernetes



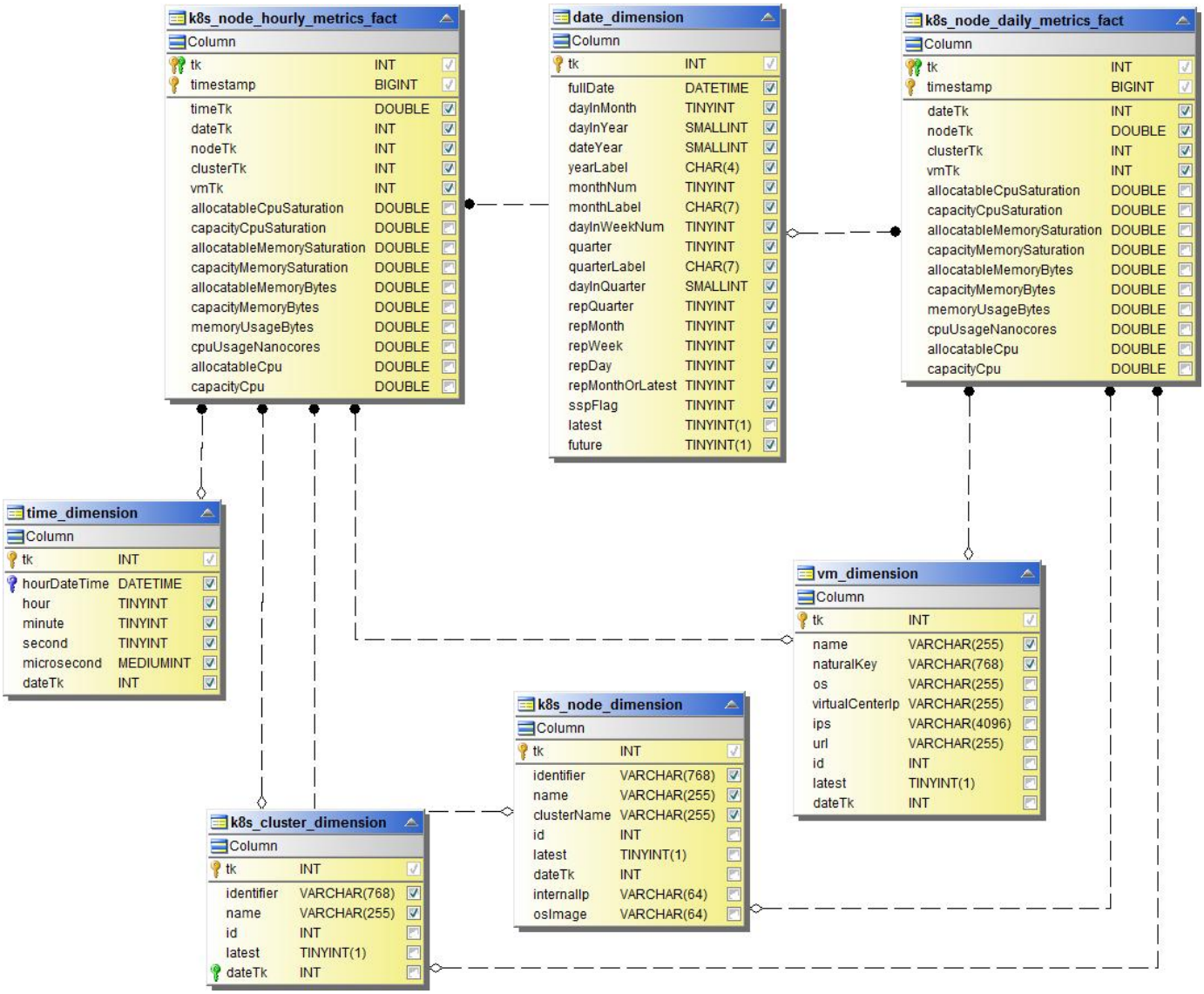
Faits sur les métriques du cluster Kubernetes



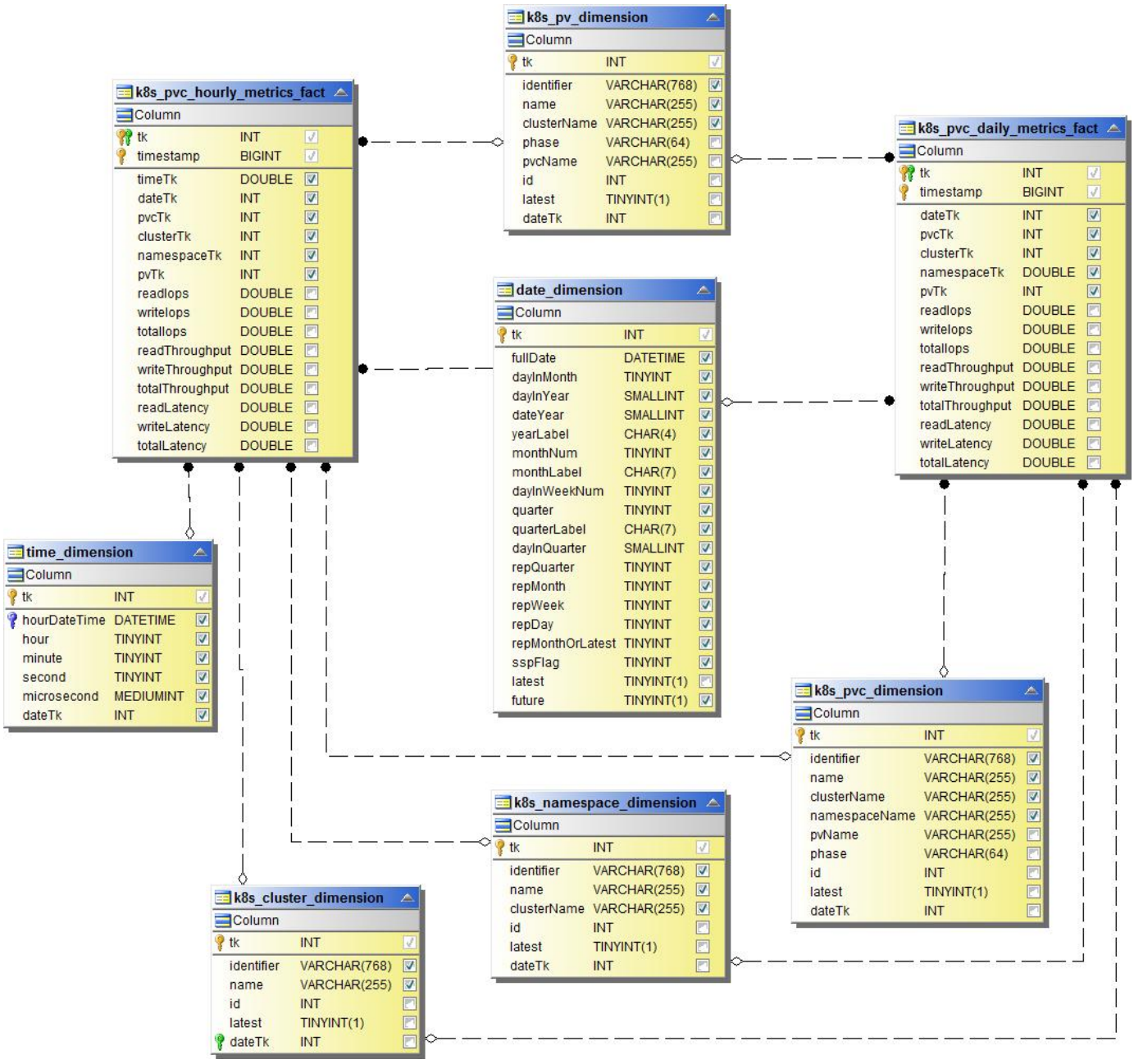
Métriques de l’espace de noms Kubernetes



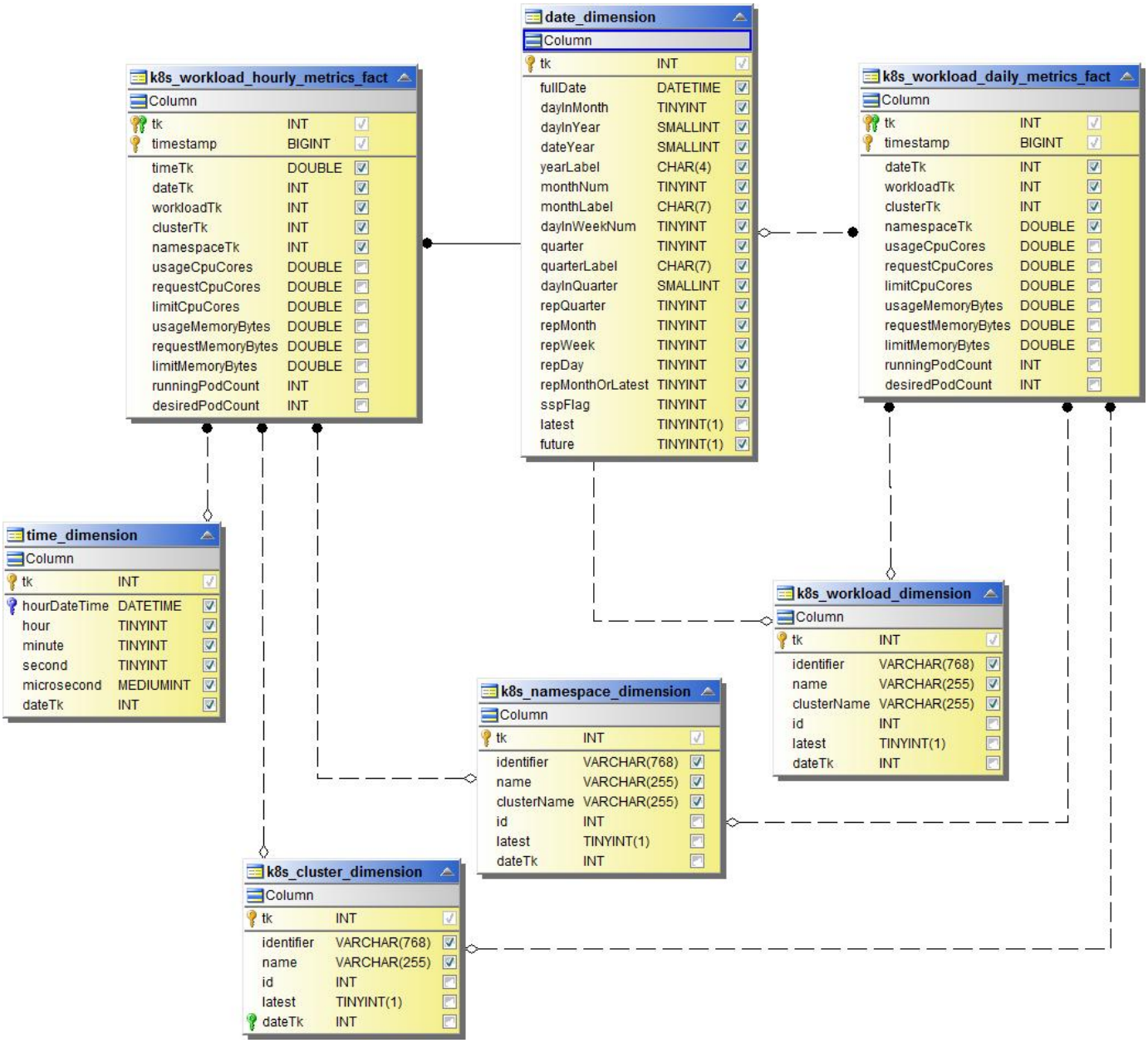
Métriques des nœuds Kubernetes



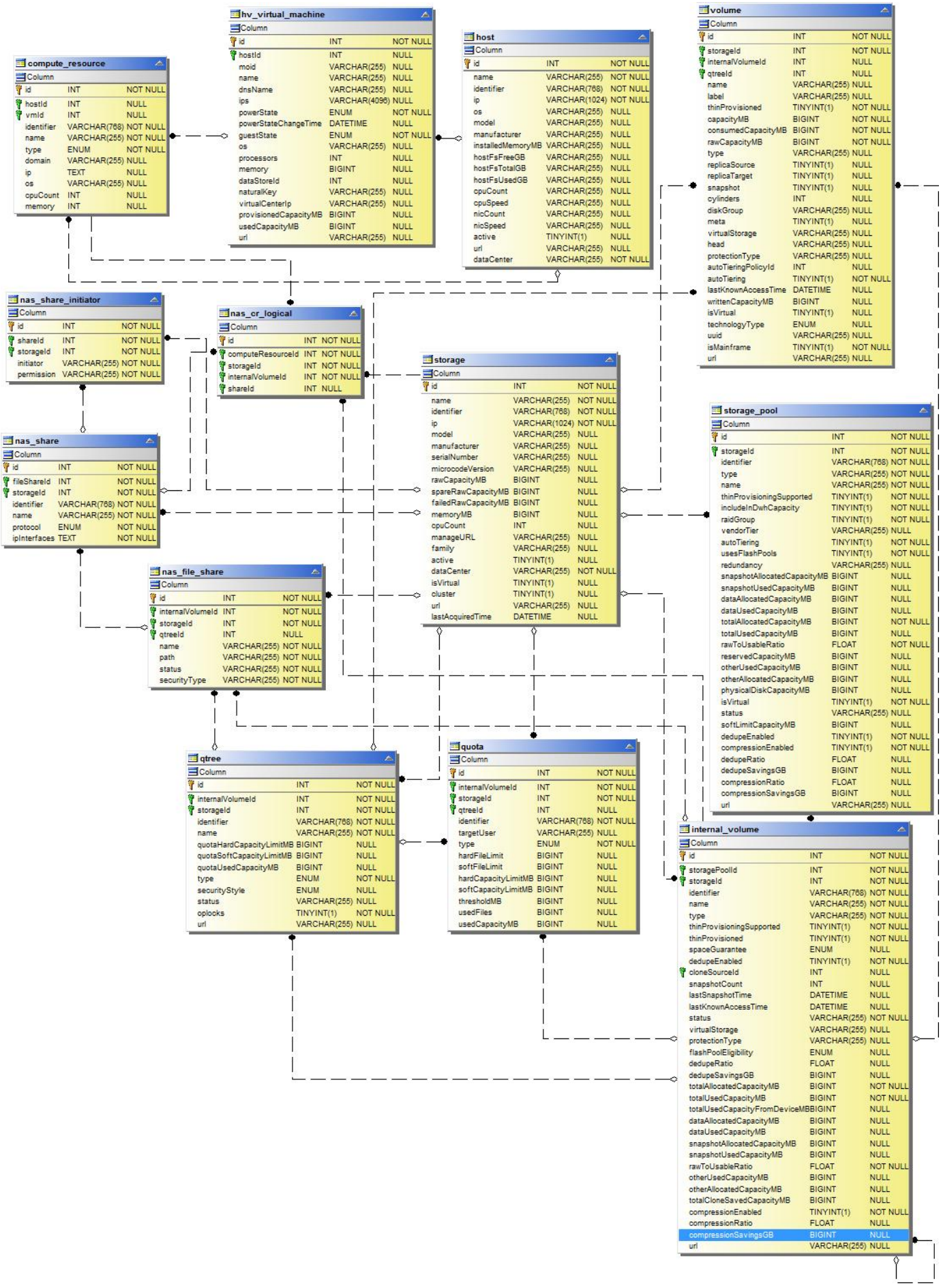
Métriques PVC Kubernetes Fait



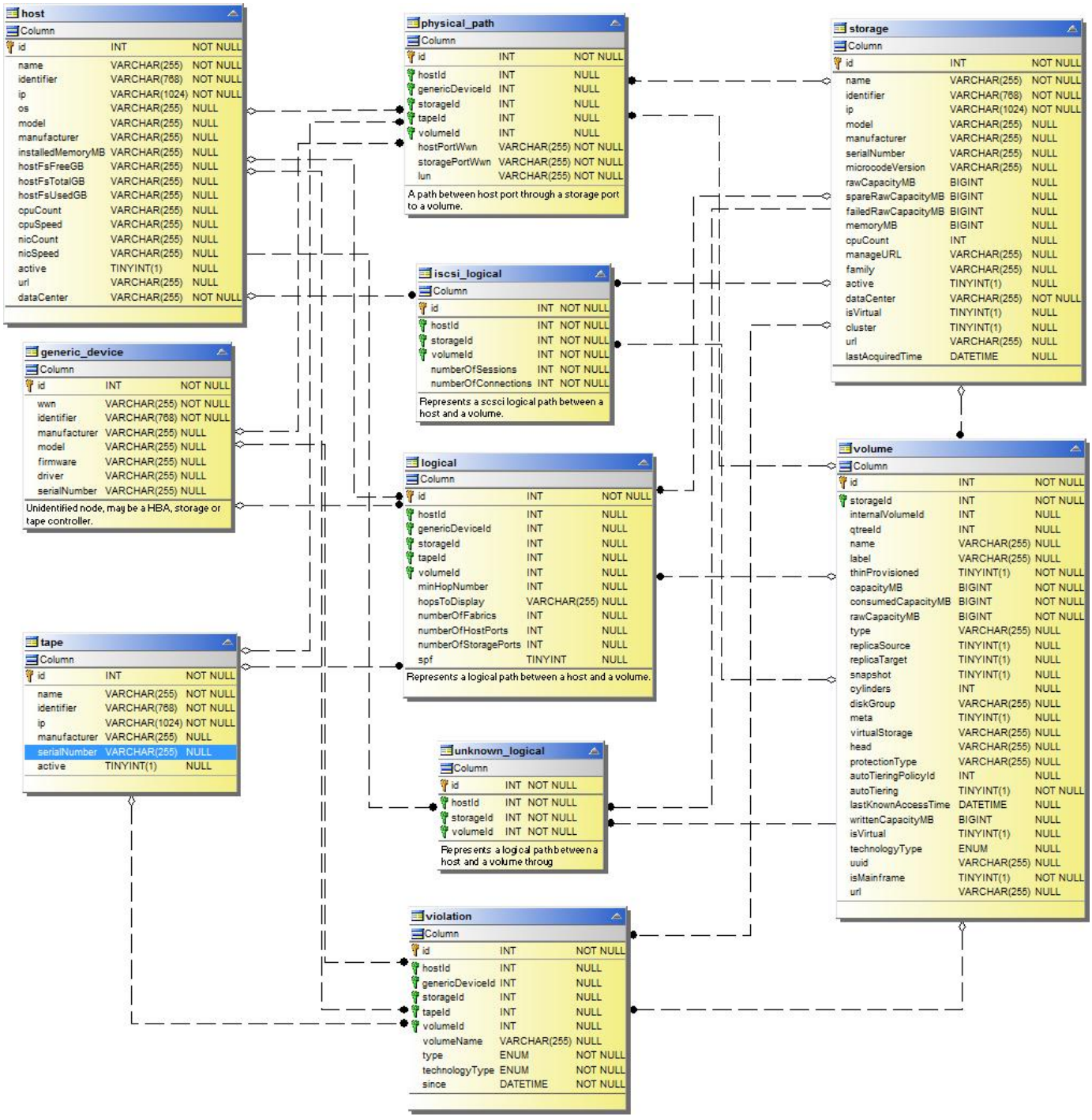
Métriques de charge de travail Kubernetes Fait


k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

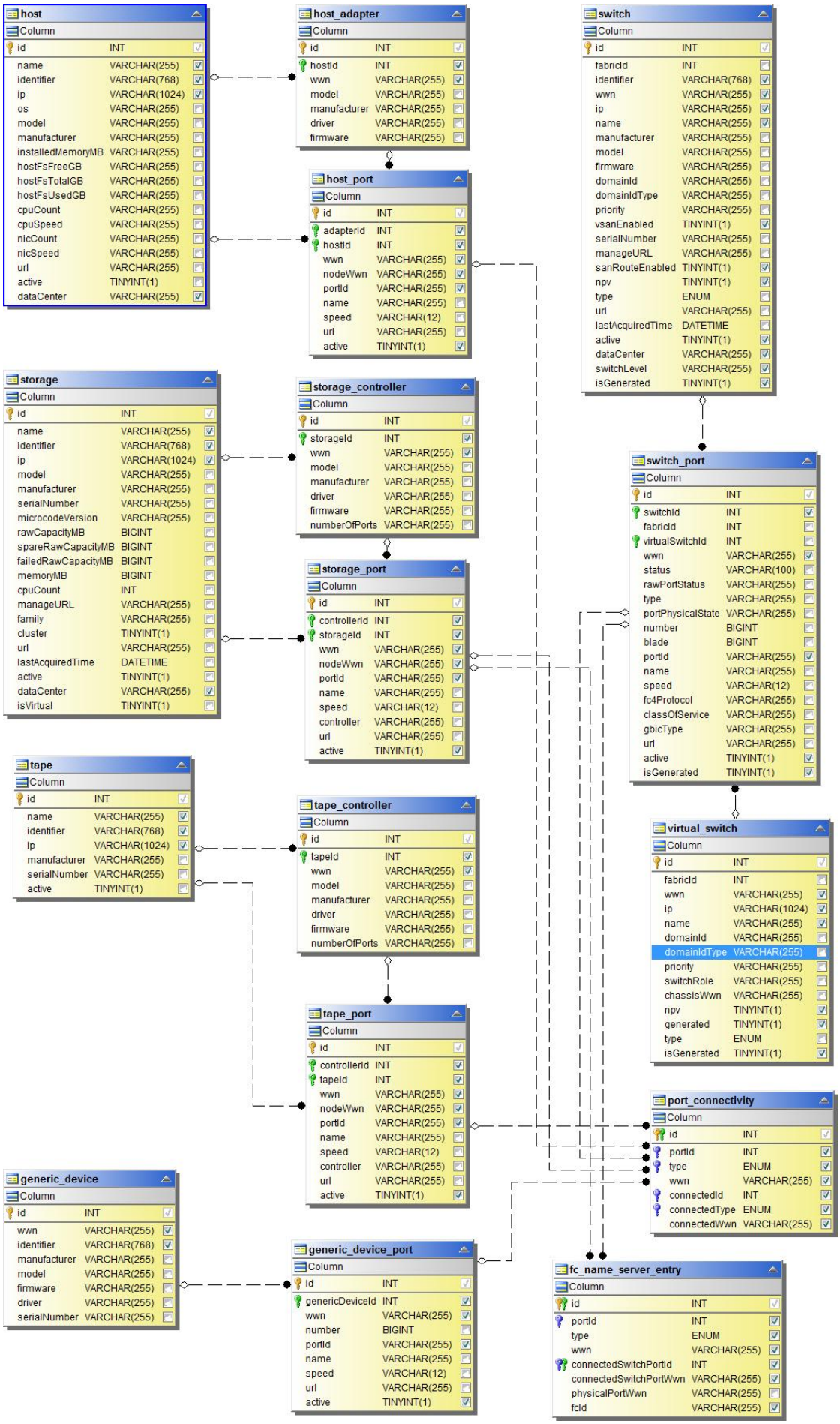
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDwhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL

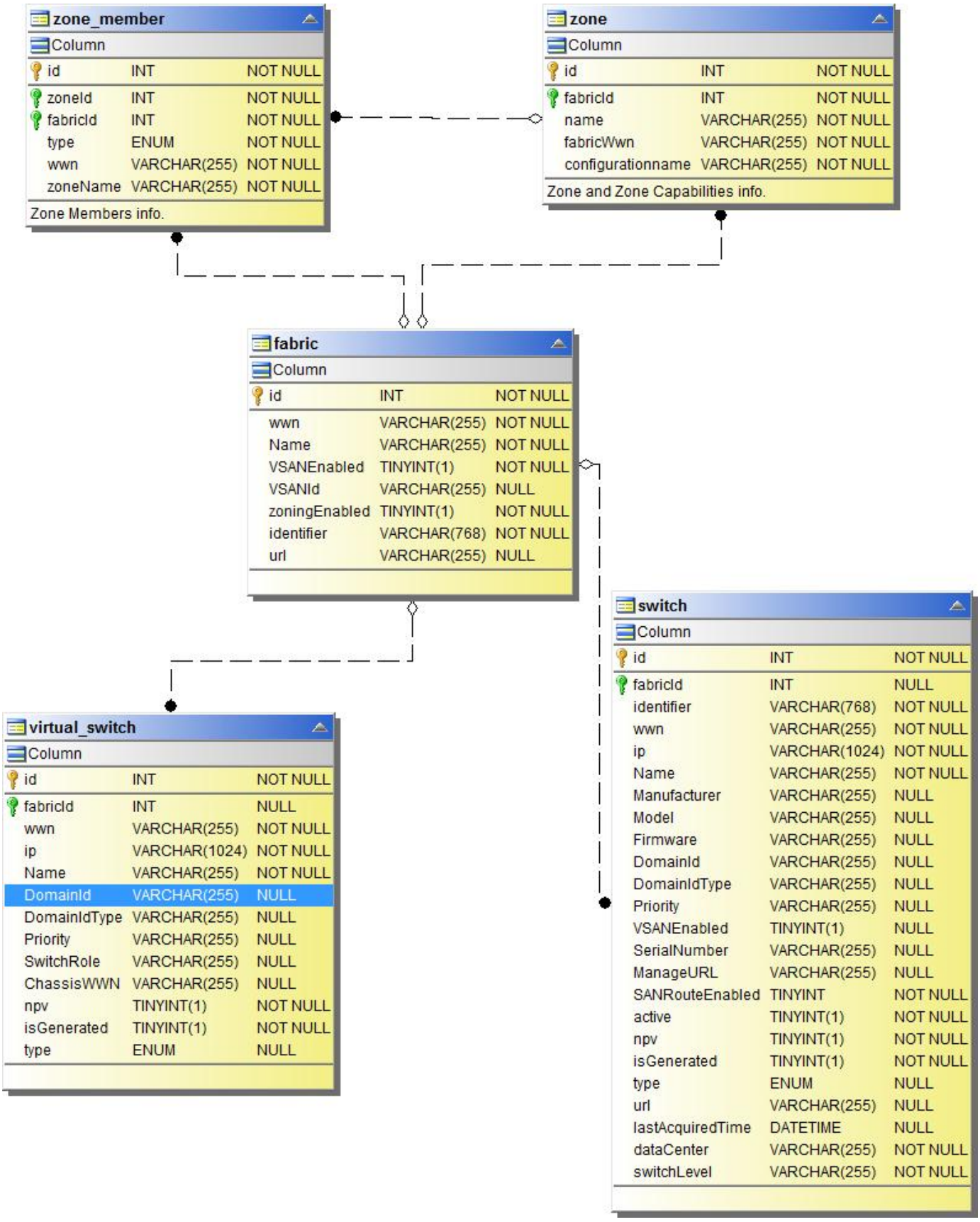
Chemins et violations



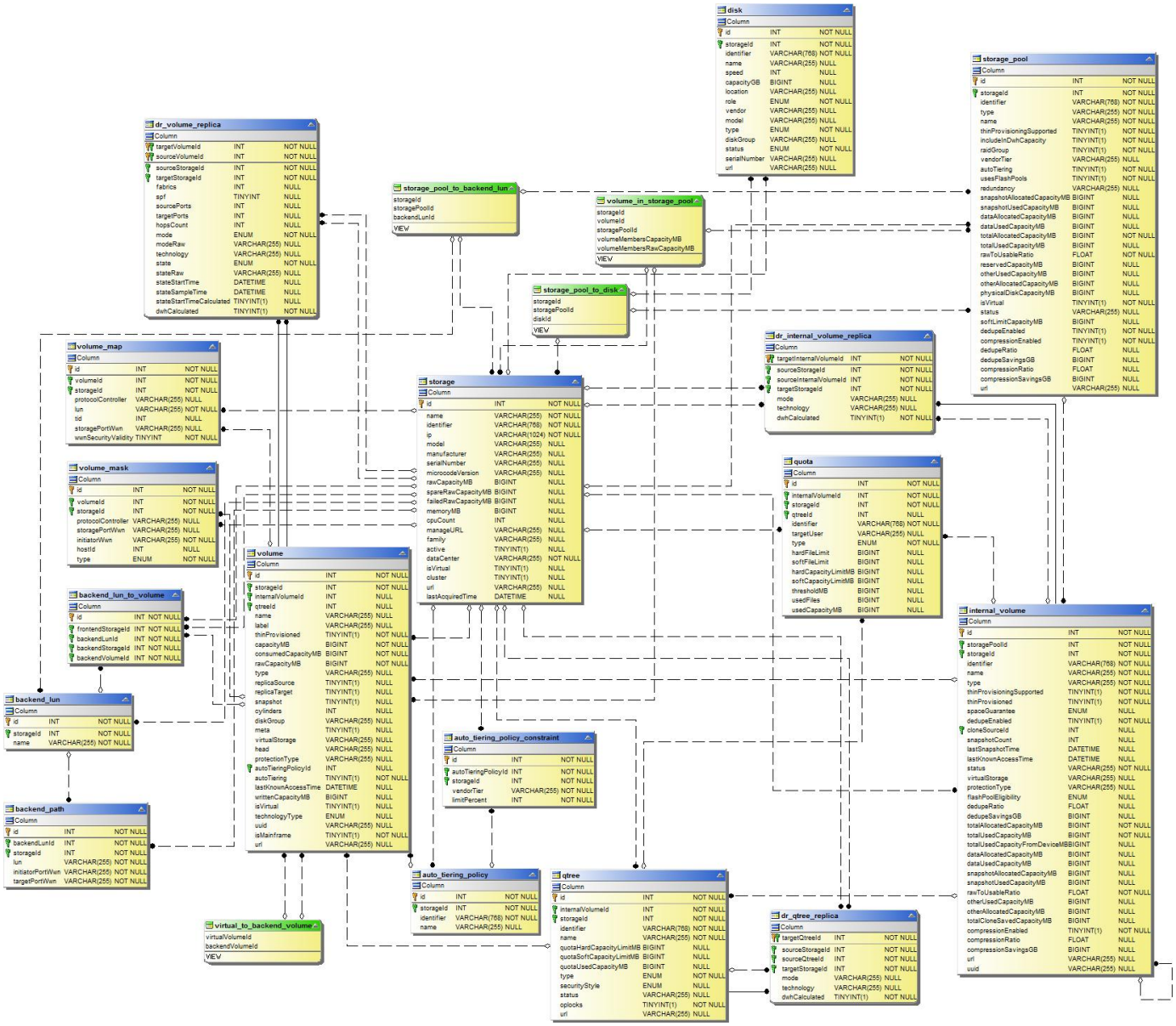
Connectivité portuaire


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(1024)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

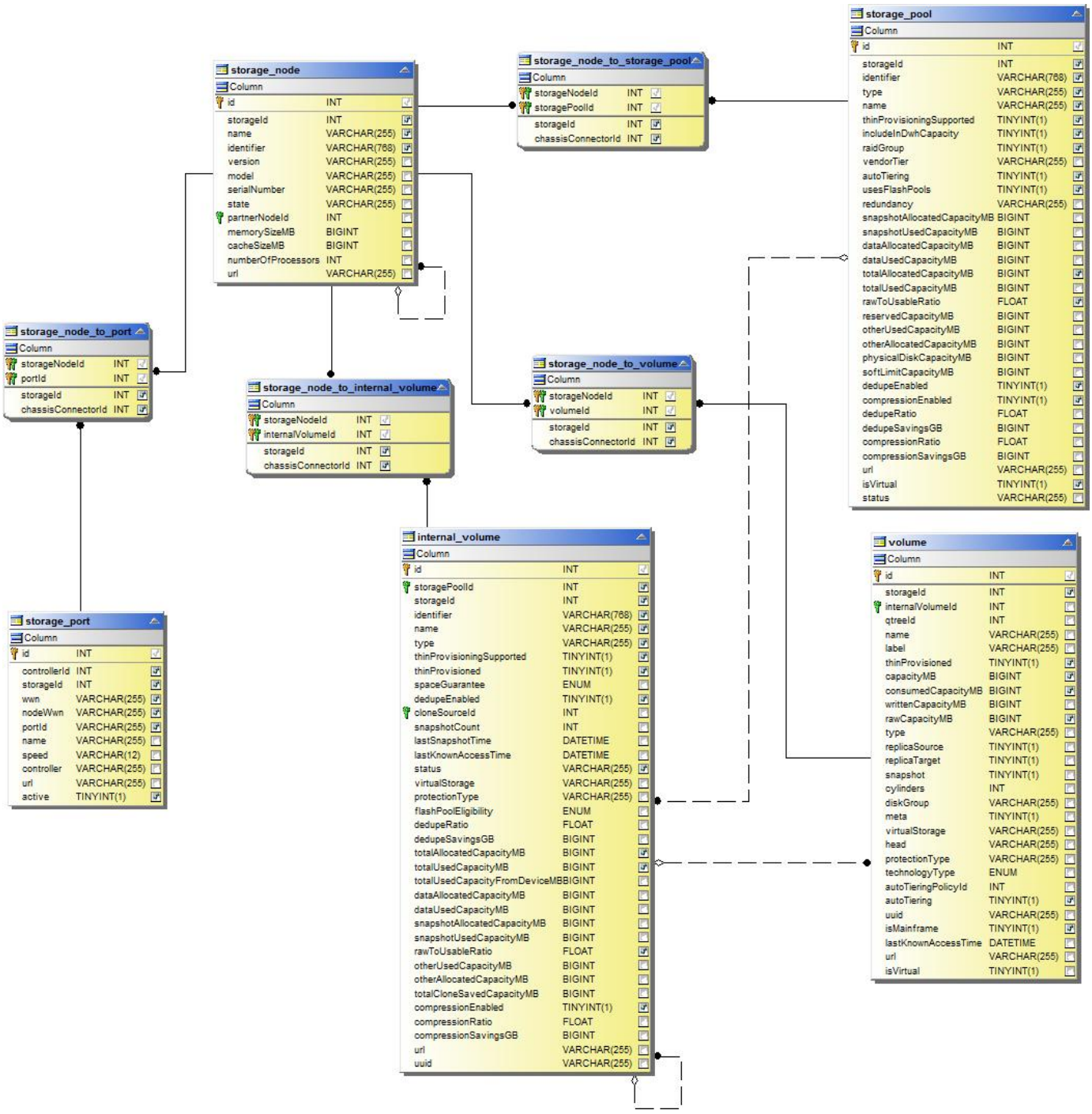
Tissu SAN


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL

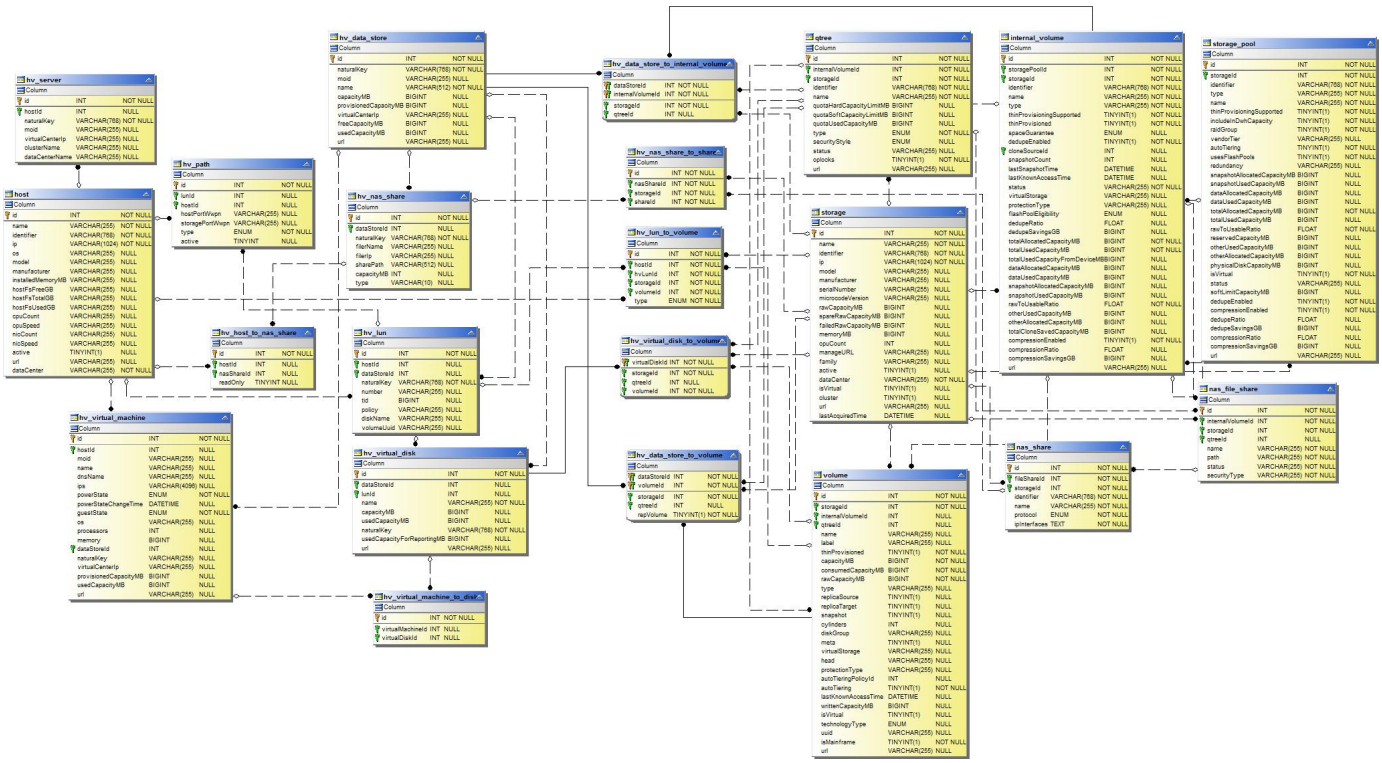
Stockage



Nœud de stockage



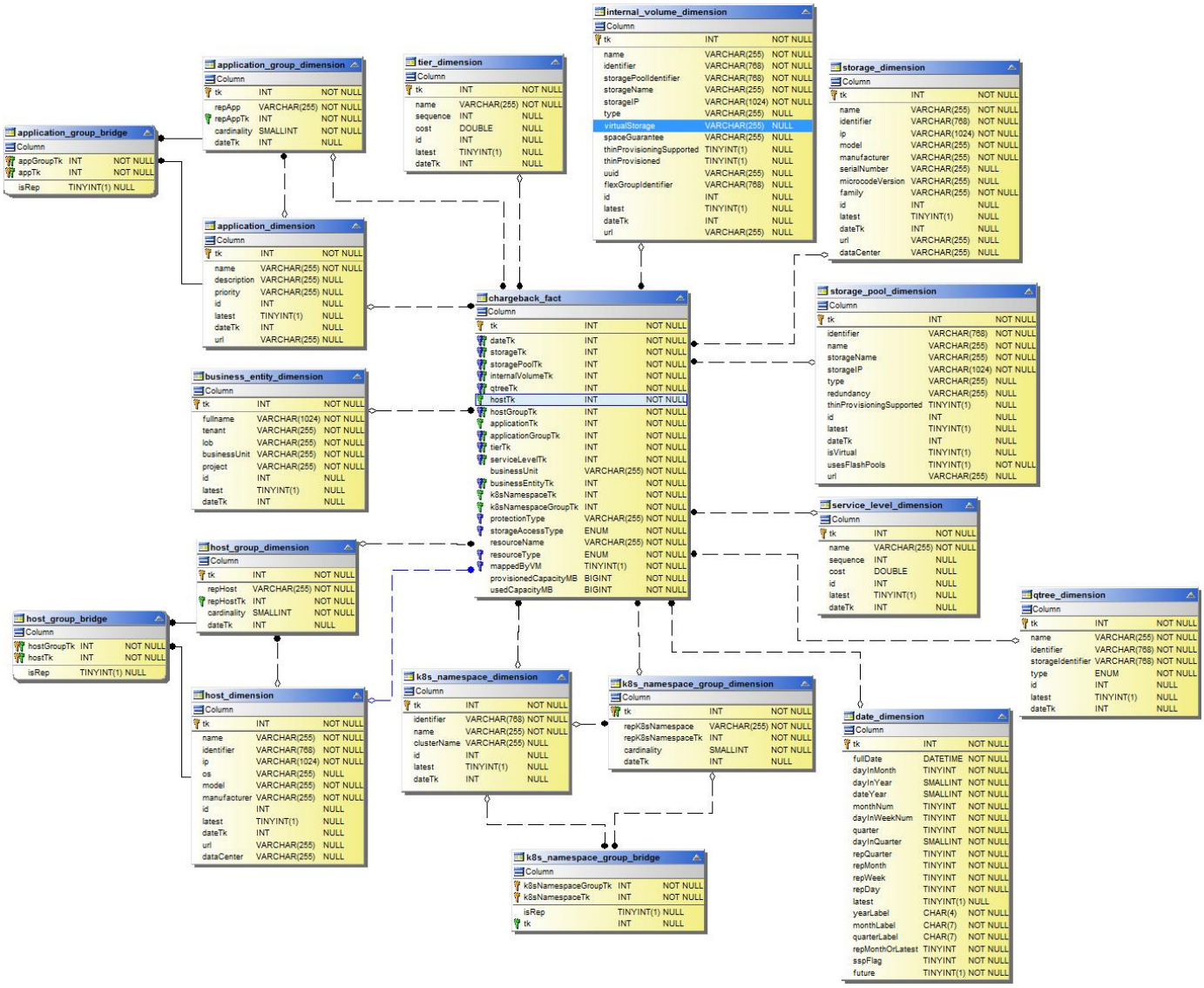
Machine virtuelle



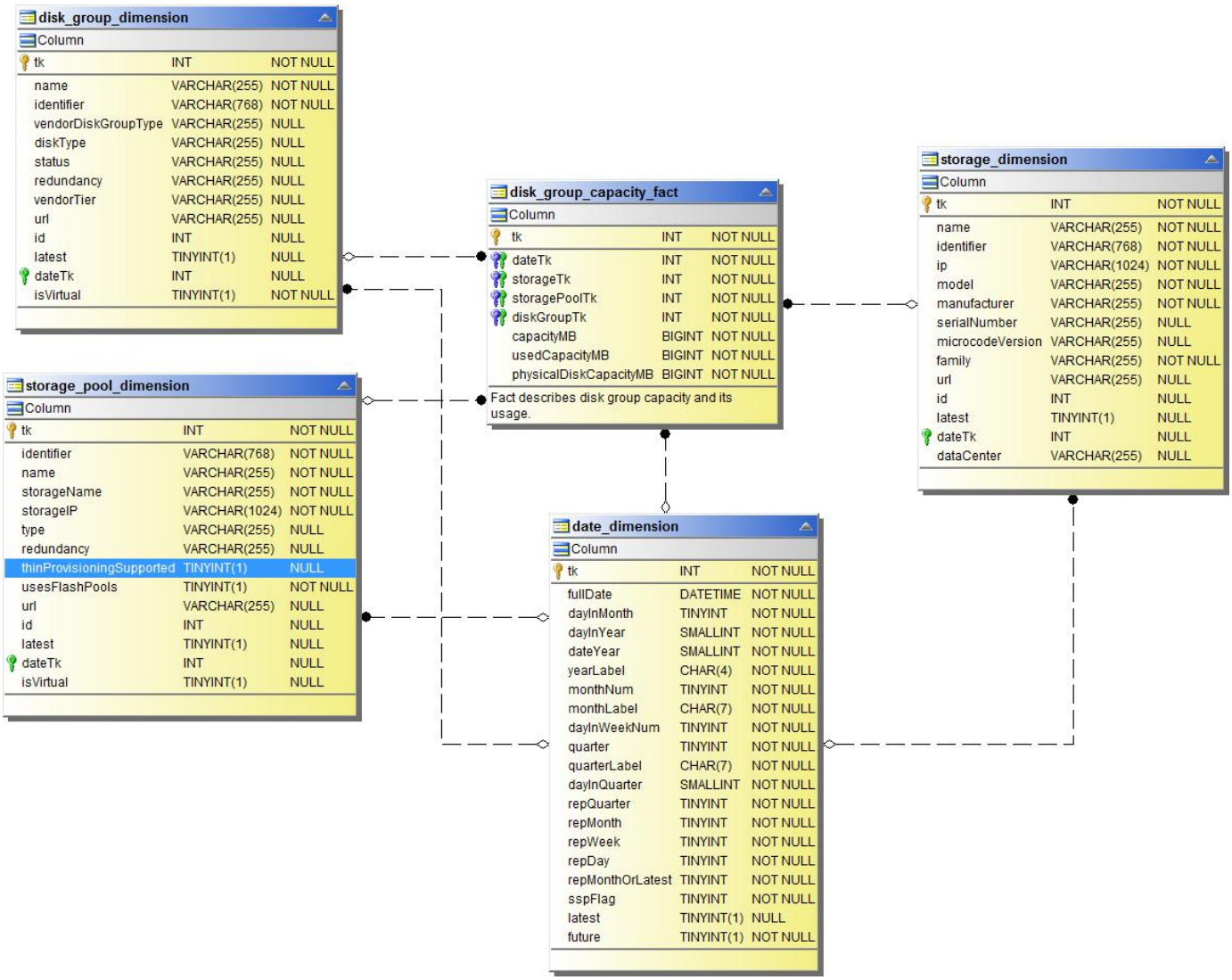
Datamart de capacité

Les images suivantes décrivent la capacité du datamart.

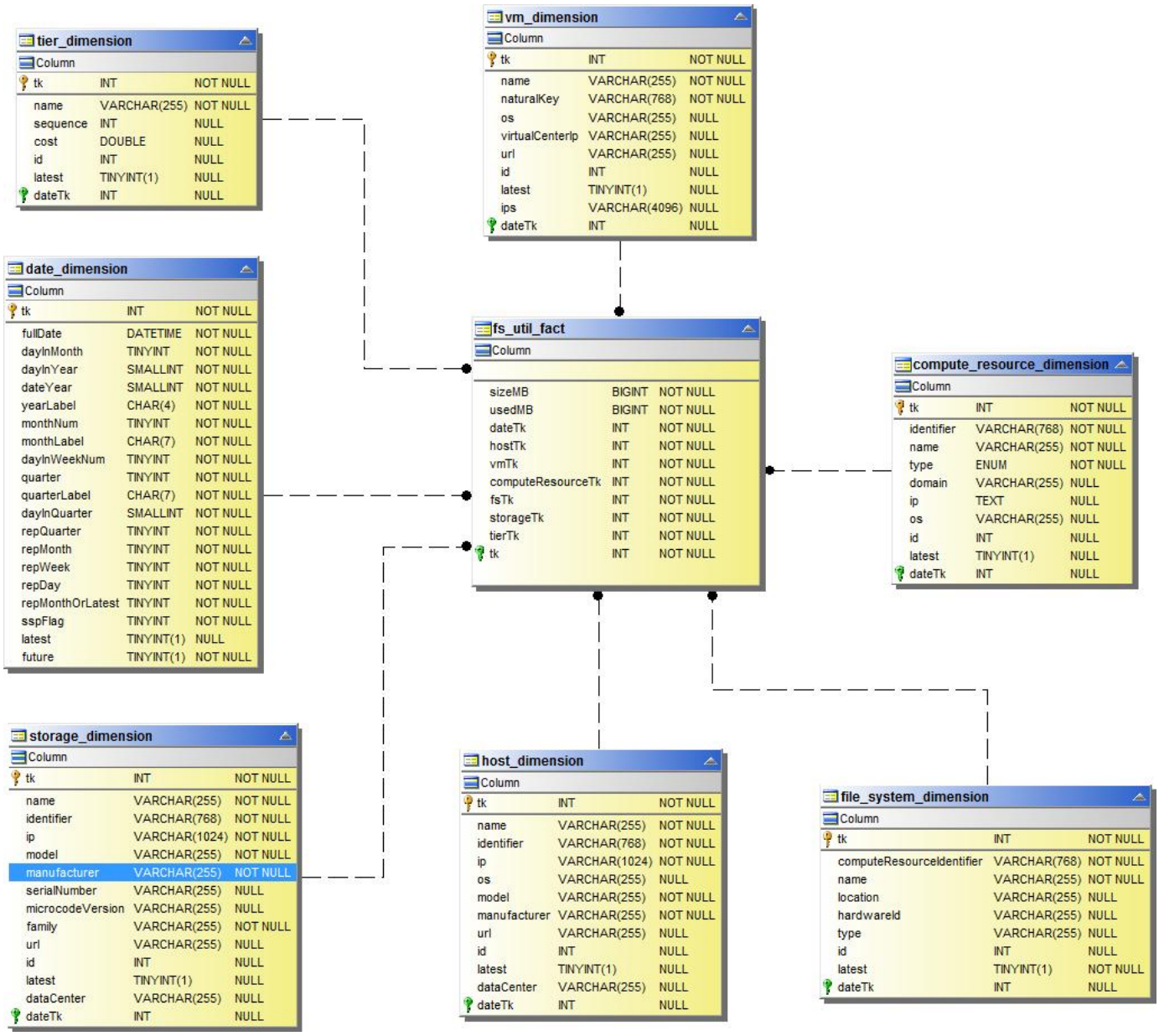
Rétrofacturation



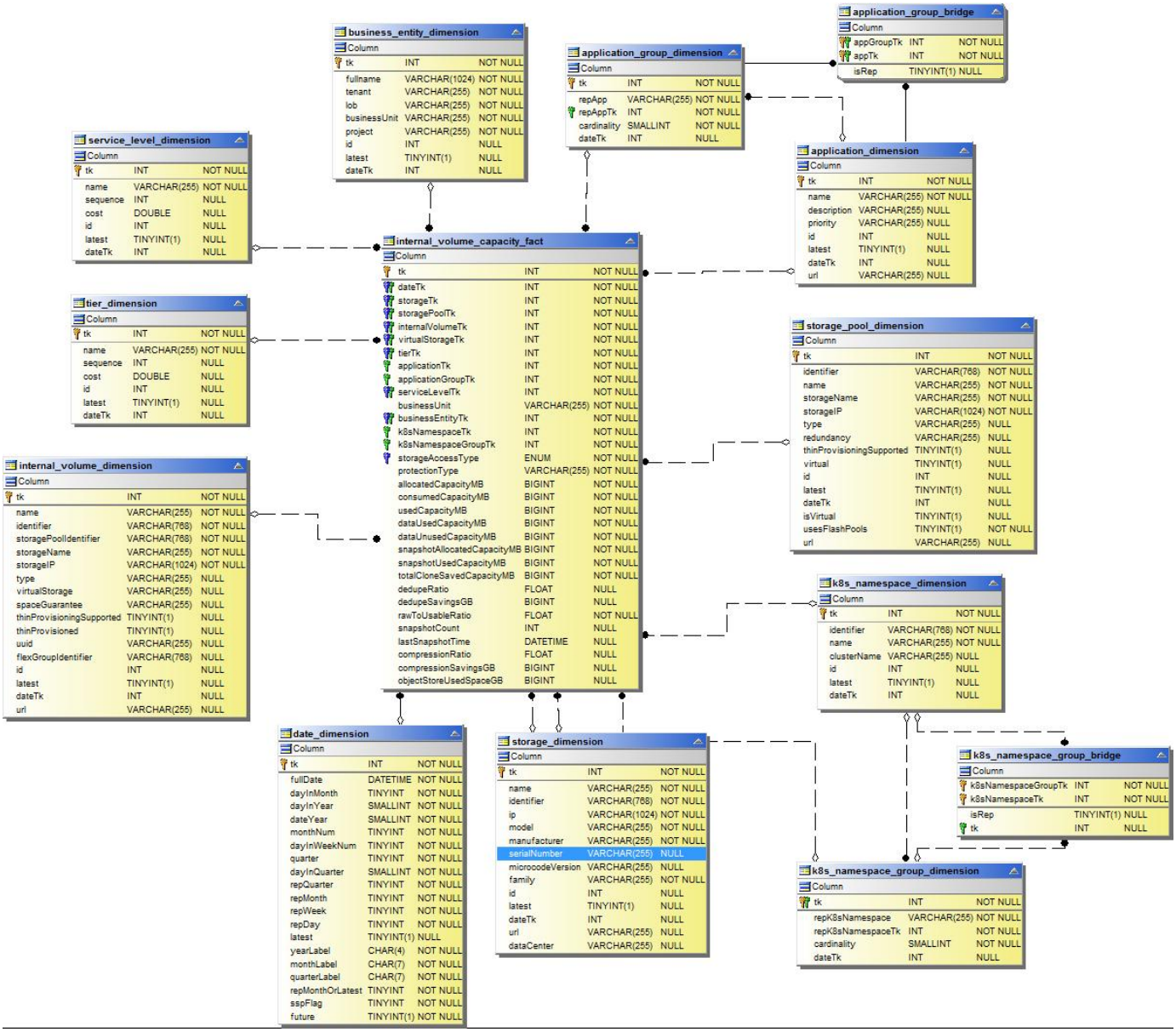
Capacité du groupe de disques



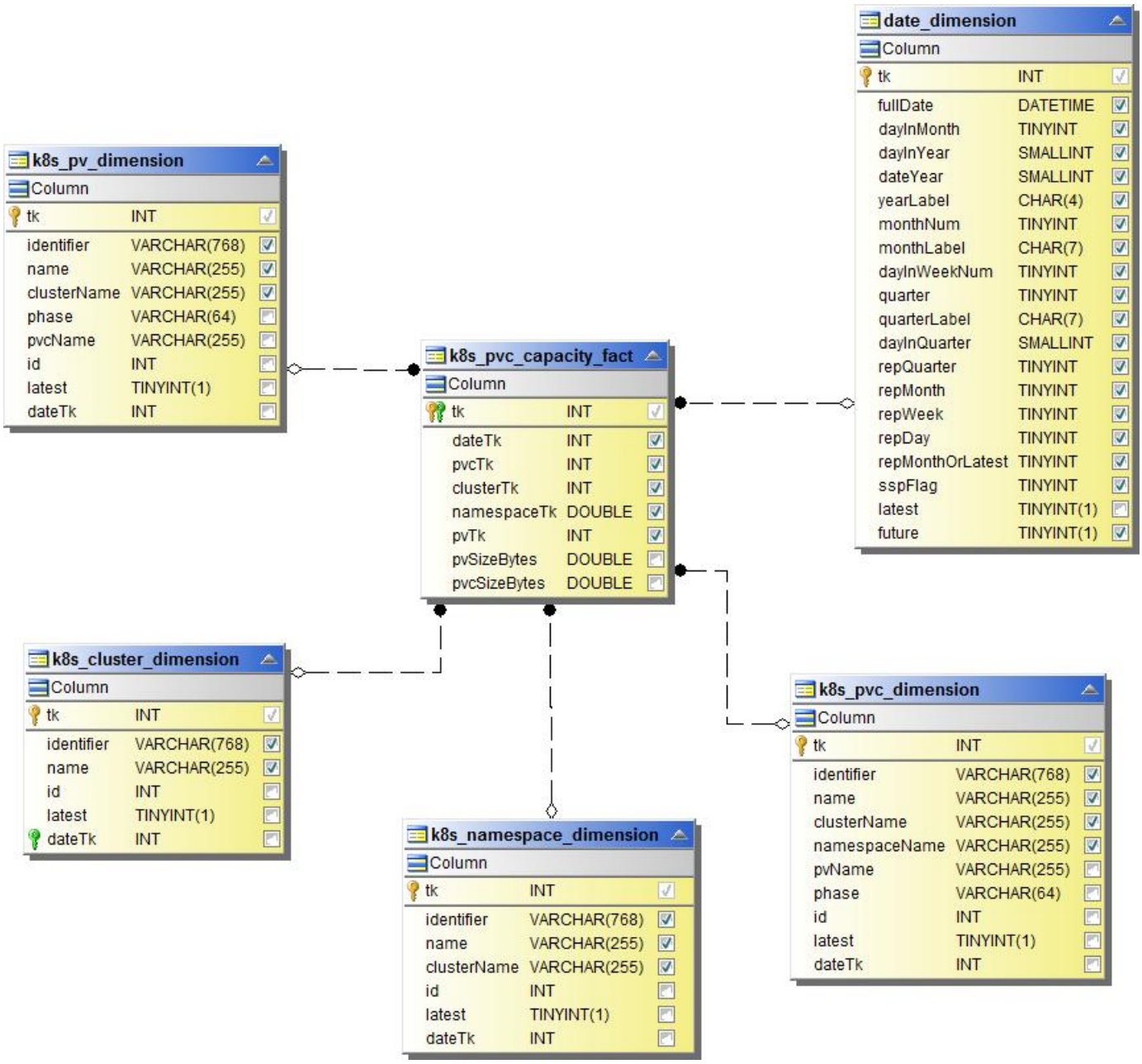
Utilisation du système de fichiers



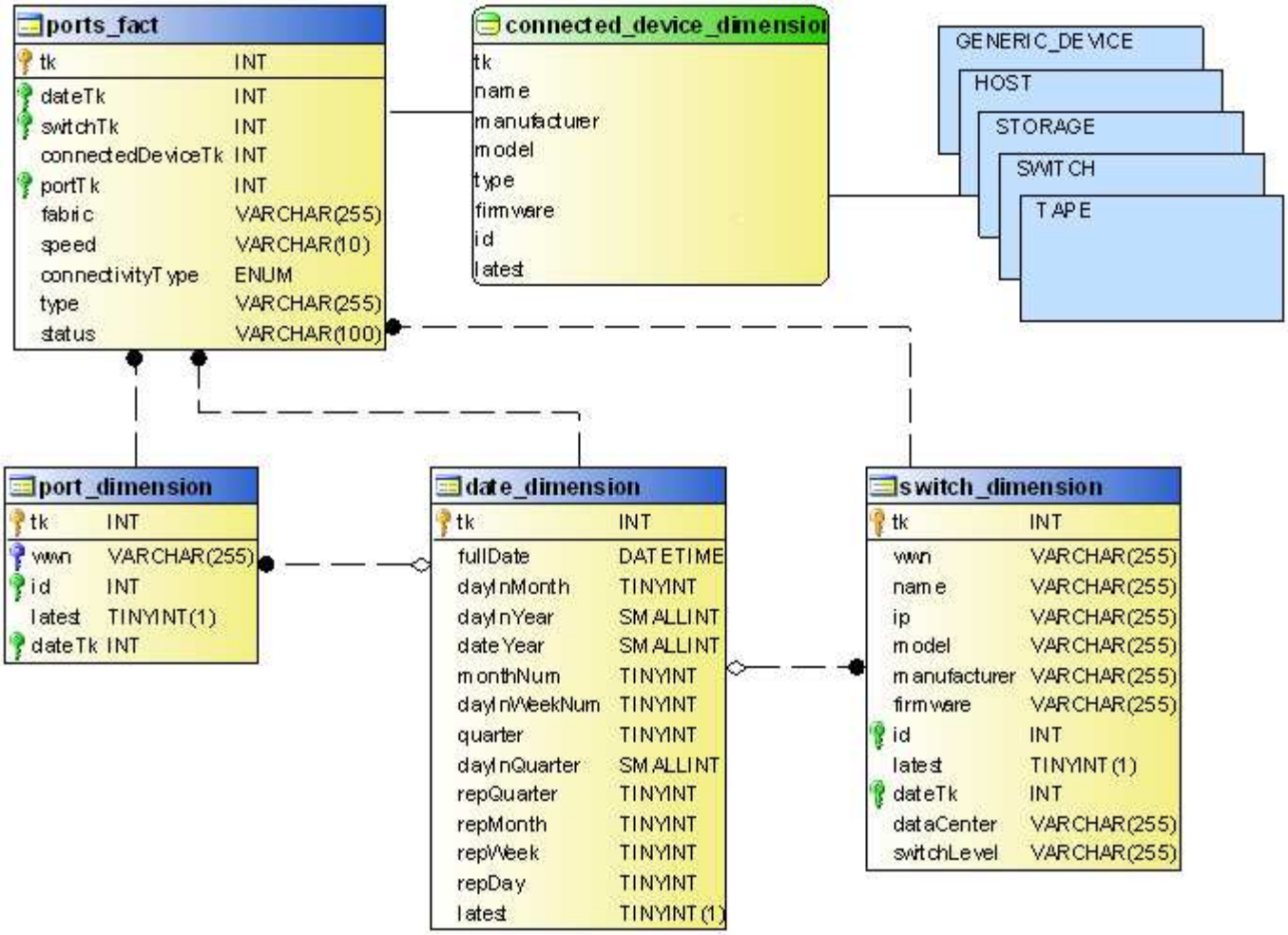
Capacité du volume interne



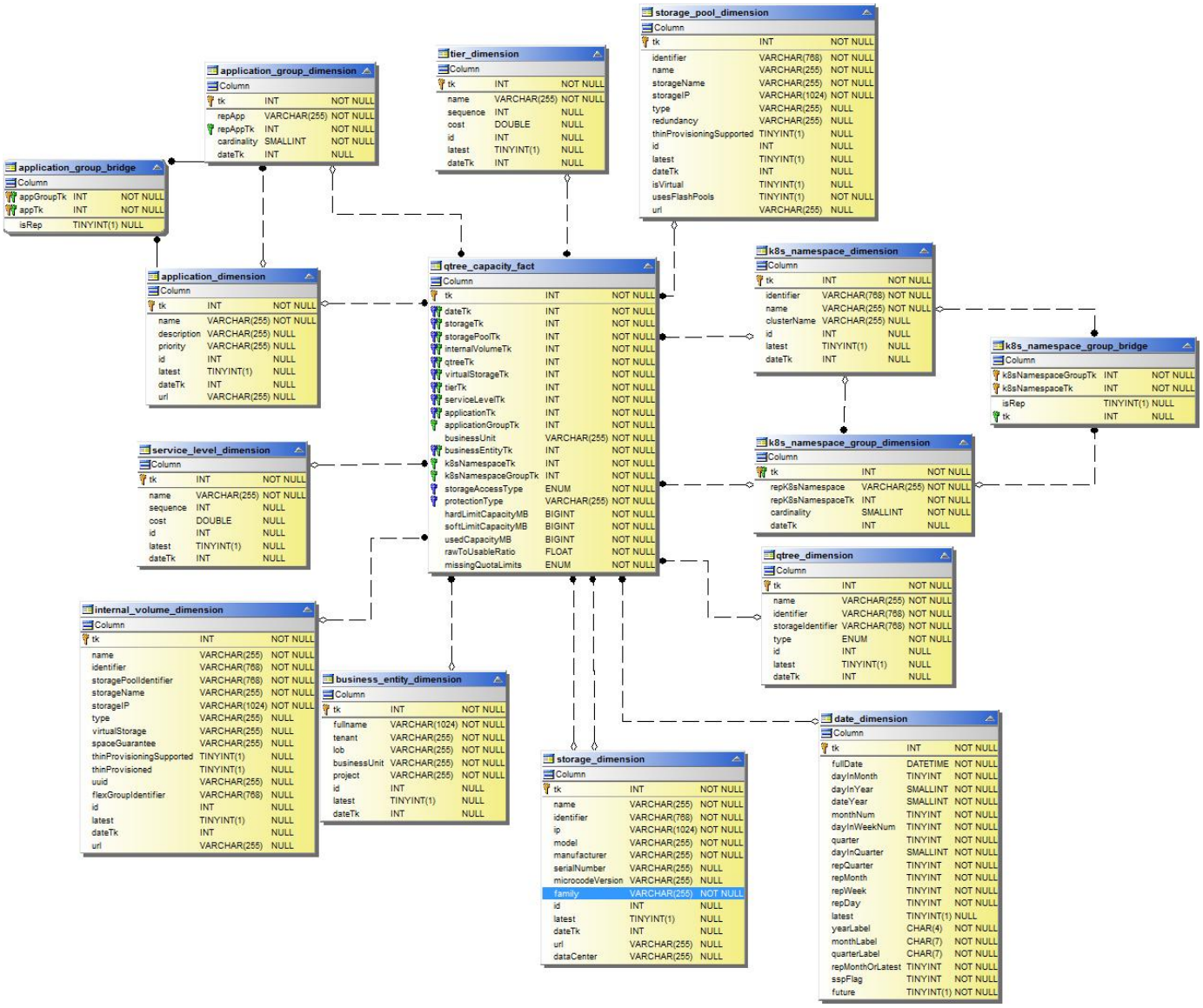
Capacité PV de Kubernetes



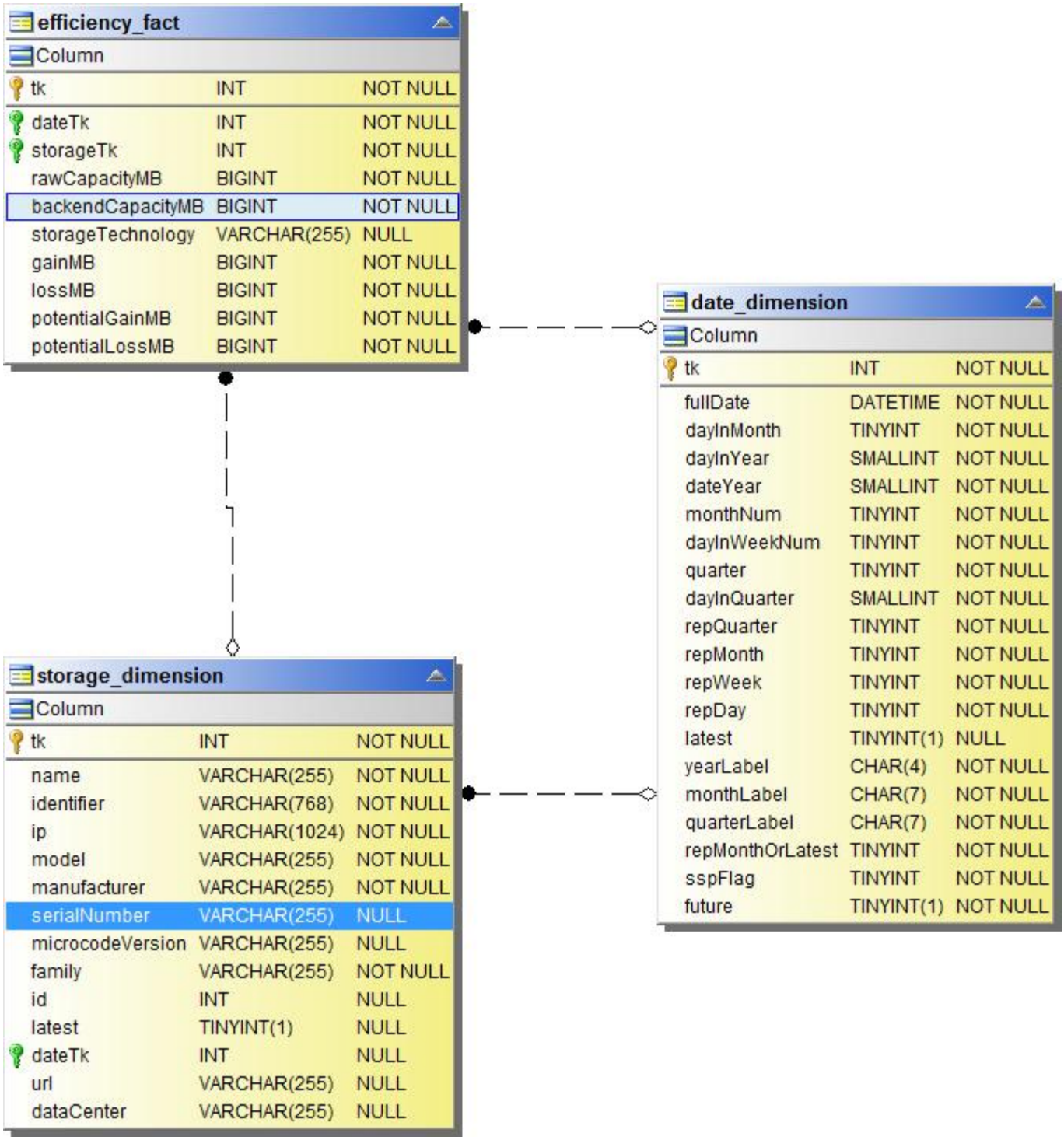
Capacité portuaire



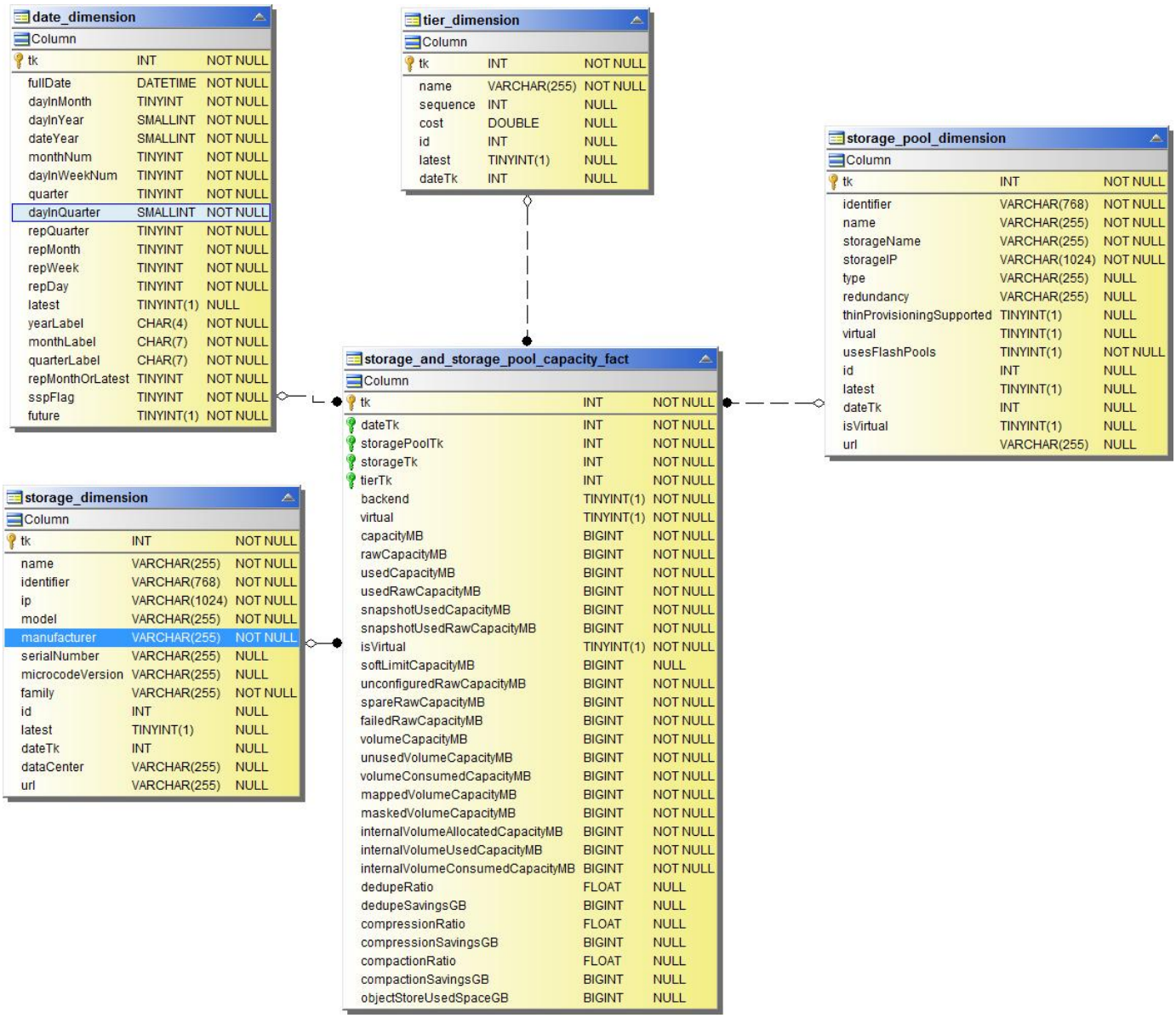
Capacité Qtree



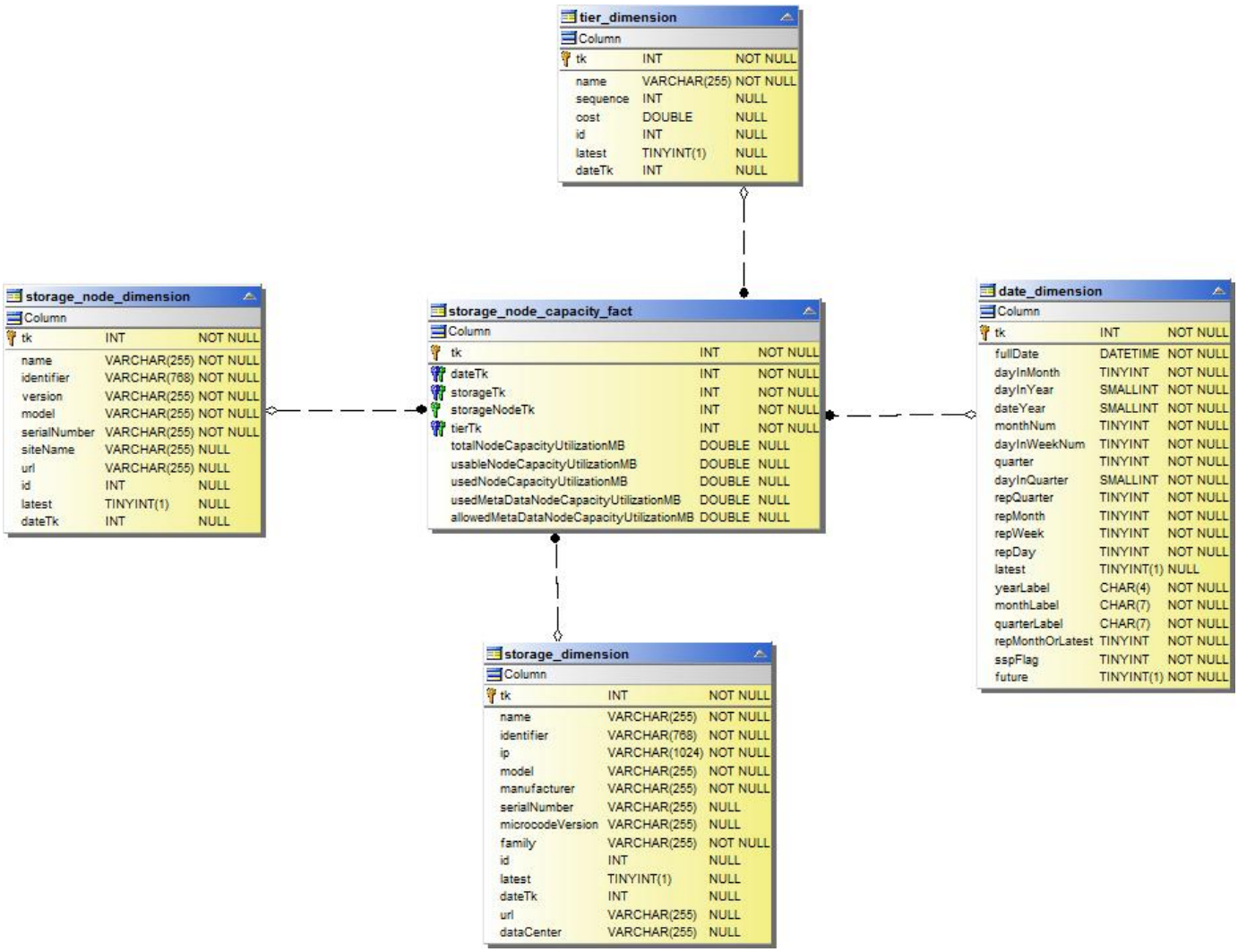
Efficacité de la capacité de stockage



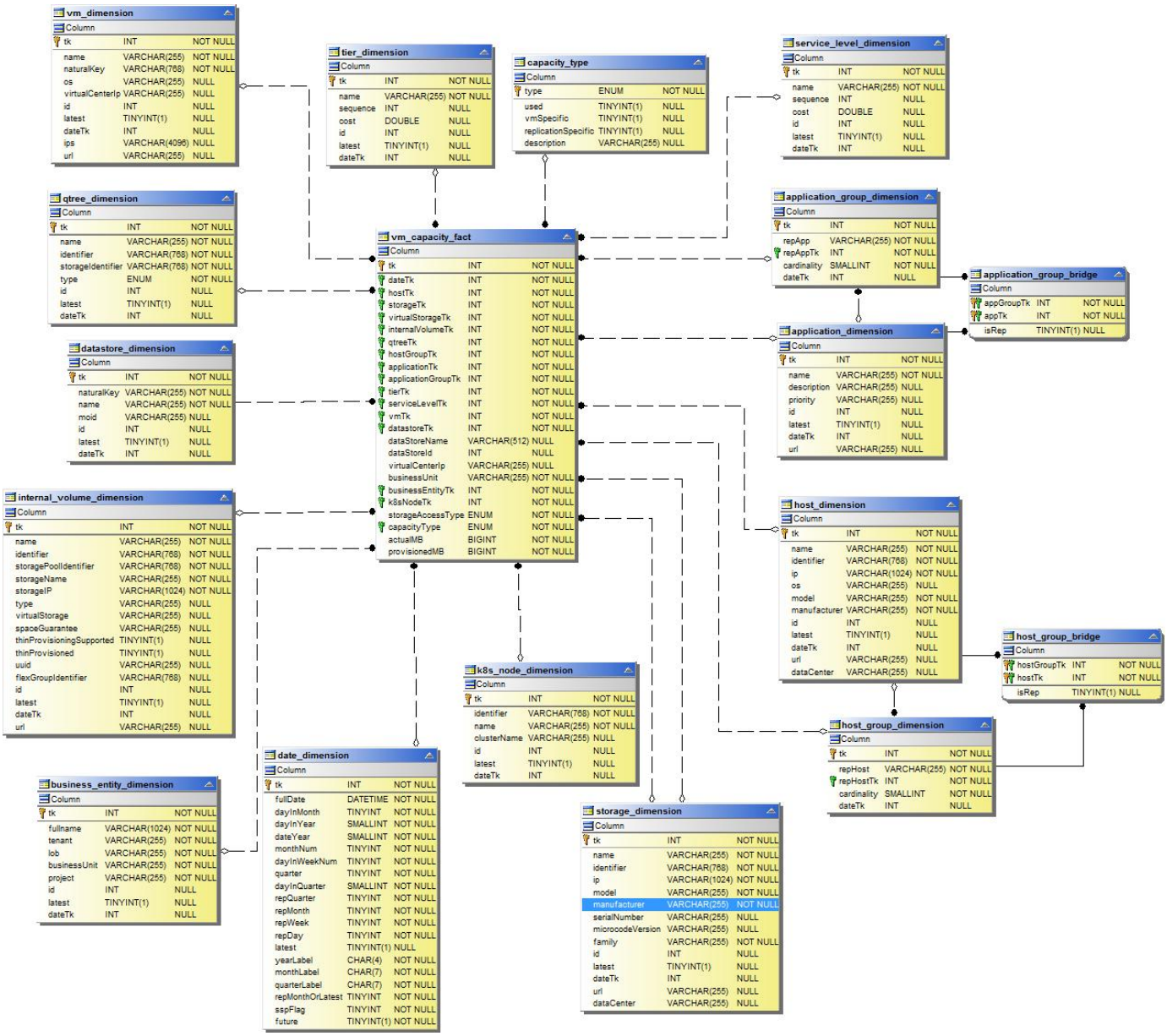
Capacité de stockage et de pool de stockage



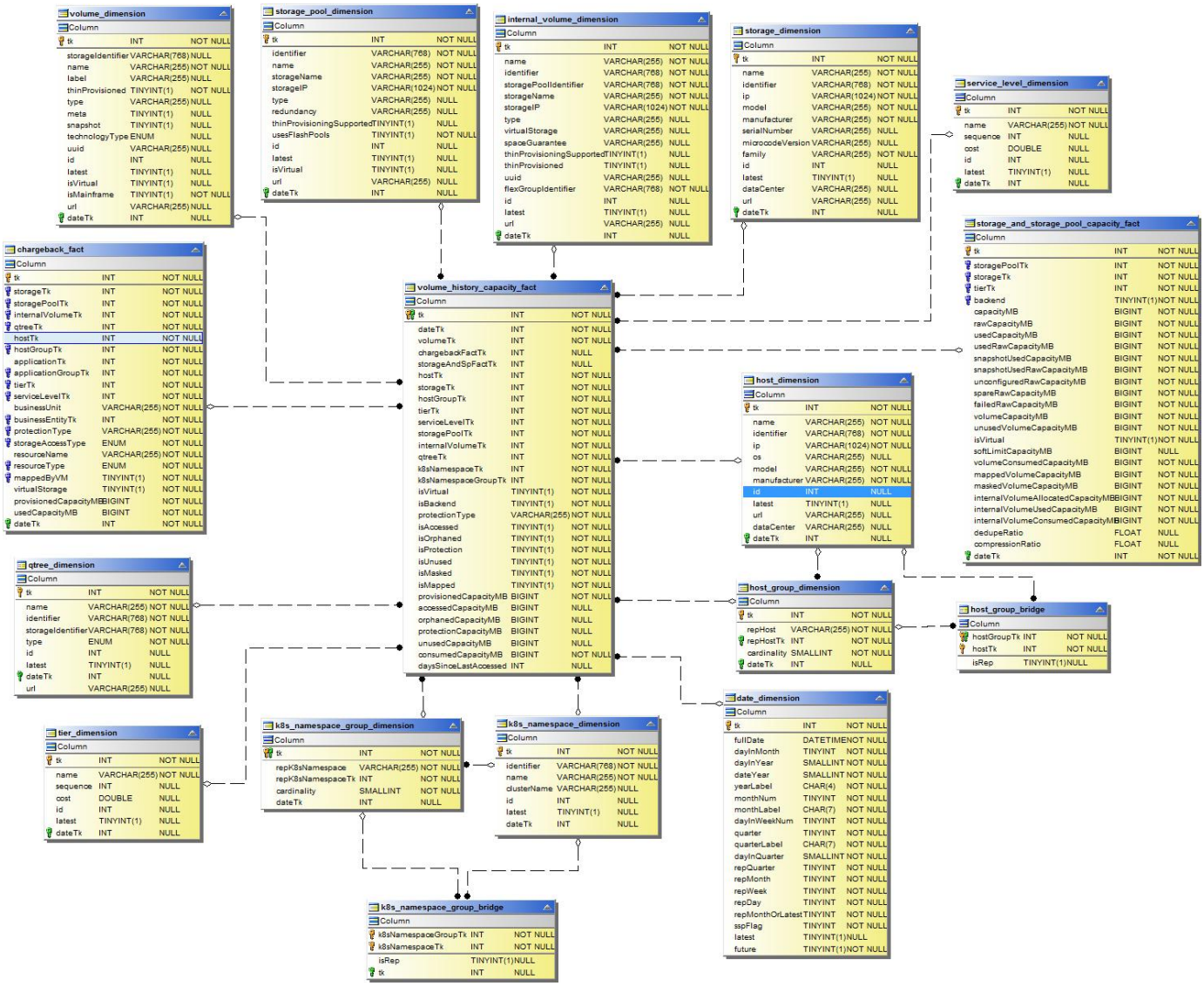
Capacité du nœud de stockage



Capacité de la machine virtuelle



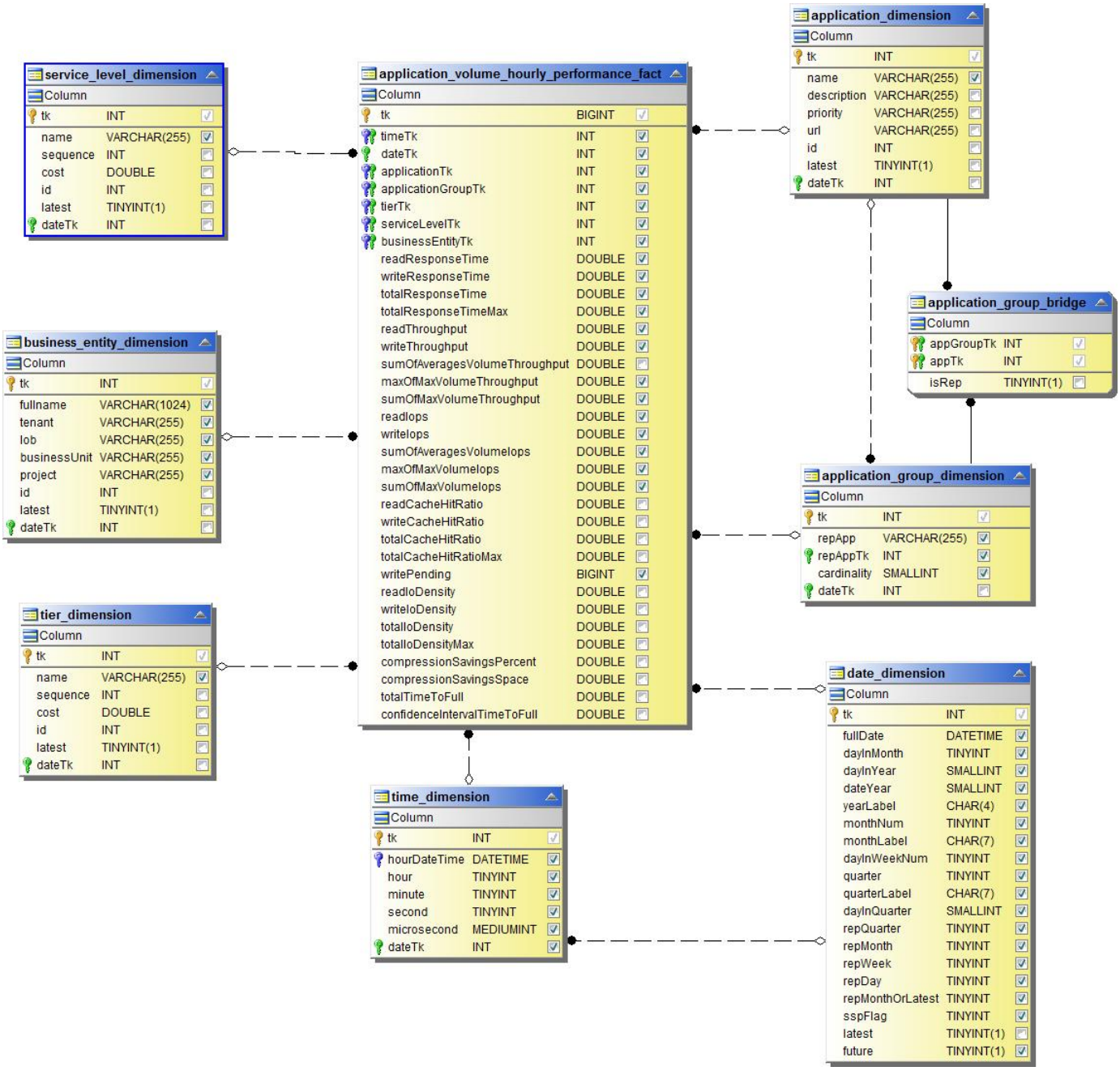
Capacité volumique



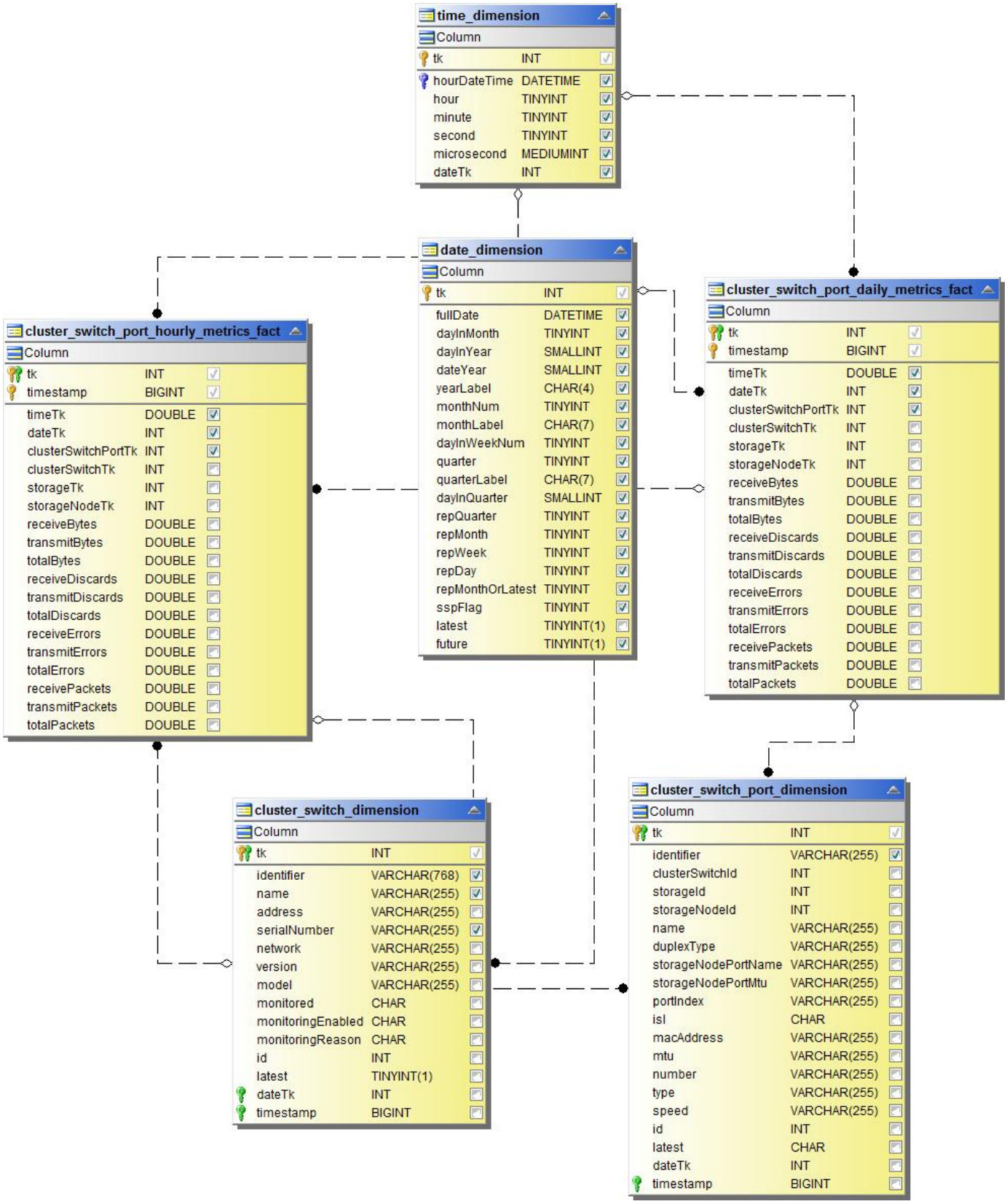
Datamart de performances

Les images suivantes décrivent les performances du datamart.

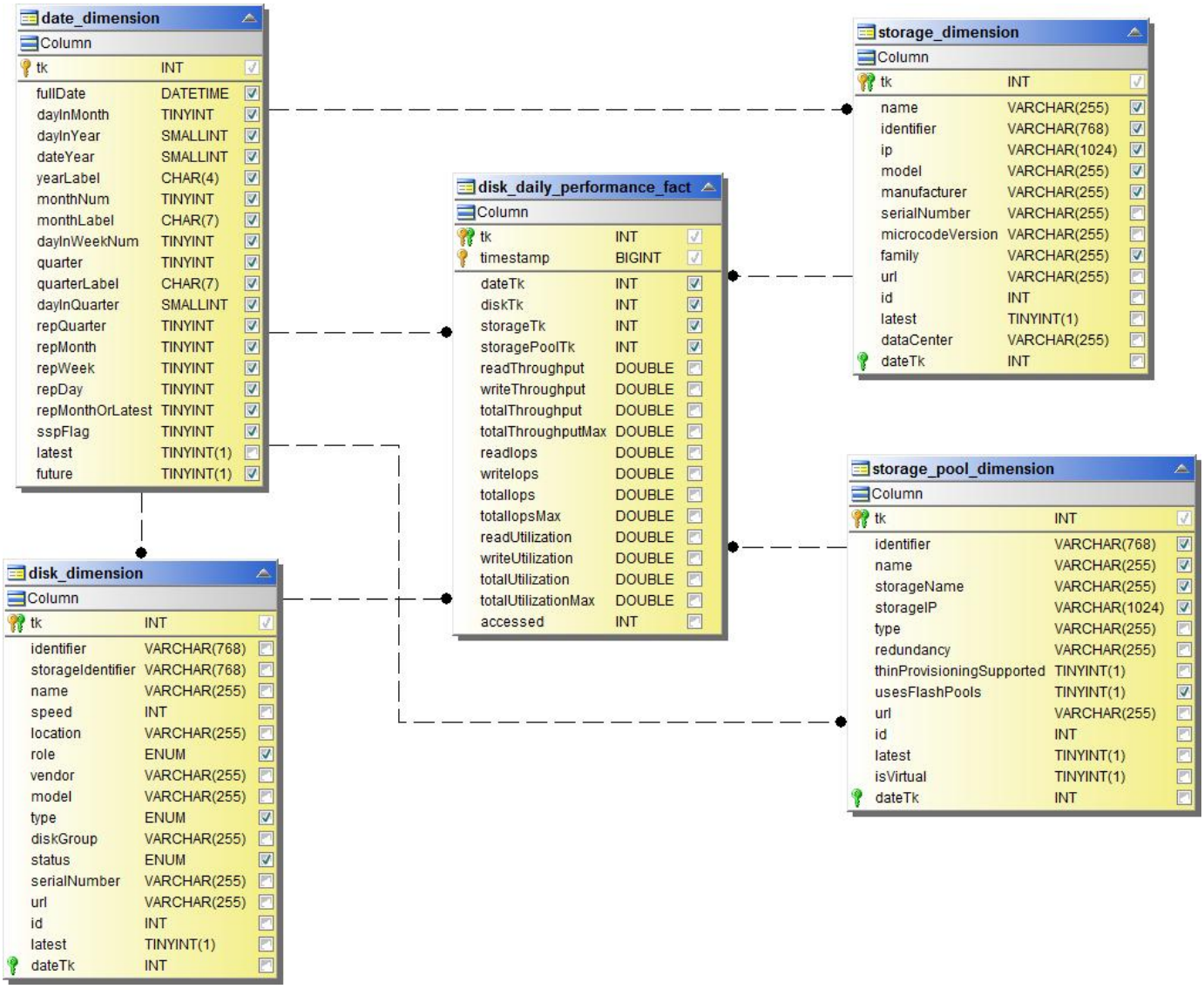
Volume d'application Performance horaire



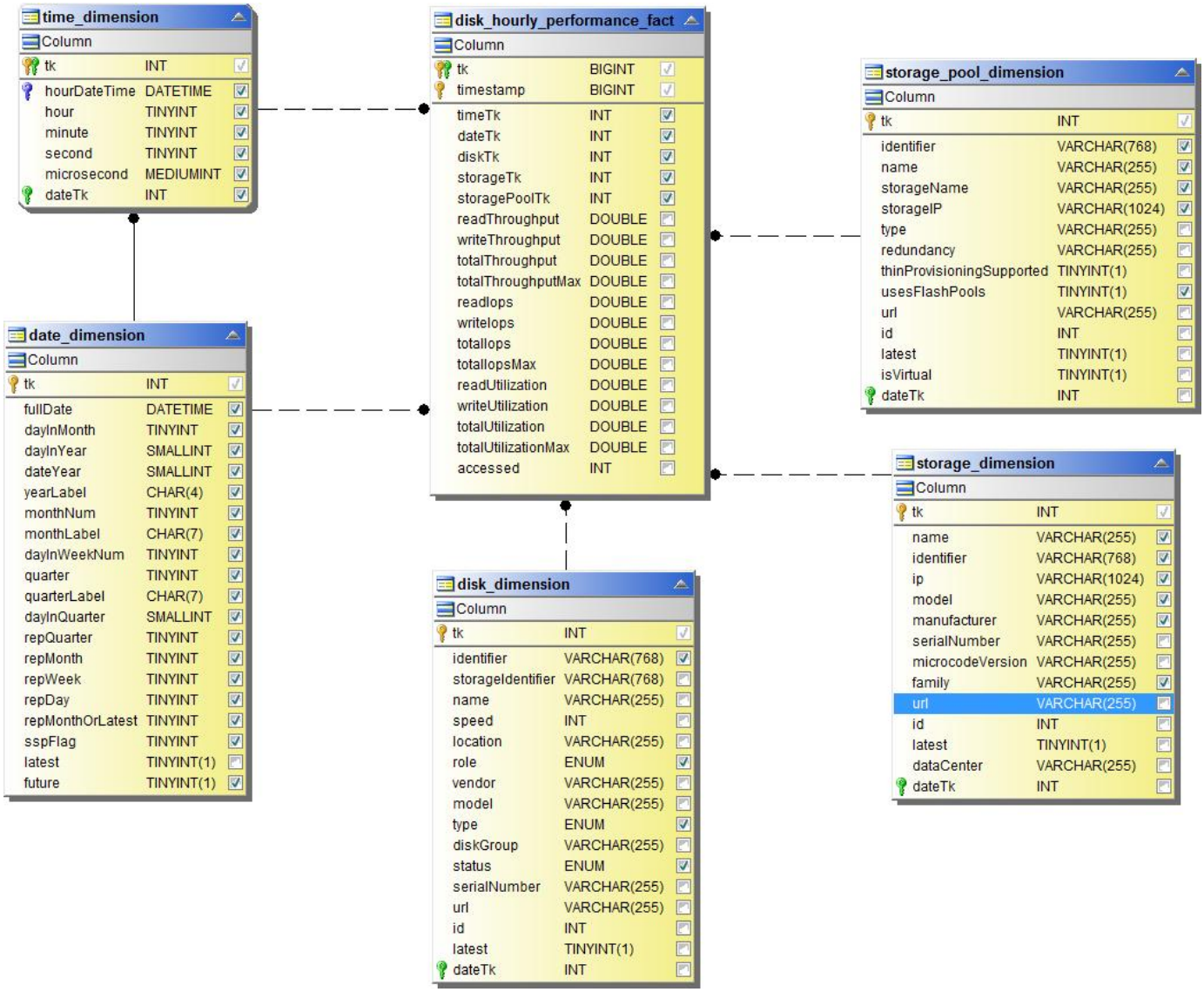
Performances du commutateur de cluster



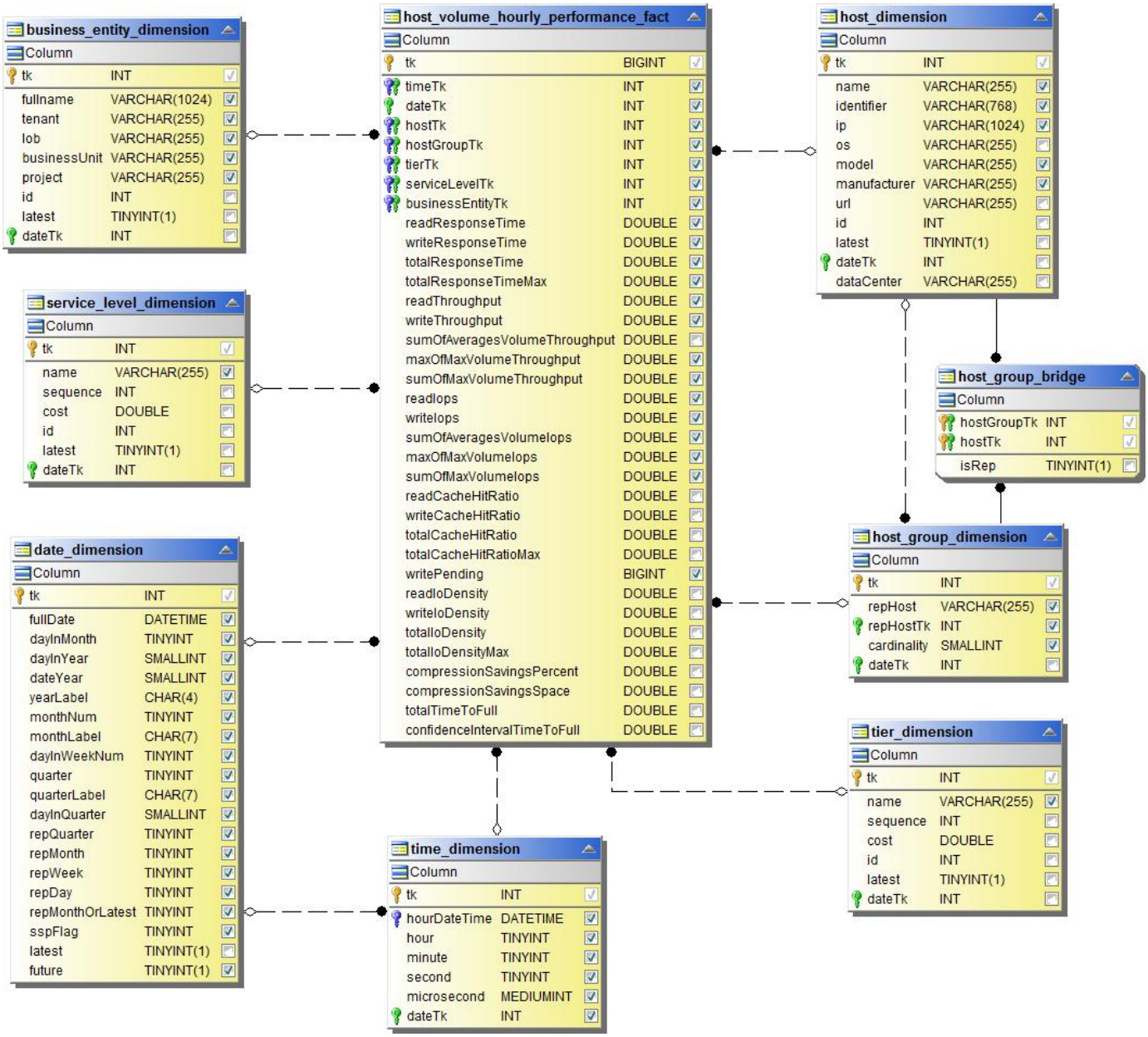
Performances quotidiennes du disque



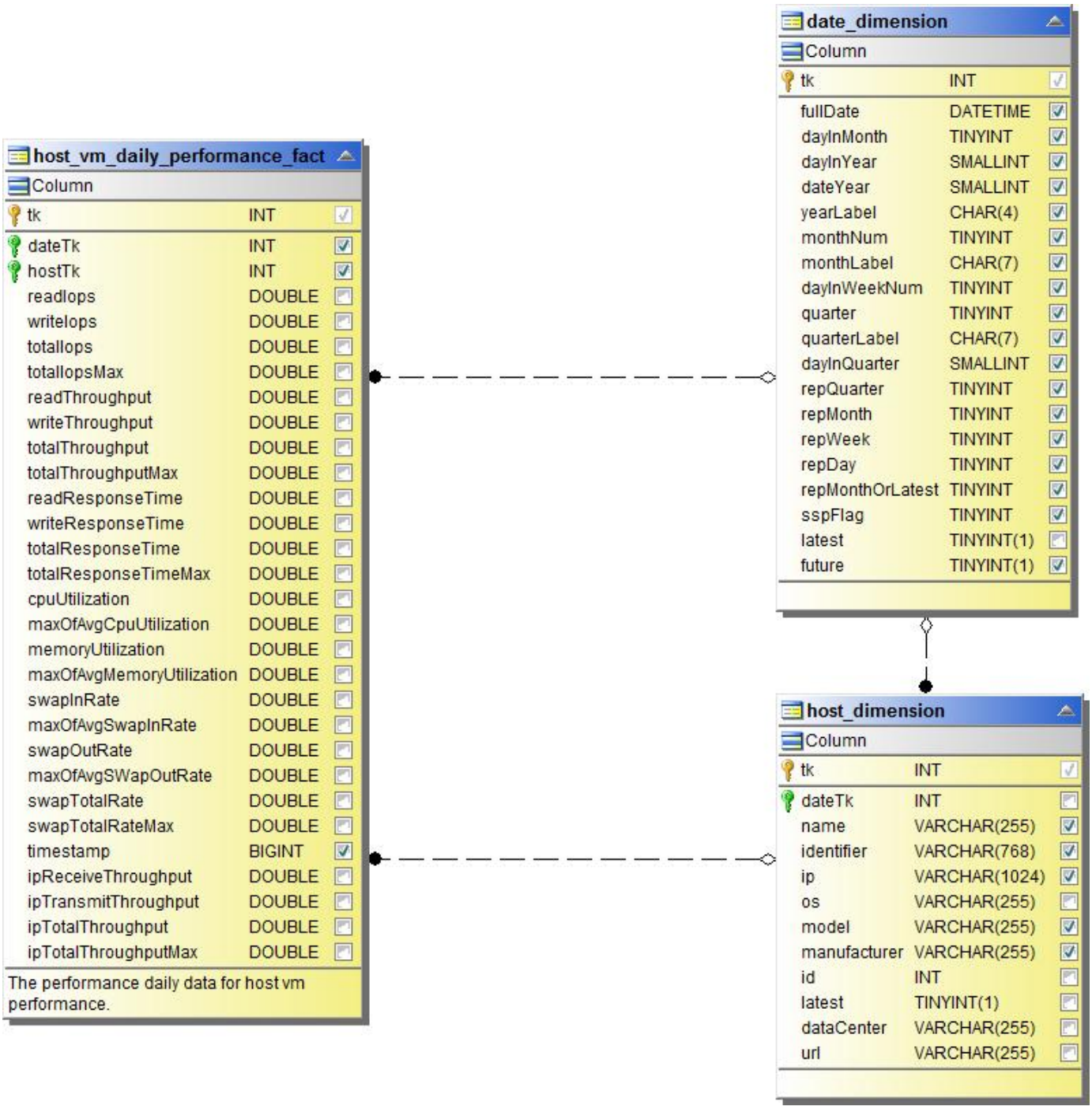
Performances horaires du disque



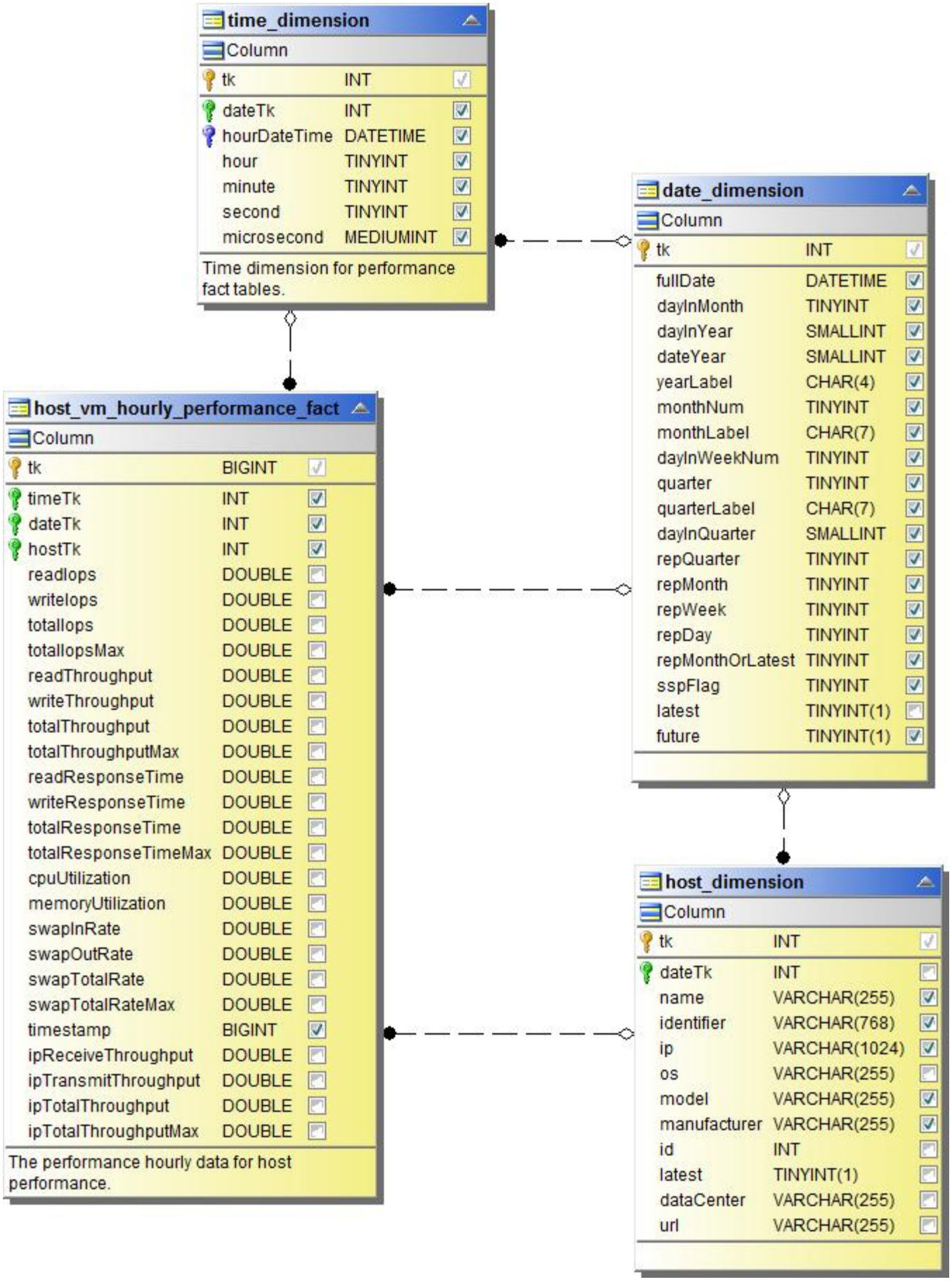
Performance horaire de l’hôte



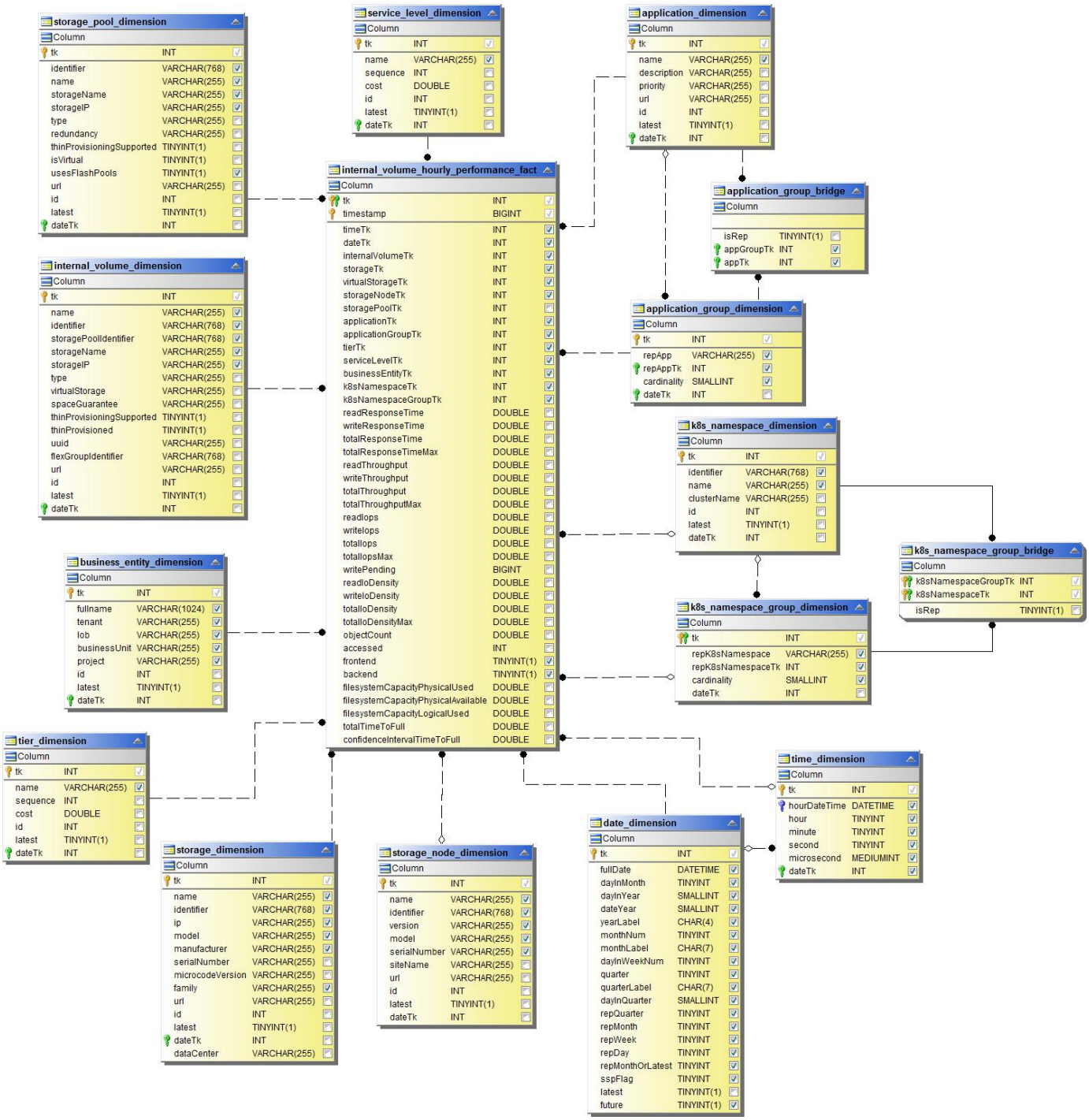
Performances quotidiennes de la machine virtuelle hôte



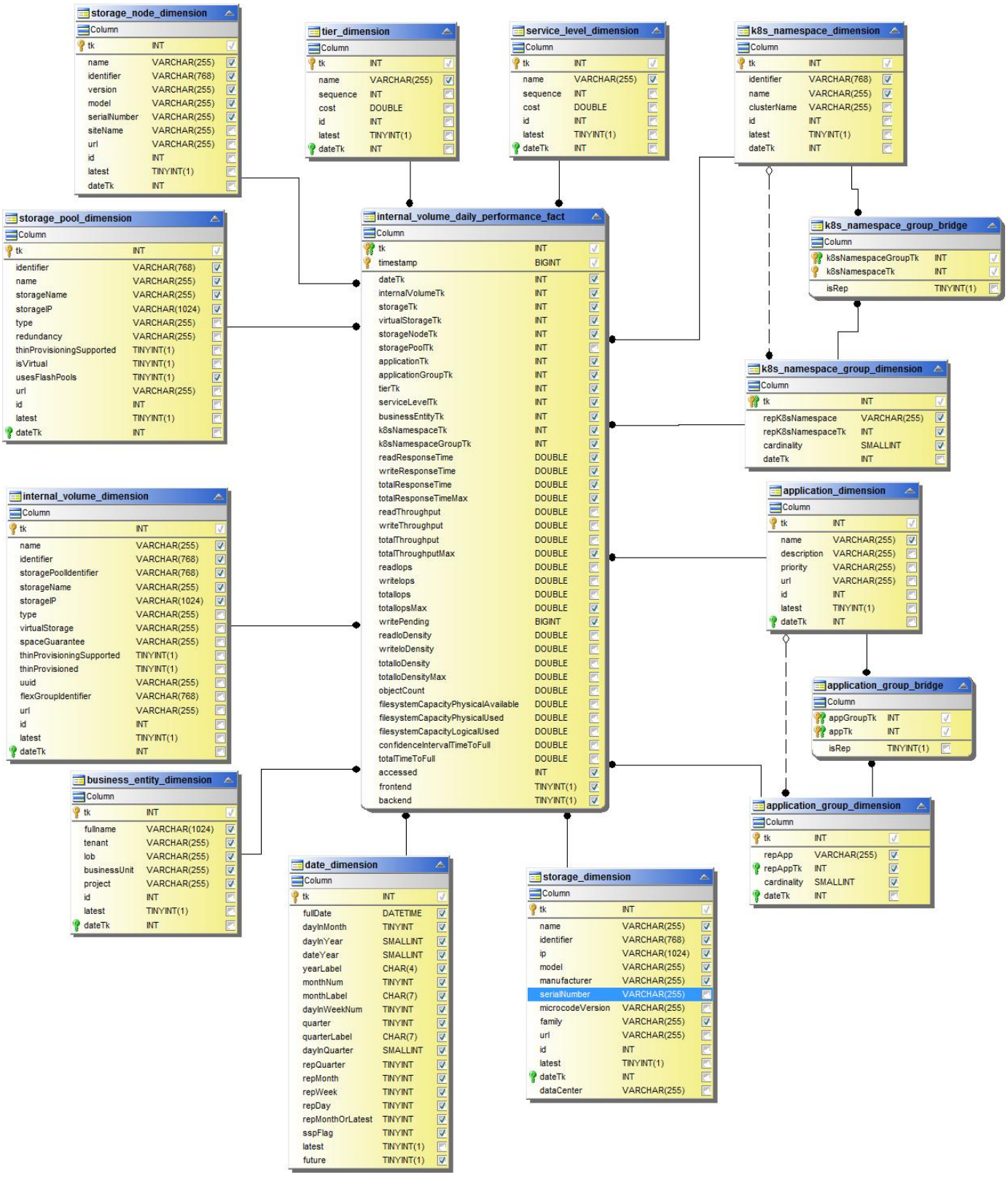
Performances horaires de la machine virtuelle hôte


time_dimension
Column
tk INT
dateTk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
Time dimension for performance fact tables.
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
host_vm_hourly_performance_fact
Column
tk BIGINT
timeTk INT
dateTk INT
hostTk INT
readIops DOUBLE
writeIops DOUBLE
totalIops DOUBLE
totalIopsMax DOUBLE
readThroughput DOUBLE
writeThroughput DOUBLE
totalThroughput DOUBLE
totalThroughputMax DOUBLE
readResponseTime DOUBLE
writeResponseTime DOUBLE
totalResponseTime DOUBLE
totalResponseTimeMax DOUBLE
cpuUtilization DOUBLE
memoryUtilization DOUBLE
swapInRate DOUBLE
swapOutRate DOUBLE
swapTotalRate DOUBLE
swapTotalRateMax DOUBLE
timestamp BIGINT
ipReceiveThroughput DOUBLE
ipTransmitThroughput DOUBLE
ipTotalThroughput DOUBLE
ipTotalThroughputMax DOUBLE
The performance hourly data for host performance.
host_dimension
Column
tk INT
dateTk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
id INT
latest TINYINT(1)
dataCenter VARCHAR(255)
url VARCHAR(255)

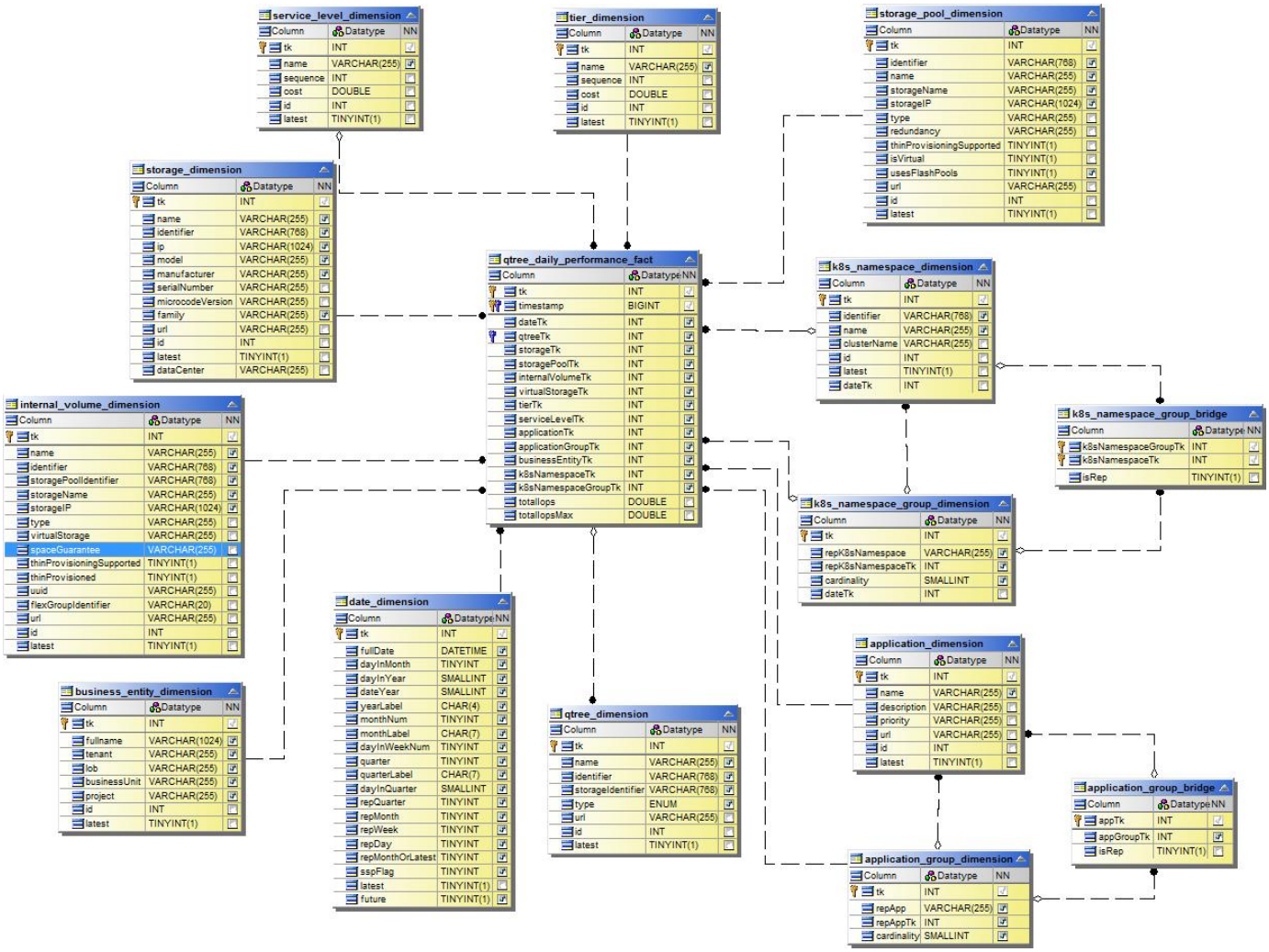
Performance horaire du volume interne



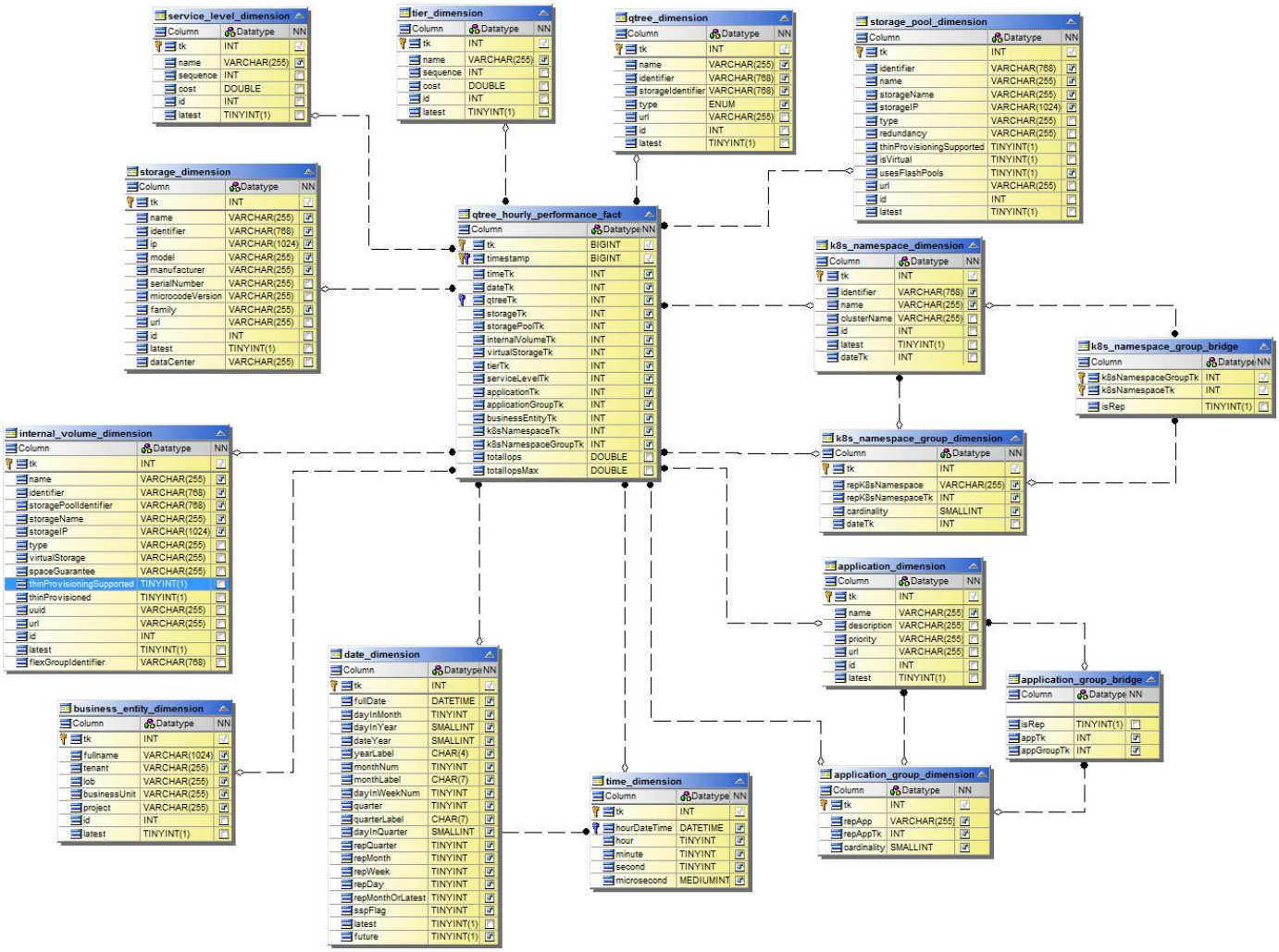
Performance quotidienne du volume interne



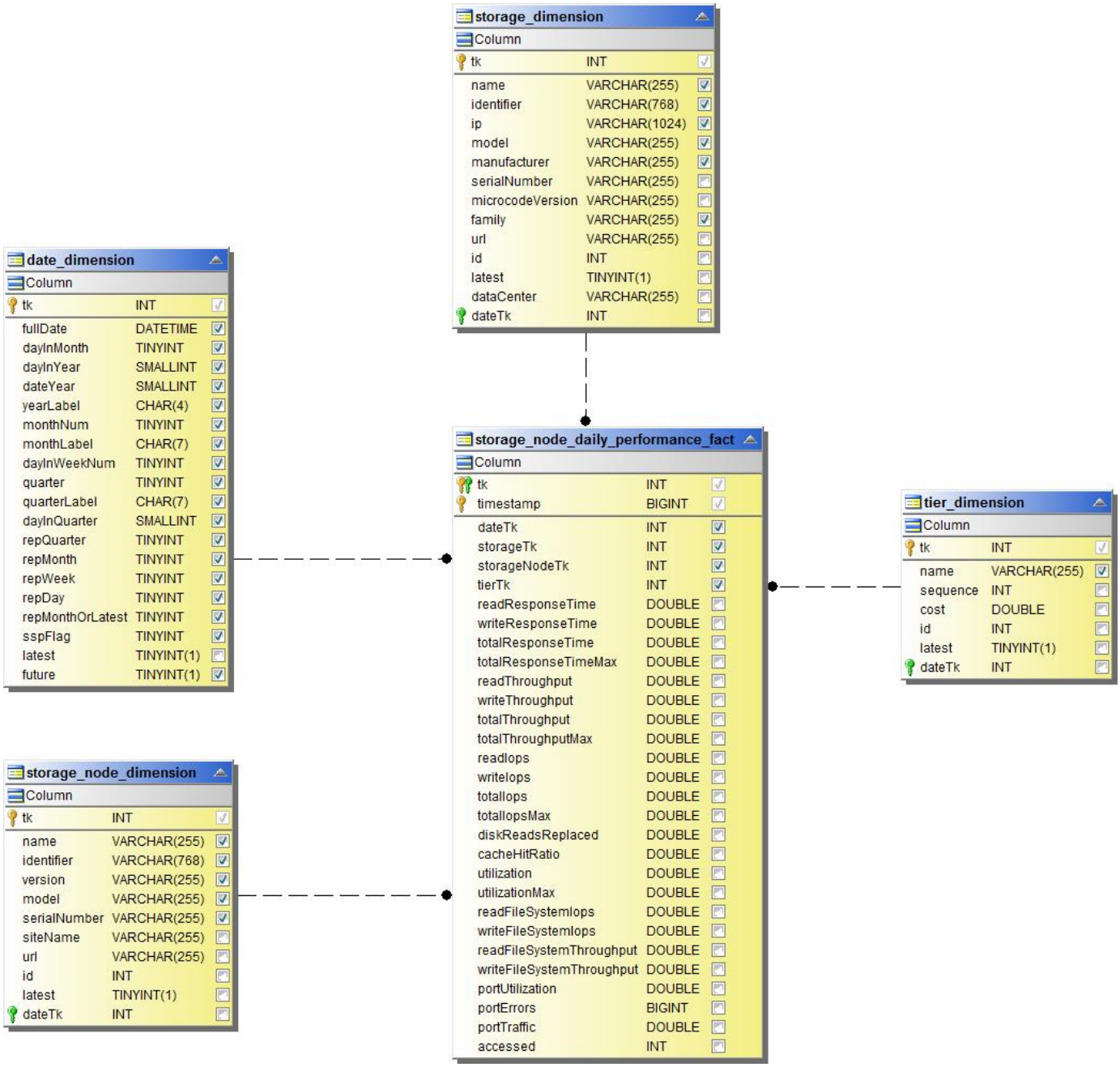
Performances quotidiennes de Qtree



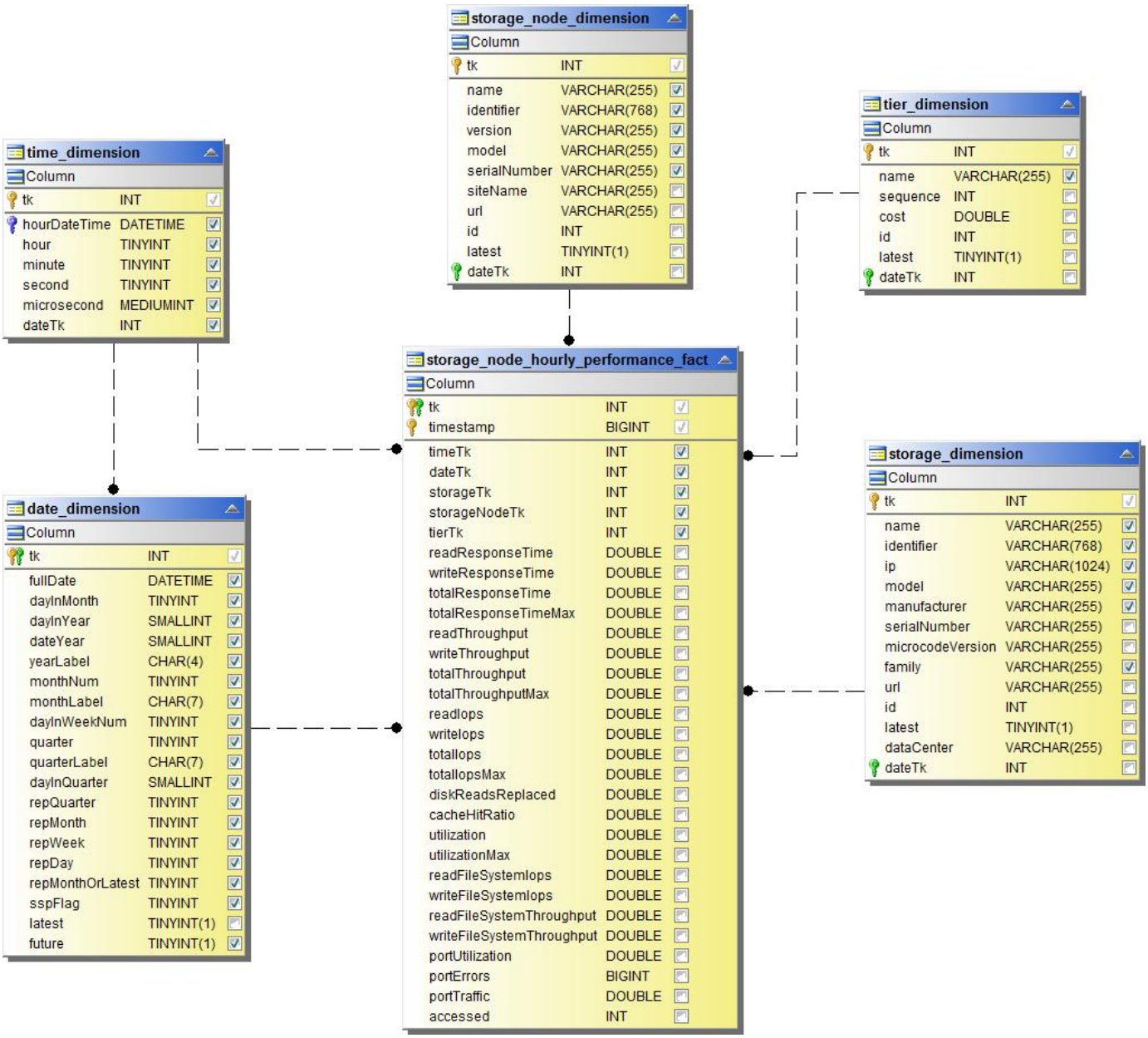
Performance horaire de Qtree



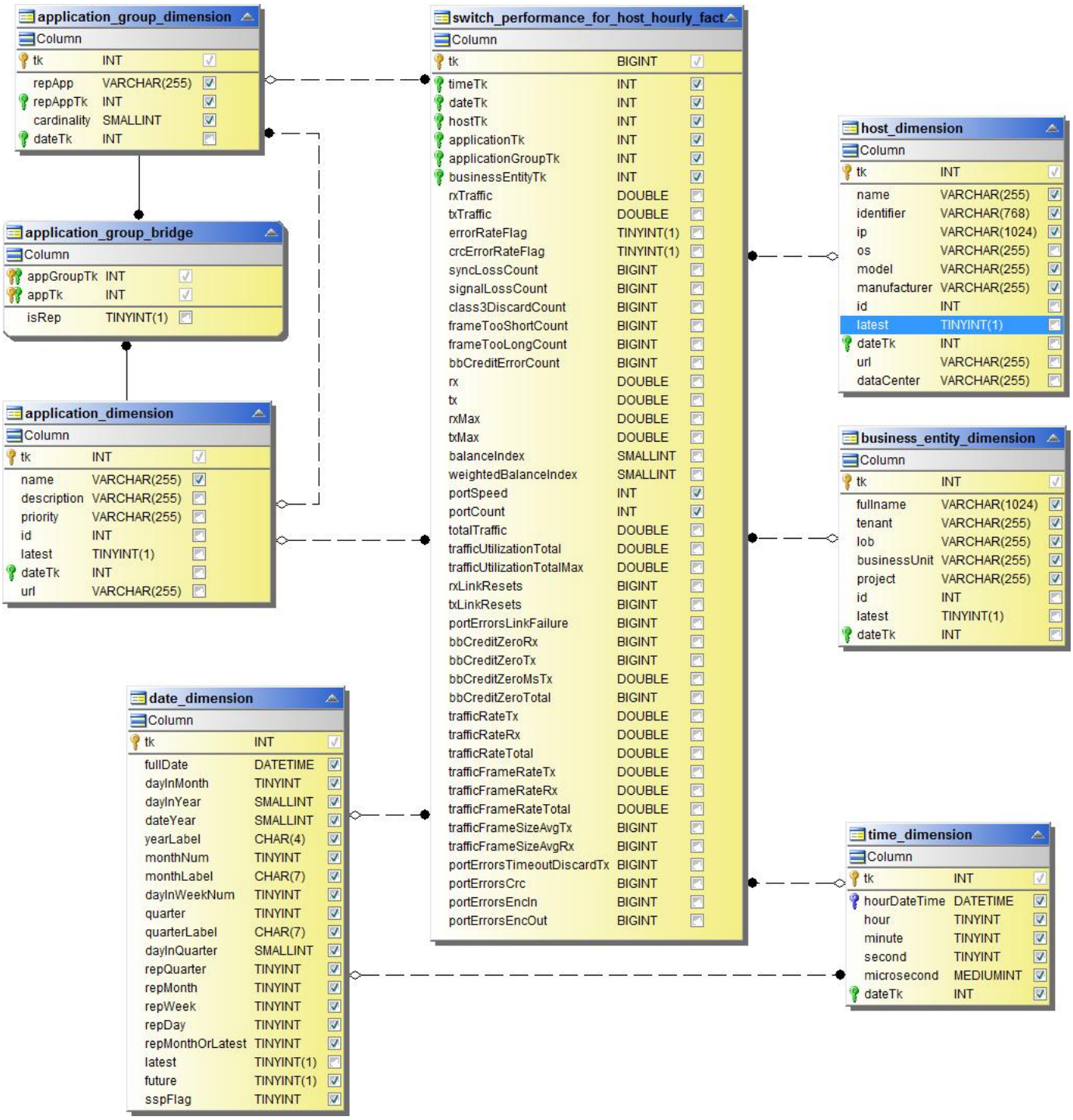
Performances quotidiennes du nœud de stockage



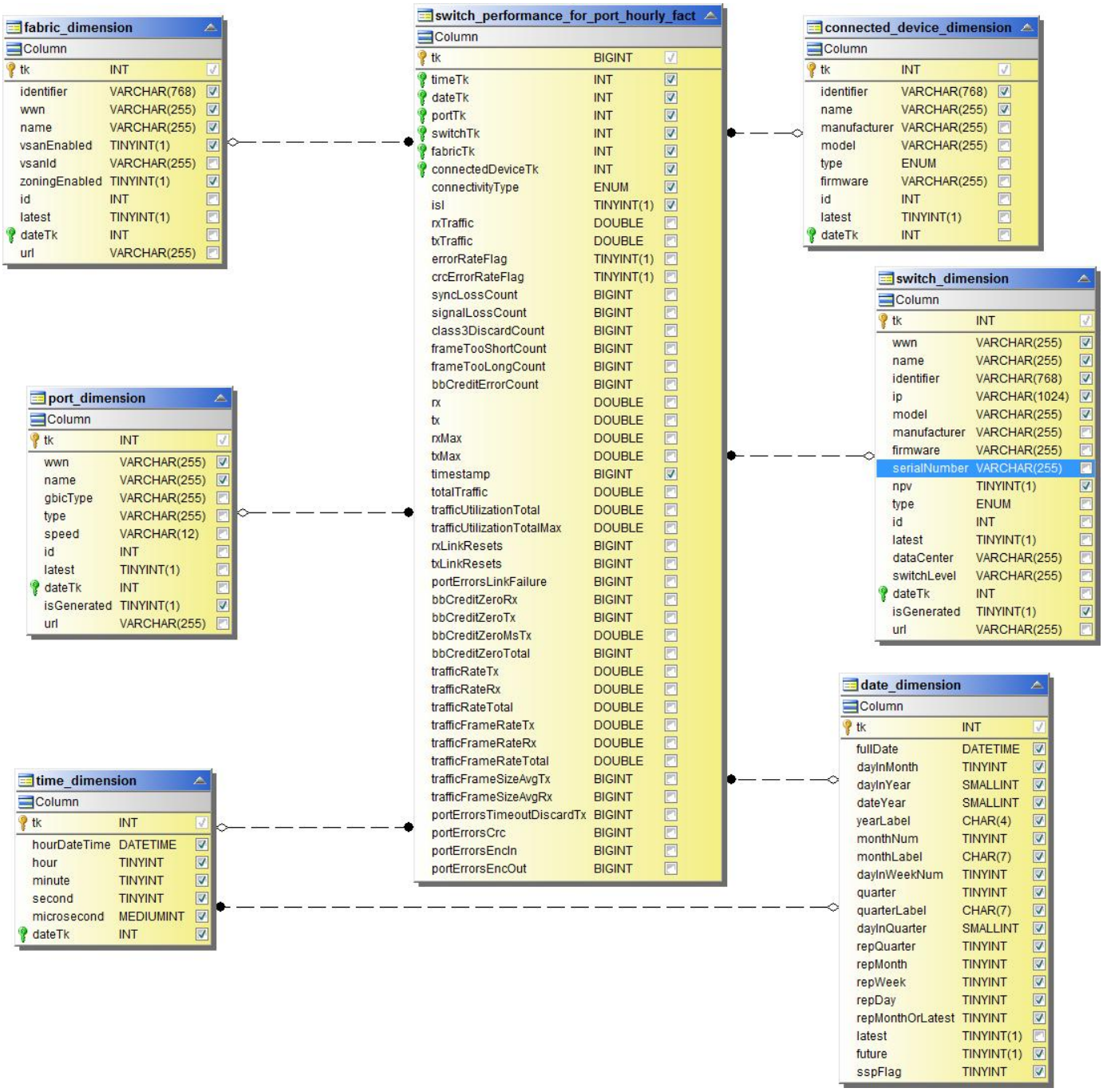
Performances horaires des nœuds de stockage



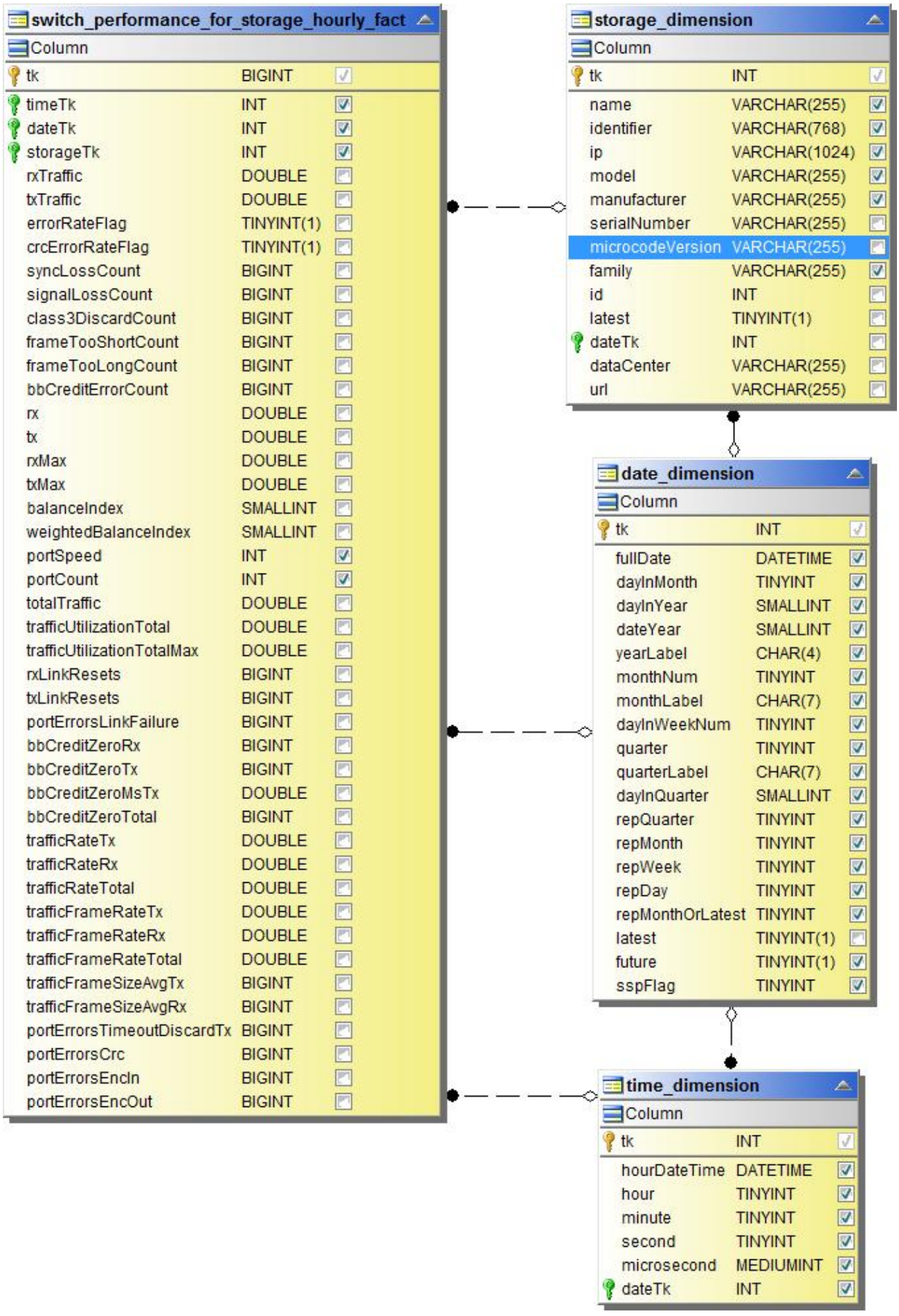
Changer les performances horaires pour l’hôte



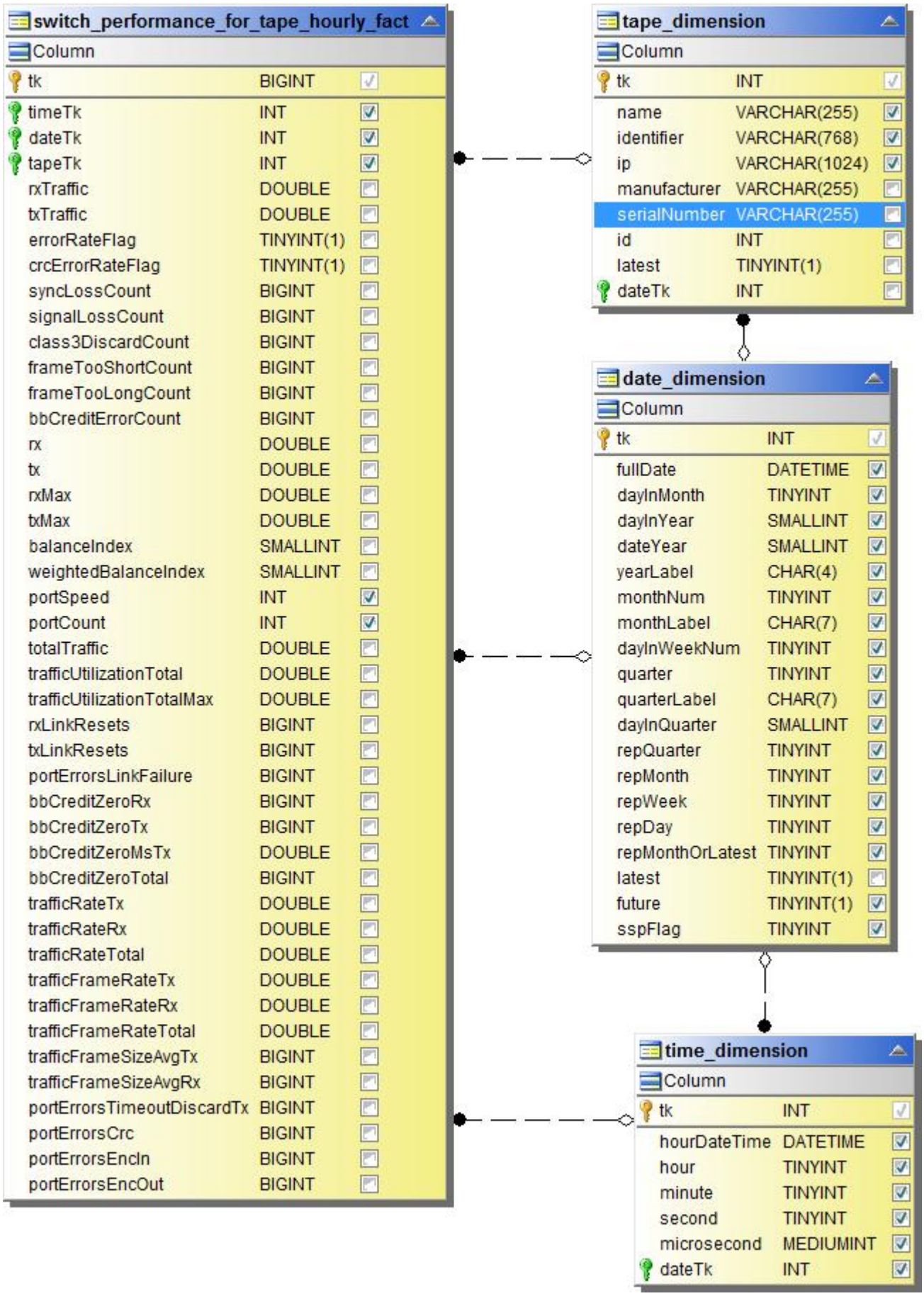
Performances horaires du commutateur pour le port



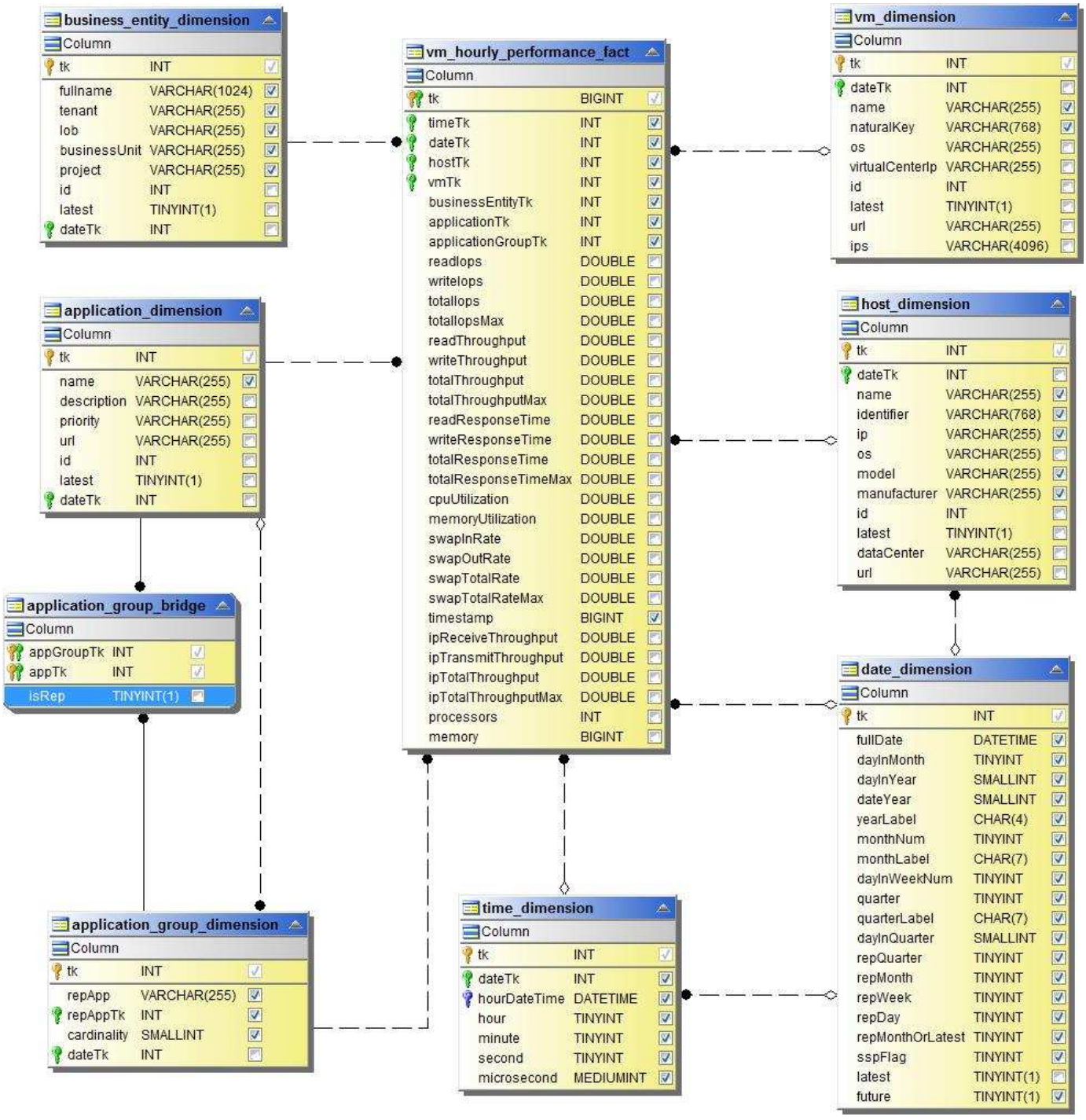
Changer les performances horaires pour le stockage


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

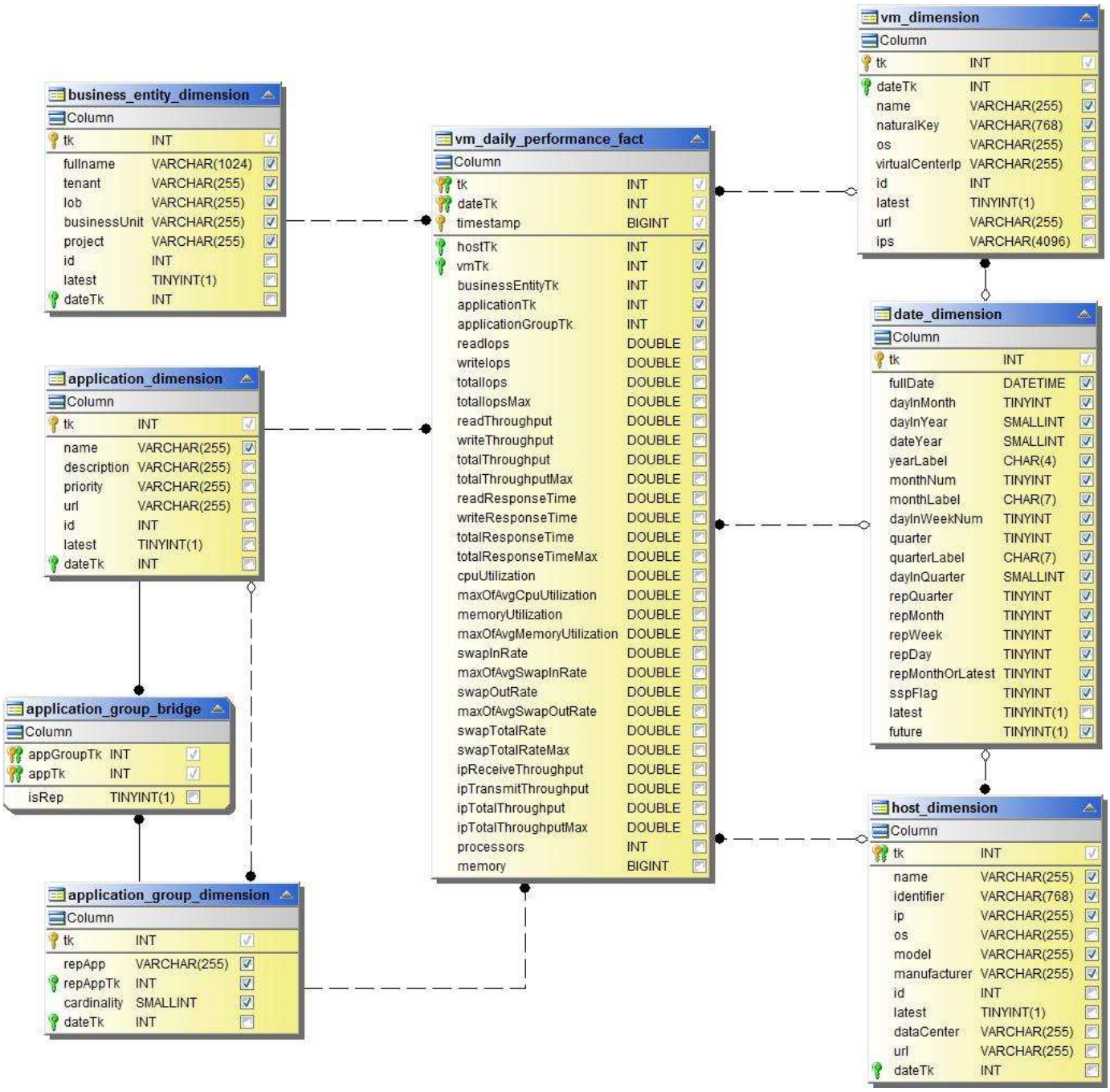
Changer les performances horaires pour la bande



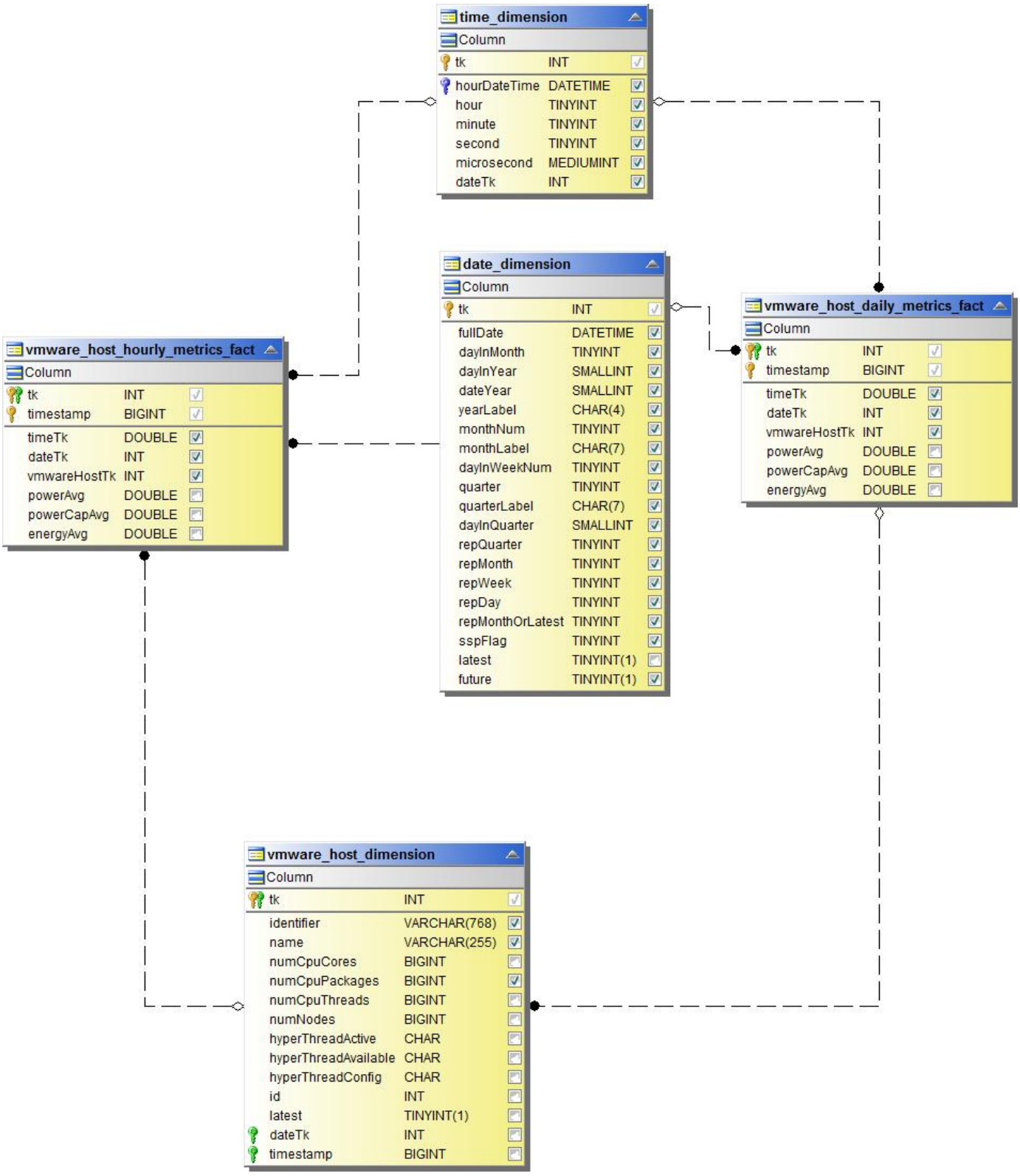
Performances de la machine virtuelle



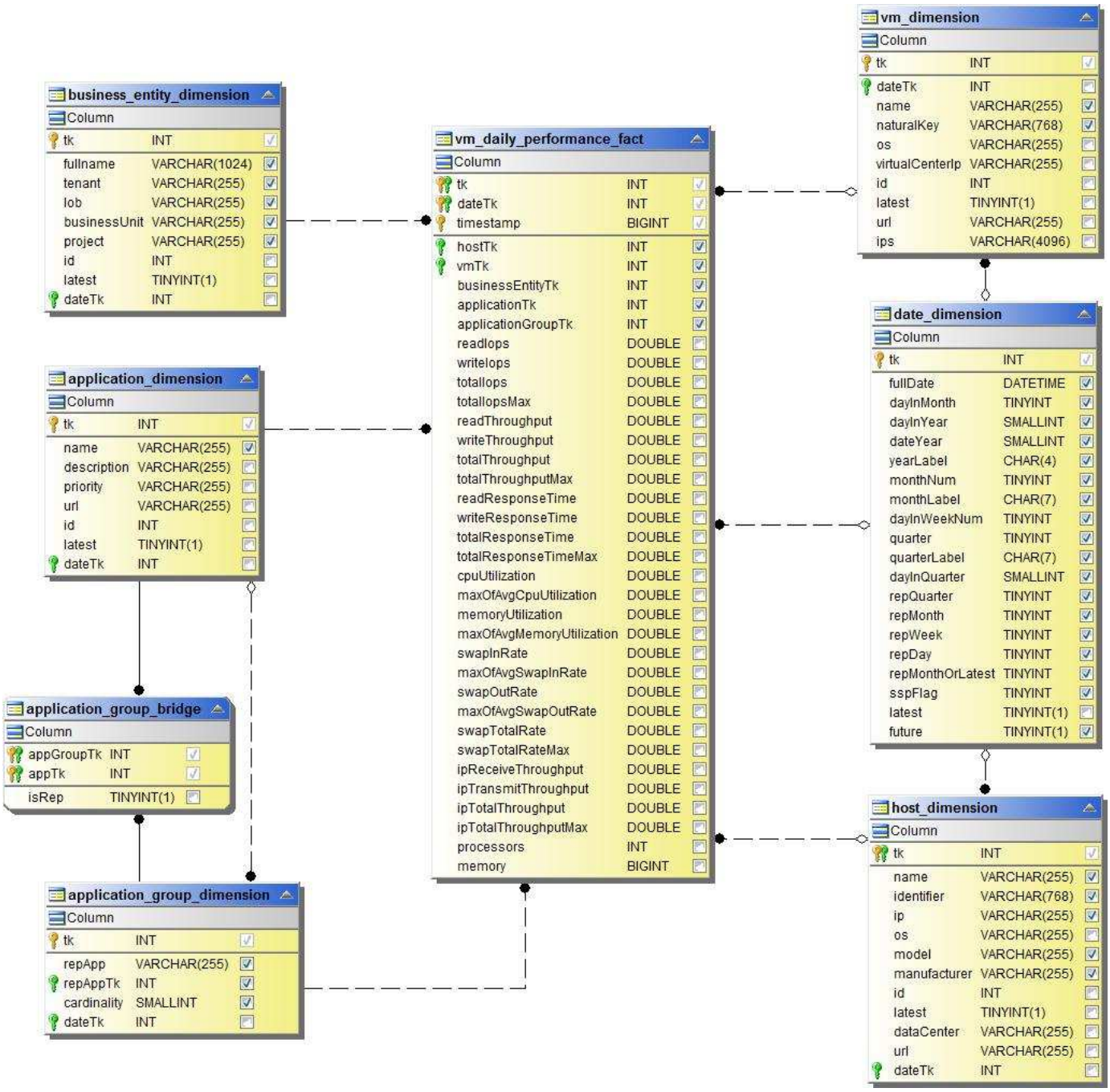
Performances quotidiennes de la machine virtuelle pour l’hôte



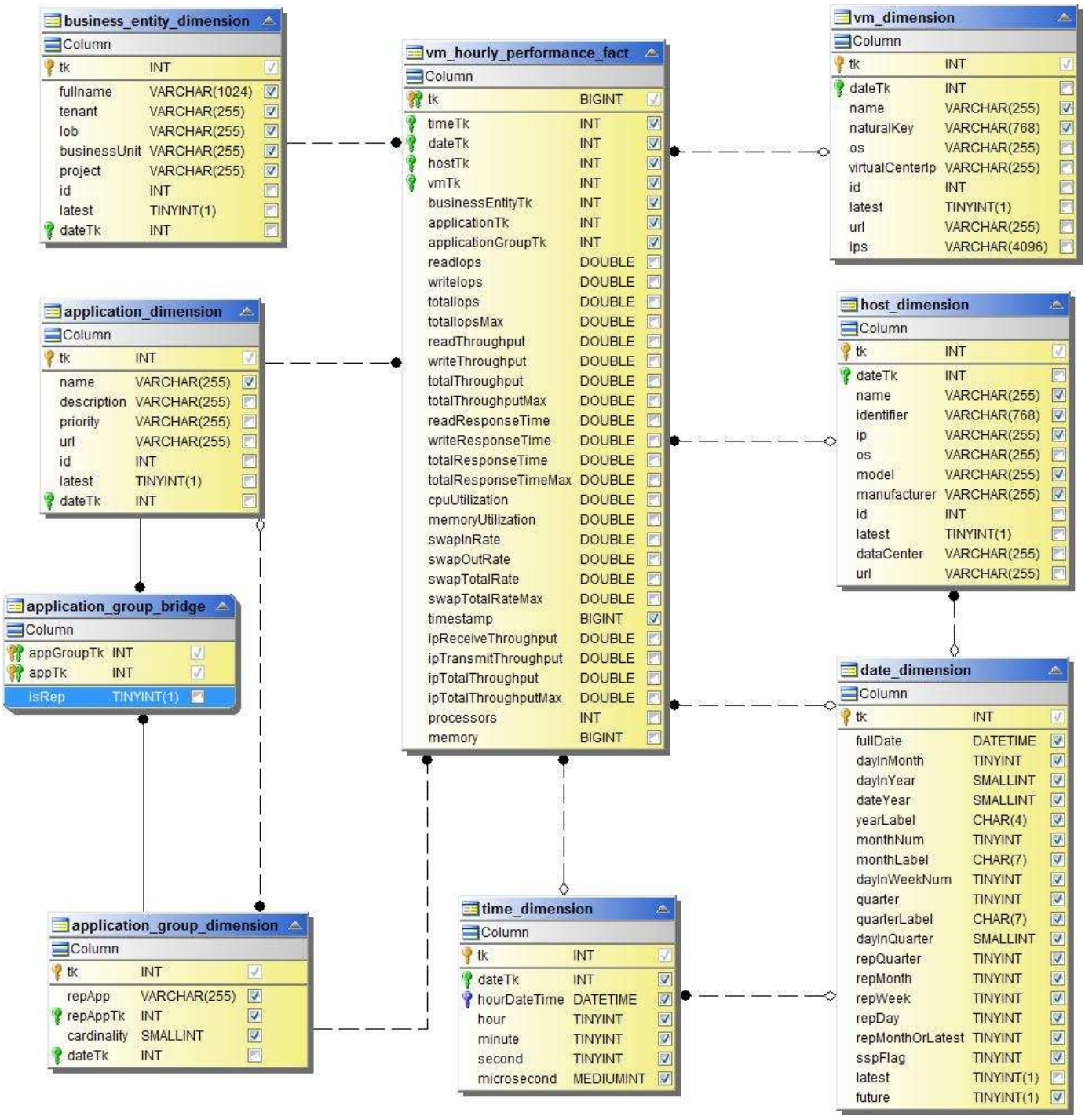
Performances horaires de la machine virtuelle pour l'hôte



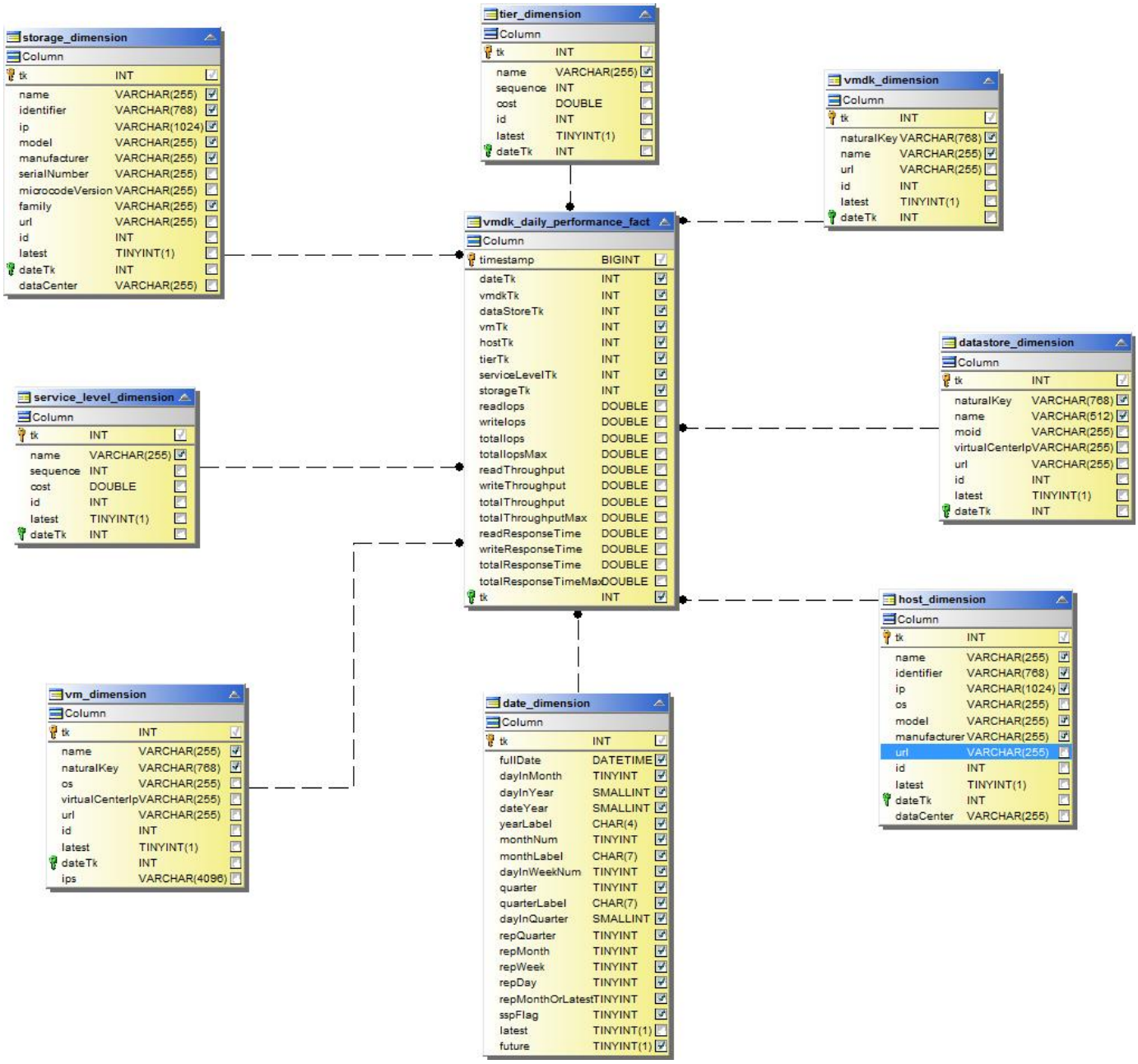
Performances quotidiennes de la machine virtuelle pour l'hôte



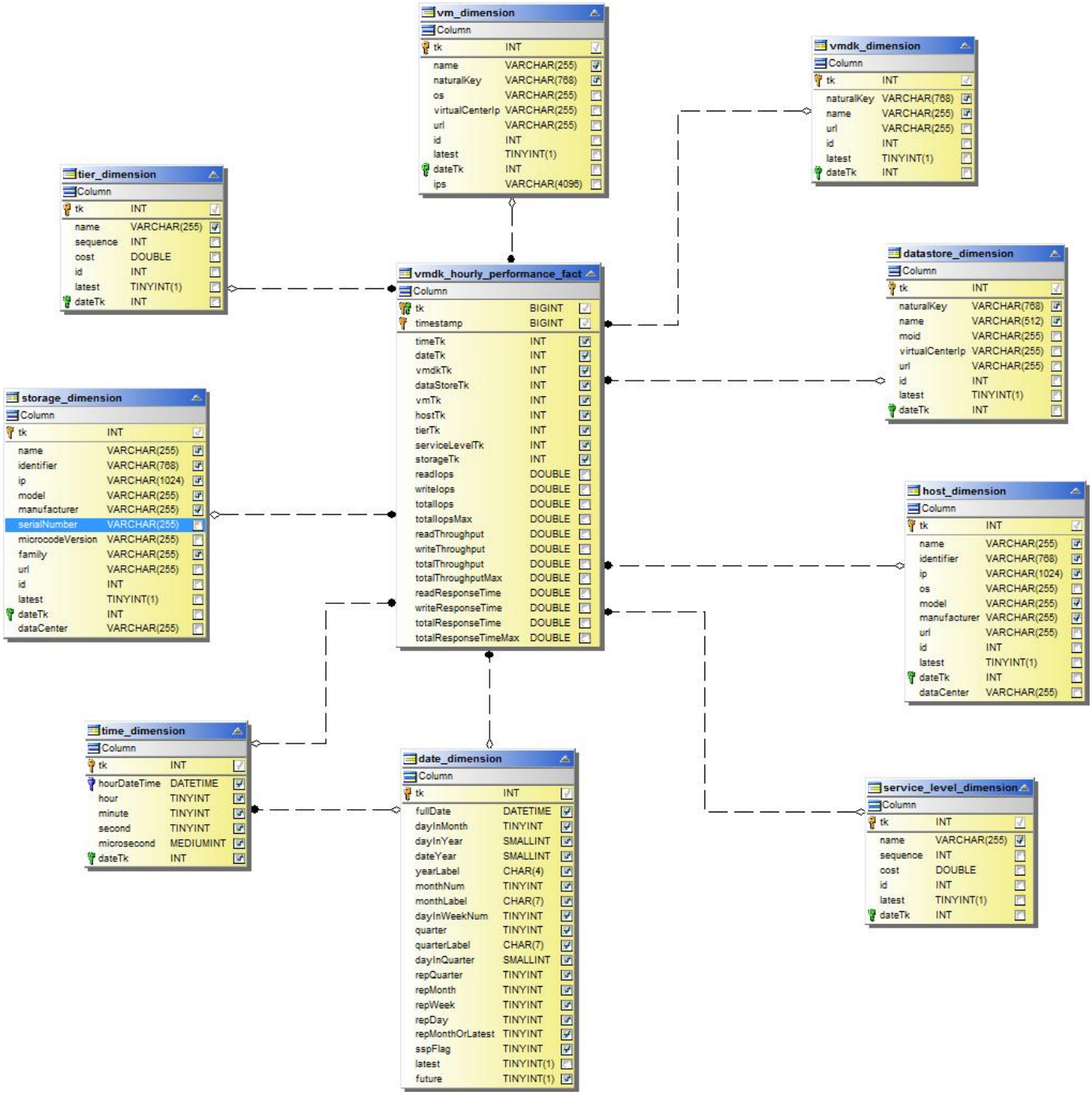
Performances horaires de la machine virtuelle pour l’hôte



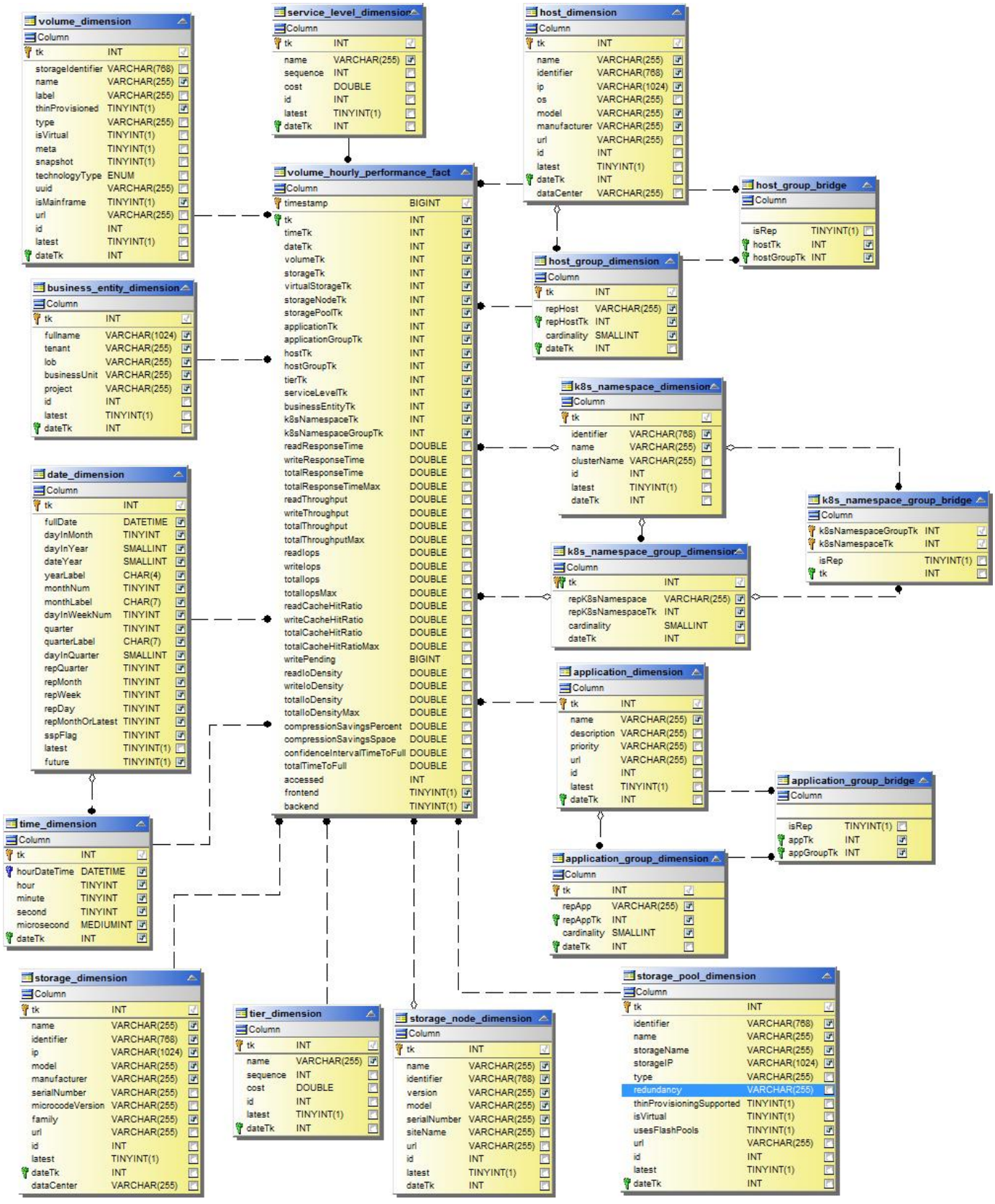
Performances quotidiennes de VMDK



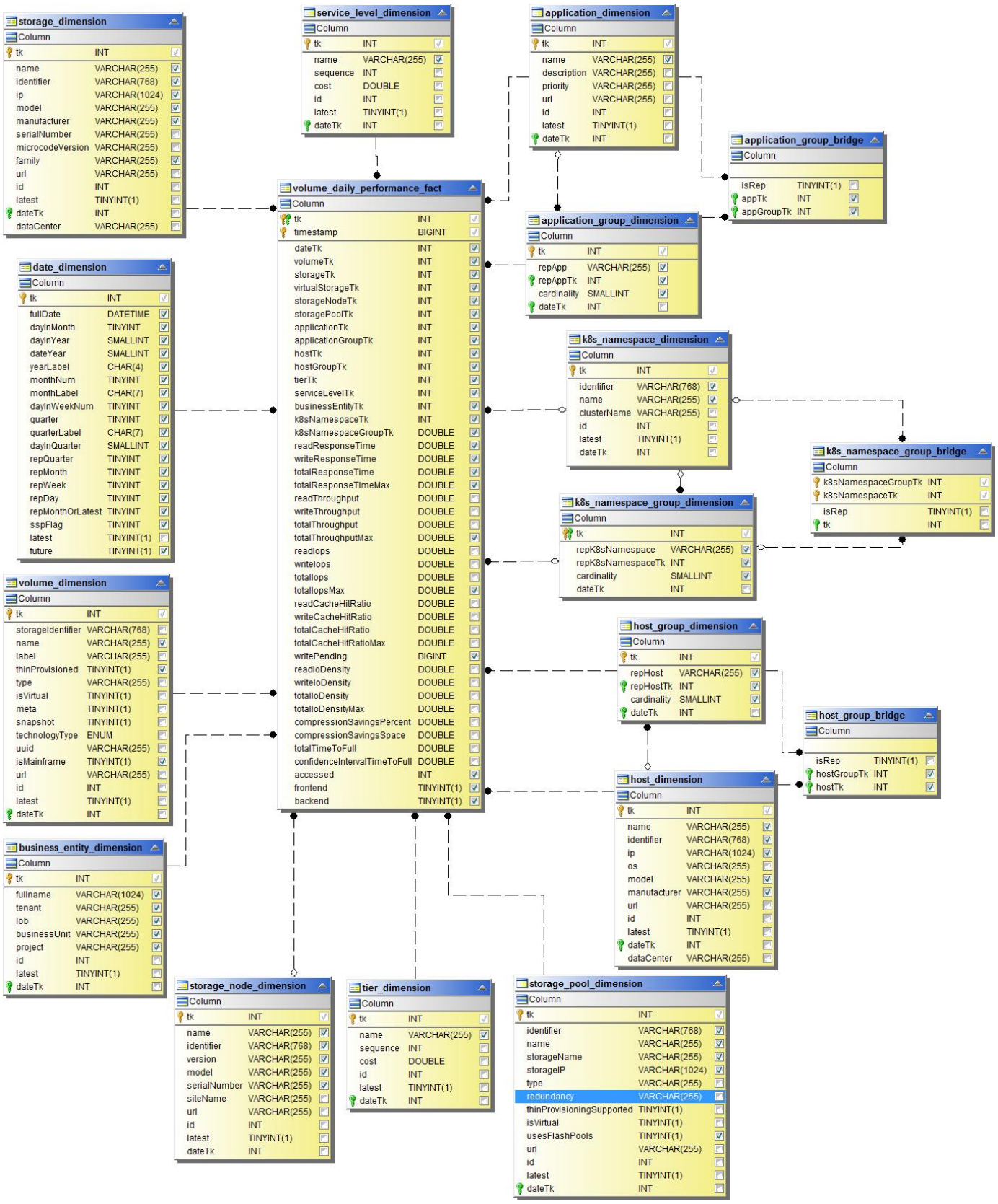
Performances horaires de VMDK



Volume Performance horaire



Volume Performance quotidienne



Schémas Data Infrastructure Insights pour la création de rapports

Ces tables de schéma et diagrammes sont fournis ici à titre de référence pour les rapports Data Infrastructure Insights .

"Tables de schéma"au format .PDF. Cliquez sur le lien pour l'ouvrir ou faites un clic droit et choisissez *Enregistrer sous…* pour télécharger.

"* Diagrammes de schéma *"

La fonctionnalité de reporting est disponible dans Data Infrastructure Insights"Édition Premium" .

Kubernetes

Présentation du cluster Kubernetes

Data Infrastructure Insights Kubernetes Explorer est un outil puissant permettant d'afficher l'état général et l'utilisation de vos clusters Kubernetes et vous permet d'explorer facilement les domaines d'investigation.

Cliquer sur **Tableaux de bord > Kubernetes Explorer** ouvre la page de liste des clusters Kubernetes. Cette page de présentation contient un tableau des clusters Kubernetes sur votre locataire.

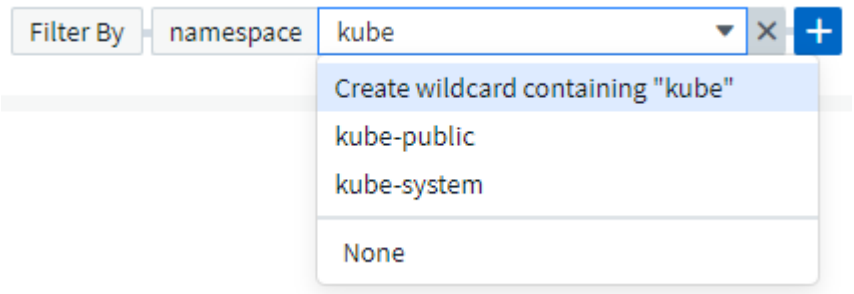
Liste des clusters

La liste des clusters affiche les informations suivantes pour chaque cluster de votre locataire :

- Cluster **Nom**. Cliquer sur le nom d'un cluster ouvrira le"**page de détail**" pour ce cluster.
- Pourcentages de **saturation**. La saturation globale est la plus élevée des saturations du processeur, de la mémoire ou du stockage.
- Nombre de **nœuds** dans le cluster. Cliquer sur ce numéro ouvrira la page de la liste des nœuds.
- Nombre de **Pods** dans le cluster. Cliquer sur ce numéro ouvrira la page de la liste des pods.
- Nombre d'**espaces de noms** dans le cluster. Cliquer sur ce numéro ouvrira la page de liste des espaces de noms.
- Nombre de **charges de travail** dans le cluster. Cliquer sur ce numéro ouvrira la page de liste de charge de travail.

Affiner le filtre

Lorsque vous filtrez, lorsque vous commencez à taper, vous avez la possibilité de créer un **filtre générique** basé sur le texte actuel. La sélection de cette option renverra tous les résultats correspondant à l'expression générique. Vous pouvez également créer des **expressions** en utilisant NOT ou AND, ou vous pouvez sélectionner l'option « Aucun » pour filtrer les valeurs nulles dans le champ.



Les filtres basés sur des caractères génériques ou des expressions (par exemple, NOT, AND, « Aucun », etc.) s'affichent en bleu foncé dans le champ de filtre. Les éléments que vous sélectionnez directement dans la liste sont affichés en bleu clair.

Les filtres Kubernetes sont contextuels, ce qui signifie par exemple que si vous êtes sur une page de nœud spécifique, le filtre pod_name répertorie uniquement les pods liés à ce nœud. De plus, si vous appliquez un filtre pour un espace de noms spécifique, le filtre pod_name répertoriera uniquement les pods sur ce nœud *et* dans cet espace de noms.

Notez que le filtrage par caractères génériques et par expressions fonctionne avec du texte ou des listes, mais pas avec des nombres, des dates ou des booléens.

Avant d'installer ou de mettre à niveau l'opérateur de surveillance NetApp Kubernetes

Lisez ces informations avant d'installer ou de mettre à niveau le"Opérateur de surveillance Kubernetes" .

Composant	Exigence
Version de Kubernetes	Kubernetes v1.20 et supérieur.
Distributions Kubernetes	AWS Elastic Kubernetes Service (EKS) Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Système d'exploitation Linux	Data Infrastructure Insights ne prend pas en charge les nœuds exécutés avec l'architecture Arm64. Surveillance du réseau : doit exécuter le noyau Linux version 4.18.0 ou supérieure. Photon OS n'est pas pris en charge.
Étiquettes	Data Infrastructure Insights prend en charge la surveillance des nœuds Kubernetes qui exécutent Linux, en spécifiant un sélecteur de nœud Kubernetes qui recherche les étiquettes Kubernetes suivantes sur ces plates-formes : Kubernetes v1.20 et versions ultérieures : Kubernetes.io/os = linux Rancher + cattle.io comme plate-forme d'orchestration/Kubernetes : cattle.io/os = linux
Commandes	Les commandes curl et kubectl doivent être disponibles. Pour de meilleurs résultats, ajoutez ces commandes au PATH.

Composant	Exigence
Connectivité	kubectl cli est configuré pour communiquer avec le cluster K8s cible et disposer d'une connectivité Internet à votre environnement Data Infrastructure Insights . Si vous êtes derrière un proxy lors de l'installation, suivez les instructions du"Configuration de la prise en charge du proxy" section de l'installation de l'opérateur. Pour un audit et des rapports de données précis, synchronisez l'heure sur la machine Agent à l'aide du protocole NTP (Network Time Protocol) ou du protocole SNTP (Simple Network Time Protocol).
Autre	Si vous utilisez OpenShift 4.6 ou supérieur, vous devez suivre les"Instructions OpenShift" en plus de veiller à ce que ces conditions préalables soient respectées.
Jeton API	Si vous redéployez l'opérateur (c'est-à-dire que vous le mettez à jour ou le remplacez), il n'est pas nécessaire de créer un nouveau jeton API ; vous pouvez réutiliser le jeton précédent.

Choses importantes à noter avant de commencer

Si vous courez avec unprocuration , avoir unréférentiel personnalisé , ou utilisentOpenShift , lisez attentivement les sections suivantes.

Lire aussi à propos deAutorisations .

Configuration de la prise en charge du proxy

Il existe deux endroits où vous pouvez utiliser un proxy sur votre locataire afin d'installer NetApp Kubernetes Monitoring Operator. Il peut s'agir des mêmes systèmes proxy ou de systèmes proxy distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système où l'extrait est exécuté à votre environnement Data Infrastructure Insights
- Proxy requis par le cluster Kubernetes cible pour communiquer avec votre environnement Data Infrastructure Insights

Si vous utilisez un proxy pour l'un ou les deux, pour installer NetApp Kubernetes Operating Monitor, vous devez d'abord vous assurer que votre proxy est configuré pour permettre une bonne communication avec votre environnement Data Infrastructure Insights . Par exemple, à partir des serveurs/VM à partir desquels vous souhaitez installer l'opérateur, vous devez pouvoir accéder à Data Infrastructure Insights et pouvoir télécharger des binaires depuis Data Infrastructure Insights.

Pour le proxy utilisé pour installer NetApp Kubernetes Operating Monitor, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, vous devrez peut-être également définir la variable d'environnement *no_proxy*.

Pour définir la ou les variables, effectuez les étapes suivantes sur votre système **avant** d'installer NetApp Kubernetes Monitoring Operator :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
   a. Si le proxy en cours de configuration ne dispose pas d'authentification (nom d'utilisateur/mot de passe), exécutez la commande suivante :

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Si le proxy en cours de configuration dispose d'une
authentification (nom d'utilisateur/mot de passe), exécutez cette
commande :
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Pour que le proxy utilisé pour votre cluster Kubernetes communique avec votre environnement Data Infrastructure Insights , installez NetApp Kubernetes Monitoring Operator après avoir lu toutes ces instructions.

Configurez la section proxy d'AgentConfiguration dans operator-config.yaml avant de déployer l'opérateur de surveillance NetApp Kubernetes.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utiliser un référentiel Docker personnalisé ou privé

Par défaut, l'opérateur de surveillance NetApp Kubernetes extrait les images de conteneur du référentiel Data Infrastructure Insights . Si vous disposez d'un cluster Kubernetes utilisé comme cible pour la surveillance et

que ce cluster est configuré pour extraire uniquement des images de conteneur à partir d'un référentiel Docker personnalisé ou privé ou d'un registre de conteneurs, vous devez configurer l'accès aux conteneurs nécessaires à l'opérateur de surveillance NetApp Kubernetes.

Exécutez « Image Pull Snippet » à partir de la mosaïque d'installation de NetApp Monitoring Operator. Cette commande se connectera au référentiel Data Infrastructure Insights , extraira toutes les dépendances d'image pour l'opérateur et se déconnectera du référentiel Data Infrastructure Insights . Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande télécharge toutes les images utilisées par l'opérateur, y compris pour les fonctionnalités optionnelles. Voir ci-dessous pour les fonctionnalités pour lesquelles ces images sont utilisées.

Fonctionnalités de l'opérateur principal et surveillance de Kubernetes

- surveillance netapp
- proxy kube-rbac
- métriques d'état de kube
- télégraphe
- utilisateur root sans distribution

Journal des événements

- bit courant
- exportateur d'événements Kubernetes

Performances et carte du réseau

- ci-net-observer

Poussez l'image Docker de l'opérateur vers votre référentiel Docker privé/local/d'entreprise conformément à vos politiques d'entreprise. Assurez-vous que les balises d'image et les chemins d'accès aux répertoires de ces images dans votre référentiel sont cohérents avec ceux du référentiel Data Infrastructure Insights .

Modifiez le déploiement de l'opérateur de surveillance dans operator-deployment.yaml et modifiez toutes les références d'image pour utiliser votre référentiel Docker privé.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modifiez AgentConfiguration dans operator-config.yaml pour refléter le nouvel emplacement du référentiel Docker. Créez un nouveau imagePullSecret pour votre référentiel privé, pour plus de détails, consultez *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation for
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Instructions OpenShift

Si vous utilisez OpenShift 4.6 ou une version ultérieure, vous devez modifier AgentConfiguration dans *operator-config.yaml* pour activer le paramètre *runPrivileged* :

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift peut implémenter un niveau de sécurité supplémentaire qui peut bloquer l'accès à certains composants Kubernetes.

Autorisations

Si le cluster que vous surveillez contient des ressources personnalisées qui n'ont pas de ClusterRole,"agrégats à visualiser" , vous devrez accorder manuellement à l'opérateur l'accès à ces ressources pour les surveiller avec les journaux d'événements.

1. Modifiez *operator-additional-permissions.yaml* avant l'installation, ou après l'installation, modifiez la ressource *ClusterRole/<namespace>-additional-permissions*
2. Créez une nouvelle règle pour les apiGroups et ressources souhaités avec les verbes ["get", "watch", "list"]. Voir \ https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Appliquez vos modifications au cluster

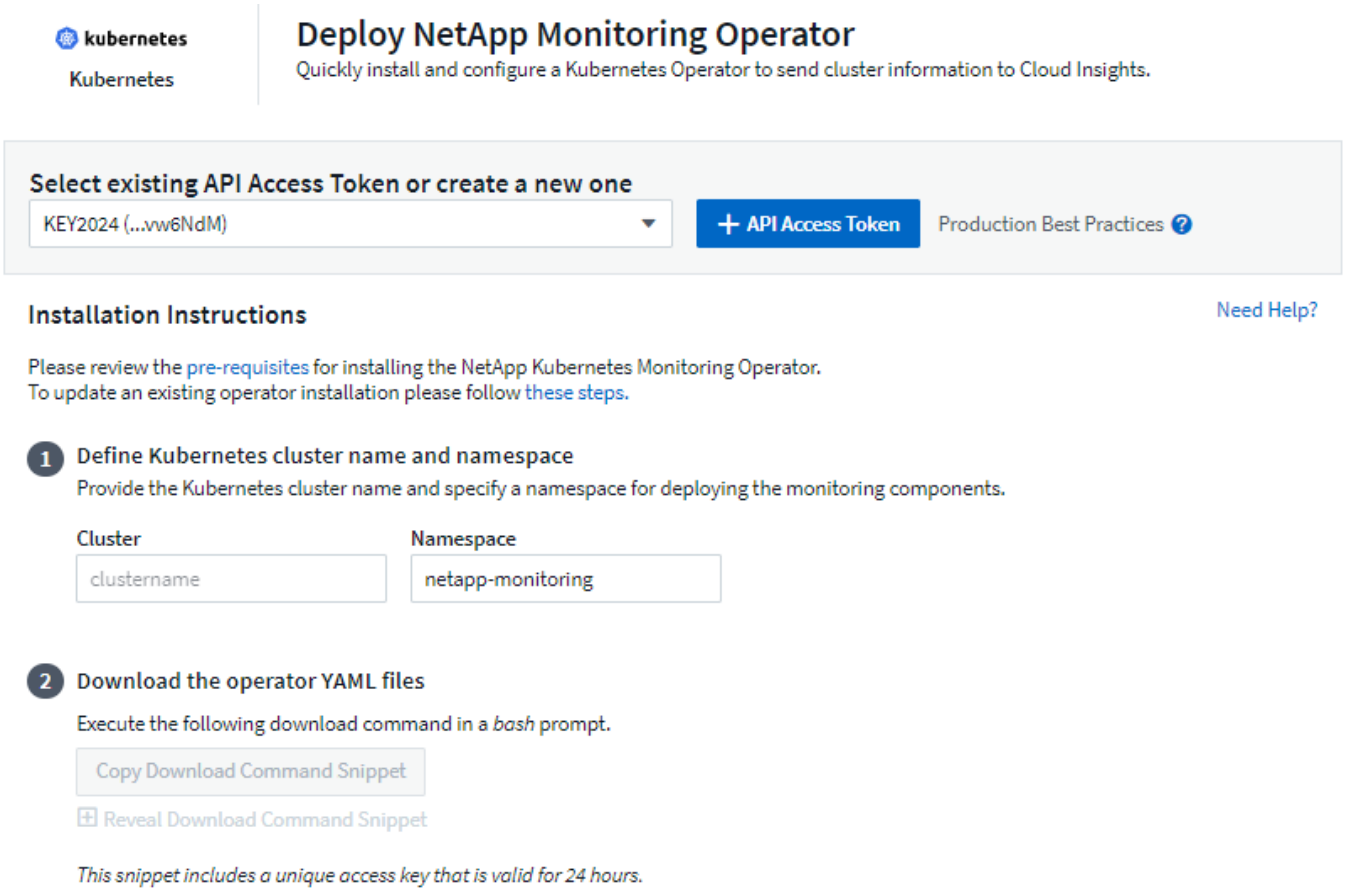
Installation et configuration de l'opérateur de surveillance Kubernetes

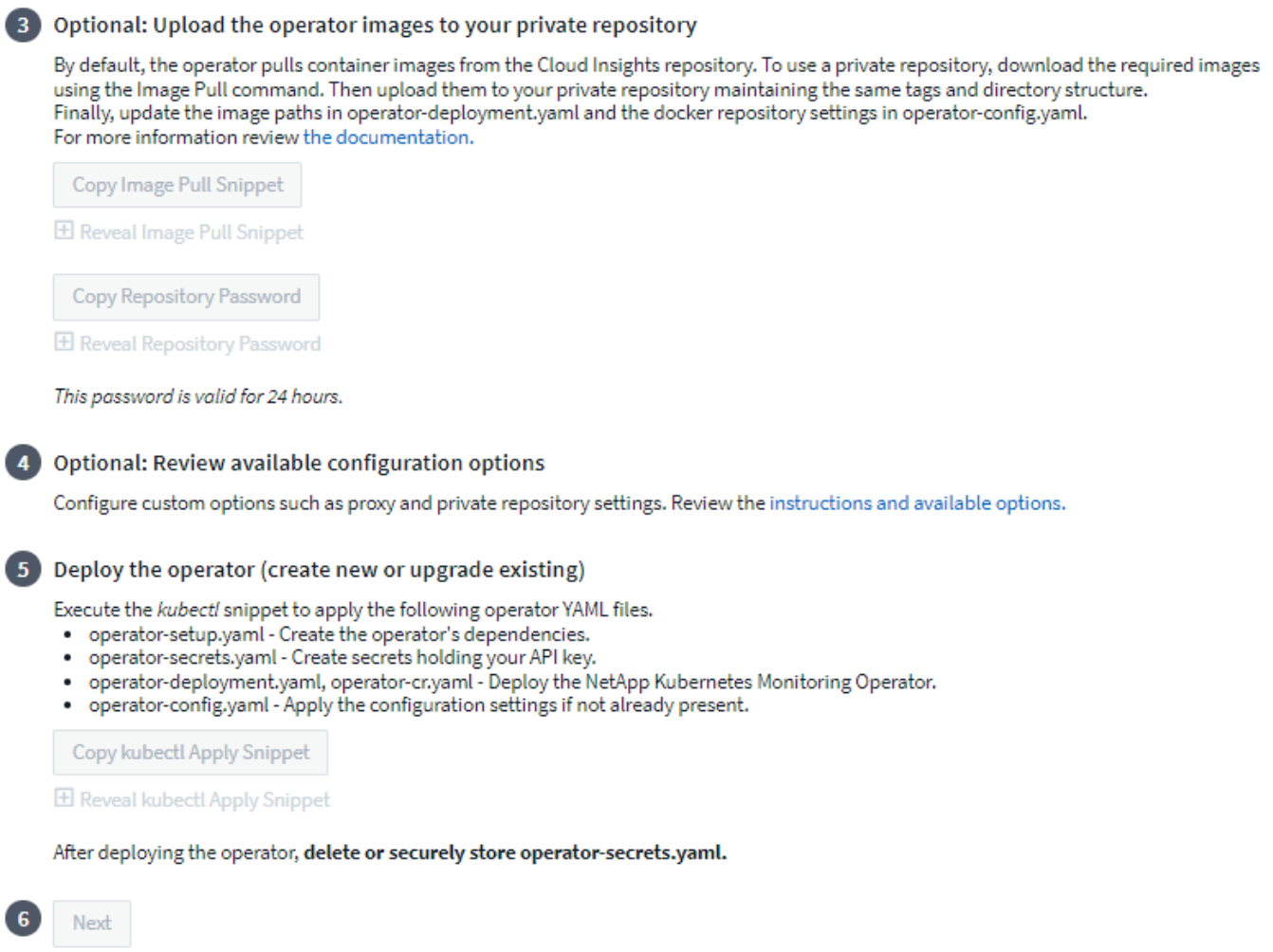
Data Infrastructure Insights propose l'opérateur de surveillance Kubernetes pour la collection Kubernetes. Accédez à **Kubernetes > Collecteurs > +Kubernetes Collector** pour déployer un nouvel opérateur.

Avant d'installer Kubernetes Monitoring Operator

Voir le"Prérequis" documentation avant d'installer ou de mettre à niveau Kubernetes Monitoring Operator.

Installation de l'opérateur de surveillance Kubernetes





Étapes pour installer l'agent Kubernetes Monitoring Operator sur Kubernetes :

1. Saisissez un nom de cluster et un espace de noms uniques. Si vous êtesmise à niveau à partir d'un opérateur Kubernetes précédent, utilisez le même nom de cluster et le même espace de noms.
2. Une fois ces informations saisies, vous pouvez copier l'extrait de commande de téléchargement dans le presse-papiers.
3. Collez l'extrait dans une fenêtre *bash* et exécutez-le. Les fichiers d'installation de l'opérateur seront téléchargés. Notez que l'extrait possède une clé unique et est valable 24 heures.
4. Si vous disposez d'un référentiel personnalisé ou privé, copiez l'extrait d'image facultatif, collez-le dans un shell *bash* et exécutez-le. Une fois les images extraites, copiez-les dans votre référentiel privé. Assurez-vous de conserver les mêmes balises et la même structure de dossiers. Mettez à jour les chemins dans *operator-deployment.yaml* ainsi que les paramètres du référentiel Docker dans *operator-config.yaml*.
5. Si vous le souhaitez, examinez les options de configuration disponibles telles que les paramètres de proxy ou de référentiel privé. Vous pouvez en savoir plus sur"options de configuration" .
6. Lorsque vous êtes prêt, déployez l'opérateur en copiant l'extrait kubectl Apply, en le téléchargeant et en l'exécutant.
7. L'installation se déroule automatiquement. Une fois terminé, cliquez sur le bouton *Suivant*.
8. Une fois l'installation terminée, cliquez sur le bouton *Suivant*. Assurez-vous également de supprimer ou de stocker en toute sécurité le fichier *operator-secrets.yaml*.

Si vous disposez d'un référentiel personnalisé, lisez à proposen utilisant un référentiel Docker

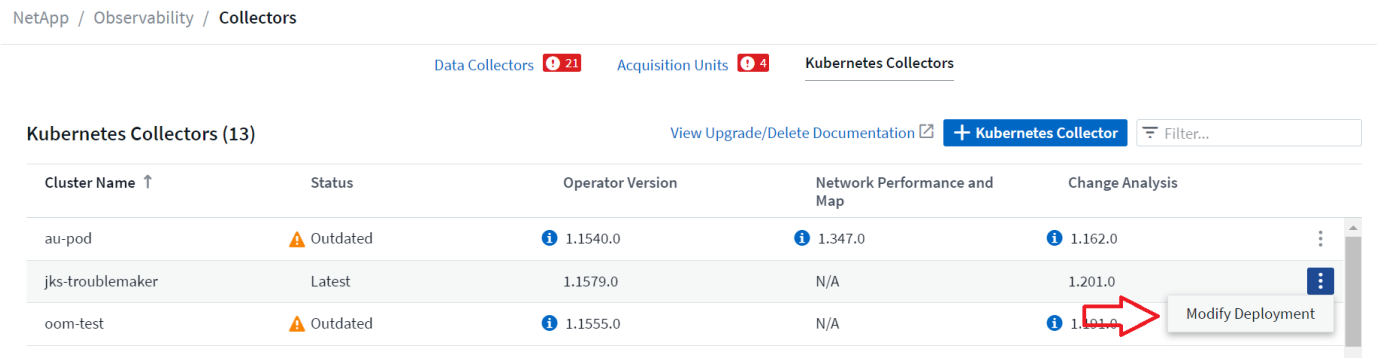
personnalisé/privé .

Composants de surveillance Kubernetes

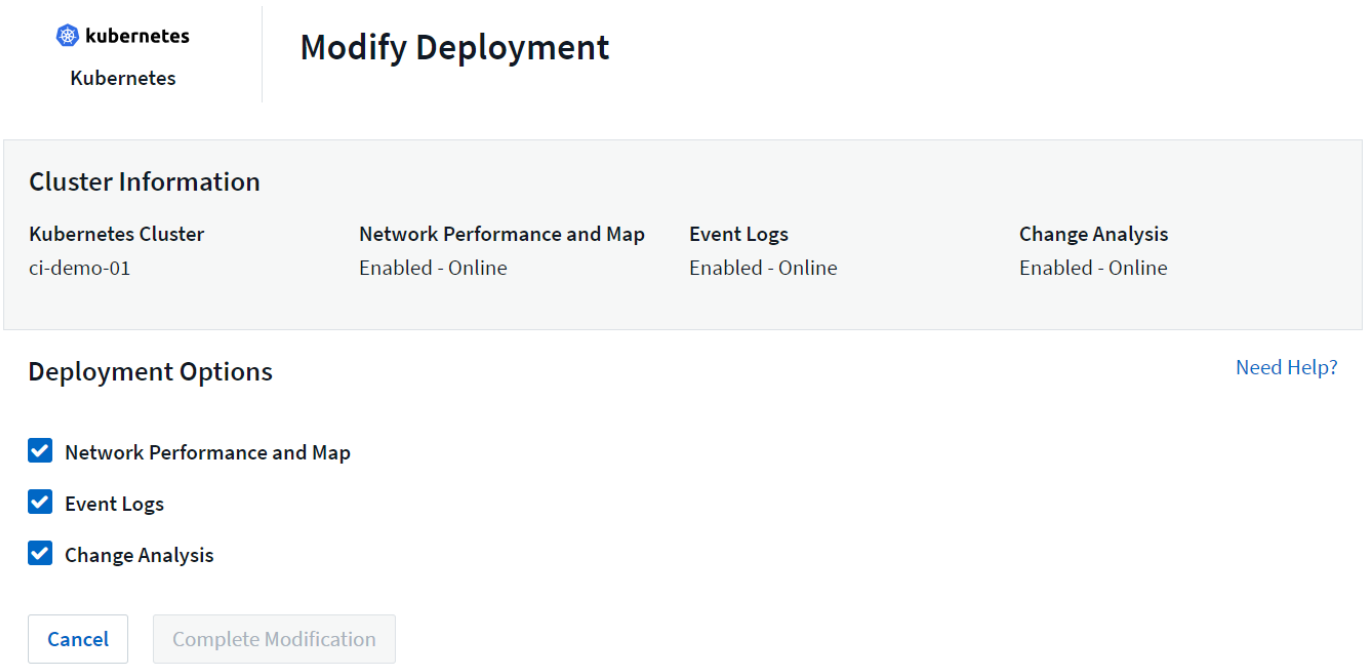
Data Infrastructure Insights Kubernetes Monitoring comprend quatre composants de surveillance :

- Mesures de cluster
- Performances et carte du réseau (facultatif)
- Journaux d'événements (facultatif)
- Analyse des changements (facultatif)

Les composants facultatifs ci-dessus sont activés par défaut pour chaque collecteur Kubernetes ; si vous décidez que vous n'avez pas besoin d'un composant pour un collecteur particulier, vous pouvez le désactiver en accédant à **Kubernetes > Collecteurs** et en sélectionnant *Modifier le déploiement* dans le menu « trois points » du collecteur à droite de l'écran.



L'écran affiche l'état actuel de chaque composant et vous permet de désactiver ou d'activer les composants de ce collecteur selon vos besoins.



Mise à niveau vers la dernière version de Kubernetes Monitoring Operator

Mises à niveau du bouton-poussoir DII

Vous pouvez mettre à niveau l'opérateur de surveillance Kubernetes via la page Collecteurs Kubernetes DII. Cliquez sur le menu à côté du cluster que vous souhaitez mettre à niveau et sélectionnez *Mettre à niveau*. L'opérateur vérifiera les signatures d'image, effectuera un instantané de votre installation actuelle et effectuera la mise à niveau. Dans quelques minutes, vous devriez voir l'état de l'opérateur progresser de « Mise à niveau en cours » à « Dernière mise à jour ». Si vous rencontrez une erreur, vous pouvez sélectionner le statut d'erreur pour plus de détails et vous référer au tableau de dépannage des mises à niveau par bouton-poussoir ci-dessous.

Mises à niveau par simple pression d'un bouton avec des référentiels privés

Si votre opérateur est configuré pour utiliser un référentiel privé, assurez-vous que toutes les images requises pour exécuter l'opérateur et leurs signatures sont disponibles dans votre référentiel. Si vous rencontrez une erreur pendant le processus de mise à niveau pour des images manquantes, ajoutez-les simplement à votre référentiel et réessayez la mise à niveau. Pour télécharger les signatures d'image dans votre référentiel, veuillez utiliser l'outil de cosignature comme suit, en veillant à télécharger les signatures pour toutes les images spécifiées sous 3 Facultatif : Télécharger les images de l'opérateur dans votre référentiel privé > Extrait d'image

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Revenir à une version précédemment exécutée

Si vous avez effectué une mise à niveau à l'aide de la fonction de mise à niveau par simple pression sur un bouton et que vous rencontrez des difficultés avec la version actuelle de l'opérateur dans les sept jours suivant la mise à niveau, vous pouvez rétrograder vers la version précédemment exécutée à l'aide de l'instantané créé pendant le processus de mise à niveau. Cliquez sur le menu à côté du cluster que vous souhaitez restaurer et sélectionnez *Restaurer*.

Mises à niveau manuelles

Déterminez si une *AgentConfiguration* existe avec l'opérateur existant (si votre espace de noms n'est pas le *netapp-monitoring* par défaut, remplacez-le par l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si une _AgentConfiguration_ existe :
```

- Installationle dernier opérateur sur l'opérateur existant.
  - Assurez-vous que vous êtesextraire les dernières images de conteneurs si vous utilisez un référentiel personnalisé.

Si *AgentConfiguration* n'existe pas :

- Notez le nom de votre cluster tel qu'il est reconnu par Data Infrastructure Insights (si votre espace de noms n'est pas le netapp-monitoring par défaut, remplacez-le par l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Créez une sauvegarde de l'opérateur existant (si votre espace de noms
n'est pas le netapp-monitoring par défaut, remplacez-le par l'espace de
noms approprié) :
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-
operator,Désinstaller>>l'opérateur existant.
* <<installing-the-kubernetes-monitoring-operator,Installation>>le
dernier opérateur.
```

  - Utilisez le même nom de cluster.
  - Après avoir téléchargé les derniers fichiers YAML de l'opérateur, reportez toutes les personnalisations trouvées dans *agent_backup.yaml* vers le fichier *operator-config.yaml* téléchargé avant le déploiement.
  - Assurez-vous que vous êtesextraire les dernières images de conteneurs si vous utilisez un référentiel personnalisé.

Arrêt et démarrage de l'opérateur de surveillance Kubernetes

Pour arrêter l'opérateur de surveillance Kubernetes :

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Pour démarrer l'opérateur de surveillance Kubernetes :
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Désinstallation

Pour supprimer l'opérateur de surveillance Kubernetes

Notez que l'espace de noms par défaut pour l'opérateur de surveillance Kubernetes est « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez cet espace de noms dans ces commandes et fichiers et dans tous les suivants.

Les versions plus récentes de l'opérateur de surveillance peuvent être désinstallées avec les commandes suivantes :

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Si l'opérateur de surveillance a été déployé dans son propre espace de noms dédié, supprimez l'espace de noms :

```
 kubectl delete ns <NAMESPACE>
Remarque : si la première commande renvoie « Aucune ressource trouvée »,
utilisez les instructions suivantes pour désinstaller les anciennes
versions de l'opérateur de surveillance.
```

Exécutez chacune des commandes suivantes dans l'ordre. Selon votre installation actuelle, certaines de ces commandes peuvent renvoyer des messages « objet non trouvé ». Ces messages peuvent être ignorés en toute sécurité.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Si une contrainte de contexte de sécurité a été créée précédemment :

```
kubectl delete scc telegraf-hostaccess
```

À propos de Kube-state-metrics

L'opérateur de surveillance NetApp Kubernetes installe ses propres métriques d'état Kube pour éviter tout conflit avec d'autres instances.

Pour plus d'informations sur Kube-State-Metrics, voir"cette page" .

Configuration/Personnalisation de l'opérateur

Ces sections contiennent des informations sur la personnalisation de la configuration de votre opérateur, l'utilisation d'un proxy, l'utilisation d'un référentiel Docker personnalisé ou privé ou l'utilisation d'OpenShift.

Options de configuration

Les paramètres les plus fréquemment modifiés peuvent être configurés dans la ressource personnalisée *AgentConfiguration*. Vous pouvez modifier cette ressource avant de déployer l'opérateur en modifiant le fichier *operator-config.yaml*. Ce fichier comprend des exemples de paramètres commentés. Voir la liste des"paramètres disponibles" pour la version la plus récente de l'opérateur.

Vous pouvez également modifier cette ressource après le déploiement de l'opérateur à l'aide de la commande suivante :

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Pour déterminer si votre version déployée de l'opérateur prend en charge
_AgentConfiguration_, exécutez la commande suivante :
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Si vous voyez un message « Erreur du serveur (NotFound) », votre opérateur
doit être mis à niveau avant de pouvoir utiliser AgentConfiguration.
```

Configuration de la prise en charge du proxy

Il existe deux endroits où vous pouvez utiliser un proxy sur votre locataire afin d'installer Kubernetes Monitoring Operator. Il peut s'agir des mêmes systèmes proxy ou de systèmes proxy distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système où l'extrait est exécuté à votre environnement Data Infrastructure Insights
- Proxy requis par le cluster Kubernetes cible pour communiquer avec votre environnement Data Infrastructure Insights

Si vous utilisez un proxy pour l'un ou les deux, afin d'installer Kubernetes Operating Monitor, vous devez d'abord vous assurer que votre proxy est configuré pour permettre une bonne communication avec votre environnement Data Infrastructure Insights . Si vous disposez d'un proxy et pouvez accéder à Data Infrastructure Insights à partir du serveur/de la machine virtuelle à partir duquel vous souhaitez installer l'opérateur, votre proxy est probablement configuré correctement.

Pour le proxy utilisé pour installer Kubernetes Operating Monitor, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, vous devrez peut-être également définir la variable d'environnement *no_proxy*.

Pour définir la ou les variables, effectuez les étapes suivantes sur votre système **avant** d'installer Kubernetes Monitoring Operator :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
    a. Si le proxy en cours de configuration ne dispose pas d'authentification (nom d'utilisateur/mot de passe), exécutez la commande suivante :

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Si le proxy en cours de configuration dispose d'une
authentification (nom d'utilisateur/mot de passe), exécutez cette
commande :
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Pour que le proxy utilisé pour votre cluster Kubernetes communique avec votre environnement Data Infrastructure Insights , installez Kubernetes Monitoring Operator après avoir lu toutes ces instructions.

Configurez la section proxy de *AgentConfiguration* dans *operator-config.yaml* avant de déployer le Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utiliser un référentiel Docker personnalisé ou privé

Par défaut, l'opérateur de surveillance Kubernetes extrait les images de conteneur du référentiel Data Infrastructure Insights . Si vous disposez d'un cluster Kubernetes utilisé comme cible pour la surveillance et que ce cluster est configuré pour extraire uniquement des images de conteneur à partir d'un référentiel Docker personnalisé ou privé ou d'un registre de conteneurs, vous devez configurer l'accès aux conteneurs nécessaires à l'opérateur de surveillance Kubernetes.

Exécutez « Image Pull Snippet » à partir de la mosaïque d'installation de NetApp Monitoring Operator. Cette commande se connectera au référentiel Data Infrastructure Insights , extraira toutes les dépendances d'image pour l'opérateur et se déconnectera du référentiel Data Infrastructure Insights . Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande télécharge toutes les images utilisées par l'opérateur, y compris pour les fonctionnalités optionnelles. Voir ci-dessous pour les fonctionnalités pour lesquelles ces images sont utilisées.

Fonctionnalités de l'opérateur principal et surveillance de Kubernetes

- surveillance netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- utilisateur root sans distribution

Journal des événements

- ci-fluent-bit
- exportateur d'événements ci-kubernetes

Performances et carte du réseau

- ci-net-observer

Poussez l'image Docker de l'opérateur vers votre référentiel Docker privé/local/d'entreprise conformément à vos politiques d'entreprise. Assurez-vous que les balises d'image et les chemins d'accès aux répertoires de ces images dans votre référentiel sont cohérents avec ceux du référentiel Data Infrastructure Insights .

Modifiez le déploiement de l'opérateur de surveillance dans operator-deployment.yaml et modifiez toutes les références d'image pour utiliser votre référentiel Docker privé.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modifiez *AgentConfiguration* dans *operator-config.yaml* pour refléter le nouvel emplacement du dépôt docker. Créez un nouveau imagePullSecret pour votre dépôt privé, pour plus de détails, consultez *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Jeton d'accès API pour les mots de passe à long terme

Certains environnements (par exemple, les dépôts proxy) exigent des mots de passe à long terme pour le dépôt docker de Data Infrastructure Insights. Le mot de passe fourni dans l'interface utilisateur lors de l'installation n'est valable que 24 heures. Au lieu de cela, on peut utiliser un jeton d'accès API comme mot de passe du dépôt docker. Ce mot de passe sera valable aussi longtemps que le jeton d'accès API est valide. On peut générer un nouveau jeton d'accès API à cette fin ou en utiliser un existant.

"Lire ici" pour obtenir des instructions sur la création d'un nouveau jeton d'accès API.

Pour extraire un jeton d'accès API existant à partir d'un fichier *operator-secrets.yaml* téléchargé, les utilisateurs peuvent exécuter la commande suivante :

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Pour extraire un jeton d'accès API existant d'une installation d'opérateur en cours d'exécution, les utilisateurs peuvent exécuter la commande suivante :

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Instructions OpenShift

Si vous utilisez OpenShift 4.6 ou une version ultérieure, vous devez modifier *AgentConfiguration* dans *operator-config.yaml* pour activer le paramètre *runPrivileged* :

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift peut implémenter un niveau de sécurité supplémentaire qui peut bloquer l'accès à certains composants Kubernetes.

Tolérances et souillures

Les DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* et *netapp-ci-net-observer-l4-ds* doivent planifier un pod sur chaque nœud de votre cluster afin de collecter correctement les données sur tous les nœuds.

L'opérateur a été configuré pour tolérer certaines **souillures** bien connues. Si vous avez configuré des taches personnalisées sur vos nœuds, empêchant ainsi les pods de s'exécuter sur chaque nœud, vous pouvez créer une **tolérance** pour ces taches"dans *AgentConfiguration*" . Si vous avez appliqué des taches personnalisées à tous les nœuds de votre cluster, vous devez également ajouter les tolérances nécessaires au déploiement de l'opérateur pour permettre la planification et l'exécution du pod de l'opérateur.

En savoir plus sur Kubernetes"Souillures et tolérances" .

Retour à la"* Page d'installation de l'opérateur de surveillance NetApp Kubernetes*"

Une note sur les secrets

Pour supprimer l'autorisation permettant à l'opérateur de surveillance Kubernetes d'afficher les secrets à l'échelle du cluster, supprimez les ressources suivantes du fichier *operator-setup.yaml* avant l'installation :

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

S'il s'agit d'une mise à niveau, supprimez également les ressources de votre cluster :

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Si l'analyse des changements est activée, modifiez *AgentConfiguration* ou *operator-config.yaml* pour supprimer le commentaire de la section de gestion des changements et inclure *kindsToIgnoreFromWatch: '"secrets"'* sous la section de gestion des changements. Notez la présence et la position des guillemets simples et doubles dans cette ligne.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Vérification des signatures d'image de l'opérateur de surveillance Kubernetes

L'image de l'opérateur et toutes les images associées qu'il déploie sont signées par NetApp. Vous pouvez vérifier manuellement les images avant l'installation à l'aide de l'outil de cosignature ou configurer un contrôleur d'admission Kubernetes. Pour plus de détails, veuillez consulter le"Documentation Kubernetes" .

La clé publique utilisée pour vérifier les signatures d'image est disponible dans la mosaïque d'installation de l'opérateur de surveillance sous *Facultatif : téléchargez les images de l'opérateur dans votre référentiel privé >*

Clé publique de signature d'image

Pour vérifier manuellement une signature d'image, procédez comme suit :

1. Copiez et exécutez l'extrait d'image
2. Copiez et saisissez le mot de passe du référentiel lorsque vous y êtes invité
3. Stocker la clé publique de signature d'image (dii-image-signing.pub dans l'exemple)
4. Vérifiez les images à l'aide de cosign. Reportez-vous à l'exemple suivant d'utilisation de cosignature

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes lors de la configuration de l'opérateur de surveillance Kubernetes :

Problème:	Essayez ceci:
Je ne vois pas d'hyperlien/connexion entre mon volume persistant Kubernetes et le périphérique de stockage back-end correspondant. Mon volume persistant Kubernetes est configuré à l'aide du nom d'hôte du serveur de stockage.	Suivez les étapes pour désinstaller l'agent Telegraf existant, puis réinstaller le dernier agent Telegraf. Vous devez utiliser Telegraf version 2.0 ou ultérieure et votre stockage de cluster Kubernetes doit être activement surveillé par Data Infrastructure Insights.

Problème:	Essayez ceci:
Je vois des messages dans les journaux ressemblant à ce qui suit : E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.MutatingWebhookConfiguration: the server could not find the requested resource E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.Lease: the server could not find the requested resource (get leases.coordination.k8s.io) etc.	Ces messages peuvent se produire si vous exécutez kube-state-metrics version 2.0.0 ou supérieure avec des versions de Kubernetes inférieures à 1.20. Pour obtenir la version de Kubernetes : *kubectl version* Pour obtenir la version de kube-state-metrics : *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Pour éviter que ces messages ne se produisent, les utilisateurs peuvent modifier leur déploiement kube-state-metrics pour désactiver les baux suivants : *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Plus précisément, ils peuvent utiliser l'argument CLI suivant : resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, La liste de ressources par défaut est : « certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,leases,limitranges,mutatingwebhookconfigurations,namespaces,networkpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas,secrets,services,statefulsets,storageclasses,validatingwebhookconfigurations,volumeattachments »
Je vois des messages d'erreur de Telegraf ressemblant à ce qui suit, mais Telegraf démarre et s'exécute : 11 oct. 14:23:41 ip-172-31-39-47 systemd[1] : Démarré L'agent serveur piloté par plug-in pour la création de rapports de métriques dans InfluxDB. 11 oct. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="échec de la création du répertoire de cache. /etc/telegraf/.cache/snowflake, err : mkdir /etc/telegraf/.ca che : permission refusée. ignoré\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827] : time="2021-10-11T14:23:41Z" level=error msg="échec d'ouverture. Ignoré. ouvrez /etc/telegraf/.cache/snowflake/ocsp_response_cache.json : aucun fichier ou répertoire de ce type\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct. 14:23:41 ip-172-31-39-47 telegraf[1827] : 2021-10-11T14:23:41Z Je ! Démarrage de Telegraf 1.19.3	Il s'agit d'un problème connu. Se référer à"Cet article GitHub" pour plus de détails. Tant que Telegraf est opérationnel, les utilisateurs peuvent ignorer ces messages d'erreur.

Problème:	Essayez ceci:
Sur Kubernetes, mes pods Telegraf signalent l'erreur suivante : « Erreur lors du traitement des informations mountstats : échec d'ouverture du fichier mountstats : /hostfs/proc/1/mountstats, erreur : ouverture de /hostfs/proc/1/mountstats : autorisation refusée »	Si SELinux est activé et appliqué, il empêche probablement les pods Telegraf d'accéder au fichier /proc/1/mountstats sur le nœud Kubernetes. Pour surmonter cette restriction, modifiez la configuration de l'agent et activez le paramètre runPrivileged. Pour plus de détails, reportez-vous aux instructions OpenShift.
Sur Kubernetes, mon pod Telegraf ReplicaSet signale l'erreur suivante : [inputs.prometheus] Erreur dans le plugin : impossible de charger la paire de clés /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key : ouvrir /etc/kubernetes/pki/etcd/server.crt : aucun fichier ou répertoire de ce type	Le pod Telegraf ReplicaSet est destiné à s'exécuter sur un nœud désigné comme maître ou pour etcd. Si le pod ReplicaSet n'est pas en cours d'exécution sur l'un de ces nœuds, vous obtiendrez ces erreurs. Vérifiez si vos nœuds maître/etcd sont contaminés. Si c'est le cas, ajoutez les tolérances nécessaires au Telegraf ReplicaSet, telegraf-rs. Par exemple, modifiez le ReplicaSet… kubectl edit rs telegraf-rs … et ajoutez les tolérances appropriées à la spécification. Ensuite, redémarrez le pod ReplicaSet.
J'ai un environnement PSP/PSA. Cela affecte-t-il mon opérateur de surveillance ?	Si votre cluster Kubernetes s'exécute avec la stratégie de sécurité des pods (PSP) ou l'admission de sécurité des pods (PSA) en place, vous devez effectuer une mise à niveau vers la dernière version de Kubernetes Monitoring Operator. Suivez ces étapes pour mettre à niveau vers l'opérateur actuel avec prise en charge de PSP/PSA : 1. Désinstaller l'opérateur de surveillance précédent : kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installation la dernière version de l'opérateur de surveillance.
J'ai rencontré des problèmes lors du déploiement de l'opérateur et j'utilise PSP/PSA.	1. Modifiez l'agent à l'aide de la commande suivante : kubectl -n <name-space> edit agent 2. Marquer « security-policy-enabled » comme « faux ». Cela désactivera les politiques de sécurité des pods et l'admission de sécurité des pods et permettra à l'opérateur de se déployer. Confirmez en utilisant les commandes suivantes : kubectl get psp (devrait indiquer que la politique de sécurité du pod a été supprimée) kubectl get all -n <namespace>
grep -i psp (devrait indiquer que rien n'est trouvé)	Erreurs « ImagePullBackoff » observées
Ces erreurs peuvent être observées si vous disposez d'un référentiel Docker personnalisé ou privé et que vous n'avez pas encore configuré l'opérateur de surveillance Kubernetes pour le reconnaître correctement. En savoir plus à propos de la configuration pour un référentiel personnalisé/privé.	J'ai un problème avec mon déploiement d'opérateur de surveillance et la documentation actuelle ne m'aide pas à le résoudre.

Problème:	Essayez ceci:

Capturez ou notez autrement la sortie des commandes suivantes et contactez l'équipe de support technique.
 	
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	Les pods net-observer (Workload Map) dans l'espace de noms Operator sont dans CrashLoopBackOff

Ces pods correspondent au collecteur de données Workload Map pour l'observabilité du réseau. Essayez ceci : • Vérifiez les journaux de l'un des pods pour confirmer la version minimale du noyau. Par exemple : ---- {"ci-tenant-id":"votre-id-de-tenant","collector-cluster":"votre-nom-de-cluster-k8s","environment":"prod","level":"error","msg":"échec de validation. Raison : la version du noyau 3.10.0 est inférieure à la version minimale du noyau 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Les pods Net-observer nécessitent que la version du noyau Linux soit au moins 4.18.0. Vérifiez la version du noyau à l'aide de la commande « uname -r » et assurez-vous qu'elle est >= 4.18.0	Les pods s'exécutent dans l'espace de noms de l'opérateur (par défaut : netapp-monitoring), mais aucune donnée n'est affichée dans l'interface utilisateur pour la carte de charge de travail ou les métriques Kubernetes dans les requêtes.
Vérifiez le réglage de l'heure sur les nœuds du cluster K8S. Pour un audit et des rapports de données précis, il est fortement recommandé de synchroniser l'heure sur la machine Agent à l'aide du protocole Network Time Protocol (NTP) ou du protocole Simple Network Time Protocol (SNTP).	Certains des pods d'observateur réseau dans l'espace de noms Operator sont en état d'attente
Net-observer est un DaemonSet et exécute un pod dans chaque nœud du cluster k8s. • Notez le pod qui est en état d'attente et vérifiez s'il rencontre un problème de ressources pour le processeur ou la mémoire. Assurez-vous que la mémoire et le processeur requis sont disponibles dans le nœud.	Je vois ce qui suit dans mes journaux immédiatement après l'installation de Kubernetes Monitoring Operator : [inputs.prometheus] Erreur dans le plugin : erreur lors de la requête HTTP vers http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : obtenir http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : numérotation TCP : recherche kube-state-metrics.<namespace>.svc.cluster.local : aucun hôte de ce type

Problème:	Essayez ceci:
Ce message n'apparaît généralement que lorsqu'un nouvel opérateur est installé et que le pod *telegraf-rs* est opérationnel avant le pod *ksm*. Ces messages devraient cesser une fois que tous les pods sont en cours d'exécution.	Je ne vois aucune métrique collectée pour les CronJobs Kubernetes qui existent dans mon cluster.
Vérifiez votre version de Kubernetes (c'est-à-dire `kubectl version`). S'il s'agit de la version 1.20.x ou d'une version antérieure, il s'agit d'une limitation attendue. La version kube-state-metrics déployée avec l'opérateur de surveillance Kubernetes prend uniquement en charge la version v1.CronJob. Avec Kubernetes 1.20.x et versions antérieures, la ressource CronJob se trouve dans v1beta.CronJob. Par conséquent, kube-state-metrics ne peut pas trouver la ressource CronJob.	Après l'installation de l'opérateur, les pods telegraf-ds entrent dans CrashLoopBackOff et les journaux des pods indiquent « su : échec d'authentification ».
Modifiez la section telegraf dans *AgentConfiguration*, et définissez *dockerMetricCollectionEnabled* sur false. Pour plus de détails, consultez le "options de configuration" de l'opérateur. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Je vois des messages d'erreur répétés ressemblant à ce qui suit dans mes journaux Telegraf : E! [agent] Erreur lors de l'écriture dans outputs.http : Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb" : délai de contexte dépassé (Client.Timeout dépassé lors de l'attente des en-têtes)
Modifiez la section Telegraf dans *AgentConfiguration* et augmentez *outputTimeout* à 10 s. Pour plus de détails, reportez-vous au manuel de l'opérateur."options de configuration" .	Il me manque des données *involvedobject* pour certains journaux d'événements.
Assurez-vous d'avoir suivi les étapes décrites dans la"Autorisations" section ci-dessus.	Pourquoi est-ce que je vois deux pods d'opérateurs de surveillance en cours d'exécution, l'un nommé netapp-ci-monitoring-operator-<pod> et l'autre nommé monitoring-operator-<pod> ?
À compter du 12 octobre 2023, Data Infrastructure Insights a remanié l'opérateur pour mieux servir nos utilisateurs ; pour que ces changements soient pleinement adoptés, vous devezsupprimer l'ancien opérateur etinstaller le nouveau .	Mes événements Kubernetes ont cessé de manière inattendue d'être signalés à Data Infrastructure Insights.
Récupérer le nom du pod exportateur d'événements : `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problème:	Essayez ceci:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Il doit s'agir soit de « netapp-ci-event-exporter » soit de « event-exporter ». Ensuite, modifiez l'agent de surveillance `kubectl -n netapp-monitoring edit agent` et définissez la valeur de LOG_FILE pour refléter le nom de pod d'exportation d'événements approprié trouvé à l'étape précédente. Plus précisément, LOG_FILE doit être défini sur « /var/log/containers/netapp-ci-event-exporter.log » ou « /var/log/containers/event-exporter*.log » …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativement, on peut aussidésinstaller etréinstaller l'agent.
Je vois que des pods déployés par l'opérateur de surveillance Kubernetes se bloquent en raison de ressources insuffisantes.	Consultez l'opérateur de surveillance Kubernetes"options de configuration" pour augmenter les limites du processeur et/ou de la mémoire selon les besoins.
Une image manquante ou une configuration non valide a entraîné l'échec du démarrage ou de la préparation des pods netapp-ci-kube-state-metrics. Désormais, le StatefulSet est bloqué et les modifications de configuration ne sont pas appliquées aux pods netapp-ci-kube-state-metrics.	Le StatefulSet est dans un"cassé" État. Après avoir résolu les problèmes de configuration, faites rebondir les pods netapp-ci-kube-state-metrics.
Les pods netapp-ci-kube-state-metrics ne parviennent pas à démarrer après l'exécution d'une mise à niveau de l'opérateur Kubernetes, générant ErrImagePull (échec de l'extraction de l'image).	Essayez de réinitialiser les pods manuellement.
Les messages « Événement rejeté car plus ancien que maxEventAgeSeconds » sont observés pour mon cluster Kubernetes sous Analyse des journaux.	Modifiez l'opérateur *agentconfiguration* et augmentez *event-exporter-maxEventAgeSeconds* (c'est-à-dire à 60 s), *event-exporter-kubeQPS* (c'est-à-dire à 100) et *event-exporter-kubeBurst* (c'est-à-dire à 500). Pour plus de détails sur ces options de configuration, consultez le"options de configuration" page.

Problème:	Essayez ceci:
Telegraf avertit ou plante à cause d'une mémoire verrouillable insuffisante.	Essayez d'augmenter la limite de mémoire verrouillable pour Telegraf dans le système d'exploitation/nœud sous-jacent. Si l'augmentation de la limite n'est pas une option, modifiez la configuration de l'agent NKMO et définissez *unprotected* sur *true*. Cela indiquera à Telegraf de ne pas tenter de réserver des pages de mémoire verrouillées. Bien que cela puisse présenter un risque de sécurité, car les secrets déchiffrés peuvent être échangés sur le disque, cela permet l'exécution dans des environnements où la réservation de mémoire verrouillée n'est pas possible. Pour plus de détails sur les options de configuration *non protégées*, reportez-vous à la"options de configuration" page.
Je vois des messages d'avertissement de Telegraf ressemblant à ce qui suit : *W! [inputs.diskio] Impossible de récupérer le nom du disque pour « vdc » : erreur de lecture de /dev/vdc : aucun fichier ou répertoire de ce type*	Pour l'opérateur de surveillance Kubernetes, ces messages d'avertissement sont sans conséquence et peuvent être ignorés. Vous pouvez également modifier la section telegraf dans AgentConfiguration et définir *runDsPrivileged* sur true. Pour plus de détails, consultez le "options de configuration de l'opérateur".

Problème:	Essayez ceci:

Mon pod Fluent-bit échoue avec les erreurs suivantes : [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Trop de fichiers ouverts [2024/10/16 14:16:23] [error] échec d'initialisation de l'entrée tail.0 [2024/10/16 14:16:23] [error] [engine] échec d'initialisation de l'entrée	Essayez de modifier vos paramètres *fsnotify* dans votre cluster :
	
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	
	Redémarrez Fluent-bit.
	
	Remarque : pour que ces paramètres soient persistants après chaque redémarrage du nœud, vous devez placer les lignes suivantes dans */etc/sysctl.conf*
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problème:	Essayez ceci:
Les pods DS de Telegraf signalent des erreurs liées au fait que le plug-in d’entrée Kubernetes ne parvient pas à effectuer des requêtes HTTP en raison de l’impossibilité de valider le certificat TLS. Par exemple : E! [inputs.kubernetes] Erreur dans le plugin : erreur lors de la requête HTTP vers"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Obtenir"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls : échec de vérification du certificat : x509 : impossible de valider le certificat pour <kubelet_IP> car il ne contient aucun SAN IP	Cela se produit si le kubelet utilise des certificats auto-signés et/ou si le certificat spécifié n'inclut pas le <kubelet_IP> dans la liste *Subject Alternative Name* des certificats. Pour résoudre ce problème, l'utilisateur peut modifier le"configuration de l'agent" , et définissez *telegraf:insecureK8sSkipVerify* sur *true*. Cela configurera le plugin d'entrée Telegraf pour ignorer la vérification. Alternativement, l'utilisateur peut configurer le kubelet pour"serveurTLSBootstrap" , ce qui déclenchera une demande de certificat à partir de l'API « certificates.k8s.io ».
Je rencontre l'erreur suivante dans les pods Fluent-bit et le pod ne peut pas démarrer : [2026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	Assurez-vous que le répertoire hôte dans lequel le fichier DB réside dispose des permissions de lecture/écriture appropriées. Plus précisément, le répertoire hôte doit accorder des permissions de lecture/écriture aux utilisateurs non-root. L'emplacement par défaut du fichier DB est /var/log/ sauf si cela est remplacé par l'option fluent-bit-dbFile *agentconfiguration*. Si SELinux est activé, essayez de définir l'option fluent-bit-seLinuxOptionsType agentconfiguration sur 'spc_t'.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Options de configuration de l'opérateur de surveillance Kubernetes

Le "Opérateur de surveillance Kubernetes" Offre de nombreuses options de personnalisation via le fichier AgentConfiguration. Vous pouvez configurer les limites de ressources, les intervalles de collecte, les paramètres de proxy, les tolérances et les paramètres spécifiques aux composants afin d'optimiser la surveillance de votre environnement Kubernetes. Utilisez ces options pour personnaliser Telegraf, Kube-State-Metrics, la collecte des journaux, le mappage des charges de travail, la gestion des modifications et d'autres composants de surveillance.

Exemple de fichier AgentConfiguration

Vous trouverez ci-dessous un exemple de fichier *AgentConfiguration*, avec la description de chaque option.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
```

```
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  ##
  ## One can modify the following settings to configure and customize the
operator.
  ## Optional settings are commented out with their default values for
reference.
  ## To update them, uncomment the line, change the value, and apply the
updated AgentConfiguration.
  ##
  agent:
    ##
    ## [REQUIRED FIELD]
    ## A uniquely identifiable user-friendly cluster name
    ## The cluster name must be unique across all clusters in your Data
Infrastructure Insights (DII) environment.
    ##
    clusterName: "my_cluster"

    ##
    ## Proxy settings
    ## If applicable, specify the proxy through which the operator should
communicate with DII.
    ## Refer to additional documentation here:
    ## https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    ##
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    ##
    ## [REQUIRED FIELD]
    ## Repository from which the operator pulls the required images
    ## By default, the operator pulls from the DII repository. To use a
private repository, set this field to the
```

```
    ## applicable repository name. Refer to additional documentation here:
    ## https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    ##
    dockerRepo: 'docker.c01.cloudinsights.netapp.com'
    ##
    ## [REQUIRED FIELD]
    ## Name of the imagePullSecret required for dockerRepo
    ## When using a private repository, set this field to the applicable
secret name.
    ##
    dockerImagePullSecret: 'netapp-ci-docker'

    ##
    ## Automatic expiring API key rotation settings
    ## Allow the operator to automatically rotate its expiring API key,
generating a new API key and
    ## using it to replace the expiring one. The expiring API key itself
must support auto rotation.
    ##
    # tokenRotationEnabled: 'true'
    ##
    ## Threshold (number of days before expiration) at which the operator
should trigger rotation.
    ## The threshold must be less than the total duration of the API key.
    ##
    # tokenRotationThresholdDays: '30'

  push-button-upgrades:
    ##
    ## Allow the operator to be upgraded using the Data Infrastructure
Insights (DII) UI
    ##
    # enabled: 'true'

    ##
    ## Frequency at which the operator polls and checks for upgrade
requests from DII
    ##
    # polltimeSeconds: '60'

    ##
    ## Allow operator upgrade to proceed even if new images are not
present
    ##
```

```
    # ignoreImageNotPresent: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreImageSignatureFailure: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreYAMLSignatureFailure: 'false'

    ##
    ## Use dockerImagePullSecret to access the image repository and verify
the existence of the new images
    ##
    # imageValidationUseSecret: 'true'

    ##
    ## Time allowed for the old operator pod to shutdown before reporting
an upgrade failure to DII
    ##
    # upgradesShutdownTime: '240'

    ##
    ## Time allowed for the new operator pod to startup before reporting
an upgrade failure to DII
    ##
    # upgradesStartupTime: '600'

  telegraf:
    ##
    ## Frequency at which telegraf collects data
    ## The frequency should not exceed 60s.
    ##
    # collectionInterval: '60s'

    ##
    ## Maximum number of metrics per batch
    ## Telegraf sends metrics to outputs in batches. This controls the
size of those writes.
    ##
```

```
    # batchSize: '10000'

    ##
    ## Maximum number of unwritten metrics per output
    ## Telegraf caches metrics until they are successfully written by the
output. This controls how many metrics
    ## can be cached. Once the buffer is filled, the oldest metrics will
get dropped.
    ##
    # bufferLimit: '150000'

    ##
    ## Rounds collection interval to collectionInterval
    ## If collectionInterval is 60s, collection will occur on-the-minute
    ##
    # roundInterval: 'true'

    ##
    ## Jitter between plugins on collection
    ## Each input plugin sleeps a random amount of time within jitter
before collecting. This can be used to prevent
    ## multiple input plugins from querying the same resources at the same
time. The maximum collection interval would
    ## be collectionInterval + collectionJitter.
    ##
    # collectionJitter: '0s'

    ##
    ## Precision to which collected metrics are rounded
    ## When set to "0s", precision will be set by the units specified by
collectionInterval.
    ##
    # precision: '0s'

    ##
    ## Frequency at which telegraf flushes and writes data
    ## Frequency should not exceed collectionInterval.
    ##
    # flushInterval: '60s'

    ##
    ## Jitter between plugins on writes
    ## Each output plugin sleeps a random amount of time within jitter
before flushing. This can be used to prevent
    ## multiple output plugins from writing the same resources at the same
time, and causing large spikes. The maximum
```

```
    ## flush interval would be flushInterval + flushJitter.
    ##
    # flushJitter: '0s'

    ##
    ## Timeout for HTTP output plugins
    ## Time allowed for http output plugins to successfully writing before
failing.
    ##
    # outputTimeout: '5s'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-ds DaemonSet
    ##
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-rs ReplicaSet
    ##
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    ##
    ## telegraf runs through the processor plugins a second time after the
aggregators plugins, by default. Use this
    ## option to skip the second run.
    ##
    # skipProcessorsAfterAggregators: 'false'

    ##
    ## Additional tolerations for netapp-ci-telegraf-ds DaemonSet and
netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet and netapp-ci-
telegraf-ds DaemonSet to view the default tolerations.
    ## If additional tolerations are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # dsTolerations: ''
```

```
    # rsTolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet to view the default
node selectors terms. If additional node
    ## selector terms are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # rsNodeSelectorTerms: ''

    ##
    ## telegraf uses lockable memory to protect secrets in memory. If
telegraf issues warnings about insufficient
    ## lockable memory, try increasing the limit of lockable memory on the
applicable nodes. If increasing this limit
    ## is not an option for the given environment, set unprotected to true
so telegraf does not attempt to use
    ## lockable memory.
    ##
    # unprotected: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf-mountstats-
poller container in privileged mode
    ## The telegraf-mountstats-poller container needs read-only access to
system files such as those in /proc/ (i.e. to
    ## monitor NFS IO metrics, etc.). Some environments impose restricts
that prevent the container from reading these
    ## system files. Unless those restrictions are lifted, users may need
to run this container in privileged mode.
    ##
    # runPrivileged: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf container in
privileged mode
    ## The telegraf container needs read-only access to system files such
as those in /dev/ (i.e. for the telegraf
    ## diskio input plugin to retrieve disk metrics). Some environments
```

```
impose restricts that prevent the container from
    ## accessing these system files. Unless those restrictions are lifted,
users may need to run this container in
    ## privileged mode.
    ##
    # runDsPrivileged: 'false'

    ##
    ## Allow the netapp-ci-telegraf-ds DaemonSet's telegraf-ds, telegraf-
init, and telegraf-mountstats-poller containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## /proc/1/mountstats, etc.). Allowing escalation privilege should
negate the need to run these containers in
    ## privileged mode.
    ##
    # allowDsPrivilegeEscalation: 'true'

    ##
    ## Allow the netapp-ci-telegraf-rs DaemonSet's telegraf-rs and
telegraf-rs-init containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## etcd credentials when applicable, etc.). Allowing escalation
privilege should negate the need to run these
    ## containers in privileged mode.
    ##
    # allowRsPrivilegeEscalation: 'true'

    ##
    ## Enable collection of block IO metrics (kubernetes.pod_to_storage)
    ##
    # dsBlockIOEnabled: 'true'

    ##
    ## Enable collection of NFS IO metrics (kubernetes.pod_to_storage)
    ##
    # dsNfsIOEnabled: 'true'

    ##
    ## Enable collection of system-specific objects/metrics for managed
k8s clusters
    ## This consists of k8s objects within the kube-system and cattle-
system namespaces for managed k8s clusters
    ## (i.e. EKS, AKS, GKE, managed Rancher, etc.).
    ##
```

```
    # managedK8sSystemMetricCollectionEnabled: 'false'

    ##
    ## Enable collection of pod ephemeral storage metrics
(kubernetes.pod_volume)
    ##
    # podVolumeMetricCollectionEnabled: 'false'

    ##
    ## Declare Rancher cluster is managed
    ## Rancher can be deployed in managed or on-premise environments. The
operator contains logic to try to determine
    ## which type of environment Rancher is running in (i.e. to factor
into managedK8sSystemMetricCollectionEnabled).
    ## If the operator logic misidentifies whether Rancher is running in a
managed environment or not, use this option
    ## to declare Rancher is managed.
    ##
    # isManagedRancher: 'false'

    ##
    ## Locations for the etcd certificate and key files
    ## The operator looks at well-known locations for the etcd certificate
and key files. If this cannot find these
    ## files, the applicable telegraf input plugin will fail. Use this
option to specify the complete filepath to these
    ## files on the nodes.
    ## Note that the well-known locations for these files are typically
root-protected. This is one of the reasons why
    ## the netapp-ci-telegraf-rs ReplicaSet's telegraf-rs-init container
needs to run with escalation privileges.
    ##
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

    ##
    ## Allow operator/telegraf communications with k8s without TLS
verification
    ## In some environments, TLS verification will not succeed (i.e.
certificates lack IP SANs). To skip the
    ## verification, use this option.
    ##
    # insecureK8sSkipVerify: 'false'

  kube-state-metrics:
    ##
```

```
    ## CPU/Mem limits and requests for netapp-ci-kube-state-metrics
StatefulSet
    ##
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    ##
    ## Comma-separated list of k8s resources for which to collect metrics
    ## Refer to the kube-state-metrics --resources CLI option
    ##
    # resources:
'cronjobs,daemonsets,deployments,horizontalpodautoscalers,ingresses,jobs,n
amespaces,nodes,persistentvolumeclaims,persistentvolumes,pods,replicasets,
resourcequotas,services,statefulsets'

    ##
    ## Comma-separated list of k8s metrics to collect
    ## Refer to the kube-state-metrics --metric-allowlist CLI option
    ##
    # metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_
daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daem
onset_status_desired_number_scheduled,kube_daemonset_status_number_availab
le,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_
ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_obser
ved_generation,kube_daemonset_status_updated_number_scheduled,kube_daemons
et_metadata_generation,kube_daemonset_labels,kube_deployment_status_replic
as,kube_deployment_status_replicas_available,kube_deployment_status_replic
as_unavailable,kube_deployment_status_replicas_updated,kube_deployment_sta
tus_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec
_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_d
eployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_g
eneration,kube_deployment_labels,kube_deployment_created,kube_job_created,
kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_s
tatus_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_co
mpletion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_
status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec
_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube
_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persisten
tvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_ac
cess_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_label
s,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persiste
ntvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_comp
letion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_
```

```
status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_co
ntainer_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_
requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_
pod_container_resource_requests_storage_bytes,kube_pod_container_resource_
requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests,kube_horizontal
podautoscaler_spec_max_replicas,kube_horizontalpodautoscaler_spec_min_repl
icas,kube_horizontalpodautoscaler_status_condition,kube_horizontalpodautos
caler_status_current_replicas,kube_horizontalpodautoscaler_status_desired_
replicas'

    ##
    ## Comma-separated list of k8s label keys that will be used to
```

```
determine which labels to export/collect
    ## Refer to the kube-state-metrics --metric-labels-allowlist CLI
option
    ##
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],horizontalpodautoscalers=[*],
ingresses=[*],jobs=[*],namespaces=[*],nodes=[*],persistentvolumeclaims=[*]
,persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],service
s=[*],statefulsets=[*]'

    ##
    ## Additional tolerations for netapp-ci-kube-state-metrics StatefulSet
    ## Inspect the netapp-ci-kube-state-metrics StatefulSet to view the
default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # tolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-kube-state-metrics
StatefulSet
    ## Inspect the kube-state-metrics StatefulSet to view the default node
selectors terms. If additional node selector
    ## terms are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''

    ##
    ## Number of kube-state-metrics shards
    ## For large clusters, kube-state-metrics may be overwhelmed with
collecting and exporting the amount of metrics
    ## generated. This can lead to collection timeouts for the netapp-ci-
telegraf-rs pod. If this is observed, use this
    ## option to increase the number of kube-state-metrics shards to
redistribute the workload.
```

```
    ##
    # shards: '2'

  logs:
    ##
    ## Allow the netapp-ci-fluent-bit-ds DaemonSet's fluent-bit container
to run with escalation privilege.
    ## This is needed to access/read root-protected files (event-exporter
pod log, fluent-bit DB file, etc.).
    ##
    # fluent-bit-allowPrivilegeEscalation: 'true'

    ##
    ## Read content from the head of the file, not the tail
    ##
    # readFromHead: "true"

    ##
    ## Network protocol for DNS (i.e. UDP, TCP, etc.)
    ##
    # dnsMode: "UDP"

    ##
    ## DNS resolver (i.e. LEGACY, ASYNC, etc.)
    ##
    # fluentBitDNSResolver: "LEGACY"

    ##
    ## Additional tolerations for netapp-ci-fluent-bit-ds DaemonSet
    ## Inspect the netapp-ci-fluent-bit-ds DaemonSet to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # fluent-bit-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-fluent-bit-ds DaemonSet
    ##
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
    # fluent-bit-memRequest: '100Mi'
```

```
    ##
    ## Top-level host path in which the kubernetes container logs reside,
including any symlinks from var/log/containers
    ## For example, if /var/log/containers/*.log is a symlink to
/kubernetes/log to
    ## /kubernetes/var/lib/docker/containers/*/*.log, fluent-bit-
containerLogPath should be set to '/kubernetes'.
    ##
    # fluent-bit-containerLogPath: '/var/lib/docker/containers'

    ## fluent-bit DB file path/location

    ##
    ## fluent-bit DB file path/location
    ## By default, fluent-bit is configured to use /var/log/netapp-
monitoring_flb_kube.db.  This path usually requires
    ## escalated privileges for read/write. Users who want to avoid
escalation privilege can use this option to specify
    ## a different DB file path/location. The custom path/location should
allow non-root users to read/write.
    ## Ideally, the path/location should be persistent.
    ##
    # fluent-bit-dbFile: '/var/log/netapp-monitoring_flb_kube.db'

    ##
    ## Additional tolerations for netapp-ci-event-exporter Deployment
    ## Inspect the netapp-ci-event-exporter Deployment to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # event-exporter-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-event-exporter Deployment
    ##
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'

    ##
    ## Max age for events to be processed and exported; older events are
```

```
discarded
    ##
    # event-exporter-maxEventAgeSeconds: '10'

    ##
    ## Client-side throttling
    ## Set event-exporter-kubeBurst to roughly match event rate
    ## Set event-exporter-kubeQPS to approximately 1/5 of event-exporter-
kubeBurst
    ##
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    ##
    ## Additional node selector terms for netapp-ci-event-exporter
Deployment
    ## Inspect the event-exporter Deployment to view the default node
selectors terms. If additional node selector terms
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # event-exporter-nodeSelectorTerms: ''

  workload-map:
    ## Run workload-map container with escalation privilege to coordinate
memlocks
    ##
    ## Allow the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container to run with escalation privilege.
    ## This is needed to coordinate memlocks.
    ##
    # allowPrivilegeEscalation: 'true'

    ##
    ## CPU/Mem limits and requests for netapp-ci-net-observer-l4-ds
DaemonSet
    ##
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
```

```
    # memRequest: '500Mi'

    ##
    ## Metric aggregation interval (in seconds)
    ## Set metricAggregationInterval between 30 and 120
    ##
    # metricAggregationInterval: '60'

    ##
    ## Interval for bpf polling
    ## Set bpfPollInterval between 3 and 15
    ##
    # bpfPollInterval: '8'

    ##
    ## Enable reverse DNS lookups on observed IPs
    ##
    # enableDNSLookup: 'true'

    ##
    ## Additional tolerations for netapp-ci-net-observer-l4-ds DaemonSet
    ## Inspect the netapp-ci-net-observer-l4-ds DaemonSet to view the
default tolerations. If additional tolerations
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # l4-tolerations: ''

    ##
    ## Run the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container in privileged mode
    ## Some environments impose restricts that prevent the net-observer
container from running.
    ## Unless those restrictions are lifted, users may need to run this
container in privileged mode.
    ##
    # runPrivileged: 'false'

  change-management:
    ##
    ## CPU/Mem limits and requests for netapp-ci-change-observer-watch-rs
ReplicaSet
    ##
```

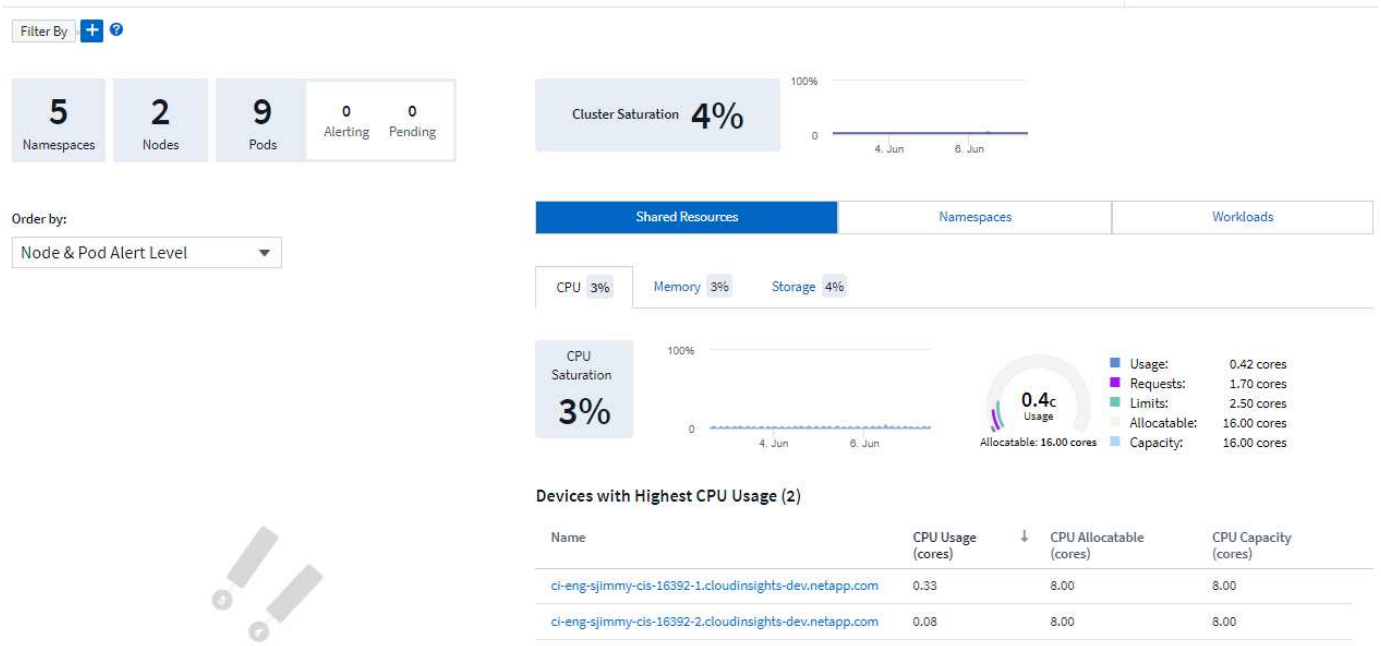
```
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    ##
    ## Interval (in seconds) after which a non-successful deployment of a
workload will be marked as failed
    ##
    # workloadFailureDeclarationIntervalSeconds: '30'

    ##
    ## Frequency (in seconds) at which workload deployments are combined
and sent
    ##
    # workloadDeployAggrIntervalSeconds: '300'

    ##
    ## Frequency (in seconds) at which non-workload deployments are
combined and sent
    ##
    # nonWorkloadDeployAggrIntervalSeconds: '15'

    ##
    ## Set of regular expressions used in env names and data maps whose
value will be redacted
    ##
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

    ##
    ## Additional node selector terms for netapp-ci-change-observer-watch-
rs ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default node selectors terms. If additional
    ## node selector terms are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
```

```
    # nodeSelectorTerms: ''

    ##
    ## Comma-separated list of additional kinds to watch
    ## Each kind should be prefixed by its API group. This list in
addition to the default set of kinds watched by the
    ## collector.
    ##
    ## Example: '"authorization.k8s.io.subjectaccessreviews"'
    ##
    # additionalKindsToWatch: ''

    ##
    ## Comma-separated list of additional field paths whose diff is
ignored as part of change analytics
    ## This list in addition to the default set of field paths ignored by
the collector.
    ##
    ## Example: '"metadata.specTime", "data.status"'
    ##
    # additionalFieldsDiffToIgnore: ''

    ##
    ## Comma-separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    ## Each kind should be prefixed by its API group.
    ##
    ## Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    ##
    # kindsToIgnoreFromWatch: ''

    ##
    ## Frequency with which log records are sent to DII from the collector
    ##
    # logRecordAggrIntervalSeconds: '20'

    ##
    ## Additional tolerations for netapp-ci-change-observer-watch-rs
ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
```

```
taint2, operator: Exists, effect: NoExecute}'
    ##
    # watch-tolerations: ''
```

Page de détails du cluster Kubernetes

La page de détails du cluster Kubernetes affiche un aperçu détaillé de votre cluster Kubernetes.



Nombre d’espaces de noms, de nœuds et de pods

Les comptes en haut de la page vous indiquent le nombre total d’espaces de noms, de nœuds et de pods dans le cluster, ainsi que le nombre de popds actuellement en alerte et en attente.

Ressources partagées et saturation

En haut à droite de la page de détails se trouve la saturation de votre cluster sous forme de pourcentage actuel ainsi qu’un graphique montrant la tendance récente au fil du temps. La saturation du cluster correspond à la saturation la plus élevée du processeur, de la mémoire ou du stockage à chaque instant.

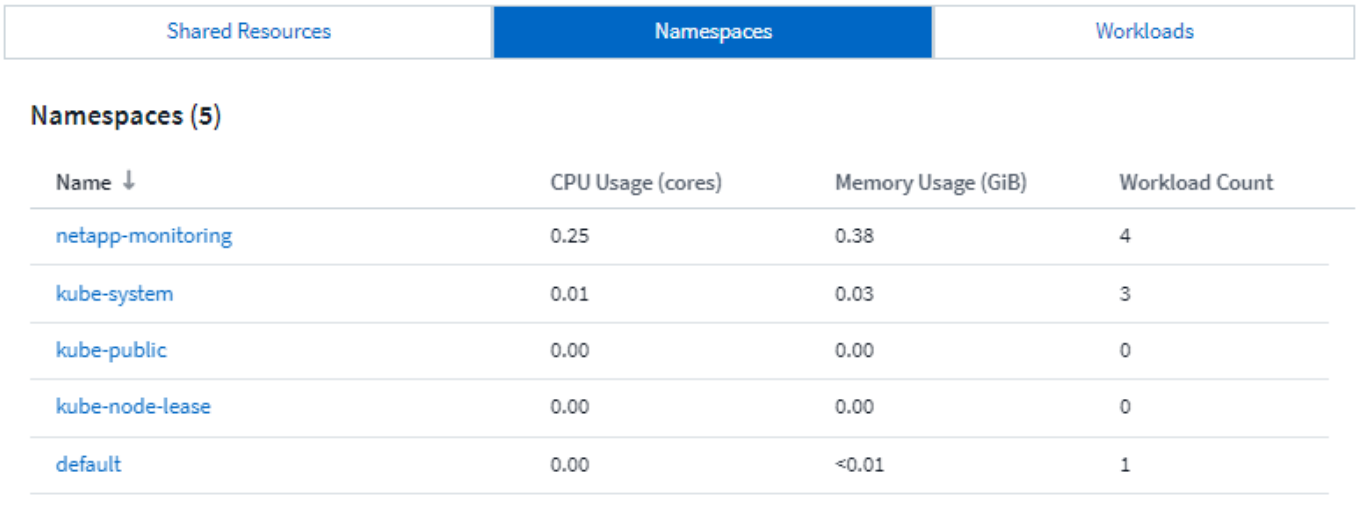
En dessous, la page affiche par défaut l’utilisation des **Ressources partagées**, avec des onglets pour le processeur, la mémoire et le stockage. Chaque onglet affiche le pourcentage de saturation et la tendance au fil du temps, avec des détails d’utilisation supplémentaires. Pour le stockage, la valeur affichée est la plus élevée entre la saturation du backend et du système de fichiers, qui sont calculées indépendamment.

Les appareils les plus utilisés sont indiqués dans un tableau en bas. Cliquez sur n’importe quel lien pour explorer ces appareils.

Espaces de noms

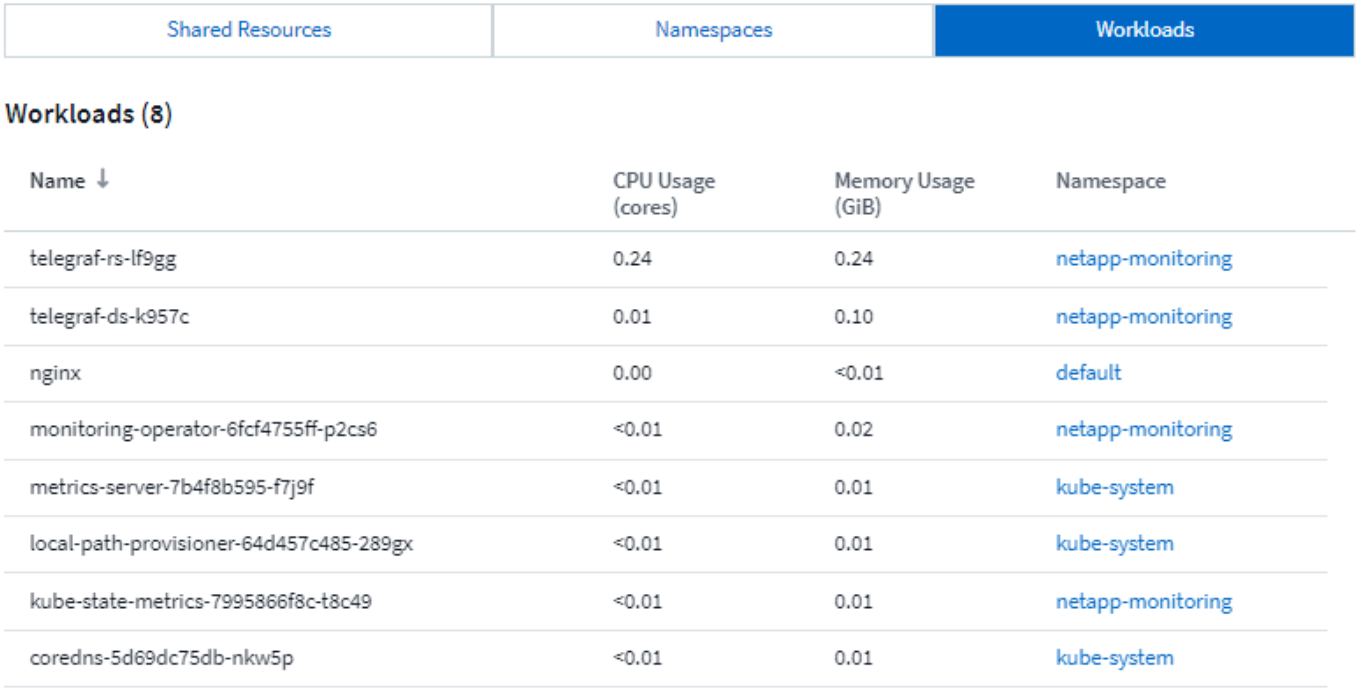
L’onglet Espaces de noms affiche une liste de tous les espaces de noms de votre environnement Kubernetes,

indiquant l'utilisation du processeur et de la mémoire ainsi qu'un nombre de charges de travail dans chaque espace de noms. Cliquez sur les liens Nom pour explorer chaque espace de noms.



Charges de travail

De même, l'onglet Charges de travail affiche une liste des charges de travail dans chaque espace de noms, indiquant à nouveau l'utilisation du processeur et de la mémoire. En cliquant sur les liens de l'espace de noms, vous accédez à chacun d'eux.



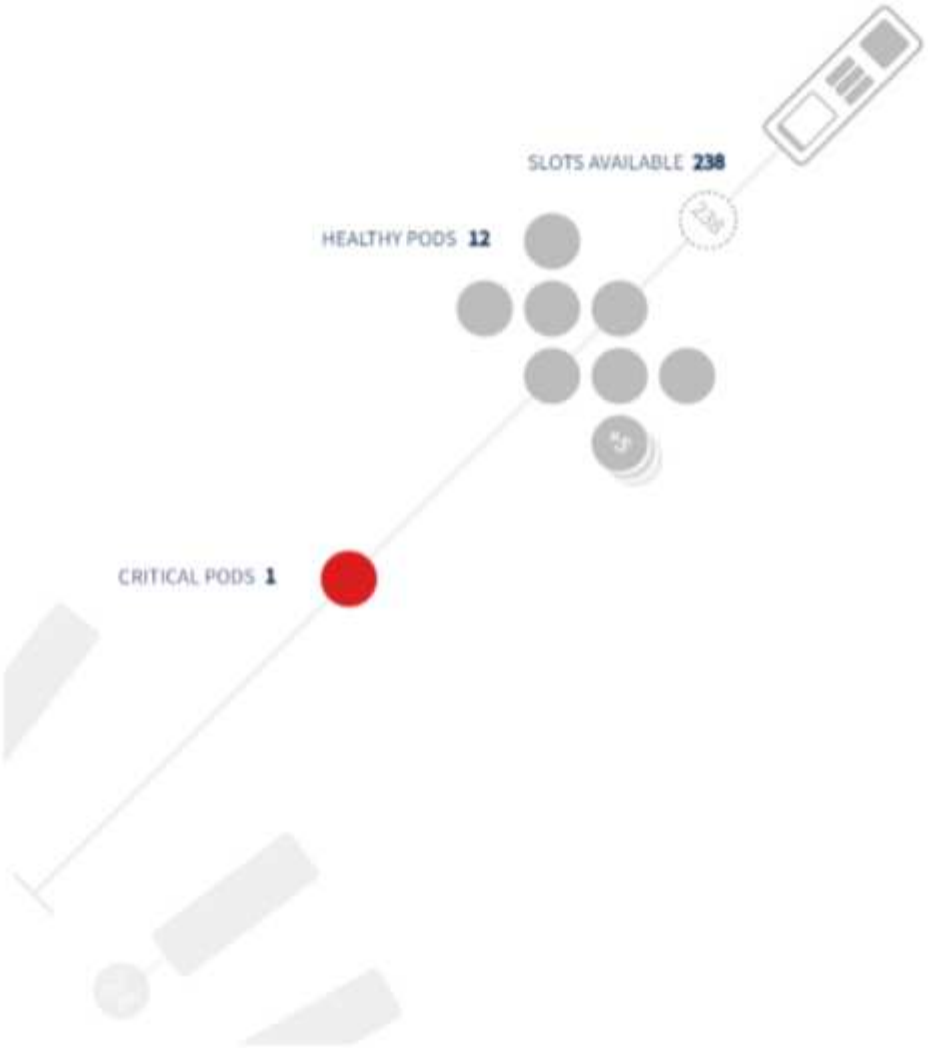
La « roue » du cluster

La section « Roue » du cluster fournit un aperçu de l'état des nœuds et des pods, que vous pouvez explorer pour obtenir plus d'informations. Si votre cluster contient plus de nœuds que ce qui peut être affiché dans cette zone de la page, vous pourrez tourner la roue à l'aide des boutons disponibles.

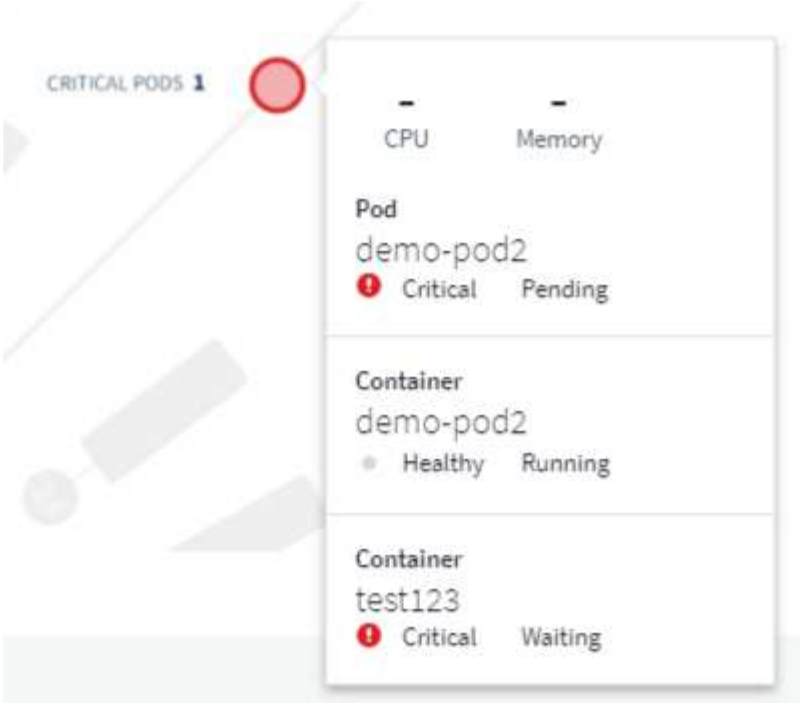
Les pods ou nœuds d'alerte sont affichés en rouge. Les zones « Avertissement » sont affichées en orange. Les pods non planifiés (c'est-à-dire non attachés) s'afficheront dans le coin inférieur de la « Roue » du cluster.

Survoler un pod (cercle) ou un nœud (barre) étendra la vue du nœud.

Cliquer sur le pod ou le nœud dans cette vue effectuera un zoom avant sur la vue du nœud développée.



À partir de là, vous pouvez survoler un élément pour afficher les détails de cet élément. Par exemple, survoler le pod critique dans cet exemple affiche les détails sur ce pod.



Vous pouvez afficher les informations sur le système de fichiers, la mémoire et le processeur en survolant les éléments du nœud.

Une note sur les jauges

Les jauges de mémoire et de processeur affichent trois couleurs, car elles indiquent la capacité utilisée par rapport à la capacité allouable et à la capacité totale.

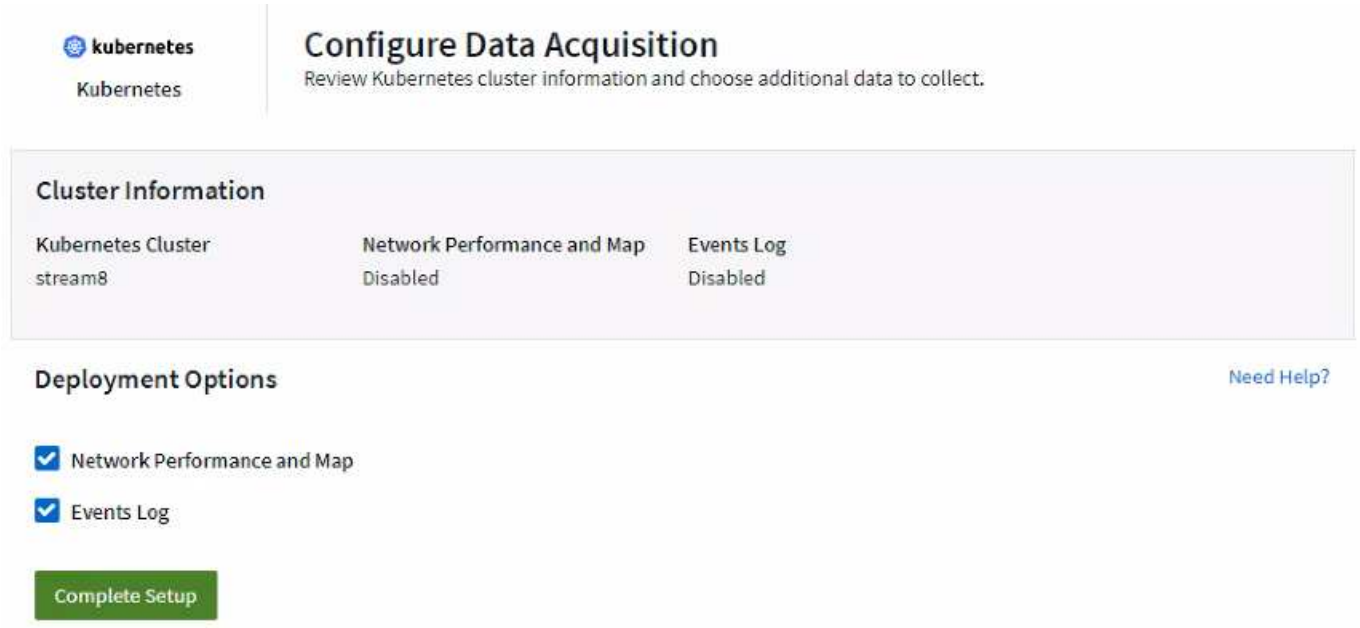
Surveillance et cartographie des performances du réseau Kubernetes

La fonctionnalité Kubernetes Network Performance Monitoring and Map simplifie le dépannage en mappant les dépendances entre les services (également appelés charges de travail) et offre une visibilité en temps réel sur les latences et les anomalies des performances du réseau pour identifier les problèmes de performances avant qu'ils n'affectent les utilisateurs. Cette capacité aide les organisations à réduire les coûts globaux en analysant et en auditant les flux de trafic Kubernetes.

Principales fonctionnalités : • La carte de charge de travail présente les dépendances et les flux de charge de travail de Kubernetes et met en évidence les problèmes de réseau et de performances. • Surveillez le trafic réseau entre les pods, les charges de travail et les nœuds Kubernetes ; identifiez la source des problèmes de trafic et de latence. • Réduisez les coûts globaux en analysant le trafic réseau entrant, sortant, interrégional et interzone.

Prérequis

Avant de pouvoir utiliser la surveillance et la cartographie des performances du réseau Kubernetes, vous devez avoir configuré le"Opérateur de surveillance NetApp Kubernetes" pour activer cette option. Lors du déploiement de l'opérateur, sélectionnez la case à cocher « Performances et carte du réseau » pour l'activer. Vous pouvez également activer cette option en accédant à une page de destination Kubernetes et en sélectionnant « Modifier le déploiement ».



Moniteurs

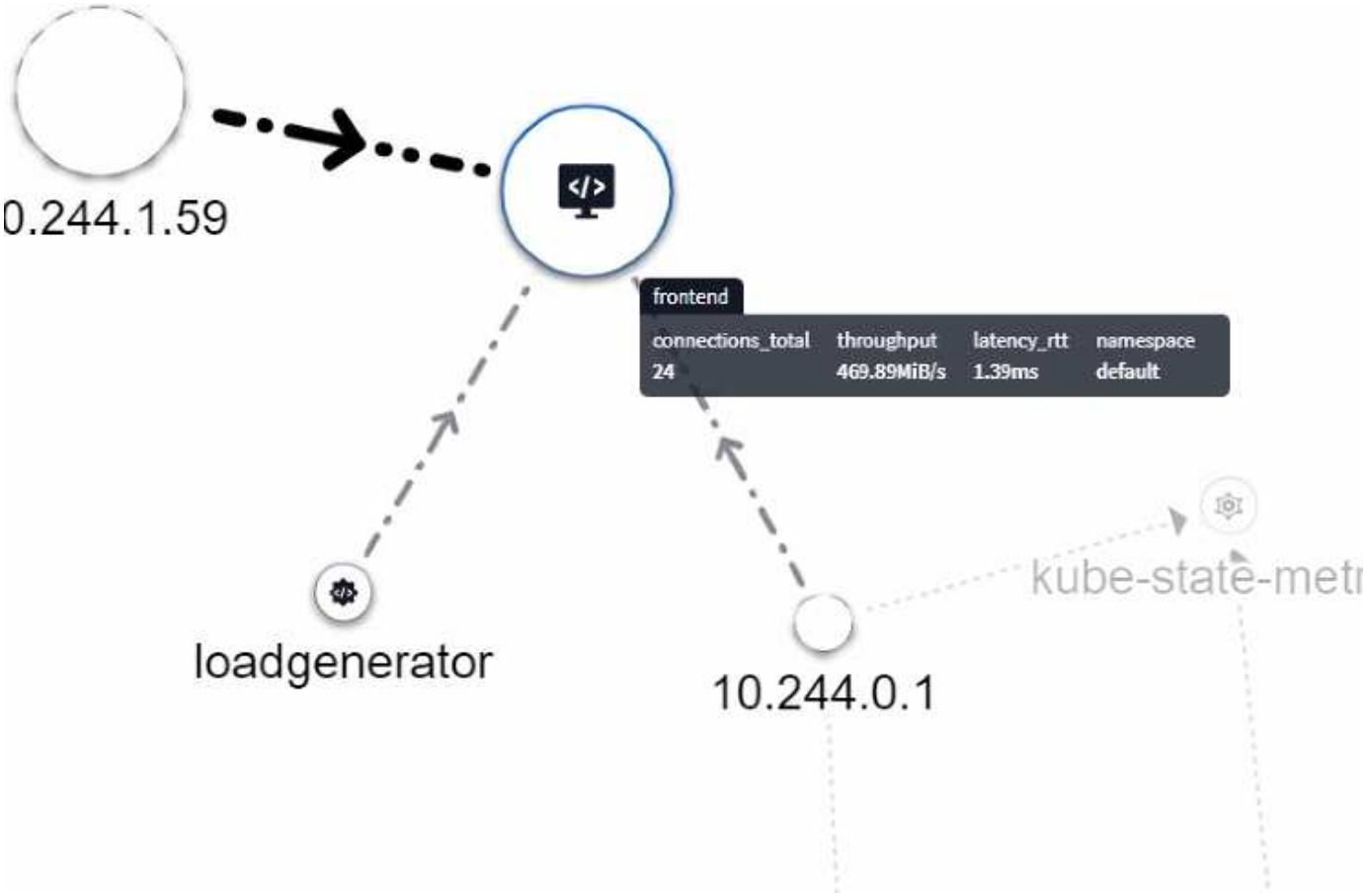
La carte de charge de travail utilise"moniteurs" pour obtenir des informations. Data Infrastructure Insights fournit un certain nombre de moniteurs Kubernetes par défaut (notez que ceux-ci peuvent être *en pause* par défaut). Vous pouvez *Reprendre* (c'est-à-dire activer) les moniteurs que vous souhaitez, ou vous pouvez créer des moniteurs personnalisés pour les objets Kubernetes, que Workload Map utilisera également.

Vous pouvez créer des alertes de métrique Data Infrastructure Insights sur n'importe lequel des types d'objets ci-dessous. Assurez-vous que les données sont regroupées par type d'objet par défaut.

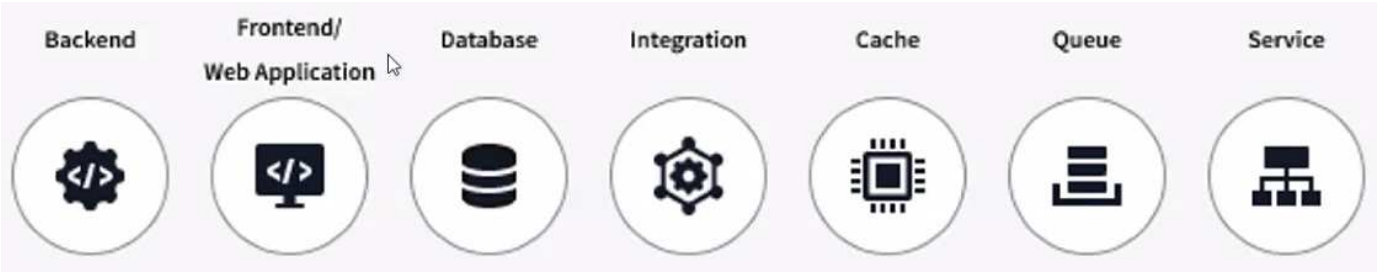
- charge de travail Kubernetes
- ensemble de démons Kubernetes
- déploiement de Kubernetes
- kubernetes.cronjob
- kubernetes.job
- kubernetes.replicaset
- kubernetes.statefulset
- kubernetes.pod
- kubernetes.network_traffic_l4

La carte

La carte montre les services/charges de travail et leurs relations entre eux. Les flèches indiquent les directions de circulation. Le survol d'une charge de travail affiche des informations récapitulatives pour cette charge de travail, comme vous pouvez le voir dans cet exemple :



Les icônes dans les cercles représentent différents types de services. Notez que les icônes ne sont visibles que si les objets sous-jacents ontétiquettes .

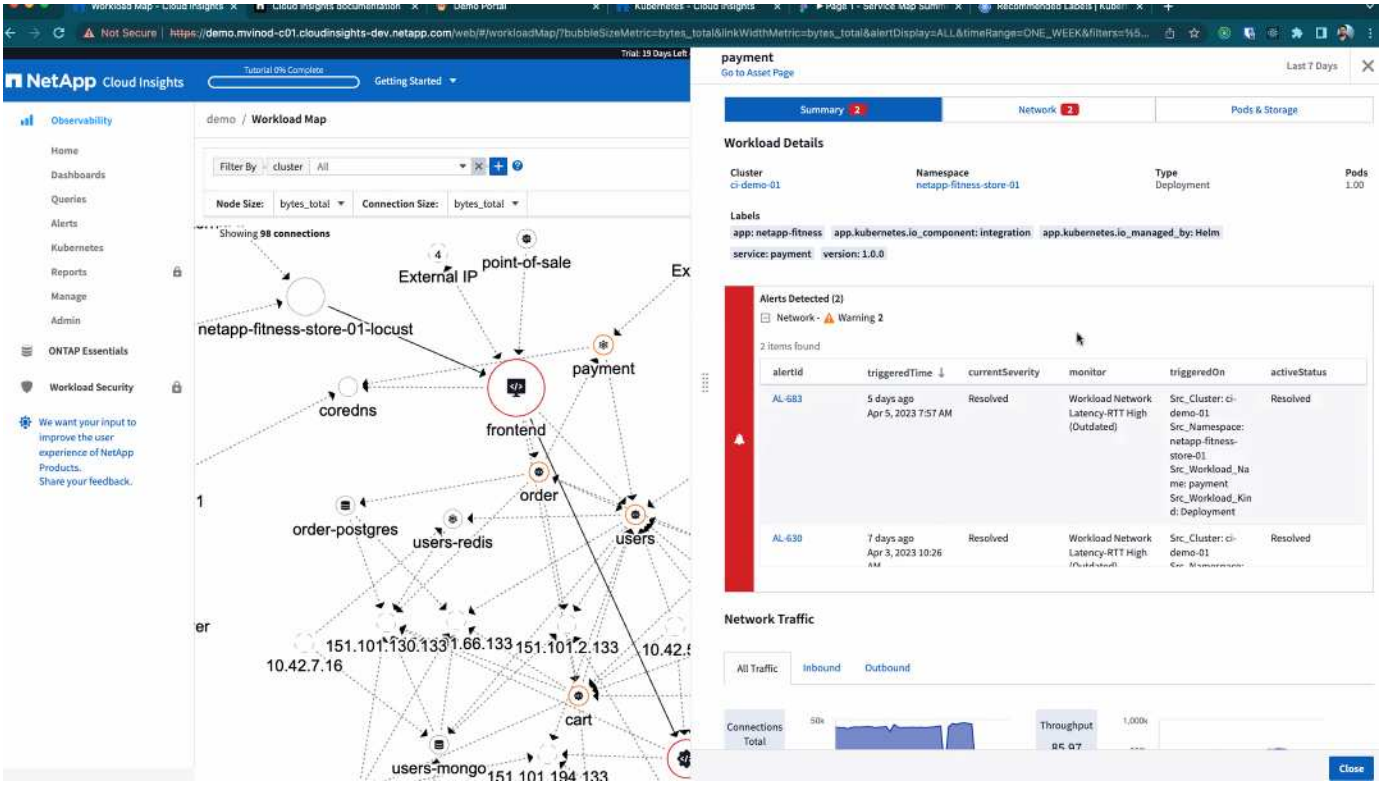


La taille de chaque cercle indique la taille du nœud. Notez que ces tailles sont relatives, le niveau de zoom de votre navigateur ou la taille de votre écran peuvent affecter les tailles réelles des cercles. De la même manière, le style de ligne de trafic vous donne un aperçu rapide de la taille de la connexion ; les lignes continues en gras correspondent à un trafic élevé, tandis que les lignes pointillées claires correspondent à un trafic plus faible.

Les nombres à l'intérieur des cercles indiquent le nombre de connexions externes actuellement traitées par le service.

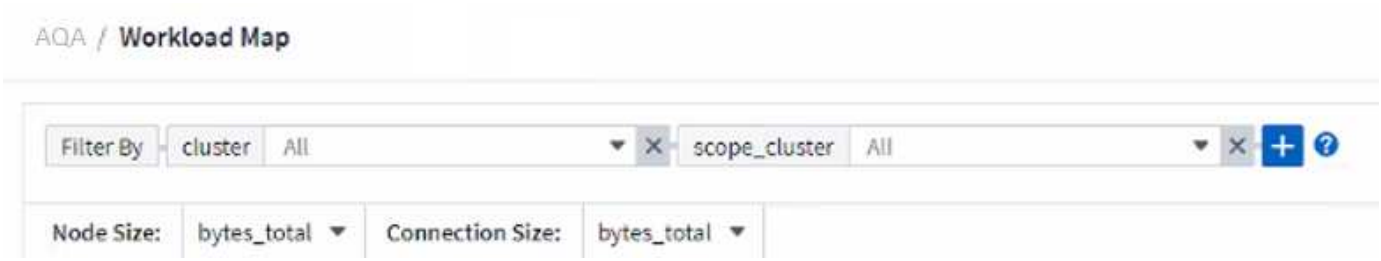
Détails et alertes de charge de travail

Les cercles affichés en couleur indiquent une alerte de niveau d'avertissement ou critique pour la charge de travail. Passez la souris sur le cercle pour obtenir un résumé du problème ou cliquez sur le cercle pour ouvrir un panneau coulissant avec plus de détails.

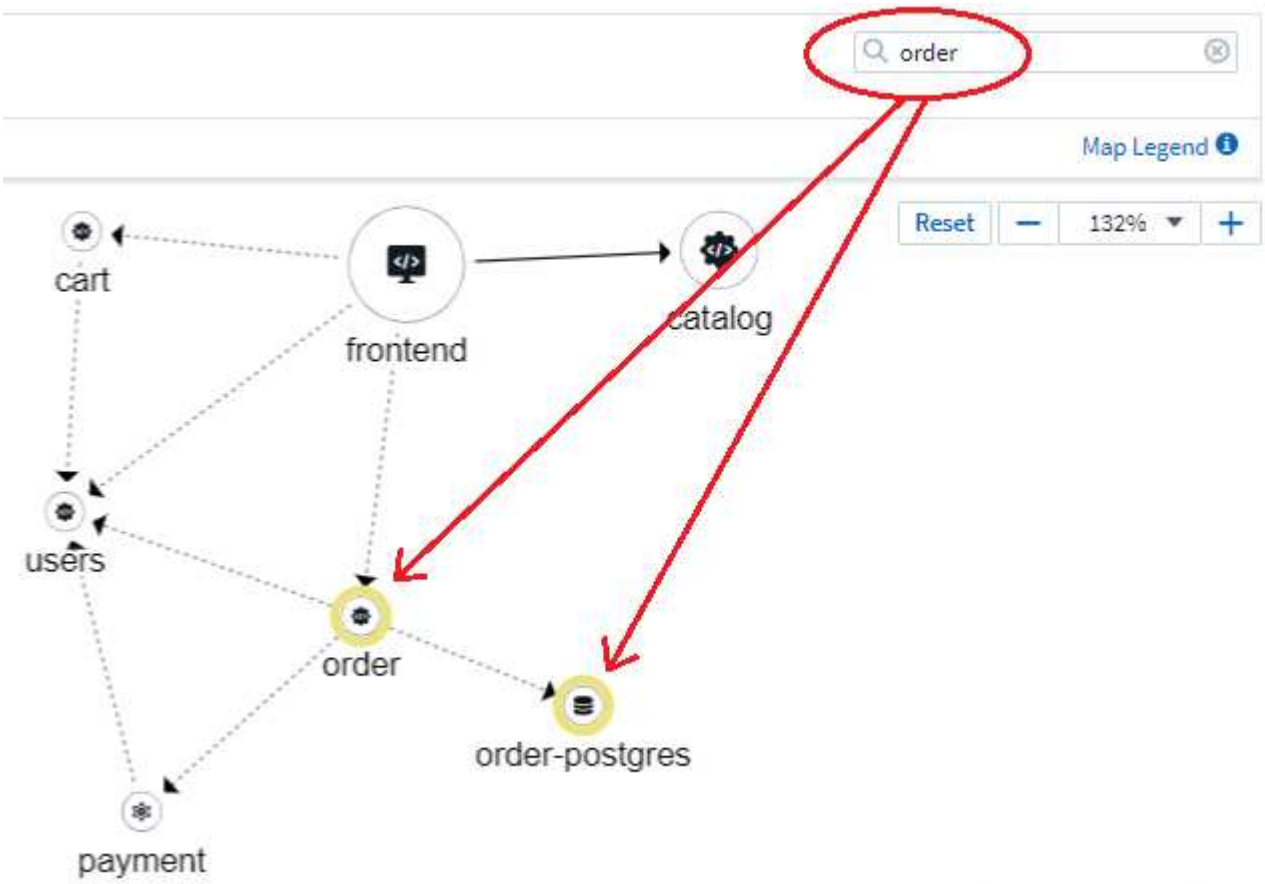


Recherche et filtrage

Comme avec d'autres fonctionnalités de Data Infrastructure Insights , vous pouvez facilement définir des filtres pour vous concentrer sur les objets spécifiques ou les attributs de charge de travail souhaités.



De même, la saisie d'une chaîne dans le champ *Rechercher* mettra en évidence les charges de travail correspondantes.



Étiquettes de charge de travail

Les étiquettes de charge de travail sont nécessaires si vous souhaitez que la carte identifie les types de charges de travail affichées (c'est-à-dire les icônes en forme de cercle). Les étiquettes sont dérivées comme suit :

- Nom du service/de l'application exécuté en termes génériques
- Si la source est un pod :
  - L'étiquette est dérivée de l'étiquette de charge de travail du pod
  - Étiquette attendue sur la charge de travail : app.kubernetes.io/component
  - Référence du nom de l'étiquette : https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Étiquettes recommandées :

- l'extrémité avant
- backend
- base de données
- cache
- file d'attente
- Kafka

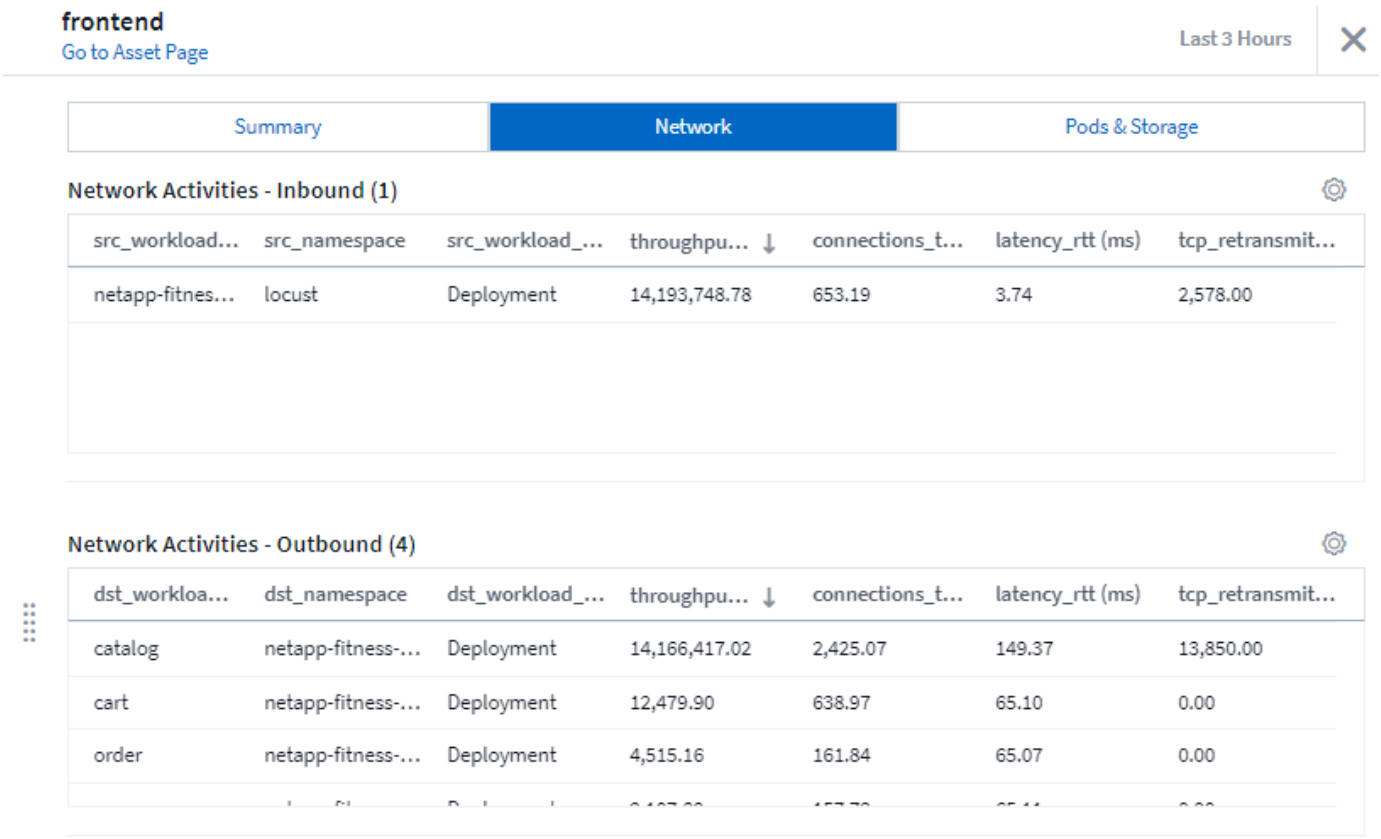
- Si la source est externe au cluster Kubernetes :
  - Data Infrastructure Insights tentera d'analyser le nom résolu DNS pour extraire le type de service.

    Par exemple, avec un nom DNS résolu de *s3.eu-north-1.amazonaws.com*, le nom résolu est analysé pour obtenir *s3* comme type de service.

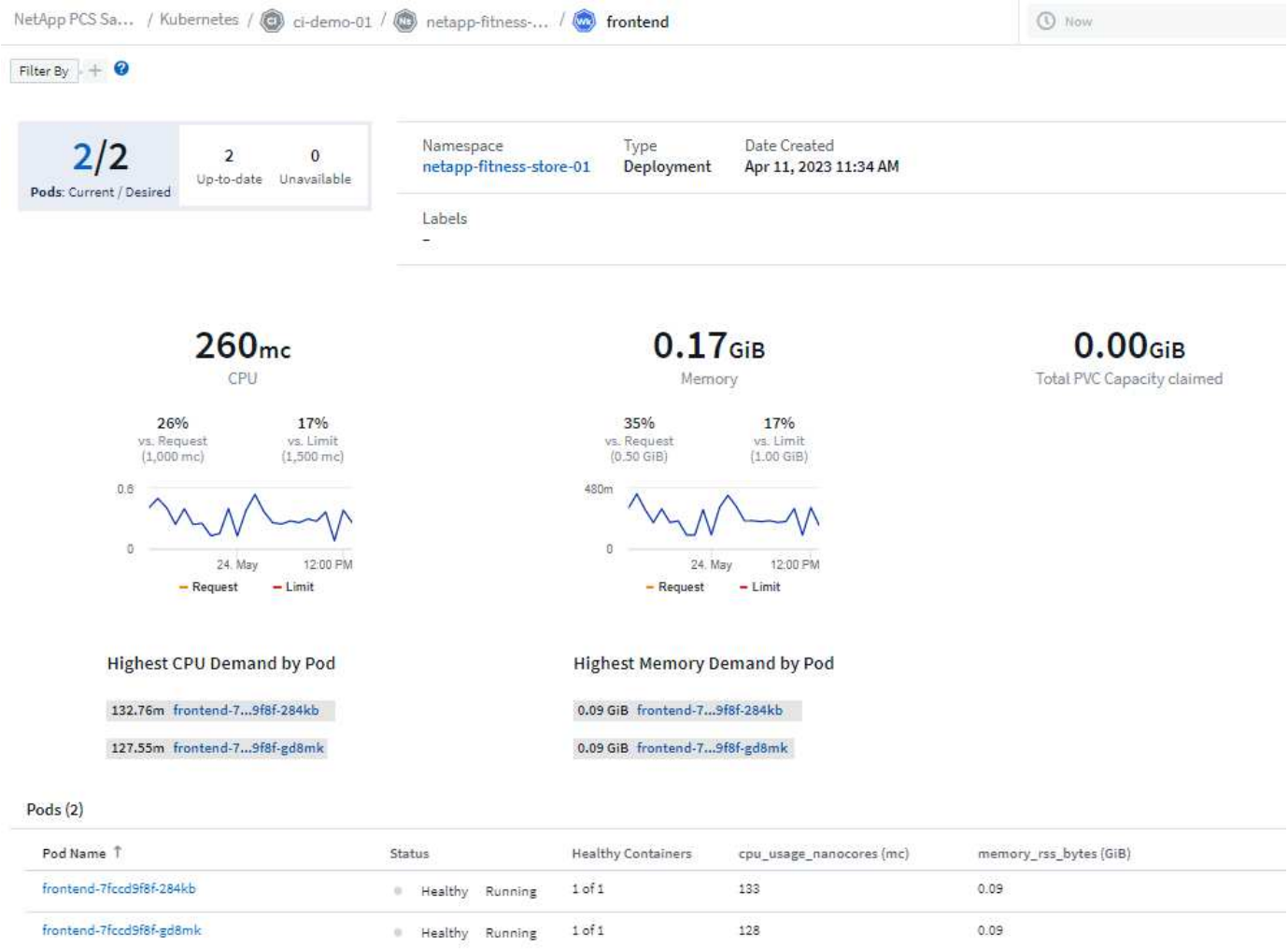
Plongez en profondeur

Un clic droit sur une charge de travail vous présente des options supplémentaires à explorer plus en détail. Par exemple, à partir d'ici, vous pouvez zoomer pour afficher les connexions pour cette charge de travail.

Vous pouvez également ouvrir le panneau coulissant des détails pour afficher directement l'onglet *Résumé*, *Réseau* ou *Pod et stockage*.



Enfin, la sélection de *Accéder à la page des ressources* ouvrira la page de destination détaillée des ressources pour la charge de travail.



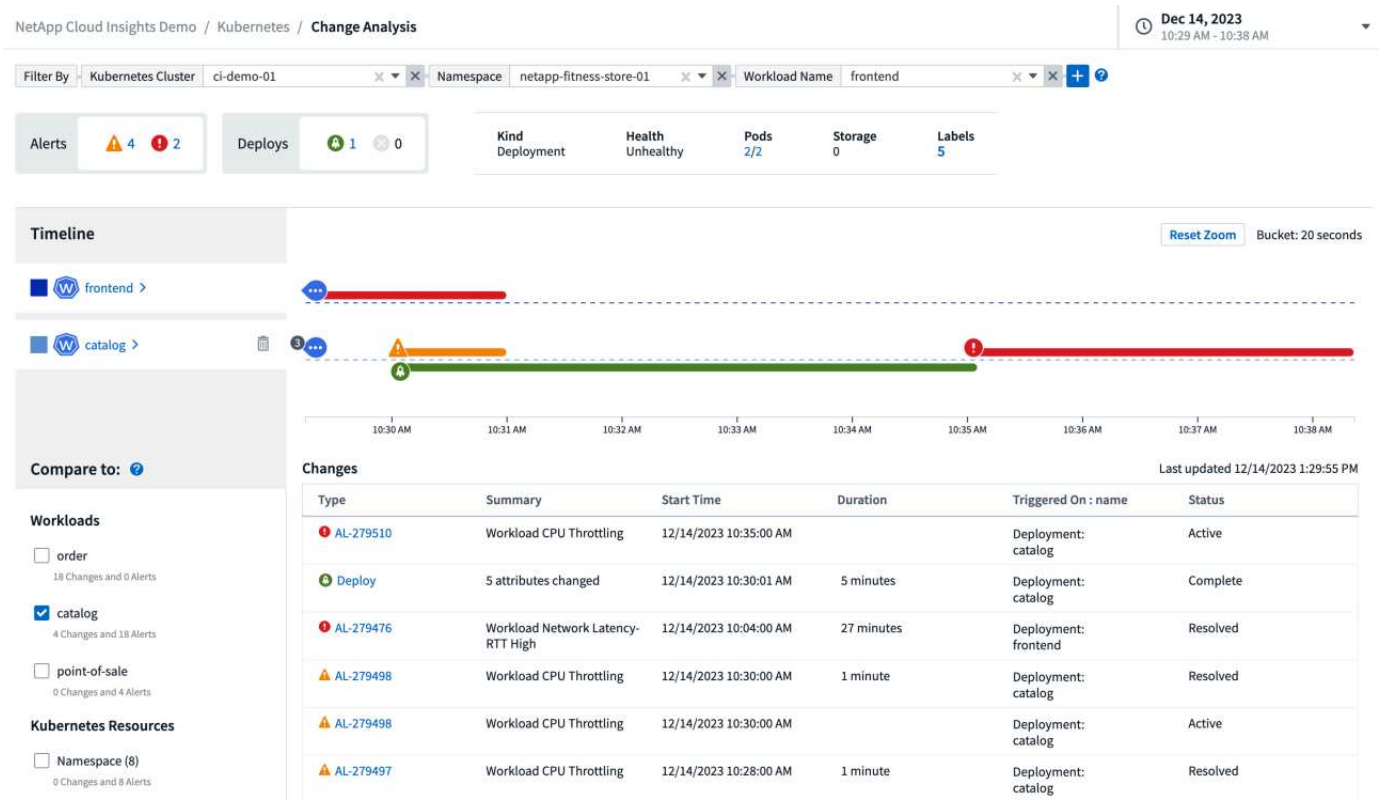
Analyse des changements Kubernetes

Kubernetes Change Analytics vous offre une vue tout-en-un des modifications récentes apportées à votre environnement K8s. Les alertes et l'état du déploiement sont à portée de main. Avec Change Analytics, vous pouvez suivre chaque changement de déploiement et de configuration et le corréler avec l'état et les performances des services, de l'infrastructure et des clusters K8.

Comment l'analyse du changement aide-t-elle ?

- Dans les environnements Kubernetes multi-locataires, des pannes peuvent survenir en raison de modifications mal configurées. Change Analytics vous aide à y parvenir en fournissant un volet unique pour visualiser et corréler l'état des charges de travail et les modifications de configuration. Cela peut aider à résoudre les problèmes des environnements Kubernetes dynamiques.

Pour afficher Kubernetes Change Analytics, accédez à **Kubernetes > Analyse des changements**.



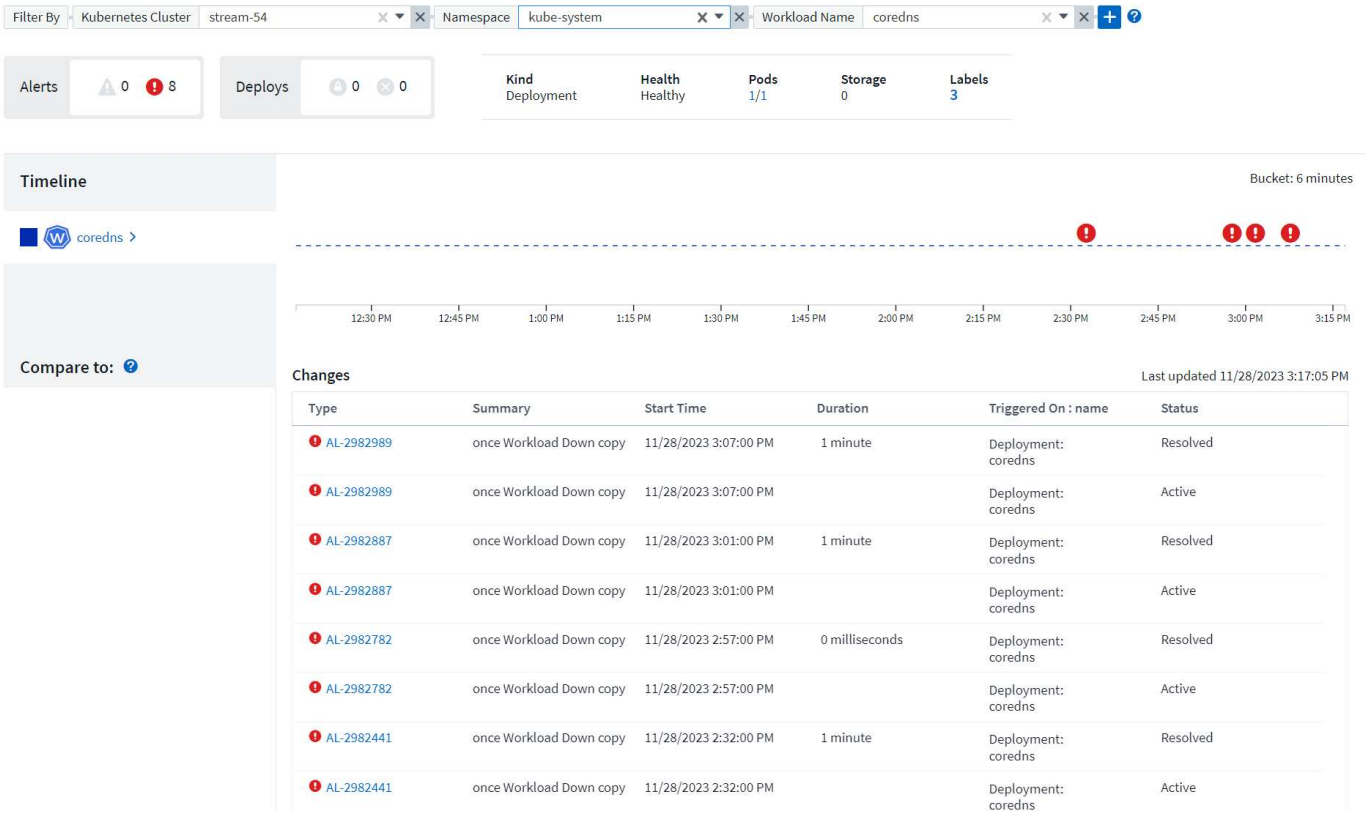
.

La page s’actualise automatiquement en fonction de la plage horaire Data Infrastructure Insights actuellement sélectionnée. Des plages de temps plus courtes signifient un rafraîchissement de l’écran plus fréquent.

Filtration

Comme pour toutes les fonctionnalités de Data Infrastructure Insights, le filtrage de la liste des modifications est intuitif : en haut de la page, saisissez ou sélectionnez des valeurs pour votre cluster Kubernetes, votre espace de noms ou votre charge de travail, ou ajoutez vos propres filtres en sélectionnant le bouton {+].

Lorsque vous filtrez jusqu’à un cluster, un espace de noms et une charge de travail spécifiques (ainsi que tous les autres filtres que vous définissez), une chronologie des déploiements et des alertes pour cette charge de travail dans cet espace de noms sur ce cluster s’affiche. Effectuez un zoom avant supplémentaire en cliquant et en faisant glisser le graphique pour vous concentrer sur une plage horaire plus spécifique.

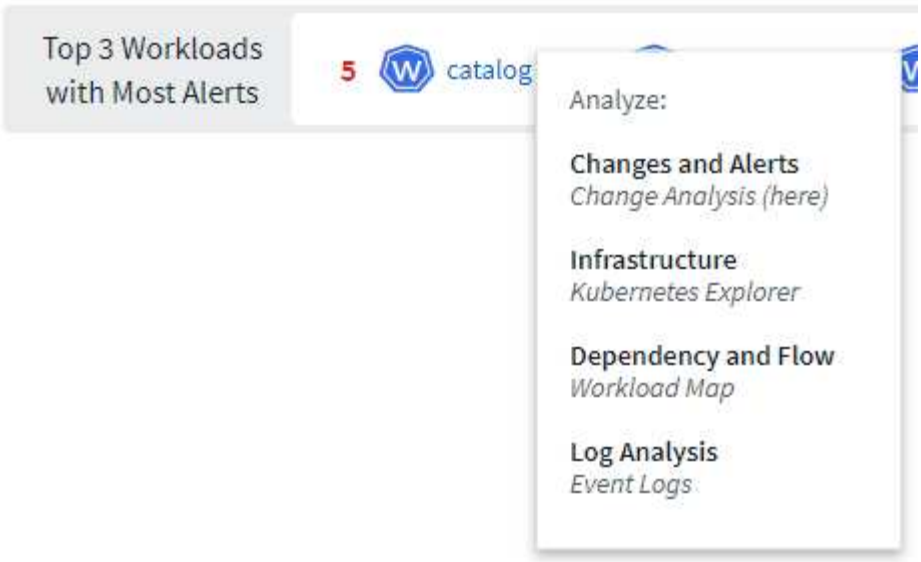


Statut rapide

Sous la zone de filtrage se trouvent un certain nombre d'indicateurs de haut niveau. Sur la gauche se trouve le nombre d'alertes (Avertissement et Critique). Ce nombre inclut les alertes *Actives* ainsi que *Résolues*. Pour voir uniquement les alertes *Actives*, définissez un filtre pour « Statut » et choisissez « Actif ».

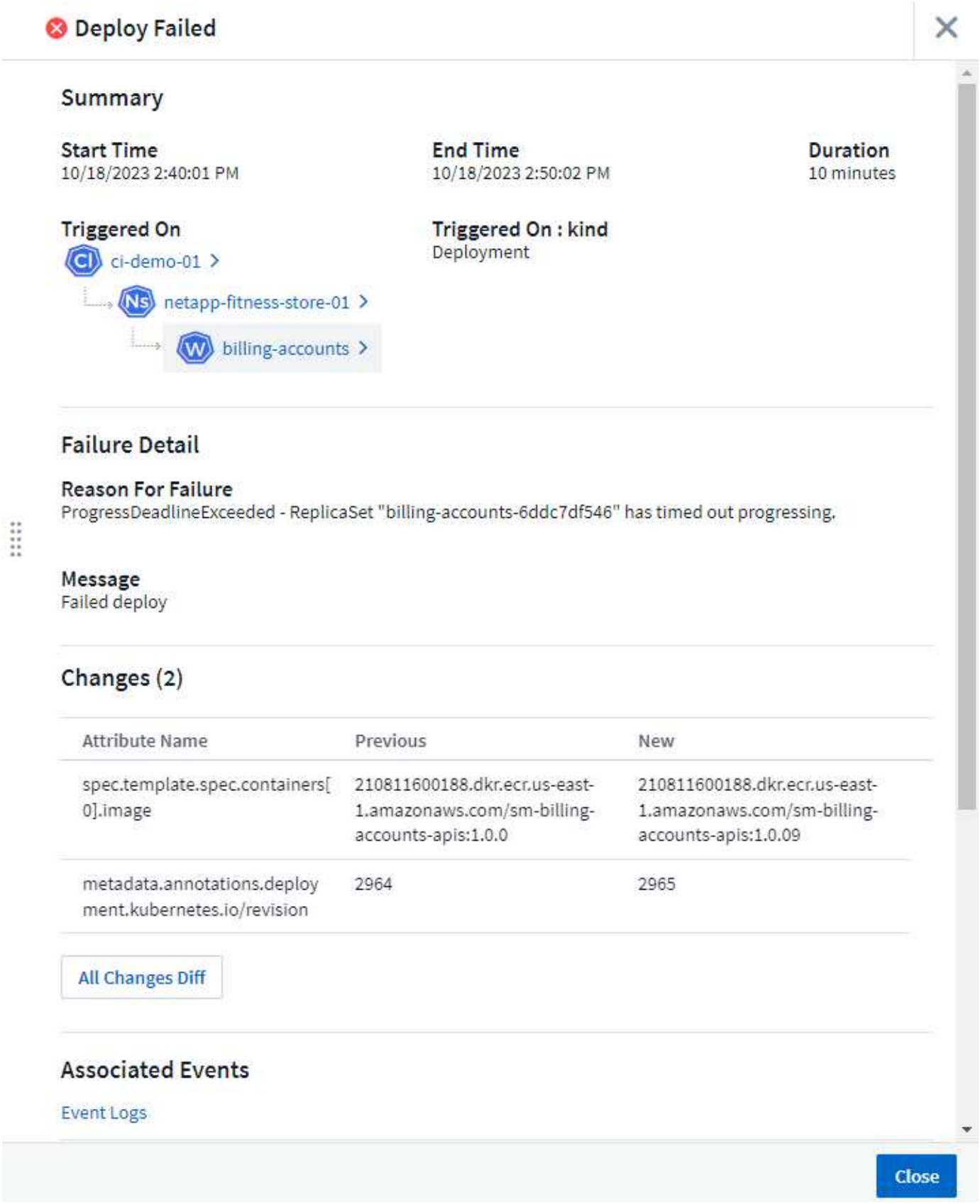
L'état de déploiement est également affiché ici. Encore une fois, la valeur par défaut est d'afficher le nombre de déploiements *Démarrés*, *Terminés* et *Échoués*. Pour voir uniquement les déploiements *Échoués*, définissez un filtre pour « Statut » et sélectionnez « Échoué ».

Les 3 charges de travail avec le plus d'alertes sont les suivantes. Le numéro en rouge à côté de chaque charge de travail indique le nombre d'alertes liées à cette charge de travail. Cliquez sur le lien de charge de travail pour explorer votre infrastructure (Kubernetes Explorer), vos dépendances (carte de charge de travail) ou votre analyse des journaux (journaux des événements).



Panneau de détails

La sélection d'une modification dans la liste ouvre un panneau décrivant la modification plus en détail. Par exemple, la sélection d'un déploiement ayant échoué affiche un résumé du déploiement, avec les heures de début et de fin, la durée et le lieu où le déploiement a été déclenché, avec des liens pour explorer ces ressources. Il affiche également la raison de l'échec, les modifications associées et tous les événements associés.



La sélection d'une alerte fournit également des détails sur l'alerte, y compris le moniteur qui a déclenché l'alerte ainsi qu'un graphique affichant une chronologie visuelle de l'alerte.

ONTAP Essentials

ONTAP Essentials est un ensemble de tableaux de bord et de workflows qui fournissent des aperçus détaillés de vos inventaires et charges de travail ONTAP . Vous pouvez voir les termes suivants utilisés lorsque vous travaillez dans ONTAP Essentials :

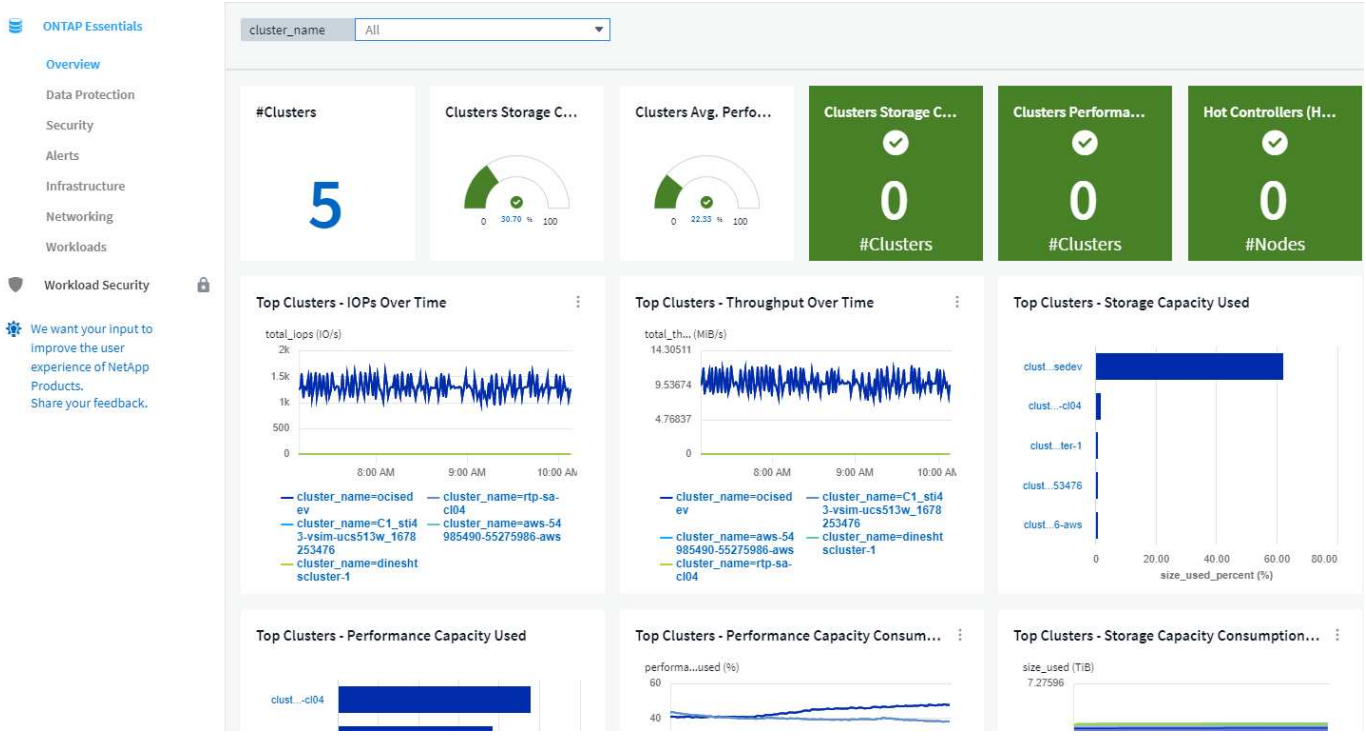
- Infrastructure/Inventaire : objets qui fournissent des services de stockage/réseau aux données utilisateur
- Charges de travail : objets qui fournissent une interface aux utilisateurs pour lire/écrire des données.
- Protection des données : objets pouvant être protégés à l'aide des technologies de protection des données NetApp

Pour des termes et définitions supplémentaires liés à ONTAP, consultez le"Collecteur de données ONTAP" documentation.

ONTAP Essentials nécessite au moins un collecteur de données ONTAP fonctionnel avec des données collectées au cours des sept derniers jours.

Aperçu

Pour commencer à explorer, sélectionnez * ONTAP Essentials* dans le menu principal Data Infrastructure Insights .



Le tableau de bord **Aperçu** affiche des informations utiles telles que le nombre de clusters sur votre locataire avec leur capacité globale et leurs pourcentages de performances. Vous verrez également des données prédictives concernant le nombre de jours prévus avant que la capacité de stockage ou la capacité de performance ne soit à court d'espace. De plus, si des contrôleurs de votre infrastructure fonctionnent avec leur CPU à plus de 65 %, ce qui met potentiellement votre cluster en danger en cas de basculement, ONTAP Essentials les affiche comme des contrôleurs « chauds ».

Les graphiques informatifs vous donnent un aperçu des performances au fil du temps ainsi que des répartitions de l'utilisation de la capacité. Chacun de ces graphiques ou points de données peut être utilisé comme point de départ pour une exploration ou une enquête.

Remarque : un nombre de « jours avant le plein » de « 0 » (zéro) indique que le nombre de jours avant le plein est estimé à plus de 90 jours. En d'autres termes, vos systèmes ne risquent pas de manquer d'espace dans un avenir proche.

Protection des données

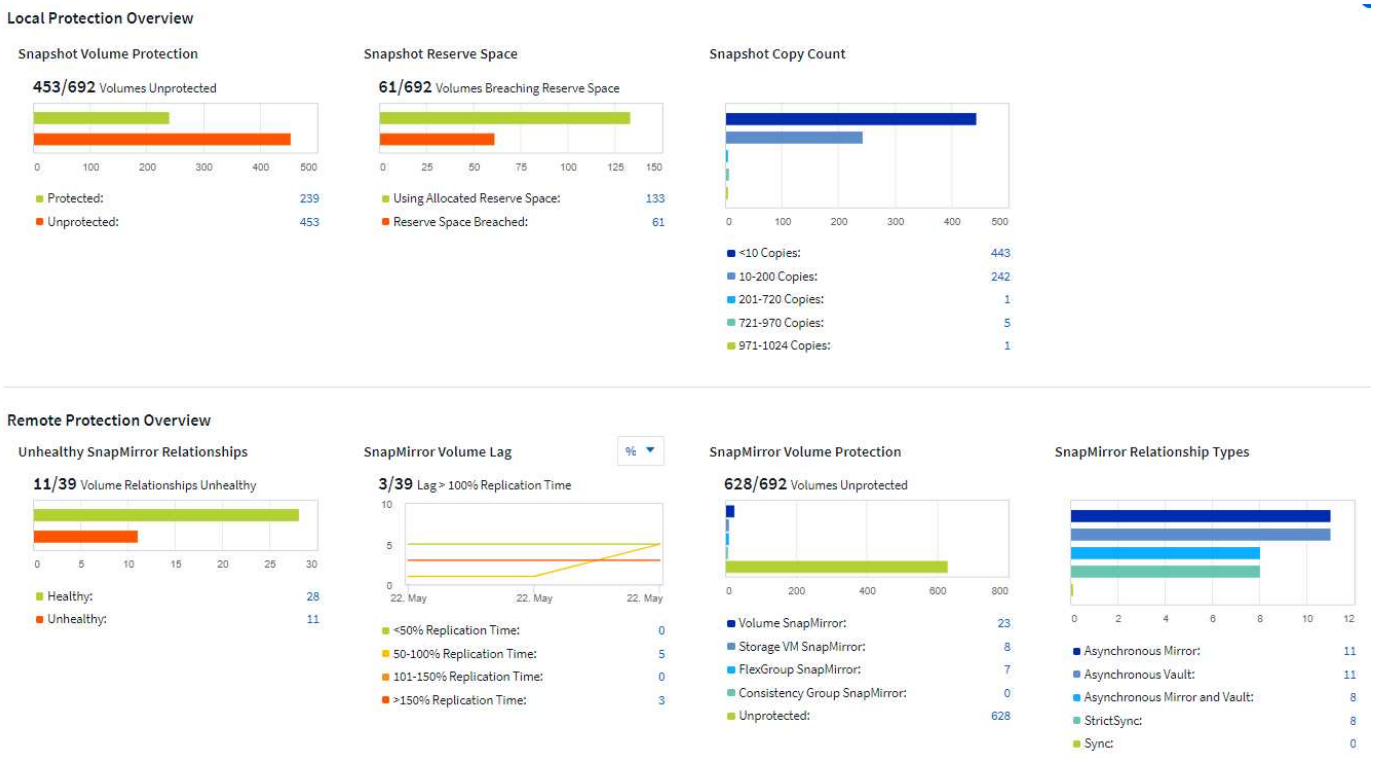
La page **Protection des données** affiche l'état des volumes protégés par des **copies instantanées** ou des *politiques SnapMirror *.

Dans la section *Présentation de la protection locale*, les graphiques fournissent les informations suivantes pour les volumes protégés par des copies Snapshot :

- Le nombre de volumes protégés par des copies Snapshot, ainsi que ceux non protégés.
- Le nombre de volumes qui utilisent ou dépassent l'espace réservé pour les copies Snapshot.
- Le nombre de volumes dans des plages spécifiques de nombre de copies Snapshot (c'est-à-dire moins de 10 copies, 10 à 200, etc.).

Dans la section *Présentation de la protection à distance*, les graphiques fournissent des informations relatives aux volumes protégés par les politiques SnapMirror :

- Le nombre de relations SnapMirror saines et malsaines.
- Nombre de relations SnapMirror subissant un décalage de l'objectif de point de récupération (RPO) en fonction de l'état du décalage.
- Nombre de relations protégées par les types de protection de volume SnapMirror tels que Volume SnapMirror, les relations SVMDR, les relations FlexGroup SnapMirror , les relations de groupe de cohérence SnapMirror Business Continuity (SMBC), ainsi que les volumes non protégés.
- Le nombre de relations protégées par les types de relations SnapMirror tels que Miroir asynchrone, Coffre asynchrone, Miroir asynchroneVault, StrictSync et Sync.



La grille *Clusters* au bas de la page fournit des détails sur les éléments suivants :

- Volumes non protégés par des snapshots.
- Volumes dépassant l'espace réservé aux instantanés.
- Les volumes non protégés par les politiques SnapMirror et les relations SnapMirror subissent un décalage.
- Relations SnapMirror malsaines.

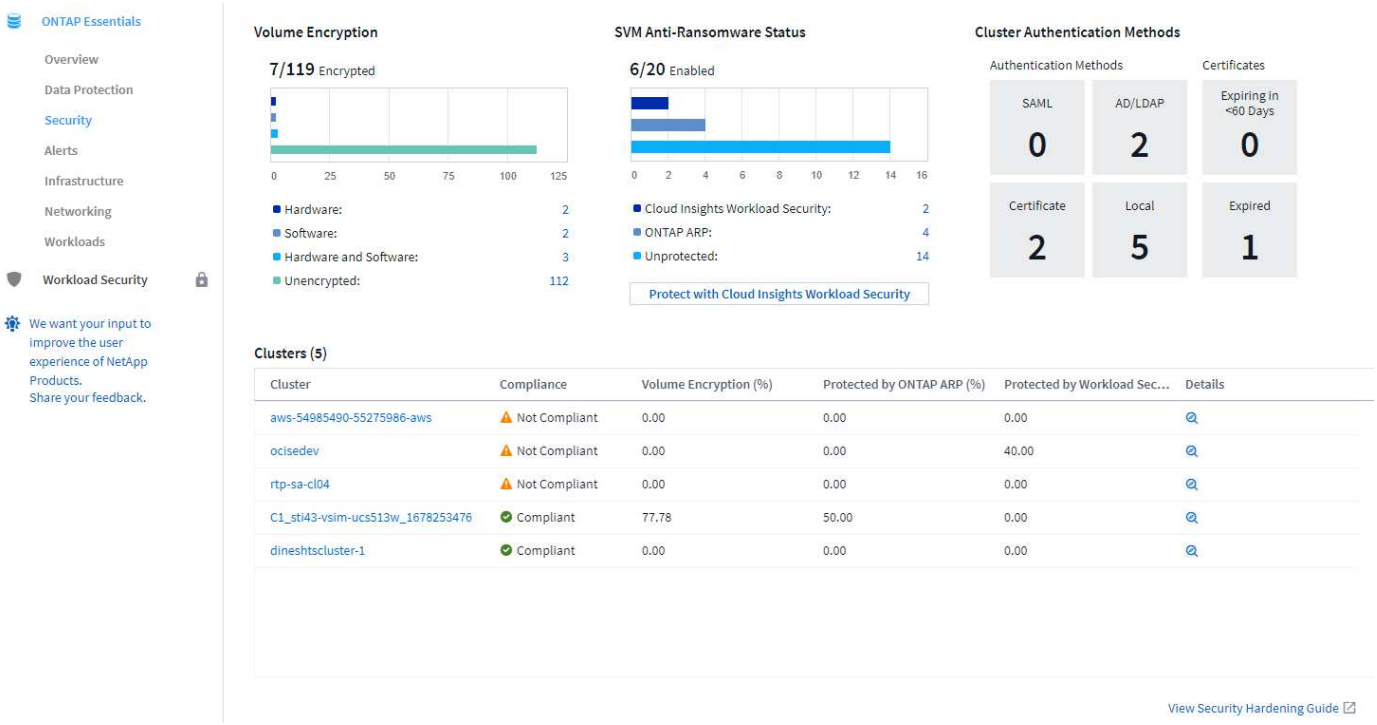
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Sécurité

Le tableau de bord de sécurité vous offre une vue instantanée de votre situation de sécurité actuelle, affichant des graphiques pour le chiffrement du volume matériel et logiciel, l'état de la protection contre la falsification des fichiers et les méthodes d'authentification du cluster. Les critères de sécurité sont évalués sur la base des recommandations définies dans le "* Guide de renforcement de la sécurité NetApp pour ONTAP 9*".

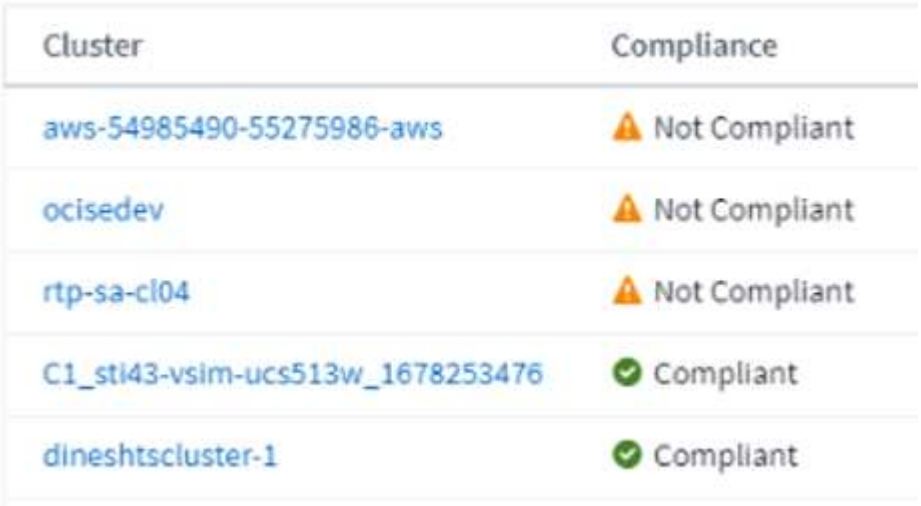
Sélectionnez l'un des comptes de chiffrement ou de protection contre la falsification de fichiers pour explorer votre environnement.



Le tableau de bord de sécurité ONTAP Essentials surveille votre environnement pour déterminer l'état de conformité du cluster. Reportez-vous à la"Catégories de conformité des clusters" pour en savoir plus. ONTAP Essentials utilise les moniteurs suivants pour déterminer la conformité :

Nom du moniteur	Nom de l'attribut (affiché dans les détails du cluster)	Valeur conforme aux attributs
Mode FIPS désactivé	Mode FIPS	Activé
Chiffres non sécurisés en cluster pour SSH	Paramètres SSH sécurisés	Oui
Protocole Telnet activé	Telnet	Désactivées
Shell distant activé	Shell distant	Désactivées
Utilisateur administrateur local par défaut activé	Utilisateur administrateur par défaut	Désactivées
Mot de passe haché MD5	MD5 en cours d'utilisation	Non
Communication entre pairs du cluster non chiffrée	Appairage de cluster	Crypté/Sans homologue
AutoSupport HTTPS AutoSupport désactivé	AutoSupport via HTTPS	Oui
Aucun serveur NTP n'est configuré	Protocole de temps réseau	Configuré
Le nombre de serveurs NTP est faible	Protocole de temps réseau	Configuré
Bannière de connexion au cluster désactivée	Bannière de connexion	Activé
Transfert de journaux non chiffré	Transfert de journaux chiffré	Oui

Notez que si un moniteur ci-dessus est désactivé, les détails du cluster afficheront la valeur « Non coché » pour l'attribut de conformité de sécurité correspondant.

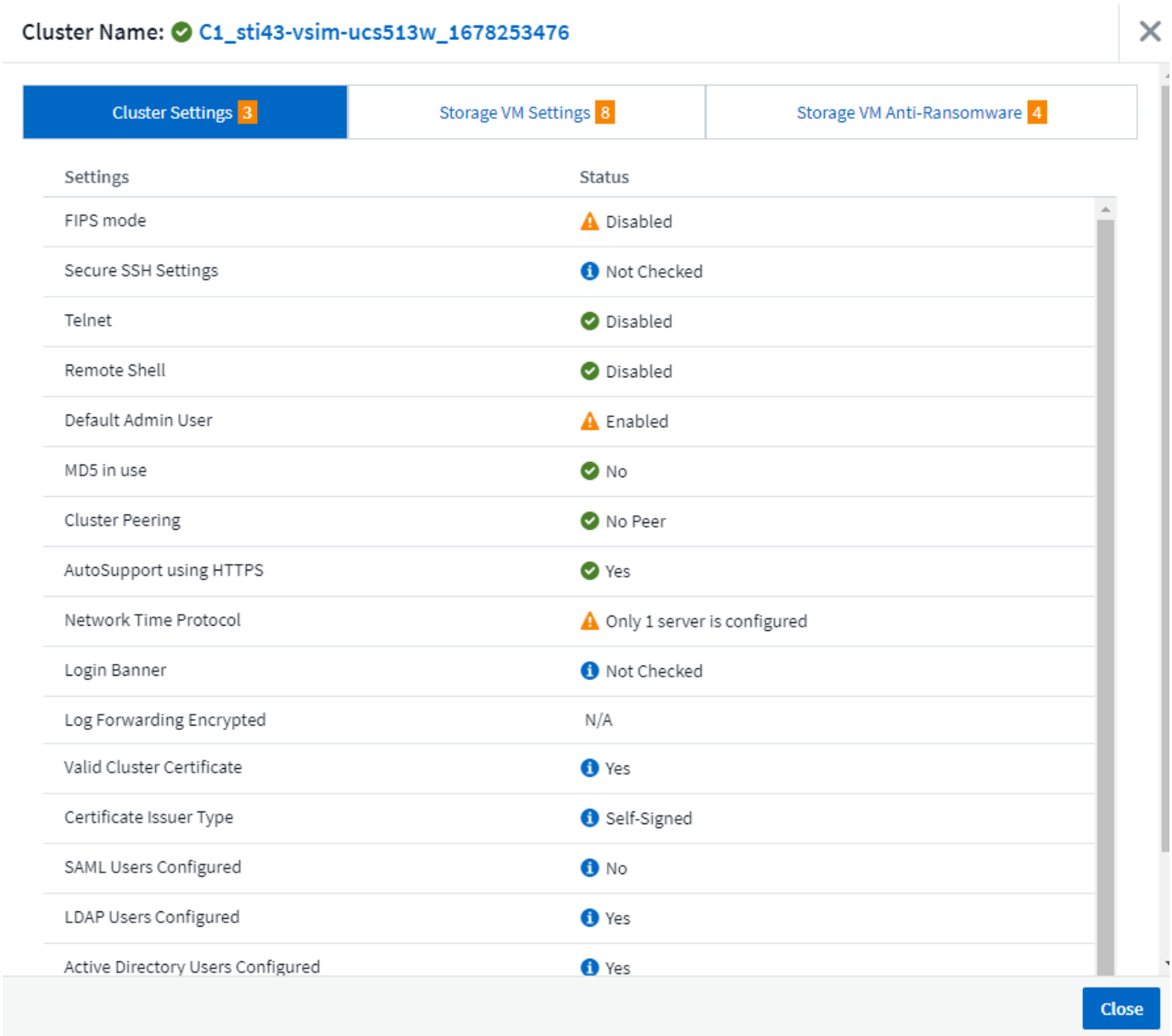


Pour les SVM, le tableau de bord de sécurité examine les moniteurs suivants :

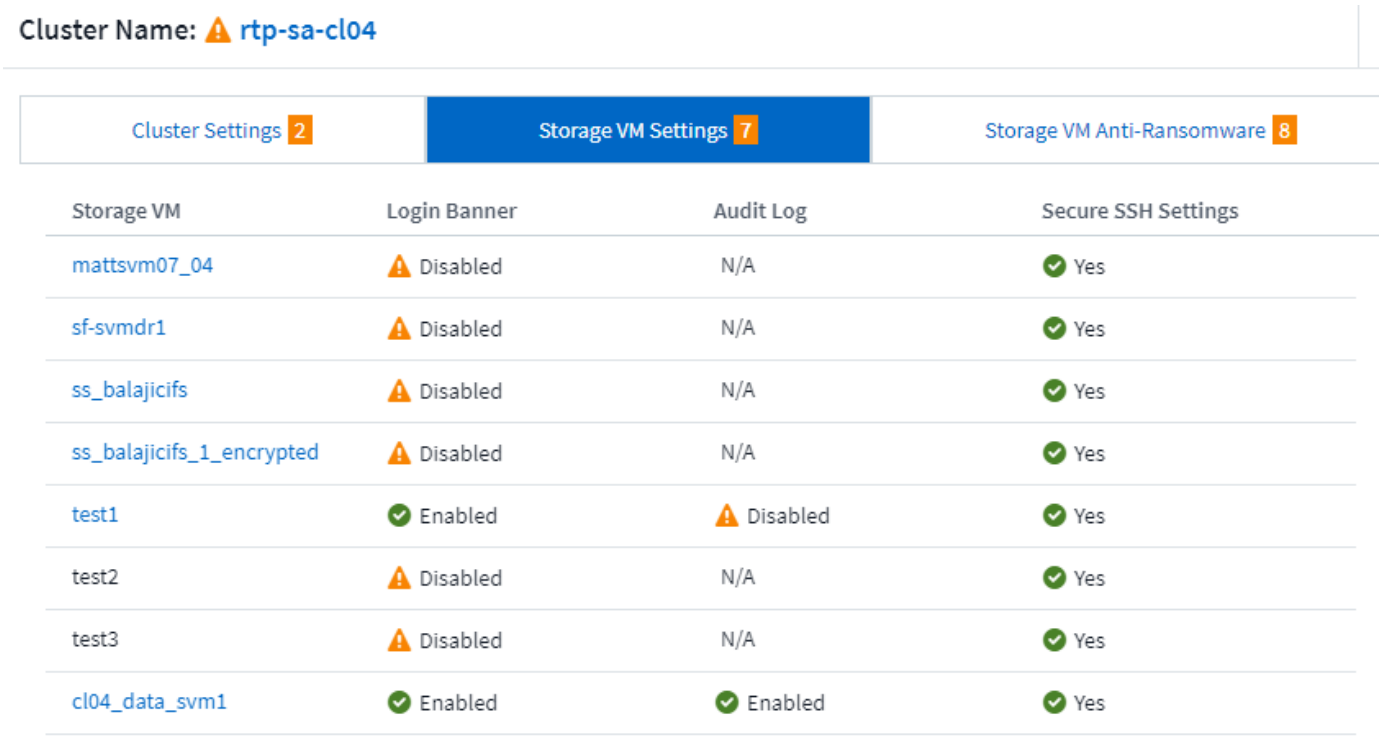
Nom du moniteur	Nom de l'attribut (affiché dans les paramètres de la machine virtuelle de stockage)	Valeur conforme aux attributs
Chiffres non sécurisés de la machine virtuelle de stockage pour SSH	Paramètres SSH sécurisés	Oui
Bannière de connexion à la machine virtuelle de stockage désactivée	Bannière de connexion	Activé
Journal d'audit de la machine virtuelle de stockage désactivé	Journal d'audit	Activé

Dans la liste des clusters, sélectionnez *Afficher les détails* pour chaque cluster afin d'ouvrir un panneau coulissant vous montrant les paramètres actuels pour *Cluster, Storage VM* ou *Anti-Ransomware*.

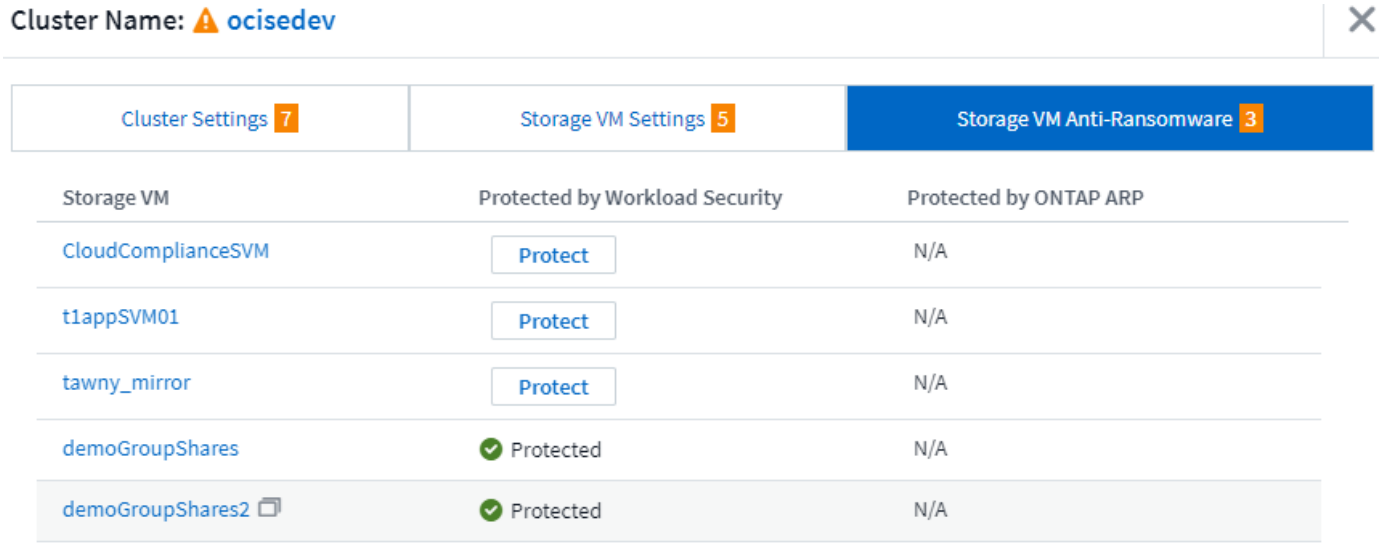
Les détails du cluster incluent l'état de la connexion, les informations sur le certificat et bien plus encore :



Les détails de la machine virtuelle de stockage affichent les informations d'audit et SSH :

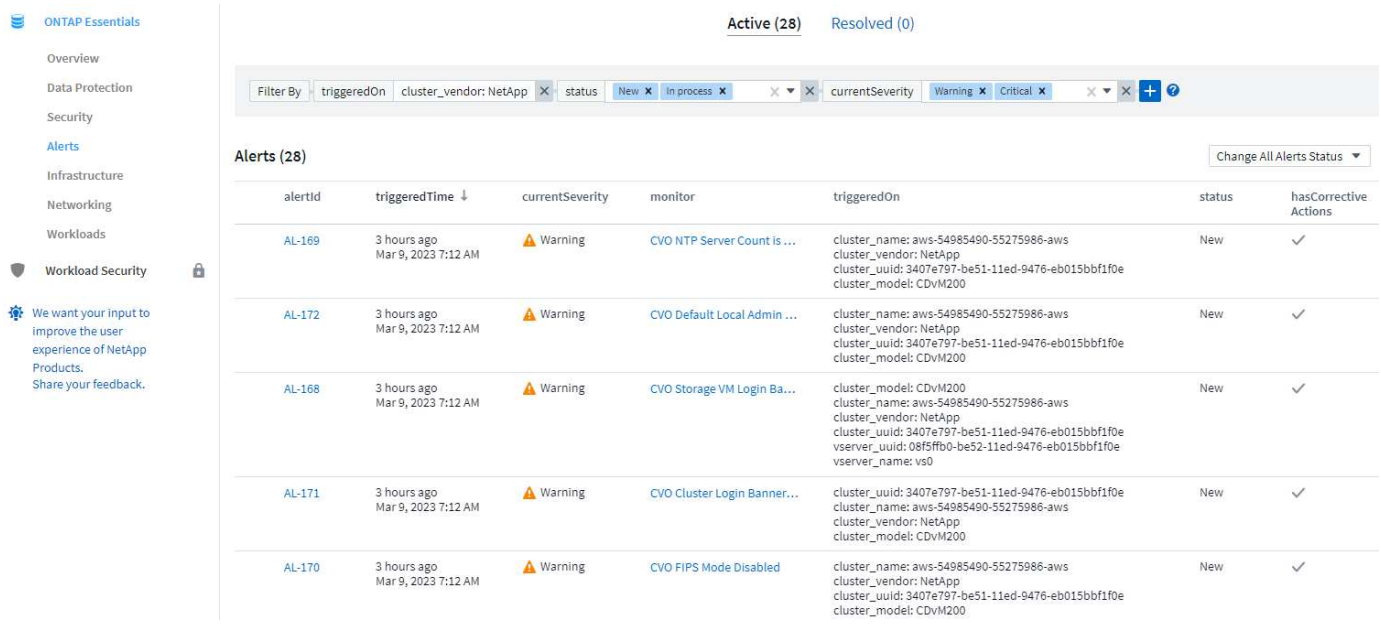


Les détails anti-ransomware indiquent si une machine virtuelle de stockage est protégée par la protection anti-ransomware d'ONTAP ou par la sécurité de la charge de travail Data Infrastructure Insights . Notez que la colonne ONTAP ARP affiche l'état actuel de la protection anti-ransomware intégrée d'ONTAP, qui est configurée sur le système ONTAP . La sécurité de la charge de travail de Data Infrastructure Insights peut être activée en sélectionnant « Protéger » dans cette
colonne.



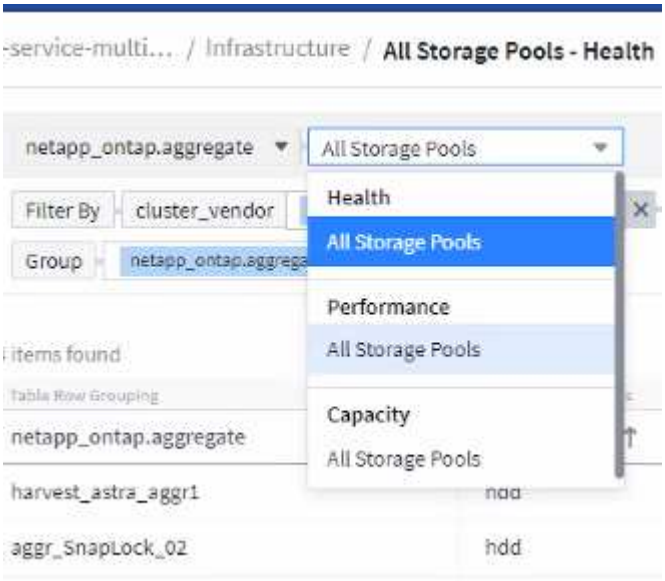
Alertes

Ici, vous pouvez consulter les alertes actives sur votre locataire et analyser rapidement les problèmes potentiels. Sélectionnez l'onglet *Résolu* pour afficher les alertes qui ont été résolues.

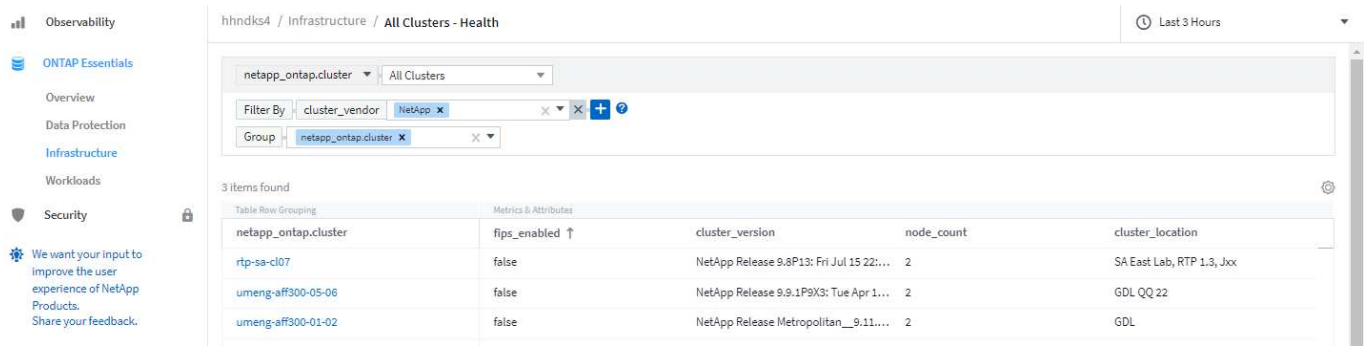


Infrastructure

La page **Infrastructure** ONTAP Essentials vous donne une vue de l'état et des performances du cluster, à l'aide de requêtes prédéfinies (mais davantage personnalisables) sur tous les objets ONTAP de base. Sélectionnez le type d'objet que vous souhaitez explorer (cluster, pool de stockage, etc.) et choisissez d'afficher les informations de santé ou de performances. Définissez des filtres pour approfondir les systèmes individuels.

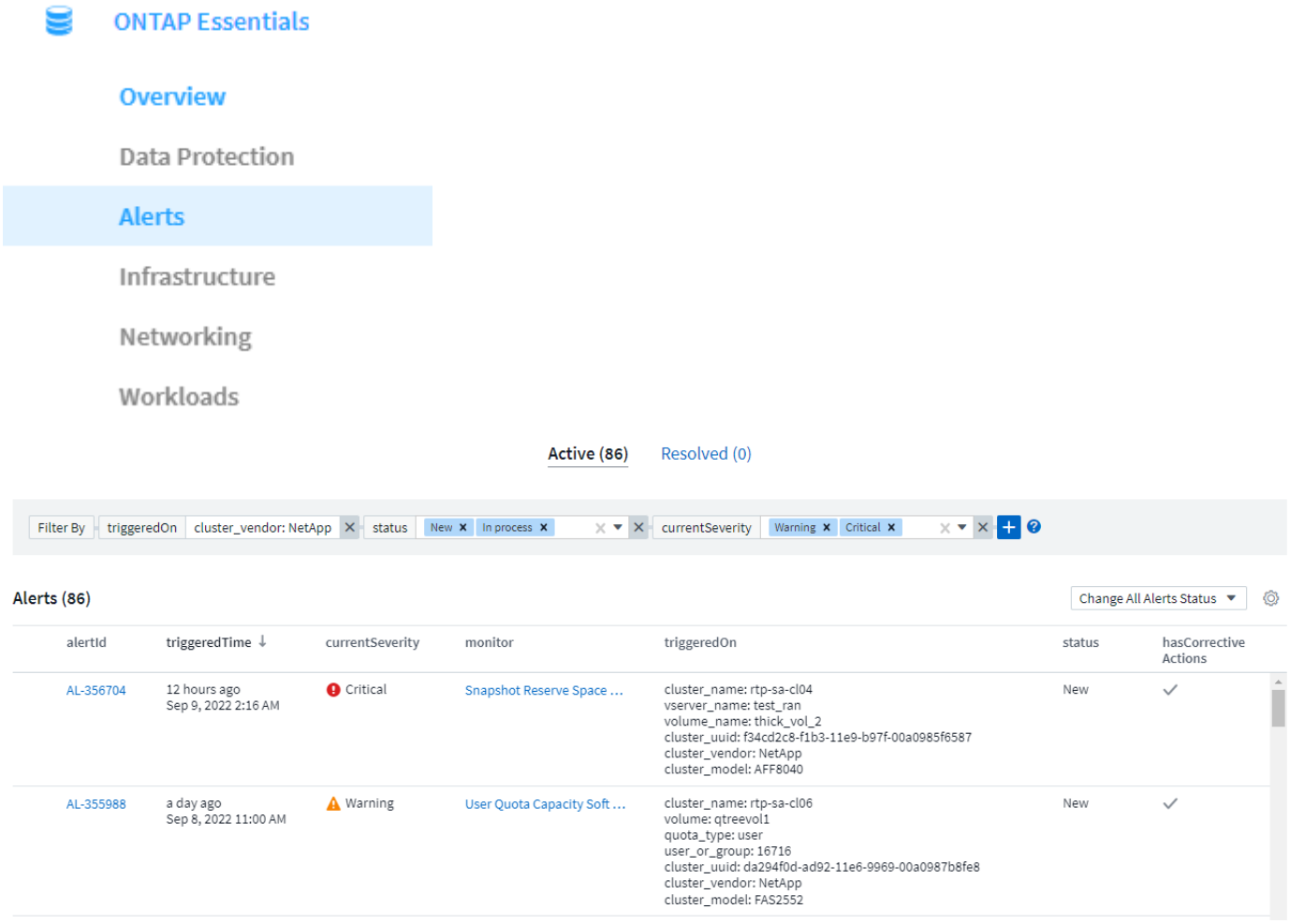


Page d'infrastructure affichant l'état du cluster :



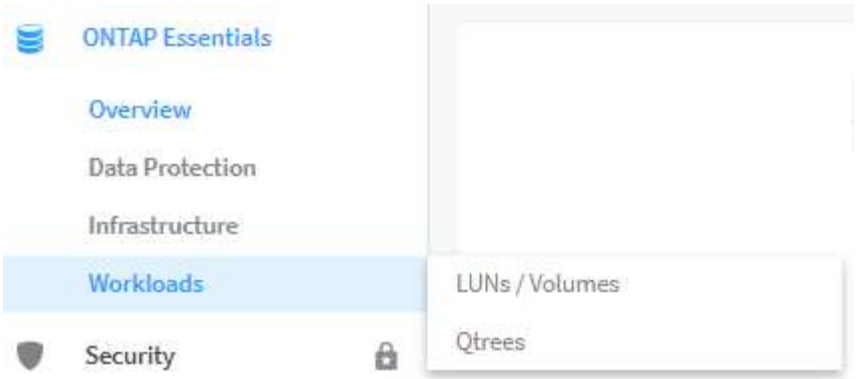
Réseautage

ONTAP Essentials Networking vous offre une vue d'ensemble de votre infrastructure FC, NVME FC, Ethernet et iSCSI. Sur ces pages, vous pouvez explorer des éléments tels que les ports de vos clusters et leurs nœuds.



Charges de travail

Affichez et explorez les charges de travail sur les LUN/volumes, les partages NFS ou SMB ou les Qtrees sur votre locataire.



netapp_ontap.lun | All LUNs

Filter By | cluster_vendor | NetApp

Group | netapp_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

Administration et autres tâches

API Data Infrastructure Insights

L'API Data Infrastructure Insights permet aux clients NetApp et aux fournisseurs de logiciels indépendants (ISV) d'intégrer Data Infrastructure Insights à d'autres applications, telles que CMDB ou d'autres systèmes de billetterie.

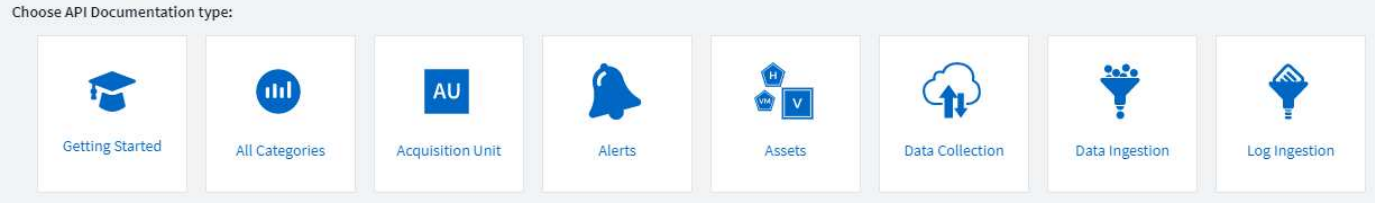
Vos Data Infrastructure Insights"rôle de l'ensemble de fonctionnalités" déterminera à quelles API vous pouvez accéder. Les rôles Utilisateur et Invité ont moins de privilèges que le rôle Administrateur. Par exemple, si vous disposez du rôle d'administrateur dans Surveiller et optimiser, mais du rôle d'utilisateur dans Rapports, vous pouvez gérer tous les types d'API à l'exception de l'entrepôt de données.

Conditions requises pour l'accès à l'API

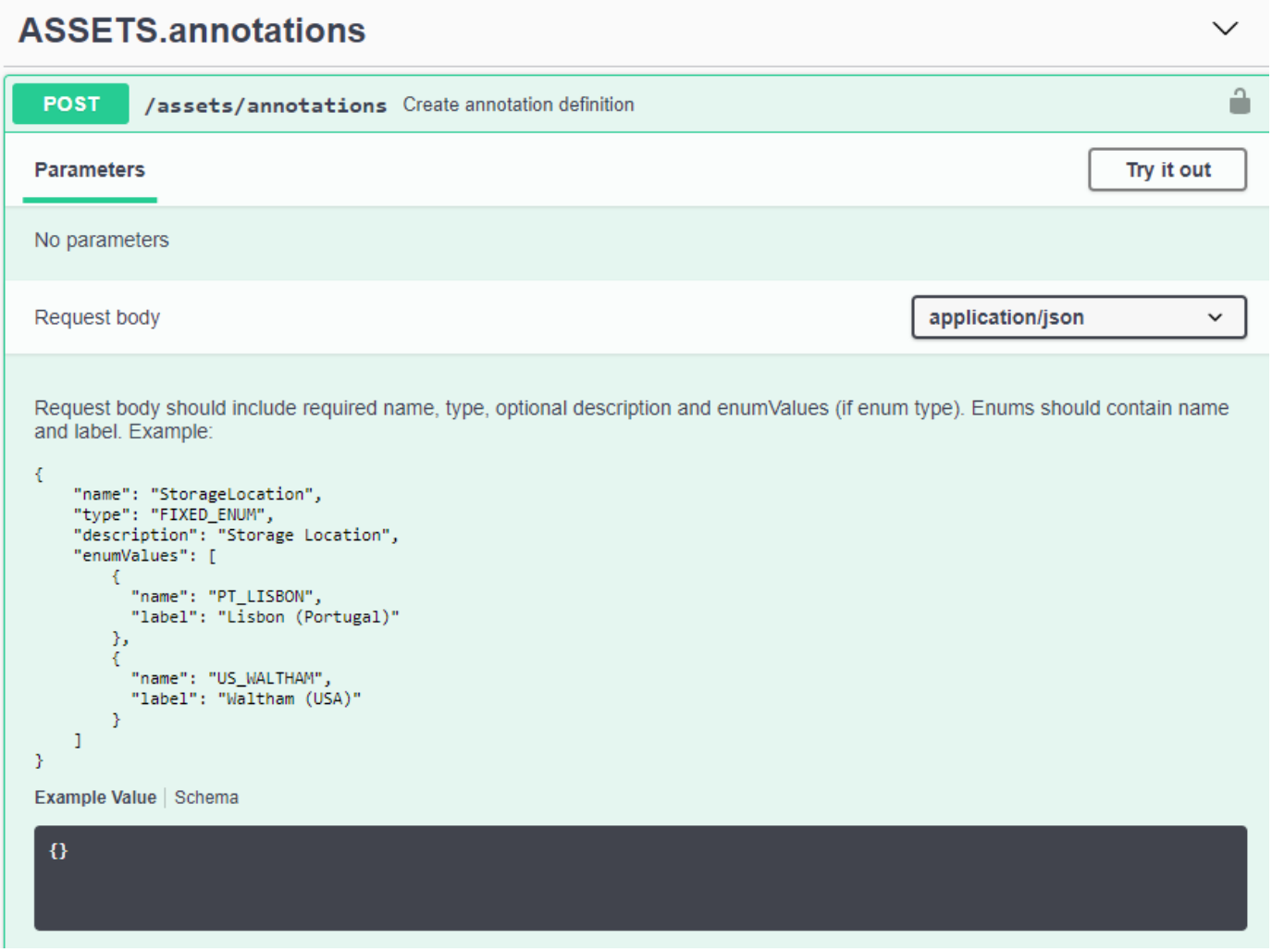
- Un modèle de jeton d'accès API est utilisé pour accorder l'accès.
- La gestion des jetons API est effectuée par les utilisateurs de Data Infrastructure Insights avec le rôle d'administrateur.

Documentation de l'API (Swagger)

Les dernières informations sur l'API sont disponibles en vous connectant à Data Infrastructure Insights et en accédant à **Admin > Accès API**. Cliquez sur le lien **Documentation API**.



La documentation de l'API est basée sur Swagger, qui fournit une brève description et des informations d'utilisation de l'API et vous permet de l'essayer dans votre locataire. Selon votre rôle d'utilisateur et/ou votre édition de Data Infrastructure Insights , les types d'API disponibles peuvent varier.



Jetons d'accès API

Avant d'utiliser l'API Data Infrastructure Insights , vous devez créer un ou plusieurs **jetons d'accès API**. Les jetons d'accès sont utilisés pour des types d'API spécifiés et peuvent accorder des autorisations de lecture et/ou d'écriture. Vous pouvez également définir l'expiration de chaque jeton d'accès. Toutes les API sous les types spécifiés sont valides pour le jeton d'accès. Chaque jeton est dépourvu de nom d'utilisateur ou de mot de passe.

Pour créer un jeton d'accès :

- Cliquez sur **Admin > Accès API**
- Cliquez sur **+Jeton d'accès API**
  - Entrez le nom du jeton
  - Sélectionner les types d'API
  - Spécifiez les autorisations accordées pour cet accès API
  - Spécifier l'expiration du jeton

Votre jeton ne sera disponible que pour la copie dans le presse-papiers et l'enregistrement pendant le processus de création. Les jetons ne peuvent pas être récupérés après leur création, il est donc fortement recommandé de copier le jeton et de l'enregistrer dans un endroit sûr. Vous serez invité à cliquer sur le bouton **Copier le jeton d'accès API** avant de pouvoir fermer l'écran de création de jeton.

Vous pouvez désactiver, activer et révoquer les jetons. Les jetons désactivés peuvent être activés.

Les jetons accordent un accès général aux API du point de vue du client ; ils gèrent l'accès aux API dans le cadre de leur propre locataire. Les administrateurs clients peuvent accorder et révoquer ces jetons sans intervention directe du personnel back-end de Data Infrastructure Insights .

L'application reçoit un jeton d'accès après qu'un utilisateur s'est authentifié et a autorisé l'accès avec succès, puis transmet le jeton d'accès comme identifiant lorsqu'il appelle l'API cible. Le jeton transmis informe l'API que le porteur du jeton a été autorisé à accéder à l'API et à effectuer des actions spécifiques spécifiées par la portée qui a été accordée lors de l'autorisation.

L'en-tête HTTP où le jeton d'accès est transmis est **X-CloudInsights-ApiKey:**.

Par exemple, utilisez ce qui suit pour récupérer les ressources de stockage :

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
Où _<API_Access_Token>_ est le jeton que vous avez enregistré lors de la
création de l'accès à l'API.
```

Consultez les pages Swagger pour des exemples spécifiques à l'API que vous souhaitez utiliser.

Type d'API

L'API Data Infrastructure Insights est basée sur des catégories et contient actuellement les types suivants :

- Le type ASSETS contient des API d'actifs, de requêtes et de recherche.
  - Actifs : énumérer les objets de niveau supérieur et récupérer un objet spécifique ou une hiérarchie d'objets.
  - Requête : récupérez et gérez les requêtes Data Infrastructure Insights .
  - Importer : importer des annotations ou des applications et les affecter à des objets
  - Recherche : localisez un objet spécifique sans connaître l'ID unique ou le nom complet de l'objet.
- Le type COLLECTE DE DONNÉES est utilisé pour récupérer et gérer les collecteurs de données.
- Le type d'INGESTION DE DONNÉES est utilisé pour récupérer et gérer les données d'ingestion et les métriques personnalisées, telles que celles des agents Telegraf
- L'INGESTION DE JOURNAUX est utilisée pour récupérer et gérer les données de journaux

Des types et/ou API supplémentaires peuvent devenir disponibles au fil du temps. Vous pouvez trouver les dernières informations sur l'API dans le"Documentation de l'API Swagger" .

Notez que les types d'API auxquels un utilisateur a accès dépendent également de la"Rôle de l'utilisateur" ils ont dans chaque ensemble de fonctionnalités Data Infrastructure Insights (surveillance, sécurité de la charge de travail, reporting).

Parcours d’inventaire

Cette section décrit comment parcourir une hiérarchie d’objets Data Infrastructure Insights .

Objets de niveau supérieur

Les objets individuels sont identifiés dans les requêtes par une URL unique (appelée « self » en JSON) et nécessitent la connaissance du type d’objet et de son identifiant interne. Pour certains objets de niveau supérieur (hôtes, stockages, etc.), l’API REST donne accès à la collection complète.

Le format général d’une URL d’API est :

```
 https://<tenant>/rest/v1/<type>/<object>
Par exemple, pour récupérer tous les stockages d'un locataire nommé
_mysite.c01.cloudinsights.netapp.com_, l'URL de la requête est :
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Enfants et objets apparentés

Les objets de niveau supérieur, tels que le stockage, peuvent être utilisés pour accéder à d’autres enfants et objets associés. Par exemple, pour récupérer tous les disques d’un stockage spécifique, concaténez l’URL « self » du stockage avec « /disks », par exemple :

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

S’agrandit

De nombreuses commandes API prennent en charge le paramètre **expand**, qui fournit des détails supplémentaires sur l’objet ou les URL des objets associés.

Le seul paramètre d’expansion commun est *expands*. La réponse contient une liste de toutes les extensions spécifiques disponibles pour l’objet.

Par exemple, lorsque vous demandez ce qui suit :

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
L'API renvoie toutes les extensions disponibles pour l'objet comme suit :
```

```
{
    "id": "1247936",
      "self": "/rest/v1/assets/storages/1247936",
      "name": "amsprdclu01",
      "simpleName": "amsprdclu01",
      "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
      "ip": "10.64.0.132",
      "serialNumber": "1-80-000011",
      "model": "FAS3270,FAS6290",
      "vendor": "NetApp",
      "microcodeVersion": "8.1.3 clustered Data ONTAP",
      "capacity": {
        "description": "Storage Capacity",
        "unitType": "MB",
        "total": {
          "value": 8.23185105E8
        },
        "storagePools": {
          "value": 5.43220974E8
        }
      },
      "isActive": true,
      "createTime": "2013-05-07T16:52:21-0700",
      "family": "FAS3200,FAS6200",
      "managementUrl": null,
      "virtualizedType": "STANDARD",
      "protocols":
      [
        "NAS",
        "NFS",
        "CIFS",
        "FC",
        "ISCSI"
      ],
      "_expands": {
        "performance": {
          "url": "/rest/v1/assets/storages/1247936/performance",
          "name": "Performance Data"
        },
        "storageNodes": {
          "url": "/rest/v1/assets/storages/1247936/storageNodes",
          "name": "Storage Storage Nodes"
        },
        "storagePools": {
          "url": "/rest/v1/assets/storages/1247936/storagePools",
          "name": "Storage Storage Pools"
        },
        "storageResources": {
          "url": "/rest/v1/assets/storages/1247936/storageResources",
          "name": "Storage Storage Resources"
        },
        "internalVolumes": {
          "url": "/rest/v1/assets/storages/1247936/internalVolumes",
          "name": "Storage Internal Volumes"
        },
        "volumes": {
          "url": "/rest/v1/assets/storages/1247936/volumes",
          "name": "Storage Volumes"
        },
        "disks": {
          "url": "/rest/v1/assets/storages/1247936/disks",
          "name": "Disks"
        },
        "datasources": {
          "url": "/rest/v1/assets/storages/1247936/datasources",
          "name": "Storage Datasources"
        },
        "ports": {
          "url": "/rest/v1/assets/storages/1247936/ports",
          "name": "Storage Ports"
        },
        "annotations": {
          "url": "/rest/v1/assets/storages/1247936/annotations",
          "name": "Storage Annotations"
        },
        "qtrees": {
          "url": "/rest/v1/assets/storages/1247936/qtrees",
          "name": "Qtrees"
        },
```

Chaque extension contient des données, une URL ou les deux. Le paramètre expand prend en charge plusieurs attributs imbriqués, par exemple :

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Développer vous permet d'intégrer de nombreuses données connexes dans une
seule réponse.  NetApp vous conseille de ne pas demander trop
d'informations à la fois ; cela peut entraîner une dégradation des
performances.
```

Pour décourager cela, les demandes de collections de niveau supérieur ne peuvent pas être étendues. Par exemple, vous ne pouvez pas demander l'extension des données pour tous les objets de stockage à la fois. Les clients doivent récupérer la liste des objets, puis choisir des objets spécifiques à développer.

Données de performance

Les données de performances sont collectées sur de nombreux appareils sous forme d'échantillons distincts. Toutes les heures (par défaut), Data Infrastructure Insights regroupe et résume les échantillons de performances.

L'API permet d'accéder à la fois aux échantillons et aux données résumées. Pour un objet avec des données de performances, un résumé des performances est disponible sous la forme *expand=performance*. Les séries chronologiques de l'historique des performances sont disponibles via *expand=performance.history* imbriqué.

Voici quelques exemples d'objets de données de performance :

- Performances de stockage
- Performances du pool de stockage
- Performances portuaires
- Performances du disque

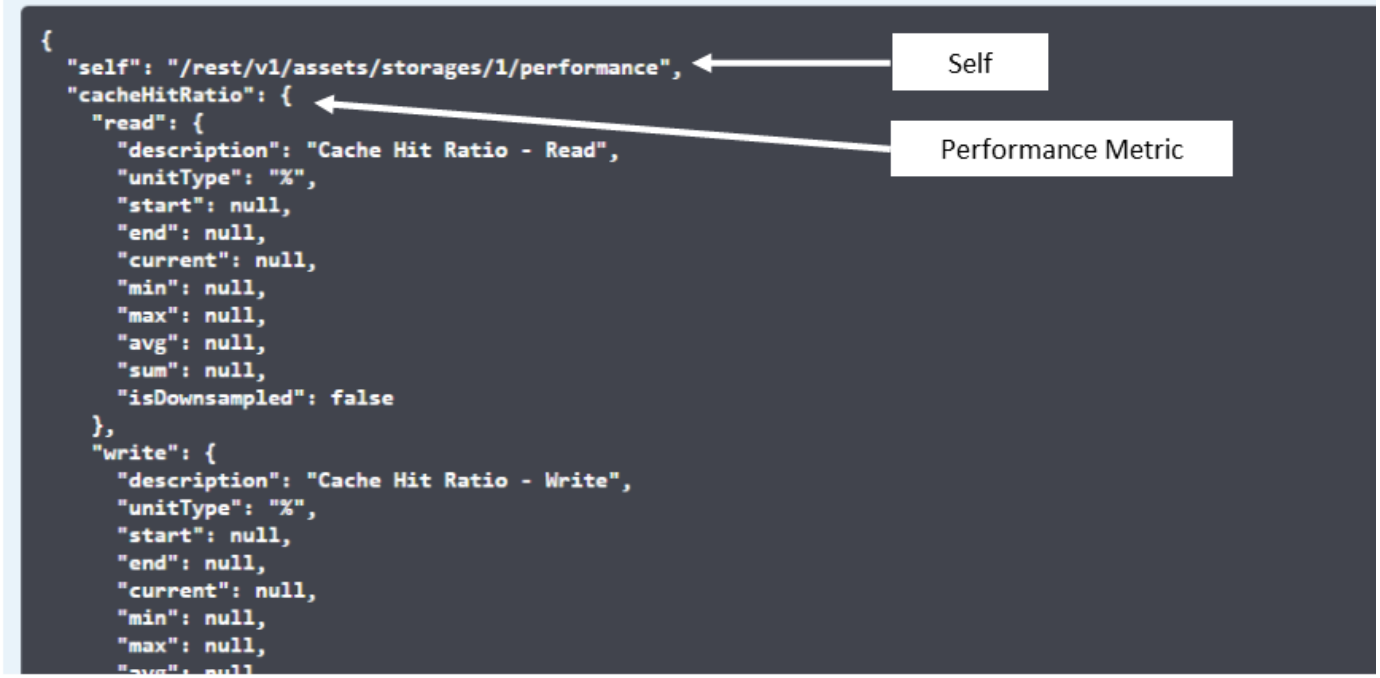
Une mesure de performance possède une description et un type et contient une collection de résumés de performances. Par exemple, la latence, le trafic et le débit.

Un résumé des performances comporte une description, une unité, une heure de début d'échantillon, une heure de fin d'échantillon et un ensemble de valeurs résumées (actuelles, min, max, moyenne, etc.) calculées à partir d'un seul compteur de performances sur une plage de temps (1 heure, 24 heures, 3 jours, etc.).

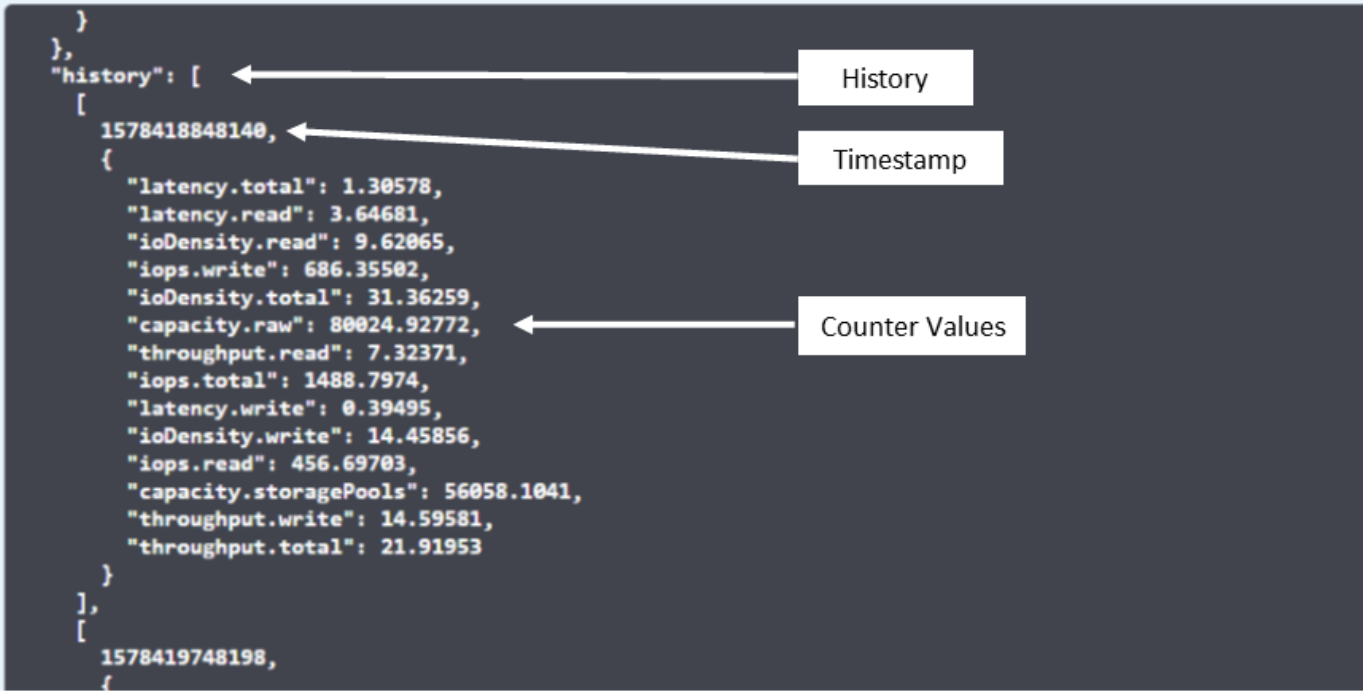
https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body



Response body



Le dictionnaire de données de performance résultant contient les clés suivantes :

- « self » est l'URL unique de l'objet

- « historique » est la liste des paires d'horodatages et de valeurs de compteurs
- Chaque autre clé du dictionnaire (« diskThroughput » et ainsi de suite) est le nom d'une mesure de performance.

Chaque type d'objet de données de performances possède un ensemble unique de mesures de performances. Par exemple, l'objet de performances de la machine virtuelle prend en charge « diskThroughput » comme mesure de performances. Chaque mesure de performance prise en charge appartient à une certaine « performanceCategory » présentée dans le dictionnaire de mesures. Data Infrastructure Insights prend en charge plusieurs types de mesures de performances répertoriés plus loin dans ce document. Chaque dictionnaire de mesures de performance comportera également le champ « description », qui est une description lisible par l'homme de cette mesure de performance et un ensemble d'entrées de compteur de résumé de performance.

Le compteur Résumé des performances est le résumé des compteurs de performances. Il présente des valeurs agrégées typiques telles que min, max et moyenne pour un compteur, ainsi que la dernière valeur observée, la plage horaire pour les données résumées, le type d'unité pour le compteur et les seuils pour les données. Seuls les seuils sont facultatifs ; le reste des attributs est obligatoire.

Des résumés de performances sont disponibles pour ces types de compteurs :

- Lecture – Résumé des opérations de lecture
- Écriture – Résumé des opérations d'écriture
- Total – Résumé de toutes les opérations. Elle peut être supérieure à la simple somme des lectures et des écritures ; elle peut inclure d'autres opérations.
- Total Max – Résumé de toutes les opérations. Il s'agit de la valeur totale maximale dans la plage de temps spécifiée.

Mesures de performance des objets

L'API peut renvoyer des métriques détaillées pour les objets de votre locataire, par exemple :

- Mesures de performances de stockage telles que les IOPS (nombre de requêtes d'entrée/sortie par seconde), la latence ou le débit.
- Mesures de performances du commutateur, telles que l'utilisation du trafic, les données BB Credit Zero ou les erreurs de port.

Voir le"Documentation de l'API Swagger" pour obtenir des informations sur les métriques pour chaque type d'objet.

Données d'historique des performances

Les données d'historique sont présentées dans les données de performances sous la forme d'une liste de paires de cartes d'horodatage et de compteur.

Les compteurs d'historique sont nommés en fonction du nom de l'objet de mesure de performances. Par exemple, l'objet de performance de la machine virtuelle prend en charge « diskThroughput », de sorte que la carte d'historique contiendra des clés nommées « diskThroughput.read », « diskThroughput.write » et « diskThroughput.total ».

L'horodatage est au format horaire UNIX.

Voici un exemple de données de performances JSON pour un disque :

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
     "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


Objets avec attributs de capacité

Les objets avec des attributs de capacité utilisent des types de données de base et CapacityItem pour la représentation.

CapacitéArticle

CapacityItem est une unité logique unique de capacité. Il a une « valeur » et un « seuil élevé » dans les unités définies par son objet parent. Il prend également en charge une carte de répartition facultative qui explique comment la valeur de capacité est construite. Par exemple, la capacité totale d'un pool de stockage de 100 To serait un CapacityItem avec une valeur de 100. La répartition peut montrer 60 To alloués aux « données » et 40 To aux « instantanés ».

Remarque : « highThreshold » représente les seuils définis par le système pour les mesures correspondantes, qu'un client peut utiliser pour générer des alertes ou des repères visuels sur les valeurs qui sont hors des plages configurées acceptables.

L'exemple suivant montre la capacité des StoragePools avec plusieurs compteurs de capacité :

Utiliser la recherche pour rechercher des objets

L'API de recherche est un point d'entrée simple vers le système. Le seul paramètre d'entrée de l'API est une chaîne de forme libre et le JSON résultant contient une liste catégorisée de résultats. Les types sont des types d'actifs différents de l'inventaire, tels que les stockages, les hôtes, les magasins de données, etc. Chaque type contiendrait une liste d'objets du type correspondant aux critères de recherche.

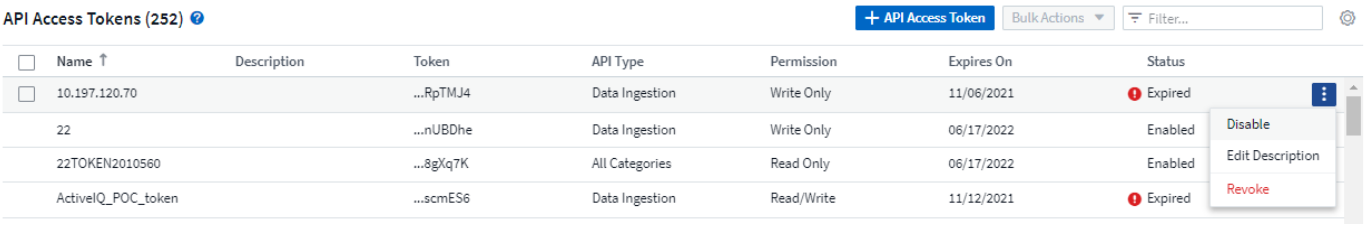
Data Infrastructure Insights est une solution extensible (largement ouverte) qui permet des intégrations avec des systèmes d'orchestration, de gestion d'entreprise, de contrôle des modifications et de billetterie tiers ainsi que des intégrations CMDB personnalisées.

L'API RESTful de Cloud Insight est un point d'intégration principal qui permet un déplacement simple et efficace des données et permet aux utilisateurs d'accéder de manière transparente à leurs données.

Désactiver ou révoquer un jeton API

Pour désactiver temporairement un jeton API, sur la page de liste des jetons API, cliquez sur le menu « trois points » pour l'API et sélectionnez *Désactiver*. Vous pouvez réactiver le jeton à tout moment en utilisant le même menu et en sélectionnant *Activer*.

Pour supprimer définitivement un jeton API, dans le menu, sélectionnez « Révoquer ». Vous ne pouvez pas réactiver un jeton révoqué ; vous devez créer un nouveau jeton.



Rotation des jetons d'accès API expirés

Les jetons d'accès API ont une date d'expiration. Lorsqu'un jeton d'accès API expire, les utilisateurs doivent générer un nouveau jeton (de type *Data Ingestion* avec des autorisations de lecture/écriture) et reconfigurer Telegraf pour utiliser le jeton nouvellement généré au lieu du jeton expiré. Les étapes ci-dessous détaillent comment procéder.

Kubernetes

Notez que ces commandes utilisent l'espace de noms par défaut « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez cet espace de noms dans ces commandes et fichiers et dans tous les suivants.

Remarque : si vous avez installé la dernière version de NetApp Kubernetes Monitoring Operator et que vous utilisez un jeton d'accès API renouvelable, les jetons expirant seront automatiquement remplacés par des jetons d'accès API nouveaux/actualisés. Il n'est pas nécessaire d'effectuer les étapes manuelles répertoriées ci-dessous.

- Créez un nouveau jeton API.
- Suivez les étapes pour"Mise à niveau manuelle" , en sélectionnant le nouveau jeton API.

Remarque : les clients qui gèrent leur NetApp Kubernetes Monitoring Operator avec un outil de gestion de configuration, tel que Kustomize, peuvent suivre les mêmes étapes pour générer et télécharger un ensemble mis à jour de fichiers YAML à envoyer vers leur référentiel.

RHEL/CentOS et Debian/Ubuntu

- Modifiez les fichiers de configuration Telegraf et remplacez toutes les instances de l'ancien jeton API par le nouveau jeton API.

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Redémarrez Telegraf.
```

```
sudo systemctl restart telegraf
```

Windows

- Pour chaque fichier de configuration Telegraf dans *C:\Program Files\telegraf\telegraf.d*, remplacez toutes les instances de l'ancien jeton API par le nouveau jeton API.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Redémarrez Telegraf.

```
Stop-Service telegraf
Start-Service telegraf
```

Surveiller votre environnement

Audit

Pour identifier les modifications attendues (pour le suivi) ou inattendues (pour le dépannage), vous pouvez afficher une piste d'audit des événements système et des activités des utilisateurs de Data Infrastructure Insights .

Affichage des événements audités

Pour afficher la page Audit, cliquez sur **Admin > Audit** dans le menu. La page Audit s'affiche, fournissant les détails suivants pour chaque entrée d'audit :

- **Heure** - Date et heure de l'événement ou de l'activité
- **Utilisateur** - L'utilisateur qui a initié l'activité
- **Rôle** - Le rôle de l'utilisateur dans Data Infrastructure Insights (invité, utilisateur, administrateur)
- **IP** - L'adresse IP associée à l'événement
- **Action** - Type d'activité, par exemple Connexion, Créer, Mettre à jour
- **Catégorie** - La catégorie d'activité
- **Détails** - Détails de l'activité

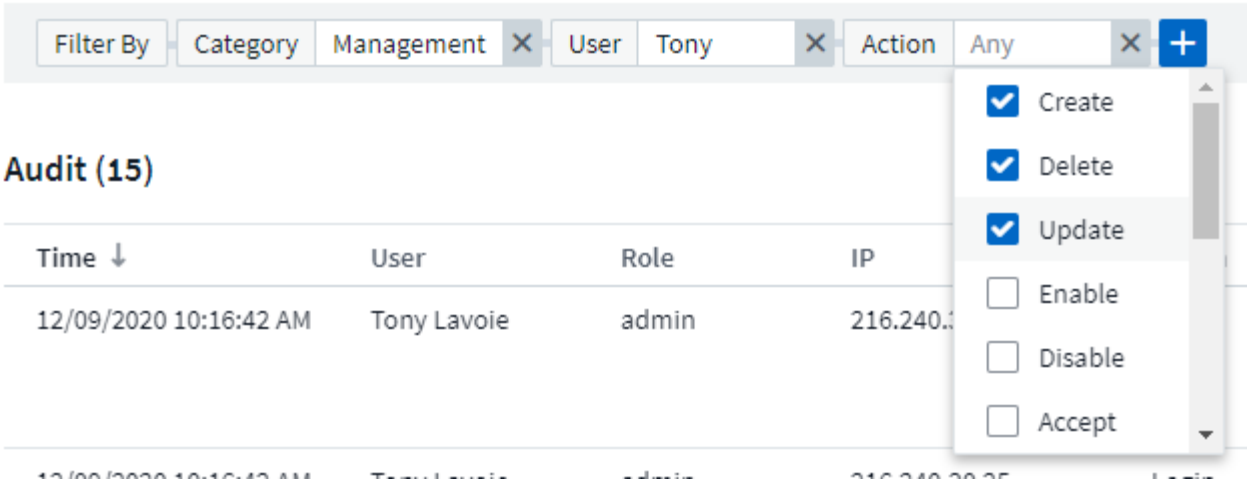
Affichage des entrées d'audit

Il existe plusieurs façons différentes d'afficher les entrées d'audit :

- Vous pouvez afficher les entrées d'audit en choisissant une période particulière (1 heure, 24 heures, 3 jours, etc.).
- Vous pouvez modifier l'ordre de tri des entrées en croissant (flèche vers le haut) ou décroissant (flèche vers le bas) en cliquant sur la flèche dans l'en-tête de la colonne.

  Par défaut, le tableau affiche les entrées par ordre chronologique décroissant.

- Vous pouvez utiliser les champs de filtre pour afficher uniquement les entrées que vous souhaitez dans le tableau. Cliquez sur le bouton [+] pour ajouter des filtres supplémentaires.



En savoir plus sur le filtrage

Vous pouvez utiliser l'un des éléments suivants pour affiner votre filtre :

Filtre	Ce qu'il fait	Exemple	Résultat
* (Astérisque)	vous permet de rechercher tout ce que vous voulez	vol*rhel	renvoie toutes les ressources commençant par « vol » et se terminant par « rhel »
? (point d'interrogation)	vous permet de rechercher un nombre spécifique de caractères	BOS-PRD??-S12	renvoie BOS-PRD***12***-S12, BOS-PRD***23***-S12, et ainsi de suite
OU	vous permet de spécifier plusieurs entités	FAS2240 OU CX600 OU FAS3270	renvoie l'un des FAS2440, CX600 ou FAS3270
PAS	vous permet d'exclure du texte des résultats de recherche	NON EMC*	renvoie tout ce qui ne commence pas par « EMC »
Aucun	recherche vide/NULL/Aucun dans n'importe quel champ sélectionné	*Aucun*	renvoie les résultats lorsque le champ cible n'est pas vide
Pas *	comme avec *None* ci-dessus, mais vous pouvez également utiliser ce formulaire pour rechercher des valeurs NULL dans les champs *texte uniquement*	Pas *	renvoie les résultats lorsque le champ cible n'est pas vide.
""	recherche une correspondance exacte	"NetApp*"	renvoie des résultats contenant la chaîne littérale exacte *NetApp**

Si vous placez une chaîne de filtre entre guillemets doubles, Insight traite tout ce qui se trouve entre le premier et le dernier guillemet comme une correspondance exacte. Tous les caractères spéciaux ou opérateurs à

l'intérieur des guillemets seront traités comme des littéraux. Par exemple, le filtrage par « * » renverra des résultats qui sont un astérisque littéral ; l'astérisque ne sera pas traité comme un caractère générique dans ce cas. Les opérateurs OR et NOT seront également traités comme des chaînes littérales lorsqu'ils sont placés entre guillemets.

Événements et actions audités

Les événements et actions audités par Data Infrastructure Insights peuvent être classés dans les grands domaines suivants :

- **Compte utilisateur** : Connexion, déconnexion, changement de rôle, etc.
- **Unité d'acquisition** : créer, supprimer, etc.

  Exemple : *Unité d'acquisition **AU-Boston-1** supprimée*.

- **Collecteur de données** : ajouter, supprimer, modifier, reporter/reprendre, changer d'unité d'acquisition, démarrer/arrêter, etc.

  Exemple : *Datasource * FlexPod Lab* supprimé, fournisseur * NetApp*, modèle * ONTAP Data Management Software*, IP **192.168.106.5***.

- **Application** : ajouter, affecter à un objet, supprimer, etc.

  Exemple : *Volume interne **ocisedev:t1appSVM01:t1appFlexVol01** ajouté à l'application **Test App***.

- **Annotation** : ajouter, attribuer, supprimer, actions de règle d'annotation, modifications de valeur d'annotation, etc.

  Exemple : *Valeur d'annotation **Boston** ajoutée au type d'annotation **SalesOffice***.

- **Requête** : ajouter, supprimer, etc.

  Exemple : *La requête **TL Sales Query** est ajoutée*.

- **Moniteur** : ajouter, supprimer, etc.

  Exemple : Surveiller *Aggr Size - CI Alerts Notifications Dev* mis à jour

- **Notification** : changement d'email, etc.

  Exemple : Destinataire *ci-alerts-notifications-dl* créé

Exportation des événements d'audit

Vous pouvez exporter les résultats de votre affichage d'audit vers un fichier .CSV, ce qui vous permettra d'analyser les données ou de les importer dans une autre application.

Étapes

1. Sur la page Audit, définissez la plage horaire souhaitée et les filtres souhaités. Data Infrastructure Insights exportera uniquement les entrées d'audit qui correspondent au filtrage et à la plage horaire que vous avez définis.
2. Cliquez sur le bouton _Exporter_ en haut à droite du tableau.

Les événements d'audit affichés seront exportés vers un fichier .CSV, jusqu'à un maximum de 10 000 lignes.

Conservation des données d'audit

La durée pendant laquelle Data Infrastructure Insights conserve les données d'audit dépend de votre abonnement :

- Environnements d'essai : les données d'audit sont conservées pendant 30 jours
- Environnements abonnés : les données d'audit sont conservées pendant 1 an plus 1 jour

Les entrées d'audit plus anciennes que la durée de conservation sont automatiquement purgées. Aucune interaction de l'utilisateur n'est nécessaire.

Les entrées d'audit plus anciennes que la durée de conservation sont automatiquement purgées. Aucune interaction de l'utilisateur n'est nécessaire.

Dépannage

Vous trouverez ici des suggestions pour résoudre les problèmes liés à Audit.

Problème:	Essayez ceci :
Je vois des messages d'audit m'indiquant qu'un moniteur a été exporté.	L'exportation d'une configuration de moniteur personnalisée est généralement utilisée par les ingénieurs NetApp lors du développement et des tests de nouvelles fonctionnalités. Si vous ne vous attendiez pas à voir ce message, pensez à explorer les actions de l'utilisateur nommé dans l'action auditée ou à contacter le support.

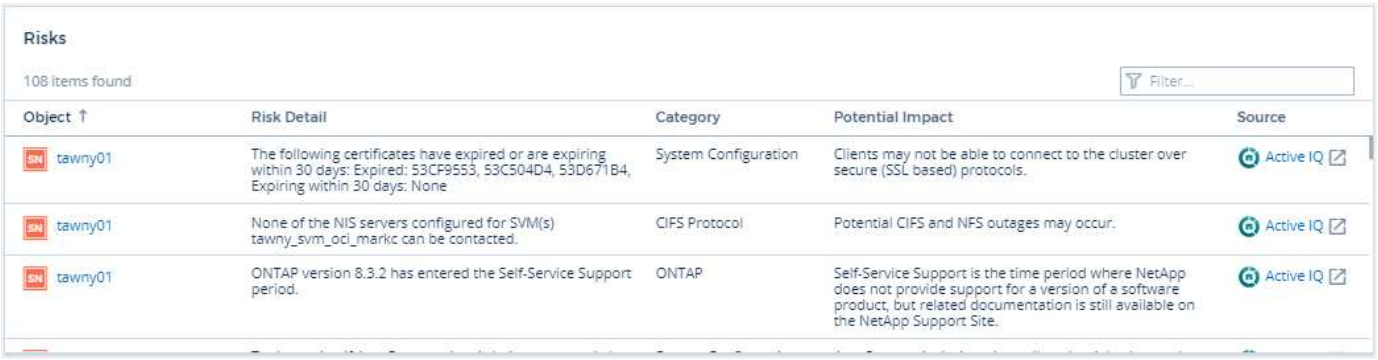
Digital Advisor Active IQ

NetApp"Digital Advisor Active IQ" (également connu sous le nom de Digital Advisor) fournit une série de visualisations, d'analyses et d'autres services liés au support aux clients NetApp pour leurs systèmes matériels/logiciels. Les données rapportées par Digital Advisor peuvent améliorer la résolution des problèmes système et également fournir un aperçu de l'optimisation et de l'analyse prédictive liées à vos appareils.

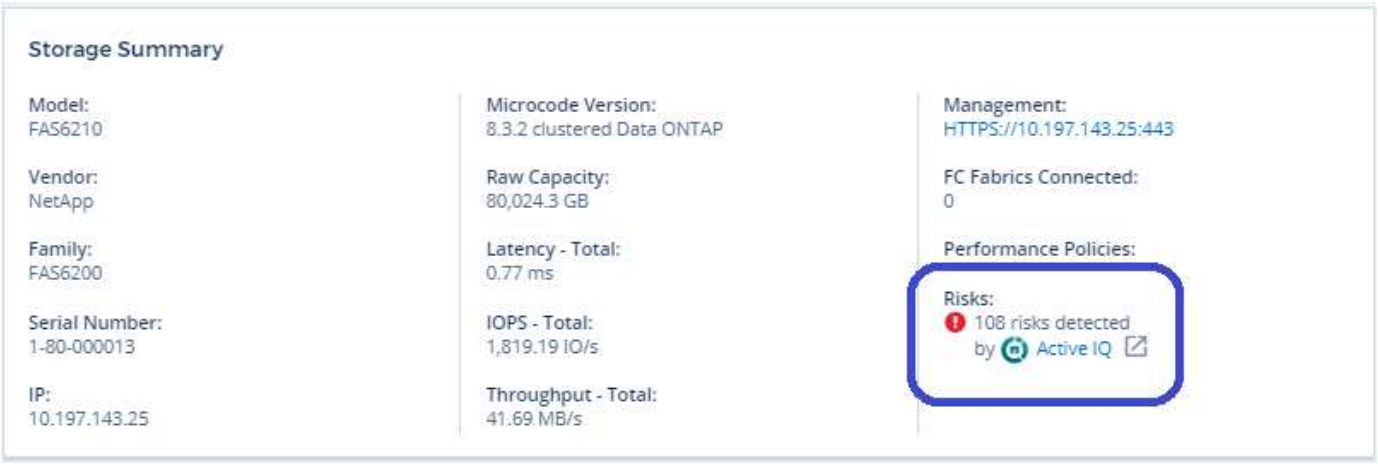
Data Infrastructure Insights collecte les **risques** pour tout système de stockage NetApp Clustered Data ONTAP surveillé et signalé par Digital Advisor. Les risques signalés pour les systèmes de stockage sont collectés automatiquement par Data Infrastructure Insights dans le cadre de sa collecte de données à partir de ces appareils. Vous devez ajouter le collecteur de données approprié à Data Infrastructure Insights pour collecter les informations sur les risques de Digital Advisor .

Data Infrastructure Insights n'affichera pas les données de risque pour les systèmes ONTAP qui ne sont pas surveillés et signalés par Digital Advisor.

Les risques signalés sont affichés dans Data Infrastructure Insights sur les pages de destination des actifs *storage* et *storage node*, dans le tableau « Risques ». Le tableau affiche les détails du risque, la catégorie de risque et l'impact potentiel du risque, et fournit également un lien vers la page Digital Advisor résumant tous les risques pour le nœud de stockage (connexion au compte de support NetApp requise).



Le nombre de risques signalés est également affiché dans le widget Résumé de la page de destination, avec un lien vers la page Digital Advisor appropriée. Sur une page de destination *stockage*, le décompte est la somme des risques de tous les nœuds de stockage sous-jacents.



Ouverture de la page du Digital Advisor

Lorsque vous cliquez sur le lien vers une page Digital Advisor , si vous n'êtes pas actuellement connecté à votre compte Digital Advisor , vous devez effectuer les étapes suivantes pour afficher la page Digital Advisor du nœud de stockage.

1. Dans le widget Résumé des Data Infrastructure Insights ou dans le tableau Risques, cliquez sur le lien «Digital Advisor».
2. Sign in à votre compte de support NetApp . Vous êtes redirigé directement vers la page du nœud de stockage dans Digital Advisor.

Interrogation sur les risques

Dans Data Infrastructure Insights, vous pouvez ajouter la colonne **monitoring.count** à une requête de stockage ou de nœud de stockage. Si le résultat renvoyé inclut les systèmes de stockage surveillés par Digital Advisor, la colonne monitoring.count affichera le nombre de risques pour le système de stockage ou le nœud.

Tableaux de bord

Vous pouvez créer des widgets (par exemple, des graphiques à secteurs, des widgets de tableau, des widgets à barres, à colonnes, à nuages de points et à valeur unique) afin de visualiser les risques liés aux objets pour le stockage et les nœuds de stockage pour les systèmes NetApp Clustered Data ONTAP surveillés par Digital Advisor. « Risques d'objet » peut être sélectionné comme colonne ou métrique dans ces widgets où le stockage ou le nœud de stockage est l'objet de concentration.

Object Risks by Array

12 items found

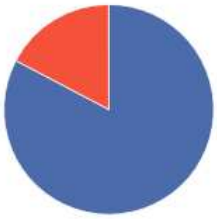
Name	Object Risks
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdsfc01	N/A
oci-3070-01	N/A

Object Risks by Node

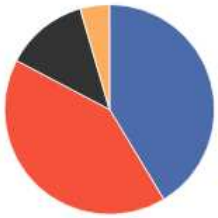
25 items found

Name	Object Risks
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A

Object Risks by Storage



Object Risks by Storage Node



Total Storage Risks

133.00

Object Risks

Sécurité de la charge de travail

À propos de la sécurité des charges de travail de stockage

Data Infrastructure Insights Storage Workload Security (anciennement Cloud Secure) aide à protéger vos données grâce à des informations exploitables sur les menaces internes. Il offre une visibilité et un contrôle centralisés de tous les accès aux données de l'entreprise dans les environnements de cloud hybride pour garantir que les objectifs de sécurité et de conformité sont atteints.

Visibilité

Bénéficiez d'une visibilité et d'un contrôle centralisés de l'accès des utilisateurs à vos données d'entreprise critiques stockées sur site ou dans le cloud.

Remplacez les outils et les processus manuels qui ne parviennent pas à fournir une visibilité rapide et précise sur l'accès et le contrôle des données. Workload Security fonctionne de manière unique sur les systèmes de stockage cloud et sur site pour vous fournir des alertes en temps réel sur le comportement malveillant des utilisateurs.

Protection

Protégez les données de l'organisation contre toute utilisation abusive par des utilisateurs malveillants ou compromis grâce à l'apprentissage automatique avancé et à la détection des anomalies.

Vous alerte de tout accès anormal aux données grâce à l'apprentissage automatique avancé et à la détection des anomalies du comportement des utilisateurs.

Conformité

Assurez la conformité de l'entreprise en auditant l'accès des utilisateurs à vos données d'entreprise critiques stockées sur site ou dans le cloud.

Commencer

Premiers pas avec la sécurité des charges de travail

Workload Security vous aide à surveiller l'activité des utilisateurs et à détecter les menaces de sécurité potentielles dans votre environnement de stockage. Avant de pouvoir commencer la surveillance, vous devez configurer les agents, les collecteurs de données et les services d'annuaire afin d'établir les bases d'une surveillance de sécurité complète.

Le système Workload Security utilise un agent pour collecter les données d'accès des systèmes de stockage et les informations utilisateur des serveurs des services d'annuaire.

Vous devez configurer les éléments suivants avant de pouvoir commencer à collecter des données :

Tâche	Informations connexes

Configurer un agent	"Exigences relatives aux agents" "Ajouter un agent"
Configurer un connecteur d'annuaire utilisateur	"Ajouter un connecteur d'annuaire utilisateur"
Configurer les collecteurs de données	Cliquez sur **Sécurité de la charge de travail > Collecteurs**. Cliquez sur le collecteur de données que vous souhaitez configurer. Consultez la section « Référence du fournisseur de collecteurs de données » de la documentation pour obtenir des informations sur les collecteurs.
Créer des comptes utilisateurs	"Gérer les comptes utilisateurs"

Workload Security peut également s'intégrer à d'autres outils. Par exemple,"voir ce guide" sur l'intégration avec Splunk.

Exigences relatives à l'agent de sécurité de la charge de travail

Déployez les agents de sécurité des charges de travail sur des serveurs dédiés répondant aux exigences minimales en matière de système d'exploitation, de processeur, de mémoire et d'espace disque afin de garantir des performances optimales de surveillance et de détection des menaces. Ce guide spécifie la configuration matérielle et réseau requise avant "installation de votre Workload Security Agent", notamment les distributions Linux prises en charge, les règles de connectivité réseau et les recommandations de dimensionnement du système.

Composant	Exigences Linux
Système opérateur	Un ordinateur exécutant une version sous licence de l'un des systèmes d'exploitation suivants : * AlmaLinux 9.4 (64 bits) à 9.5 (64 bits), 10 (64 bits), y compris SELinux * CentOS Stream 9 (64 bits) * Debian 11 (64 bits), 12 (64 bits), y compris SELinux * OpenSUSE Leap 15.3 (64 bits) à 15.6 (64 bits) * Oracle Linux 8.10 (64 bits), 9.1 (64 bits) à 9.6 (64 bits), y compris SELinux * Red Hat Enterprise Linux 8.10 (64 bits), 9.1 (64 bits) à 9.6 (64 bits), 10 (64 bits), y compris SELinux * Rocky 9.4 (64 bits) à 9.6 (64 bits), y compris SELinux * SUSE Linux Enterprise Server 15 SP4 (64 bits) à 15 SP6 (64 bits), y compris SELinux * Ubuntu 20.04 LTS (64 bits), 22.04 LTS (64 bits), 24.04 LTS (64 bits) Cet ordinateur ne doit exécuter aucun autre logiciel de niveau application. Un serveur dédié est recommandé.
Commandes	'unzip' est requis pour l'installation. De plus, la commande « sudo su – » est requise pour l'installation, l'exécution de scripts et la désinstallation.
processeur	4 cœurs de processeur
Mémoire	16 Go de RAM

Composant	Exigences Linux
Espace disque disponible	L'espace disque doit être alloué de cette manière : /opt/netapp 36 Go (minimum 35 Go d'espace libre après la création du système de fichiers) Remarque : il est recommandé d'allouer un peu d'espace disque supplémentaire pour permettre la création du système de fichiers. Assurez-vous qu'il y a au moins 35 Go d'espace libre dans le système de fichiers. Si /opt est un dossier monté à partir d'un stockage NAS, assurez-vous que les utilisateurs locaux ont accès à ce dossier. L'installation de l'agent ou du collecteur de données peut échouer si les utilisateurs locaux ne disposent pas de l'autorisation d'accéder à ce dossier. voir le"dépannage" section pour plus de détails.
Réseau	Connexion Ethernet 100 Mbps à 1 Gbps, adresse IP statique, connectivité IP à tous les appareils et un port requis pour l'instance Workload Security (80 ou 443).

Remarque : l'agent Workload Security peut être installé sur la même machine qu'une unité d'acquisition et/ou un agent Data Infrastructure Insights . Cependant, il est recommandé de les installer sur des machines séparées. Dans le cas où ceux-ci sont installés sur la même machine, veuillez allouer de l'espace disque comme indiqué ci-dessous :

Espace disque disponible	50-55 Go Pour Linux, l'espace disque doit être alloué de cette manière : /opt/netapp 25-30 Go /var/log/netapp 25 Go

Recommandations supplémentaires

- Il est fortement recommandé de synchroniser l'heure sur le système ONTAP et sur la machine Agent à l'aide du **Network Time Protocol (NTP)** ou du **Simple Network Time Protocol (SNTP)**.

Règles d'accès au réseau cloud

Pour les environnements de sécurité des charges de travail **basés aux États-Unis** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité de la charge de travail	<nom_site>.cs01.cloudinsights.netapp.com <nom_site>.c01.cloudinsights.netapp.com <nom_site>.c02.cloudinsights.netapp.com	Accès aux Data Infrastructure Insights
TCP	443	Agent de sécurité de la charge de travail	agentlogin.cs01.cloudinsights.netapp.com	Accès aux services d'authentification

Pour les environnements de sécurité des charges de travail **basés en Europe** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité de la charge de travail	<nom_site>.cs01-eu-1.cloudinsights.netapp.com <nom_site>.c01-eu-1.cloudinsights.netapp.com <nom_site>.c02-eu-1.cloudinsights.netapp.com	Accès aux Data Infrastructure Insights
TCP	443	Agent de sécurité de la charge de travail	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accès aux services d'authentification

Pour les environnements de sécurité des charges de travail **basés sur la région APAC** :

Protocole	Port	Source	Destination	Description
TCP	443	Agent de sécurité de la charge de travail	<nom_site>.cs01-ap-1.cloudinsights.netapp.com <nom_site>.c01-ap-1.cloudinsights.netapp.com <nom_site>.c02-ap-1.cloudinsights.netapp.com	Accès aux Data Infrastructure Insights
TCP	443	Agent de sécurité de la charge de travail	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Accès aux services d'authentification

Règles du réseau

Protocole	Port	Source	Destination	Description
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agent de sécurité de la charge de travail	URL du serveur LDAP	Se connecter à LDAP
TCP	443	Agent de sécurité de la charge de travail	Adresse IP de gestion du cluster ou du SVM (selon la configuration du collecteur SVM)	Communication API avec ONTAP

Protocole	Port	Source	Destination	Description
TCP	35000 - 55000	Adresses IP LIF des données SVM	Agent de sécurité de la charge de travail	Communication d' ONTAP à l’agent de sécurité de la charge de travail pour les événements Fpolicy. Ces ports doivent être ouverts vers l’agent de sécurité de la charge de travail pour ONTAP puisse lui envoyer des événements, y compris tout pare-feu sur l’agent de sécurité de la charge de travail lui-même (le cas échéant). NOTEZ que vous n’avez pas besoin de réserver **tous** ces ports, mais les ports que vous réservez pour cela doivent être dans cette plage. Il est recommandé de commencer par réserver environ 100 ports, et d’augmenter si nécessaire.

Protocole	Port	Source	Destination	Description
TCP	35000-55000	IP de gestion de cluster	Agent de sécurité de la charge de travail	Communication de l'IP de gestion du cluster ONTAP à l'agent de sécurité de la charge de travail pour les **événements EMS**. Ces ports doivent être ouverts vers l'agent de sécurité de la charge de travail pour ONTAP puisse lui envoyer des **événements EMS**, y compris tout pare-feu sur l'agent de sécurité de la charge de travail lui-même (le cas échéant). NOTEZ que vous n'avez pas besoin de réserver **tous** ces ports, mais les ports que vous réservez pour cela doivent être dans cette plage. Il est recommandé de commencer par réserver environ 100 ports, et d'augmenter si nécessaire.
SSH	22	Agent de sécurité de la charge de travail	Gestion des clusters	Nécessaire pour le blocage des utilisateurs CIFS/SMB.

Dimensionnement du système

Voir le"Vérificateur de taux d'événements" documentation pour obtenir des informations sur le dimensionnement.

Déployer des agents de sécurité de charge de travail

Les agents de sécurité des charges de travail sont essentiels pour surveiller l'activité des utilisateurs et détecter les menaces potentielles à la sécurité de votre infrastructure de stockage. Ce guide fournit des instructions d'installation étape par étape, les meilleures pratiques pour la gestion des agents (y compris les fonctionnalités de pause/reprise et d'épinglage/désépinglage) et les exigences de configuration post-déploiement. Avant de

commencer, assurez-vous que votre serveur d'agent répond aux exigences suivantes : "exigences système".

Avant de commencer

- Le privilège sudo est requis pour l'installation, l'exécution de scripts et la désinstallation.
- Lors de l'installation de l'agent, un utilisateur local *cssys* et un groupe local *cssys* sont créés sur la machine. Si les paramètres d'autorisation ne permettent pas la création d'un utilisateur local et nécessitent plutôt Active Directory, un utilisateur avec le nom d'utilisateur *cssys* doit être créé sur le serveur Active Directory.
- Vous pouvez en savoir plus sur la sécurité de Data Infrastructure Insights"ici" .

Meilleures pratiques

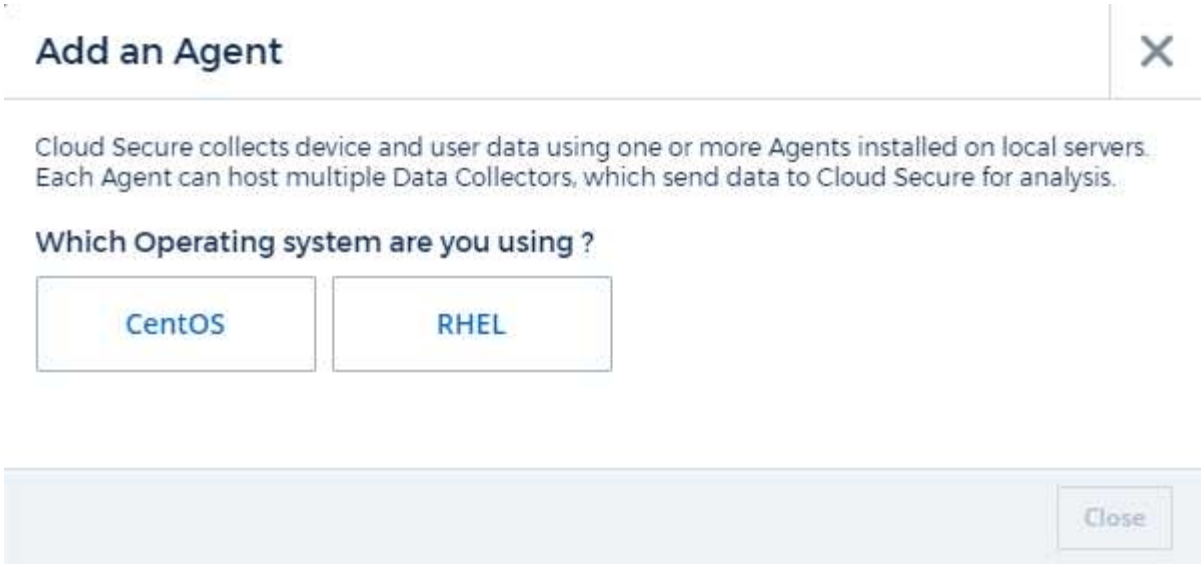
Gardez les points suivants à l'esprit avant de configurer votre agent Workload Security.

Pause et reprise	Pause : Supprime les politiques fpolicies d' ONTAP. Généralement utilisé lorsque les clients effectuent des opérations de maintenance prolongées pouvant prendre beaucoup de temps, comme le redémarrage des machines virtuelles d'agents ou le remplacement du stockage. Résumé : Ajoute à nouveau fpolicies à ONTAP.
Épingler et désépingler	Unpin récupère immédiatement la dernière version (si disponible) et met à jour l'agent et le collecteur. Durant cette mise à niveau, fpolicies se déconnectera puis se reconnectera. Cette fonctionnalité est conçue pour les clients qui souhaitent contrôler le calendrier des mises à jour automatiques. Voir ci-dessous pourInstructions pour épingler/déépingler .
Approche recommandée	Pour les configurations importantes, il est conseillé d'utiliser Pin et Unpin plutôt que de mettre en pause les collecteurs. Il n'est pas nécessaire de faire une pause et de reprendre pendant l'utilisation de l'épinglage et du désépinglage. Les clients peuvent conserver leurs agents et collecteurs épinglés et, dès réception d'une notification par e-mail concernant une nouvelle version, disposent d'un délai de 30 jours pour mettre à jour sélectivement leurs agents un par un. Cette approche minimise l'impact de la latence sur les politiques fpolicies et offre un meilleur contrôle sur le processus de mise à niveau.

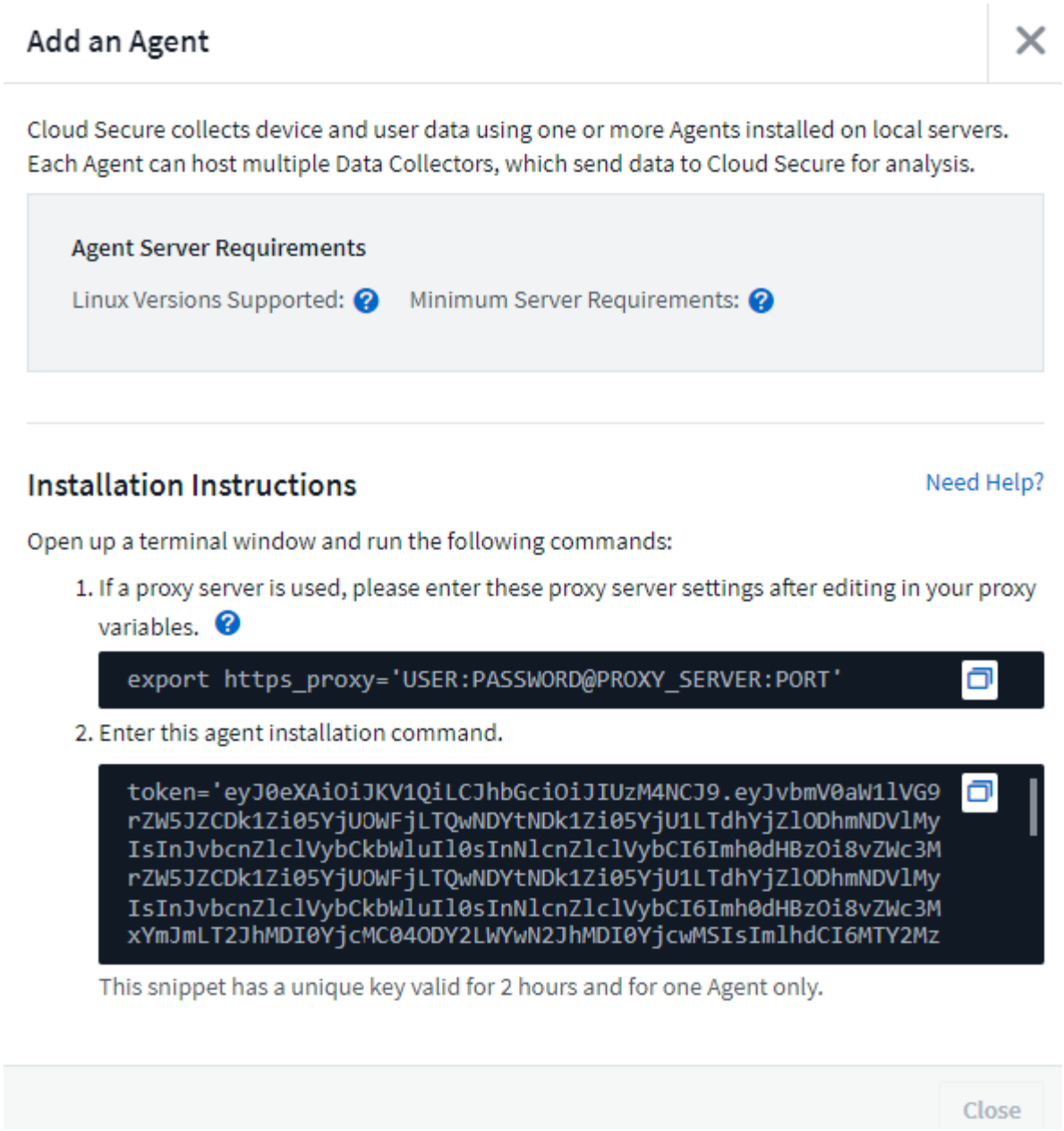
Étapes pour installer l'agent

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Workload Security.
2. Sélectionnez **Collecteurs > Agents > +Agent**

   Le système affiche la page Ajouter un agent :



3. Vérifiez que le serveur d'agent répond à la configuration système minimale requise.
4. Pour vérifier que le serveur d'agent exécute une version prise en charge de Linux, cliquez sur *Versions prises en charge (i)*.
5. Si votre réseau utilise un serveur proxy, veuillez définir les détails du serveur proxy en suivant les instructions de la section Proxy.



6. Cliquez sur l'icône Copier dans le presse-papiers pour copier la commande d'installation.
7. Exécutez la commande d'installation dans une fenêtre de terminal.
8. Le système affiche le message suivant lorsque l'installation se termine avec succès :

Après avoir terminé

1. Vous devez configurer un"Collecteur d'annuaires utilisateurs" .
2. Vous devez configurer un ou plusieurs collecteurs de données.

Configuration du réseau

Exécutez les commandes suivantes sur le système local pour ouvrir les ports qui seront utilisés par Workload Security. S'il existe un problème de sécurité concernant la plage de ports, vous pouvez utiliser une plage de ports plus petite, par exemple *35000:35100*. Chaque SVM utilise deux ports.

Étapes

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Suivez les étapes suivantes en fonction de votre plateforme :

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Exemple de sortie :

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`(pour CentOS 8)

Exemple de sortie :

```
35000-55000/tcp
```

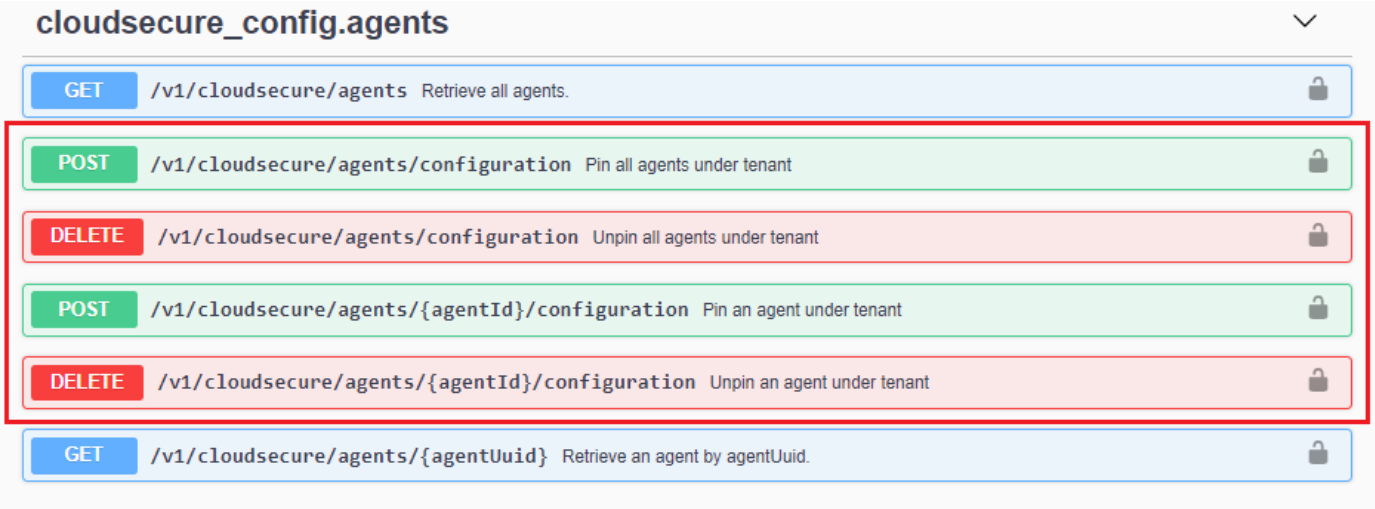
« Épingler » un agent sur la version actuelle

Par défaut, Data Infrastructure Insights Workload Security met à jour automatiquement les agents. Certains clients peuvent souhaiter suspendre la mise à jour automatique, ce qui laisse un agent à sa version actuelle jusqu'à ce que l'un des événements suivants se produise :

- Le client reprend les mises à jour automatiques de l'agent.
- 30 jours sont passés. Notez que les 30 jours commencent le jour de la mise à jour la plus récente de l'agent, et non le jour où l'agent est mis en pause.

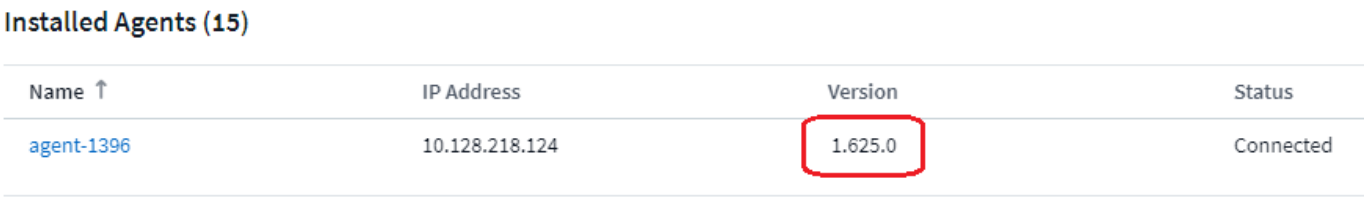
Dans chacun de ces cas, l'agent sera mis à jour lors de la prochaine actualisation de Workload Security.

Pour suspendre ou reprendre les mises à jour automatiques des agents, utilisez les API *cloudsecure_config.agents* :



Notez que l'action de pause ou de reprise peut prendre jusqu'à cinq minutes pour prendre effet.

Vous pouvez afficher vos versions d'agent actuelles sur la page **Sécurité de la charge de travail > Collecteurs**, dans l'onglet **Agents**.



Dépannage des erreurs de l'agent

Les problèmes connus et leurs résolutions sont décrits dans le tableau suivant.

Problème:	Résolution:
L'installation de l'agent ne parvient pas à créer le dossier /opt/netapp/cloudsecure/agent/logs/agent.log et le fichier install.log ne fournit aucune information pertinente.	Cette erreur se produit lors de l'amorçage de l'agent. L'erreur n'est pas enregistrée dans les fichiers journaux car elle se produit avant l'initialisation de l'enregistreur. L'erreur est redirigée vers la sortie standard et est visible dans le journal de service à l'aide de l' `journalctl -u cloudsecure-agent.service` commande. Cette commande peut être utilisée pour résoudre le problème plus en détail. est
L'installation de l'agent échoue avec le message « Cette distribution Linux n'est pas prise en charge. Sortie de l'installation'.	Cette erreur apparaît lorsque vous tentez d'installer l'agent sur un système non pris en charge. Voir "Exigences relatives aux agents" .
L'installation de l'agent a échoué avec l'erreur : « -bash : unzip : commande introuvable »	Installez, décompressez, puis exécutez à nouveau la commande d'installation. Si Yum est installé sur la machine, essayez « yum install unzip » pour installer le logiciel de décompression. Après cela, recopiez la commande depuis l'interface utilisateur d'installation de l'agent et collez-la dans l'interface de ligne de commande pour exécuter à nouveau l'installation.

Problème:	Résolution:

L'agent a été installé et était en cours d'exécution. Cependant, l'agent s'est arrêté soudainement.	Connectez-vous en SSH à la machine de l'agent. Vérifiez l'état du service de l'agent via `sudo systemctl status cloudsecure-agent.service` . 1. Vérifiez si les journaux affichent un message « Échec du démarrage du service démon Workload Security ». 2. Vérifiez si l'utilisateur cssys existe ou non dans la machine Agent. Exécutez les commandes suivantes une par une avec l'autorisation root et vérifiez si l'utilisateur et le groupe cssys existent.
	`sudo id cssys`
	`sudo groups cssys` 3. S'il n'en existe aucun, une politique de surveillance centralisée peut avoir supprimé l'utilisateur cssys. 4. Créez l'utilisateur et le groupe cssys manuellement en exécutant les commandes suivantes.
	`sudo useradd cssys`
	`sudo groupadd cssys` 5. Redémarrez ensuite le service de l'agent en exécutant la commande suivante :
	`sudo systemctl restart cloudsecure-agent.service` 6. Si le problème persiste, veuillez vérifier les autres options de dépannage.

Impossible d'ajouter plus de 50 collecteurs de données à un agent.	Seuls 50 collecteurs de données peuvent être ajoutés à un agent. Il peut s'agir d'une combinaison de tous les types de collecteurs, par exemple, Active Directory, SVM et d'autres collecteurs.
L'interface utilisateur indique que l'agent est dans l'état NOT_CONNECTED.	Étapes pour redémarrer l'agent. 1. Connectez-vous en SSH à la machine de l'agent. 2. Redémarrez ensuite le service de l'agent en exécutant la commande suivante : `sudo systemctl restart cloudsecure-agent.service` 3. Vérifiez l'état du service de l'agent via `sudo systemctl status cloudsecure-agent.service` . 4. L'agent doit passer à l'état CONNECTÉ.
L'agent VM est derrière le proxy Zscaler et l'installation de l'agent échoue. En raison de l'inspection SSL du proxy Zscaler, les certificats de sécurité de la charge de travail sont présentés comme s'ils étaient signés par Zscaler CA, de sorte que l'agent ne fait pas confiance à la communication.	Désactivez l'inspection SSL dans le proxy Zscaler pour l'URL *.cloudinsights.netapp.com. Si Zscaler effectue une inspection SSL et remplace les certificats, Workload Security ne fonctionnera pas.

Problème:	Résolution:
Lors de l'installation de l'agent, l'installation se bloque après la décompression.	La commande « chmod 755 -Rf » échoue. La commande échoue lorsque la commande d'installation de l'agent est exécutée par un utilisateur sudo non root qui possède des fichiers dans le répertoire de travail, appartenant à un autre utilisateur, et les autorisations de ces fichiers ne peuvent pas être modifiées. En raison de l'échec de la commande chmod, le reste de l'installation ne s'exécute pas. 1. Créez un nouveau répertoire nommé « cloudsecure ». 2. Allez dans ce répertoire. 3. Copiez et collez la commande d'installation complète « token=…… … ./cloudsecure-agent-install.sh » et appuyez sur Entrée. 4. L'installation devrait pouvoir se poursuivre.
Si l'agent ne parvient toujours pas à se connecter à Saas, veuillez ouvrir un dossier auprès du support NetApp . Fournissez le numéro de série Data Infrastructure Insights pour ouvrir un dossier et joignez les journaux au dossier comme indiqué.	Pour joindre des journaux au dossier : 1. Exécutez le script suivant avec l'autorisation root et partagez le fichier de sortie (cloudsecure-agent-symptoms.zip). a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Exécutez les commandes suivantes une par une avec l'autorisation root et partagez la sortie. a. id cssys b. groups cssys c. cat /etc/os-release
Le script cloudsecure-agent-symptom-collector.sh échoue avec l'erreur suivante. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Collecte du journal de service Collecte des journaux d'application Collecte des configurations d'agent Prise d'un instantané de l'état du service Prise d'un instantané de la structure du répertoire de l'agent ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh : ligne 52 : zip : commande introuvable ERREUR : Échec de la création de /tmp/cloudsecure-agent-symptoms.zip	L'outil Zip n'est pas installé. Installez l'outil zip en exécutant la commande « yum install zip ». Exécutez ensuite à nouveau cloudsecure-agent-symptom-collector.sh.
L'installation de l'agent échoue avec useradd : impossible de créer le répertoire /home/cssys	Cette erreur peut se produire si le répertoire de connexion de l'utilisateur ne peut pas être créé sous /home, en raison d'un manque d'autorisations. La solution de contournement serait de créer un utilisateur cssys et d'ajouter son répertoire de connexion manuellement à l'aide de la commande suivante : *sudo useradd user_name -m -d HOME_DIR* -m : Créez le répertoire personnel de l'utilisateur s'il n'existe pas. -d : Le nouvel utilisateur est créé en utilisant HOME_DIR comme valeur pour le répertoire de connexion de l'utilisateur. Par exemple, *sudo useradd cssys -m -d /cssys*, ajoute un utilisateur *cssys* et crée son répertoire de connexion sous root.

Problème:	Résolution:
L'agent ne s'exécute pas après l'installation. *Systemctl status cloudsecure-agent.service* affiche ce qui suit : [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled) Active: activation (redémarrage automatique) (Result: exit-code) since Tue 2021-08-03 21:12:26 PDT; Il y a 2 s Processus : 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (code=exited status=126) PID principal : 25889 (code=exited, status=126), 03 août 21:12:26 démo systemd[1] : cloudsecure-agent.service : processus principal terminé, code=exited, status=126/n/a 03 août 21:12:26 démo systemd[1] : l'unité cloudsecure-agent.service est entrée en état d'échec. 03 août 21:12:26 démo systemd[1] : cloudsecure-agent.service a échoué.	Cela peut échouer car l'utilisateur *cssys* n'a peut-être pas l'autorisation d'installer. Si /opt/netapp est un montage NFS et si l'utilisateur *cssys* n'a pas accès à ce dossier, l'installation échouera. *cssys* est un utilisateur local créé par le programme d'installation de Workload Security qui n'est peut-être pas autorisé à accéder au partage monté. Vous pouvez le vérifier en essayant d'accéder à /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent en utilisant l'utilisateur *cssys*. Si le message « Autorisation refusée » est renvoyé, l'autorisation d'installation n'est pas présente. Au lieu d'un dossier monté, installez-le dans un répertoire local sur la machine.
L'agent a été initialement connecté via un serveur proxy et le proxy a été défini lors de l'installation de l'agent. Le serveur proxy a maintenant changé. Comment la configuration du proxy de l'agent peut-elle être modifiée ?	Vous pouvez modifier le fichier agent.properties pour ajouter les détails du proxy. Suivez ces étapes : 1. Accédez au dossier contenant le fichier de propriétés : cd /opt/netapp/cloudsecure/conf 2. À l'aide de votre éditeur de texte préféré, ouvrez le fichier *agent.properties* pour le modifier. 3. Ajoutez ou modifiez les lignes suivantes : AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Enregistrez le fichier. 5. Redémarrez l'agent : sudo systemctl restart cloudsecure-agent.service

Suppression d'un agent de sécurité de charge de travail

Lorsque vous supprimez un agent Workload Security, tous les collecteurs de données associés à l'agent doivent d'abord être supprimés.

Suppression d'un agent

> La suppression d'un agent supprime tous les collecteurs de données associés à l'agent. Si vous prévoyez de configurer les collecteurs de données avec un agent différent, vous devez créer une sauvegarde des configurations du collecteur de données avant de supprimer l'agent.

Avant de commencer

1. Assurez-vous que tous les collecteurs de données associés à l'agent sont supprimés du portail Workload Security.

   Remarque : ignorez cette étape si tous les collecteurs associés sont à l'état ARRÊTÉ.

Étapes pour supprimer un agent :

1. Connectez-vous à la machine virtuelle de l'agent via SSH et exécutez la commande suivante. Lorsque vous y êtes invité, entrez « y » pour continuer.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Cliquez sur **Sécurité de la charge de travail > Collecteurs > Agents**

   Le système affiche la liste des agents configurés.

3. Cliquez sur le menu d'options de l'agent que vous supprimez.
4. Cliquez sur **Supprimer**.

   Le système affiche la page **Supprimer l'agent**.

5. Cliquez sur **Supprimer** pour confirmer la suppression.

Configuration d'un collecteur d'annuaires utilisateurs Active Directory (AD)

Workload Security peut être configuré pour collecter les attributs utilisateur à partir des serveurs Active Directory.

Avant de commencer

- Vous devez être administrateur ou propriétaire de compte Data Infrastructure Insights pour effectuer cette tâche.
- Vous devez disposer de l'adresse IP du serveur hébergeant le serveur Active Directory.
- Un agent doit être configuré avant de configurer un connecteur d'annuaire utilisateur.

Étapes pour configurer un collecteur d'annuaires utilisateurs

1. Dans le menu Sécurité de la charge de travail, cliquez sur : **Collecteurs > Collecteurs d'annuaires utilisateurs > + Collecteur d'annuaires utilisateurs** et sélectionnez **Active Directory**

   Le système affiche l'écran Ajouter un répertoire d'utilisateurs.

Configurez le collecteur d'annuaires utilisateurs en saisissant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique pour le répertoire utilisateur. Par exemple *GlobalADCollector*
Agent	Sélectionnez un agent configuré dans la liste
IP du serveur/nom de domaine	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant l'annuaire actif

Nom de la forêt	Niveau de forêt de la structure du répertoire. Le nom de forêt autorise les deux formats suivants : *x.y.z* ⇒ nom de domaine direct tel que vous l'avez sur votre SVM. [Exemple : hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Noms distinctifs relatifs [Exemple : DC=hq,DC= companyname,DC=com] Ou vous pouvez spécifier comme suit : *OU=engineering,DC=hq,DC= companyname,DC=com* [pour filtrer par UO spécifique engineering] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [pour obtenir uniquement l'utilisateur spécifique avec <username> de l'UO <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [pour obtenir tous les utilisateurs Acrobat au sein des utilisateurs de cette organisation] Les domaines Active Directory approuvés sont également pris en charge.
Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : *username@companyname.com* ou *username@domainname.com*. De plus, l'autorisation de lecture seule du domaine est requise. L'utilisateur doit être membre du groupe de sécurité *Contrôleurs de domaine en lecture seule*.
Mot de passe BIND	Mot de passe du serveur d'annuaire (c'est-à-dire le mot de passe du nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionner le port

Saisissez les attributs requis du serveur d'annuaire suivants si les noms d'attributs par défaut ont été modifiés dans Active Directory. Le plus souvent, ces noms d'attributs ne sont pas modifiés dans Active Directory, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans Directory Server
Nom d'affichage	nom
SID	objectid
Nom d'utilisateur	sAMAccountName

Cliquez sur Inclure les attributs facultatifs pour ajouter l'un des attributs suivants :

Attributs	Nom d'attribut dans le serveur d'annuaire
Adresse email	mail
Numéro de téléphone	numéro de téléphone
Rôle	titre

Pays	co
État	État
Département	département
Photo	vignettephoto
GestionnaireDN	directeur
Groupes	membreDe

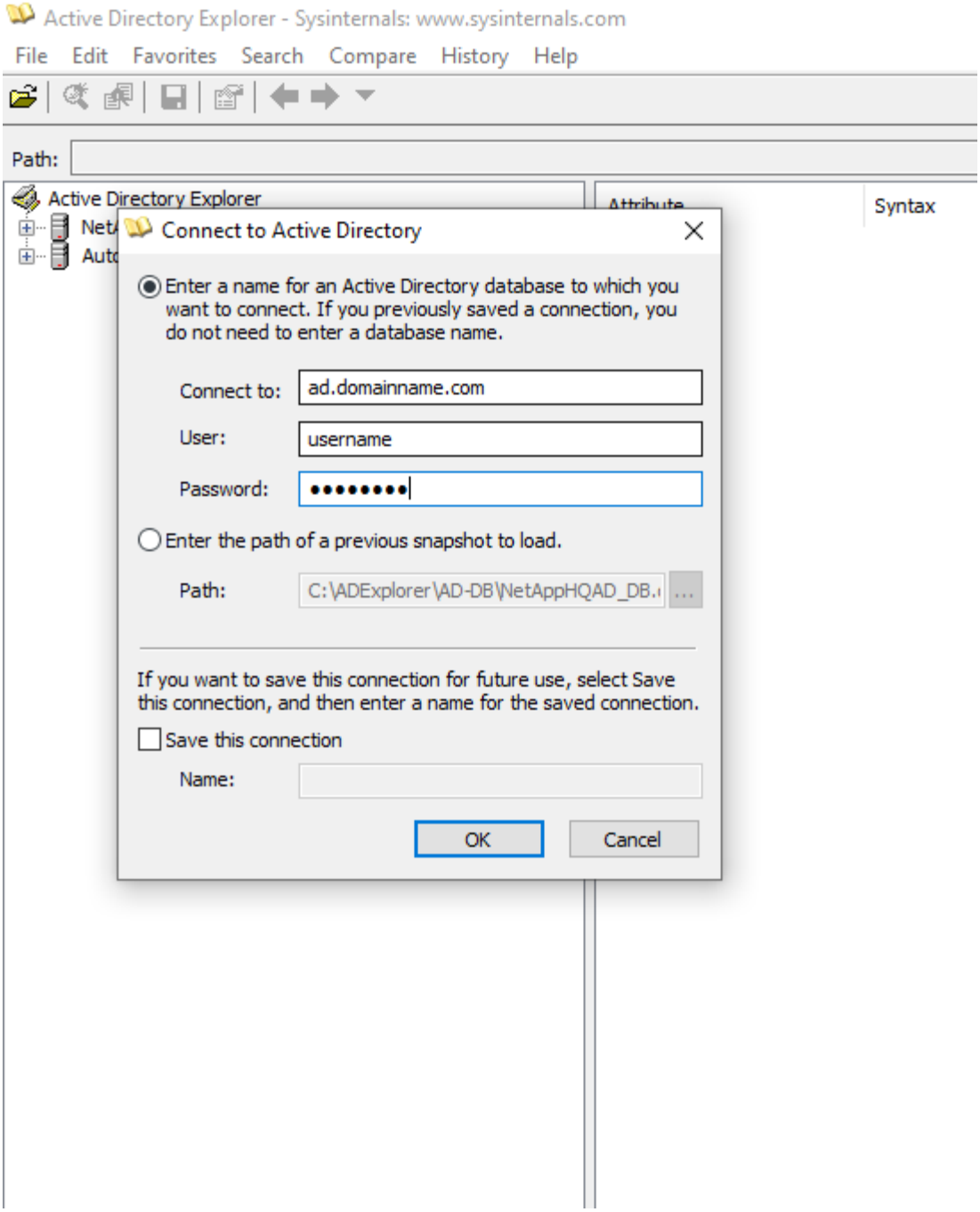
Test de la configuration de votre collecteur d'annuaires utilisateurs

Vous pouvez valider les autorisations utilisateur et les définitions d'attributs LDAP à l'aide des procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation de l'utilisateur LDAP de Workload Security :

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Utilisez AD Explorer pour parcourir une base de données AD, afficher les propriétés et les attributs des objets, afficher les autorisations, afficher le schéma d'un objet, exécuter des recherches sophistiquées que vous pouvez enregistrer et réexécuter.
  - Installer"Explorateur AD" sur n'importe quelle machine Windows pouvant se connecter au serveur AD.
  - Connectez-vous au serveur AD à l'aide du nom d'utilisateur/mot de passe du serveur d'annuaire AD.



Dépannage des erreurs de configuration du collecteur d'annuaires utilisateurs

Le tableau suivant décrit les problèmes connus et les résolutions qui peuvent survenir lors de la configuration du collecteur :

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Informations d'identification non valides fournies pour le serveur LDAP ».	Nom d'utilisateur ou mot de passe incorrect fourni. Modifiez et fournissez le nom d'utilisateur et le mot de passe corrects.

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Impossible d'obtenir l'objet correspondant à DN=DC=hq,DC=domainname,DC=com fourni comme nom de forêt. »	Nom de forêt incorrect fourni. Modifiez et fournissez le nom de forêt correct.
Les attributs facultatifs de l'utilisateur de domaine n'apparaissent pas dans la page Profil utilisateur de Workload Security.	Cela est probablement dû à une incompatibilité entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Modifiez et fournissez le(s) nom(s) d'attribut facultatif(s) correct(s).
Collecteur de données dans un état d'erreur avec « Échec de la récupération des utilisateurs LDAP ». Motif de l'échec : Impossible de se connecter au serveur, la connexion est nulle.	Redémarrez le collecteur en cliquant sur le bouton *Redémarrer*.
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ».	Assurez-vous d'avoir fourni des valeurs valides pour les champs obligatoires (serveur, nom de forêt, DN de liaison, mot de passe de liaison). Assurez-vous que l'entrée bind-DN est toujours fournie sous la forme « Administrateur@<domain_forest_name> » ou sous la forme d'un compte utilisateur avec des privilèges d'administrateur de domaine.
L'ajout d'un connecteur d'annuaire utilisateur entraîne l'état « RÉESSAI ». Affiche l'erreur « Impossible de définir l'état du collecteur, raison pour laquelle la commande TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] a échoué en raison de java.net.ConnectionException : connexion refusée. »	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le FQDN correct.
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Échec de l'établissement de la connexion LDAP ».	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le FQDN correct.
L'ajout d'un connecteur d'annuaire utilisateur génère l'état « Erreur ». L'erreur indique : « Échec du chargement des paramètres. Motif : la configuration de la source de données comporte une erreur. Raison spécifique : /connector/conf/application.conf : 70 : ldap.ldap-port est de type STRING plutôt que NUMBER »	Valeur incorrecte pour le port fourni. Essayez d'utiliser les valeurs de port par défaut ou le numéro de port correct pour le serveur AD.
J'ai commencé avec les attributs obligatoires, et cela a fonctionné. Après avoir ajouté les attributs facultatifs, les données des attributs facultatifs ne sont pas récupérées à partir d'AD.	Cela est probablement dû à une incompatibilité entre les attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Modifiez et fournissez le nom d'attribut obligatoire ou facultatif correct.

Problème:	Résolution:
Après le redémarrage du collecteur, quand la synchronisation AD aura-t-elle lieu ?	La synchronisation AD se produira immédiatement après le redémarrage du collecteur. Il faudra environ 15 minutes pour récupérer les données utilisateur d'environ 300 000 utilisateurs, et elles sont actualisées automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées d'AD vers CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas de non actualisation. Si le locataire est supprimé, les données seront supprimées.
Le connecteur d'annuaire utilisateur génère l'état « Erreur ». "Le connecteur est en état d'erreur. Nom du service : usersLdap. Motif de l'échec : échec de la récupération des utilisateurs LDAP. Motif de l'échec : 80090308 : LdapErr : DSID-0C090453, commentaire : erreur AcceptSecurityContext, données 52e, v3839	Nom de forêt incorrect fourni. Voir ci-dessus comment fournir le nom de forêt correct.
Le numéro de téléphone n'est pas renseigné dans la page de profil utilisateur.	Cela est probablement dû à un problème de mappage d'attributs avec Active Directory. 1. Modifiez le collecteur Active Directory particulier qui récupère les informations de l'utilisateur à partir d'Active Directory. 2. Notez que sous les attributs facultatifs, il existe un nom de champ « Numéro de téléphone » mappé à l'attribut Active Directory « telephonenumber ». 4. Maintenant, utilisez l'outil Active Directory Explorer comme décrit ci-dessus pour parcourir Active Directory et voir le nom d'attribut correct. 3. Assurez-vous que dans Active Directory, il existe un attribut nommé « telephonenumber » qui contient bien le numéro de téléphone de l'utilisateur. 5. Disons que dans Active Directory, il a été modifié en « numéro de téléphone ». 6. Modifiez ensuite le collecteur d'annuaires utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacez « telephonenumber » par « phonenumber ». 7. Enregistrez le collecteur Active Directory, le collecteur redémarrera et récupérera le numéro de téléphone de l'utilisateur et l'affichera dans la page de profil utilisateur.
Si le certificat de chiffrement (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaires d'utilisateurs Workload Security ne peut pas se connecter au serveur AD.	Désactivez le chiffrement du serveur AD avant de configurer un collecteur d'annuaires utilisateurs. Une fois les détails de l'utilisateur récupérés, ils resteront là pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les utilisateurs nouvellement ajoutés dans AD ne seront pas récupérés. Pour effectuer une nouvelle récupération, le collecteur d'annuaires utilisateurs doit être connecté à AD.
Les données d'Active Directory sont présentes dans CloudInsights Security. Vous souhaitez supprimer toutes les informations utilisateur de CloudInsights.	Il n'est pas possible de supprimer UNIQUEMENT les informations utilisateur Active Directory de CloudInsights Security. Afin de supprimer l'utilisateur, le locataire complet doit être supprimé.

Configuration d’un collecteur de serveur d’annuaire LDAP

Vous configurez Workload Security pour collecter les attributs utilisateur à partir des serveurs d’annuaire LDAP.

Avant de commencer

- Vous devez être administrateur ou propriétaire de compte Data Infrastructure Insights pour effectuer cette tâche.
- Vous devez disposer de l’adresse IP du serveur hébergeant le serveur d’annuaire LDAP.
- Un agent doit être configuré avant de configurer un connecteur d’annuaire LDAP.

Étapes pour configurer un collecteur d’annuaires utilisateurs

1. Dans le menu Sécurité de la charge de travail, cliquez sur : **Collecteurs > Collecteurs d’annuaires utilisateurs > + Collecteur d’annuaires utilisateurs** et sélectionnez **Serveur d’annuaire LDAP**

   Le système affiche l’écran Ajouter un répertoire d’utilisateurs.

Configurez le collecteur d’annuaires utilisateurs en saisissant les données requises dans les tableaux suivants :

Nom	Description
Nom	Nom unique pour le répertoire utilisateur. Par exemple *GlobalLDAPCollector*
Agent	Sélectionnez un agent configuré dans la liste
IP du serveur/nom de domaine	Adresse IP ou nom de domaine complet (FQDN) du serveur hébergeant le serveur d’annuaire LDAP
Base de recherche	Base de recherche du serveur LDAP Search Base autorise les deux formats suivants : *x.y.z* ⇒ nom de domaine direct tel que vous l’avez sur votre SVM. [Exemple : hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Noms distinctifs relatifs [Exemple : DC=hq,DC= companyname,DC=com] Ou vous pouvez spécifier comme suit : *OU=engineering,DC=hq,DC= companyname,DC=com* [pour filtrer par UO spécifique engineering] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [pour obtenir uniquement l’utilisateur spécifique avec <username> de l’UO <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [pour obtenir tous les utilisateurs Acrobat au sein des utilisateurs de cette organisation]

Lier DN	L'utilisateur est autorisé à rechercher dans le répertoire. Par exemple : uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com pour un utilisateur john@dorp.company.com. dorp.company.com
--comptes	--utilisateurs
--John	--Anna
Mot de passe BIND	Mot de passe du serveur d'annuaire (c'est-à-dire le mot de passe du nom d'utilisateur utilisé dans Bind DN)
Protocole	ldap, ldaps, ldap-start-tls
Ports	Sélectionner le port

Saisissez les attributs requis du serveur d'annuaire suivants si les noms d'attributs par défaut ont été modifiés dans le serveur d'annuaire LDAP. Le plus souvent, ces noms d'attributs ne sont pas modifiés dans le serveur d'annuaire LDAP, auquel cas vous pouvez simplement continuer avec le nom d'attribut par défaut.

Attributs	Nom d'attribut dans Directory Server
Nom d'affichage	nom
UNIXID	numéro d'identifiant utilisateur
Nom d'utilisateur	uid

Cliquez sur Inclure les attributs facultatifs pour ajouter l'un des attributs suivants :

Attributs	Nom d'attribut dans le serveur d'annuaire
Adresse email	mail
Numéro de téléphone	numéro de téléphone
Rôle	titre
Pays	co
État	État
Département	numéro de département
Photo	photo
GestionnaireDN	directeur
Groupes	membreDe

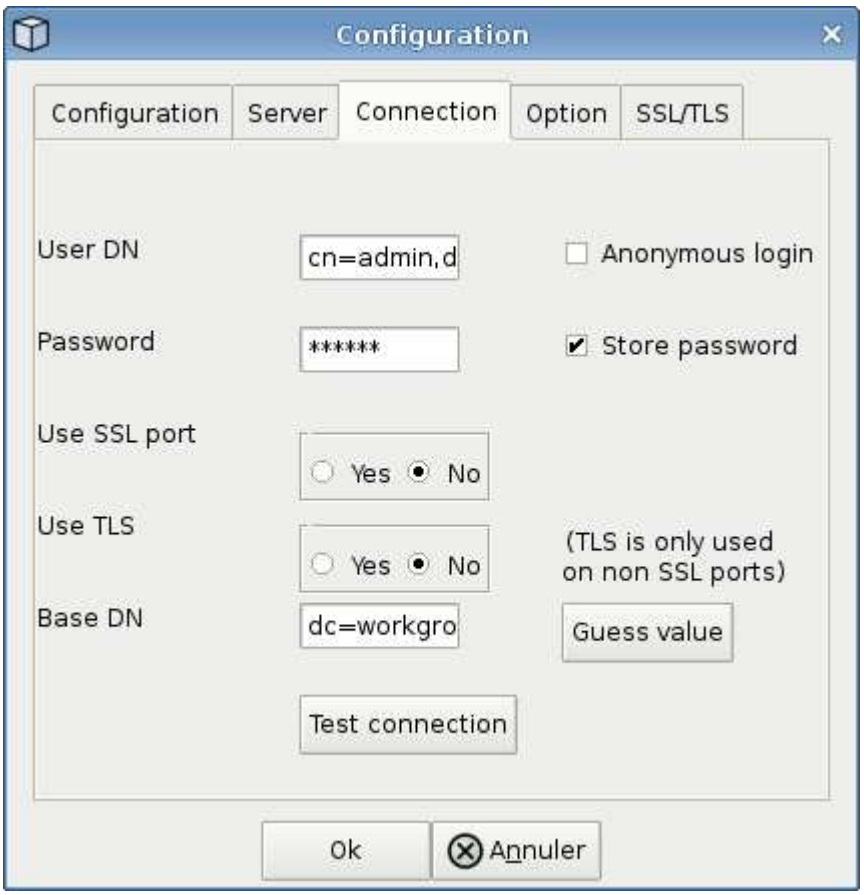
Test de la configuration de votre collecteur d'annuaires utilisateurs

Vous pouvez valider les autorisations utilisateur et les définitions d'attributs LDAP à l'aide des procédures suivantes :

- Utilisez la commande suivante pour valider l'autorisation de l'utilisateur LDAP de Workload Security :

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilisez LDAP Explorer pour naviguer dans une base de données LDAP,
afficher les propriétés et les attributs des objets, afficher les
autorisations, afficher le schéma d'un objet, exécuter des recherches
sophistiquées que vous pouvez enregistrer et réexécuter.
```

- Installer LDAP Explorer(http://ldaptool.sourceforge.net/) ou Java LDAP Explorer(http://jxplorer.org/) sur n'importe quelle machine Windows pouvant se connecter au serveur LDAP.
- Connectez-vous au serveur LDAP en utilisant le nom d'utilisateur/mot de passe du serveur d'annuaire LDAP.



Dépannage des erreurs de configuration du collecteur d'annuaires LDAP

Le tableau suivant décrit les problèmes connus et les résolutions qui peuvent survenir lors de la configuration du collecteur :

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Informations d'identification non valides fournies pour le serveur LDAP ».	Nom unique de liaison, mot de passe de liaison ou base de recherche incorrects fournis. Modifiez et fournissez les informations correctes.
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Impossible d'obtenir l'objet correspondant à DN=DC=hq,DC=domainname,DC=com fourni comme nom de forêt. »	Base de recherche incorrecte fournie. Modifiez et fournissez le nom de forêt correct.
Les attributs facultatifs de l'utilisateur de domaine n'apparaissent pas dans la page Profil utilisateur de Workload Security.	Cela est probablement dû à une incompatibilité entre les noms des attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Les champs sont sensibles à la casse. Modifiez et fournissez le(s) nom(s) d'attribut facultatif(s) correct(s).
Collecteur de données dans un état d'erreur avec « Échec de la récupération des utilisateurs LDAP ». Motif de l'échec : Impossible de se connecter au serveur, la connexion est nulle.	Redémarrez le collecteur en cliquant sur le bouton *Redémarrer*.
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ».	Assurez-vous d'avoir fourni des valeurs valides pour les champs obligatoires (serveur, nom de forêt, DN de liaison, mot de passe de liaison). Assurez-vous que l'entrée bind-DN est toujours fournie sous la forme uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état « RETRYING ». Affiche l'erreur « Échec de la détermination de l'état du collecteur, réessayez donc »	Assurez-vous que l'adresse IP du serveur et la base de recherche correctes sont fournies ////
Lors de l'ajout d'un annuaire LDAP, l'erreur suivante s'affiche : « Échec de la détermination de l'état du collecteur après 2 tentatives. Veuillez redémarrer le collecteur (code d'erreur : AGENT008) »	Assurez-vous que l'adresse IP du serveur et la base de recherche correctes sont fournies
L'ajout d'un connecteur d'annuaire LDAP entraîne l'état « RETRYING ». Affiche l'erreur « Impossible de définir l'état du collecteur, raison pour laquelle la commande TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] a échoué en raison de java.net.ConnectionException : connexion refusée. »	IP ou FQDN incorrect fourni pour le serveur AD. Modifiez et fournissez l'adresse IP ou le FQDN correct. ////
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Échec de l'établissement de la connexion LDAP ».	IP ou FQDN incorrect fourni pour le serveur LDAP. Modifiez et fournissez l'adresse IP ou le FQDN correct. Ou valeur incorrecte pour le port fourni. Essayez d'utiliser les valeurs de port par défaut ou le numéro de port correct pour le serveur LDAP.

Problème:	Résolution:
L'ajout d'un connecteur d'annuaire LDAP génère l'état « Erreur ». L'erreur indique : « Échec du chargement des paramètres. Motif : la configuration de la source de données comporte une erreur. Raison spécifique : /connector/conf/application.conf : 70 : ldap.ldap-port est de type STRING plutôt que NUMBER »	Valeur incorrecte pour le port fourni. Essayez d'utiliser les valeurs de port par défaut ou le numéro de port correct pour le serveur AD.
J'ai commencé avec les attributs obligatoires, et cela a fonctionné. Après avoir ajouté les attributs facultatifs, les données des attributs facultatifs ne sont pas récupérées à partir d'AD.	Cela est probablement dû à une incompatibilité entre les attributs facultatifs ajoutés dans CloudSecure et les noms d'attributs réels dans Active Directory. Modifiez et fournissez le nom d'attribut obligatoire ou facultatif correct.
Après le redémarrage du collecteur, quand la synchronisation LDAP aura-t-elle lieu ?	La synchronisation LDAP se produira immédiatement après le redémarrage du collecteur. Il faudra environ 15 minutes pour récupérer les données utilisateur d'environ 300 000 utilisateurs, et elles sont actualisées automatiquement toutes les 12 heures.
Les données utilisateur sont synchronisées depuis LDAP vers CloudSecure. Quand les données seront-elles supprimées ?	Les données utilisateur sont conservées pendant 13 mois en cas de non actualisation. Si le locataire est supprimé, les données seront supprimées.
Le connecteur d'annuaire LDAP génère l'état « Erreur ». "Le connecteur est en état d'erreur. Nom du service : usersLdap. Motif de l'échec : échec de la récupération des utilisateurs LDAP. Motif de l'échec : 80090308 : LdapErr : DSID-0C090453, commentaire : erreur AcceptSecurityContext, données 52e, v3839	Nom de forêt incorrect fourni. Voir ci-dessus comment fournir le nom de forêt correct.
Le numéro de téléphone n'est pas renseigné dans la page de profil utilisateur.	Cela est probablement dû à un problème de mappage d'attributs avec Active Directory. 1. Modifiez le collecteur Active Directory particulier qui récupère les informations de l'utilisateur à partir d'Active Directory. 2. Notez que sous les attributs facultatifs, il existe un nom de champ « Numéro de téléphone » mappé à l'attribut Active Directory « telephonenumber ». 4. Maintenant, utilisez l'outil Active Directory Explorer comme décrit ci-dessus pour parcourir le serveur d'annuaire LDAP et voir le nom d'attribut correct. 3. Assurez-vous que dans l'annuaire LDAP, il existe un attribut nommé « telephonenumber » qui contient bien le numéro de téléphone de l'utilisateur. 5. Disons que dans l'annuaire LDAP, il a été modifié en « numéro de téléphone ». 6. Modifiez ensuite le collecteur d'annuaires utilisateurs CloudSecure. Dans la section des attributs facultatifs, remplacez « telephonenumber » par « phonenumber ». 7. Enregistrez le collecteur Active Directory, le collecteur redémarrera et récupérera le numéro de téléphone de l'utilisateur et l'affichera dans la page de profil utilisateur.

Problème:	Résolution:
Si le certificat de chiffrement (SSL) est activé sur le serveur Active Directory (AD), le collecteur d'annuaires d'utilisateurs Workload Security ne peut pas se connecter au serveur AD.	Désactivez le chiffrement du serveur AD avant de configurer un collecteur d'annuaires utilisateurs. Une fois les détails de l'utilisateur récupérés, ils resteront là pendant 13 mois. Si le serveur AD est déconnecté après avoir récupéré les détails de l'utilisateur, les utilisateurs nouvellement ajoutés dans AD ne seront pas récupérés. Pour récupérer à nouveau, le collecteur de répertoires utilisateurs doit être connecté à AD.

Configuration du collecteur de données ONTAP SVM

Le collecteur de données ONTAP SVM permet à Workload Security de surveiller les activités d'accès aux fichiers et aux utilisateurs sur les machines virtuelles de stockage NetApp ONTAP (SVM). Ce guide vous guide à travers la configuration et la gestion du collecteur de données SVM pour fournir une surveillance de sécurité complète de votre environnement ONTAP .

Avant de commencer

- Ce collecteur de données est pris en charge avec les éléments suivants :
  - Data ONTAP 9.2 et versions ultérieures. Pour de meilleures performances, utilisez une version Data ONTAP supérieure à 9.13.1.
  - Protocole SMB version 3.1 et antérieure.
  - Versions NFS jusqu'à NFS 4.1 inclus (notez que NFS 4.1 est pris en charge avec ONTAP 9.15 ou version ultérieure).
  - Flexgroup est pris en charge à partir d' ONTAP 9.4 et des versions ultérieures
  - FlexCache est pris en charge pour NFS avec ONTAP 9.7 et les versions ultérieures.
  - FlexCache est pris en charge pour SMB avec ONTAP 9.14.1 et les versions ultérieures.
  - ONTAP Select est pris en charge
- Seuls les types de données SVM sont pris en charge. Les SVM avec des volumes infinis ne sont pas pris en charge.
- SVM comporte plusieurs sous-types. Parmi ceux-ci, seuls *default*, *sync_source* et *sync_destination* sont pris en charge.
- Un agent"doit être configuré" avant de pouvoir configurer les collecteurs de données.
- Assurez-vous que vous disposez d'un connecteur d'annuaire utilisateur correctement configuré, sinon les événements afficheront les noms d'utilisateur codés et non le nom réel de l'utilisateur (tel que stocké dans Active Directory) dans la page « Analyse forensique des activités ».
- ONTAP Persistent Store est pris en charge à partir de la version 9.14.1.
- Pour des performances optimales, vous devez configurer le serveur FPolicy pour qu'il soit sur le même sous-réseau que le système de stockage.
- Pour connaître les meilleures pratiques et recommandations complètes concernant la configuration de la stratégie FPolicy de sécurité des charges de travail, consultez le document suivant :"Article de la base de connaissances sur les meilleures pratiques FPolicy" .

- Vous devez ajouter un SVM en utilisant l'une des deux méthodes suivantes :
  - En utilisant l'adresse IP du cluster, le nom SVM et le nom d'utilisateur et le mot de passe de gestion du cluster. ***C'est la méthode recommandée.***
    - Le nom SVM doit être exactement tel qu'il est affiché dans ONTAP et est sensible à la casse.
  - En utilisant l'adresse IP, le nom d'utilisateur et le mot de passe de gestion du serveur virtuel SVM
  - Si vous ne pouvez pas ou ne souhaitez pas utiliser le nom d'utilisateur et le mot de passe complets de gestion du cluster/SVM de l'administrateur, vous pouvez créer un utilisateur personnalisé avec des privilèges moindres comme mentionné dans le« Une note sur les autorisations » section ci-dessous. Cet utilisateur personnalisé peut être créé pour l'accès SVM ou Cluster.
    - Vous pouvez également utiliser un utilisateur AD disposant d'un rôle possédant au moins les autorisations du rôle csrole, comme indiqué dans la section « Remarque concernant les autorisations » ci-dessous. Voir également le"Documentation ONTAP" .
- Assurez-vous que les applications correctes sont définies pour le SVM en exécutant la commande suivante :

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

Exemple de sortie :

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Assurez-vous que le SVM dispose d'un serveur CIFS configuré : clustershell:> `vserver cifs show`

  Le système renvoie le nom du serveur virtuel, le nom du serveur CIFS et des champs supplémentaires.

- Définissez un mot de passe pour l'utilisateur SVM vsadmin. Si vous utilisez un utilisateur personnalisé ou un utilisateur administrateur de cluster, ignorez cette étape. clustershell:> `security login password -username vsadmin -vserver svmname`
- Déverrouillez l'utilisateur SVM vsadmin pour l'accès externe. Si vous utilisez un utilisateur personnalisé ou un utilisateur administrateur de cluster, ignorez cette étape. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Assurez-vous que la politique de pare-feu du LIF de données est définie sur « mgmt » (et non sur « données »). Ignorez cette étape si vous utilisez un LIF de gestion dédié pour ajouter le SVM. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Lorsqu'un pare-feu est activé, vous devez définir une exception pour autoriser le trafic TCP pour le port à l'aide du collecteur de données Data Data ONTAP .

Voir"Exigences relatives aux agents" pour les informations de configuration. Ceci s'applique aux agents sur site et aux agents installés dans le Cloud.

- Lorsqu'un agent est installé dans une instance AWS EC2 pour surveiller une SVM Cloud ONTAP , l'agent et le stockage doivent se trouver dans le même VPC. S'ils se trouvent dans des VPC distincts, il doit y avoir un itinéraire valide entre les VPC.

Tester la connectivité pour les collecteurs de données

La fonctionnalité de connectivité de test (introduite en mars 2025) vise à aider les utilisateurs finaux à identifier les causes spécifiques des échecs lors de la configuration des collecteurs de données dans Data Infrastructure Insights (DII) Workload Security. Cela permet aux utilisateurs de corriger eux-mêmes les problèmes liés à la communication réseau ou aux rôles manquants.

Cette fonctionnalité aidera les utilisateurs à déterminer si tous les contrôles liés au réseau sont en place avant de configurer un collecteur de données. De plus, il informera les utilisateurs des fonctionnalités auxquelles ils peuvent accéder en fonction de la version ONTAP , des rôles et des autorisations qui leur sont attribués dans ONTAP.

La connectivité de test n'est pas prise en charge pour les collecteurs d'annuaires utilisateurs

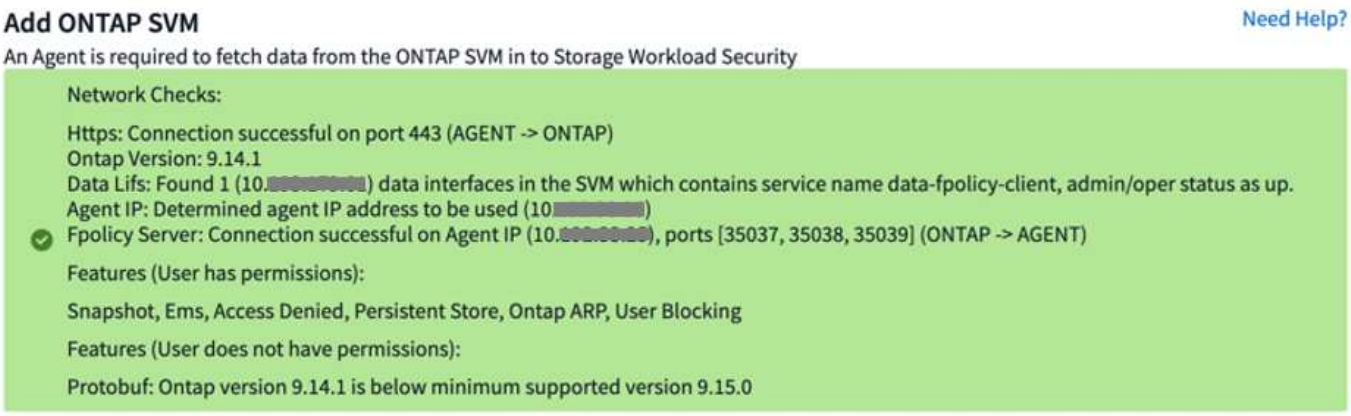
Conditions préalables aux tests de connexion

- Les informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne pleinement.
- La vérification de l'accès aux fonctionnalités n'est pas prise en charge en mode SVM.
- Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.
- Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*), fournissez les autorisations obligatoires et les autorisations spécifiques aux fonctionnalités que vous souhaitez utiliser.

Assurez-vous de revoir leAutorisations section ci-dessous également.

Tester la connexion

L'utilisateur peut accéder à la page d'ajout/modification du collecteur, saisir les détails du niveau du cluster (en mode cluster) ou les détails du niveau SVM (en mode SVM) et cliquer sur le bouton **Tester la connexion**. Workload Security traitera ensuite la demande et affichera un message de réussite ou d'échec approprié.



Points à noter pour ONTAP Multi Admin Verify (MAV)

Certaines fonctionnalités, telles que la création et la suppression d'instantanés ou le blocage des utilisateurs (SMB), peuvent ne pas fonctionner en fonction des commandes MAV ajoutées dans votre version de ONTAP.

Suivez les étapes ci-dessous pour ajouter des exclusions à vos commandes MAV afin de permettre à Workload Security de créer ou de supprimer des instantanés et de bloquer des utilisateurs.

Commandes pour autoriser la création et la suppression d'instantanés :

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Commande pour autoriser le blocage des utilisateurs :

```
multi-admin-verify rule delete -operation set
```

Conditions préalables au blocage de l'accès utilisateur

Gardez à l'esprit les points suivants pour"Blocage de l'accès utilisateur" :

Les informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne.

Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes de"Blocage de l'accès utilisateur" pour donner des autorisations à Workload Security pour bloquer l'utilisateur.

Remarque sur les autorisations

Autorisations lors de l'ajout via Cluster Management IP :

Si vous ne pouvez pas utiliser l'utilisateur administrateur de gestion de cluster pour autoriser Workload Security à accéder au collecteur de données ONTAP SVM, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles indiqués dans les commandes ci-dessous. Utilisez le nom d'utilisateur « csuser » et le mot de passe « csuser » lors de la configuration du collecteur de données Workload Security pour utiliser l'adresse IP de gestion de cluster.

Remarque : vous pouvez créer un rôle unique à utiliser pour toutes les autorisations de fonctionnalités pour un utilisateur personnalisé. S'il existe un utilisateur existant, supprimez d'abord l'utilisateur et le rôle existants à l'aide de ces commandes :

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Pour créer le nouvel utilisateur, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP :

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Autorisations lors de l'ajout via Vserver Management IP :

Si vous ne pouvez pas utiliser l'utilisateur administrateur de gestion de cluster pour autoriser Workload Security à accéder au collecteur de données ONTAP SVM, vous pouvez créer un nouvel utilisateur nommé « csuser » avec les rôles indiqués dans les commandes ci-dessous. Utilisez le nom d'utilisateur « csuser » et le mot de passe « csuser » lors de la configuration du collecteur de données Workload Security pour utiliser l'adresse IP de gestion du serveur virtuel.

Remarque : vous pouvez créer un rôle unique à utiliser pour toutes les autorisations de fonctionnalités pour un utilisateur personnalisé. S'il existe un utilisateur existant, supprimez d'abord l'utilisateur et le rôle existants à l'aide de ces commandes :

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Pour créer le nouvel utilisateur, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP . Pour plus de simplicité, copiez ces commandes dans un éditeur de texte et remplacez <vservername> par le nom de votre Vserver avant d'exécuter ces commandes sur ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Mode Protobuf

Workload Security configurera le moteur FPolicy en mode protobuf lorsque cette option est activée dans les paramètres *Configuration avancée* du collecteur. Le mode Protobuf est pris en charge dans ONTAP version 9.15 et ultérieure.

Vous trouverez plus de détails sur cette fonctionnalité dans le"Documentation ONTAP" .

Des autorisations spécifiques sont requises pour protobuf (certaines ou toutes peuvent déjà exister) :

Mode cluster :

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Mode serveur virtuel :
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

Autorisations pour la protection autonome contre les ransomwares ONTAP et accès ONTAP refusé

Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour accorder des autorisations à Workload Security afin de collecter des informations liées à ARP à partir d' ONTAP.

Pour plus d'informations, lisez à propos de"Intégration avec ONTAP Accès refusé"

et"Intégration avec la protection autonome contre les ransomwares ONTAP"

Configurer le collecteur de données

Étapes de configuration

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Data Infrastructure Insights .
2. Cliquez sur **Sécurité de la charge de travail > Collecteurs > +Collecteurs de données**

   Le système affiche les collecteurs de données disponibles.

3. Passez la souris sur la mosaïque * NetApp SVM et cliquez sur **+Surveiller**.

Le système affiche la page de configuration ONTAP SVM. Saisissez les données requises pour chaque champ.

Champ	Description
Nom	Nom unique pour le collecteur de données
Agent	Sélectionnez un agent configuré dans la liste.
Connectez-vous via l'IP de gestion pour :	Sélectionnez l'adresse IP du cluster ou l'adresse IP de gestion SVM
Adresse IP de gestion du cluster / SVM	L'adresse IP du cluster ou du SVM, selon votre sélection ci-dessus.
Nom de SVM	Le nom du SVM (ce champ est obligatoire lors de la connexion via l'IP du cluster)
Nom d'utilisateur	Nom d'utilisateur pour accéder au SVM/Cluster Lors de l'ajout via l'IP du cluster, les options sont : 1. Administrateur de cluster 2. 'csutilisateur' 3. Utilisateur AD ayant un rôle similaire à csuser. Lors de l'ajout via SVM IP, les options sont : 4. vsadmin 5. 'csutilisateur' 6. Nom d'utilisateur AD ayant un rôle similaire à csuser.
Mot de passe	Mot de passe pour le nom d'utilisateur ci-dessus
Filtrer les parts/volumes	Choisissez d'inclure ou d'exclure les actions/volumes de la collecte d'événements
Saisissez les noms de partage complets à exclure/inclure	Liste séparée par des virgules des partages à exclure ou à inclure (selon le cas) de la collecte d'événements
Saisissez les noms de volumes complets à exclure/inclure	Liste séparée par des virgules des volumes à exclure ou à inclure (selon le cas) de la collecte d'événements
Surveiller l'accès aux dossiers	Lorsque cette option est cochée, elle active les événements pour la surveillance de l'accès aux dossiers. Notez que la création/le changement de nom et la suppression des dossiers seront surveillés même sans cette option sélectionnée. L'activation de cette option augmentera le nombre d'événements surveillés.
Définir la taille du tampon d'envoi ONTAP	Définit la taille du tampon d'envoi ONTAP Fpolicy. Si une version ONTAP antérieure à 9.8p7 est utilisée et qu'un problème de performances est constaté, la taille du tampon d'envoi ONTAP peut être modifiée pour obtenir de meilleures performances ONTAP . Contactez le support NetApp si vous ne voyez pas cette option et souhaitez l'explorer.

Après avoir terminé

- Dans la page Collecteurs de données installés, utilisez le menu d'options à droite de chaque collecteur pour modifier le collecteur de données. Vous pouvez redémarrer le collecteur de données ou modifier les attributs de configuration du collecteur de données.

Configuration recommandée pour MetroCluster

Ce qui suit est recommandé pour MetroCluster:

1. Connectez deux collecteurs de données, l'un au SVM source et l'autre au SVM de destination.
2. Les collecteurs de données doivent être connectés par *Cluster IP*.
3. À tout moment, le collecteur de données du SVM « en cours d'exécution » s'affichera comme *Running*. Le collecteur de données du SVM « arrêté » actuel s'affichera comme *Arrêté*.
4. À chaque basculement, l'état du collecteur de données passe de *Running* à *Stopped* et vice versa.
5. Il faudra jusqu'à deux minutes au collecteur de données pour passer de l'état *Arrêté* à l'état *En cours d'exécution*.

Politique de service

Si vous utilisez la stratégie de service avec ONTAP **version 9.9.1 ou plus récente**, afin de vous connecter au collecteur de sources de données, le service *data-fpolicy-client* est requis avec le service de données *data-nfs* et/ou *data-cifs*.

Exemple:

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

Dans les versions d' ONTAP antérieures à 9.9.1, *data-fpolicy-client* n'a pas besoin d'être défini.

Collecteur de données de lecture-pause

Si le collecteur de données est à l'état *En cours d'exécution*, vous pouvez suspendre la collecte. Ouvrez le menu « trois points » du collecteur et sélectionnez PAUSE. Pendant que le collecteur est en pause, aucune donnée n'est collectée à partir d' ONTAP et aucune donnée n'est envoyée du collecteur à ONTAP. Cela signifie qu'aucun événement Fpolicy ne circulera d' ONTAP vers le collecteur de données, et de là vers Data Infrastructure Insights.

Notez que si de nouveaux volumes, etc. sont créés sur ONTAP alors que le collecteur est en pause, Workload Security ne collectera pas les données et ces volumes, etc. ne seront pas reflétés dans les tableaux de bord ou les tables.

Un collecteur ne peut pas être mis en pause s'il a des utilisateurs restreints. Restaurez l'accès utilisateur avant de suspendre le collecteur.

Gardez à l'esprit les points suivants :

- La purge des instantanés ne se produira pas selon les paramètres configurés sur un collecteur en pause.
- Les événements EMS (comme ONTAP ARP) ne seront pas traités sur un collecteur suspendu. Cela signifie que si ONTAP identifie une attaque de falsification de fichier, Data Infrastructure Insights Workload Security ne pourra pas acquérir cet événement.
- Les e-mails de notifications de santé ne seront PAS envoyés pour un collecteur en pause.

- Les actions manuelles ou automatiques (telles que le snapshot ou le blocage d'utilisateur) ne seront pas prises en charge sur un collecteur en pause.
- Lors des mises à niveau de l'agent ou du collecteur, des redémarrages/redémarrages de la machine virtuelle de l'agent ou du redémarrage du service de l'agent, un collecteur en pause restera dans l'état *Paused*.
- Si le collecteur de données est dans l'état *Erreur*, le collecteur ne peut pas être modifié en état *En pause*. Le bouton Pause ne sera activé que si l'état du collecteur est *Running*.
- Si l'agent est déconnecté, le collecteur ne peut pas être modifié en état *Paused*. Le collecteur passera à l'état *Arrêté* et le bouton Pause sera désactivé.

Magasin persistant

Le magasin persistant est pris en charge avec ONTAP 9.14.1 et versions ultérieures. Notez que les instructions de nom de volume varient d' ONTAP 9.14 à 9.15.

Le magasin persistant peut être activé en sélectionnant la case à cocher dans la page d'édition/ajout du collecteur. Après avoir coché la case, un champ de texte s'affiche pour accepter le nom du volume. Le nom du volume est un champ obligatoire pour activer le magasin persistant.

- Pour ONTAP 9.14.1, vous devez créer le volume avant d'activer la fonctionnalité et fournir le même nom dans le champ *Nom du volume*. La taille de volume recommandée est de 16 Go.
- Pour ONTAP 9.15.1, le volume sera créé automatiquement avec une taille de 16 Go par le collecteur, en utilisant le nom fourni dans le champ *Nom du volume*.

Des autorisations spécifiques sont requises pour le magasin persistant (certaines ou toutes ces autorisations peuvent déjà exister) :

Mode cluster :

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Mode serveur virtuel :

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrer les collecteurs

Vous pouvez facilement migrer un collecteur Workload Security d'un agent à un autre, permettant ainsi un équilibrage efficace de la charge des collecteurs entre les agents.

Prérequis

- L'agent source doit être dans l'état *connecté*.
- Le collecteur à migrer doit être dans l'état *running*.

Note:

- Migrate est pris en charge pour les collecteurs de données et d'annuaires d'utilisateurs.
- La migration d'un collecteur n'est pas prise en charge pour les locataires gérés manuellement.

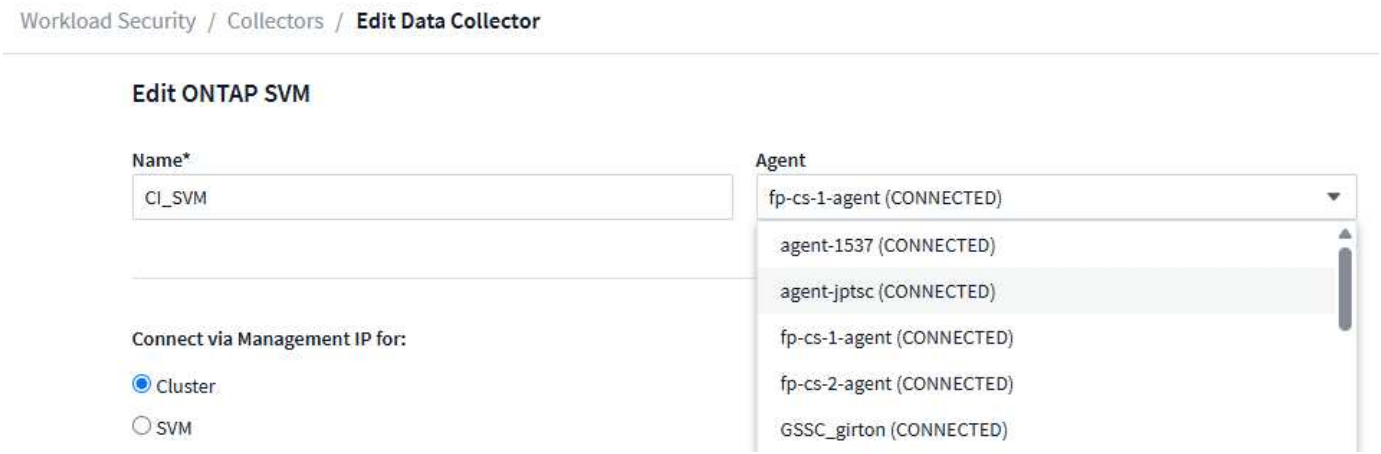
Migrer le collecteur

Pour migrer un collecteur, suivez ces étapes :

1. Accédez à la page « Modifier le collecteur ».
2. Sélectionnez un agent de destination dans la liste déroulante des agents.
3. Cliquez sur le bouton « Enregistrer le collecteur ».

Workload Security traitera la demande. Une fois la migration réussie, l'utilisateur sera redirigé vers la page de la liste des collecteurs. En cas d'échec, un message approprié sera affiché sur la page d'édition.

Remarque : toutes les modifications de configuration précédemment effectuées sur la page « Modifier le collecteur » resteront appliquées lorsque le collecteur sera migré avec succès vers l'agent de destination.



Dépannage

Voir le"Dépannage du collecteur SVM" page pour des conseils de dépannage.

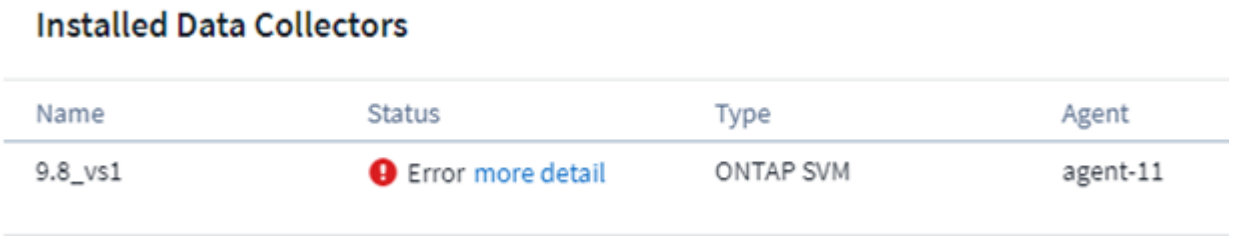
Dépannage du collecteur de données ONTAP SVM

Workload Security utilise des collecteurs de données pour collecter les données d'accès aux fichiers et aux utilisateurs à partir des appareils. Vous trouverez ici des conseils pour résoudre les problèmes liés à ce collecteur.

Voir le"Configuration du collecteur SVM" page pour obtenir des instructions sur la configuration de ce collecteur.

En cas d'erreur, vous pouvez cliquer sur *plus de détails* dans la colonne *Statut* de la page Collecteurs de

données installés pour obtenir des détails sur l'erreur.



Les problèmes connus et leurs résolutions sont décrits ci-dessous.

Problème : le collecteur de données s'exécute pendant un certain temps et s'arrête après un temps aléatoire, échouant avec : « Message d'erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : serveur fpolicy externe surchargé. **Essayez ceci :** le taux d'événements d' ONTAP était bien supérieur à ce que la boîte d'agent peut gérer. La connexion a donc été interrompue.

Vérifiez le trafic de pointe dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez le vérifier à partir de la page **CloudSecure > Analyse forensique des activités > Toutes les activités**.

Si le trafic agrégé de pointe est supérieur à ce que l'Agent Box peut gérer, reportez-vous à la page du vérificateur de taux d'événements pour savoir comment dimensionner le déploiement du collecteur dans une Agent Box.

Si l'agent a été installé dans la boîte Agent avant le 4 mars 2021, exécutez les commandes suivantes dans la boîte Agent :

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Redémarrez le collecteur à partir de l'interface utilisateur après le redimensionnement.

{vider}

Problème : le collecteur signale le message d'erreur : « Aucune adresse IP locale trouvée sur le connecteur pouvant atteindre les interfaces de données du SVM ». **Essayez ceci :** cela est probablement dû à un problème de réseau côté ONTAP . Veuillez suivre ces étapes :

1. Assurez-vous qu'il n'y a pas de pare-feu sur le LIF de données SVM ou sur le LIF de gestion qui bloque la connexion depuis le SVM.
2. Lors de l'ajout d'un SVM via une adresse IP de gestion de cluster, assurez-vous que la durée de vie des données et la durée de vie de gestion du SVM sont pingables à partir de la machine virtuelle de l'agent. En cas de problème, vérifiez la passerelle, le masque de réseau et les routes du lif.

   Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'adresse IP de gestion du cluster et d'envoyer une requête ping à l'adresse IP de l'agent. Assurez-vous que l'adresse IP de l'agent est pingable :

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

3. Si vous avez essayé de vous connecter via l'IP du cluster et que cela ne fonctionne pas, essayez de vous connecter directement via l'IP SVM. Veuillez consulter ci-dessus les étapes de connexion via l'IP SVM.
4. Lors de l'ajout du collecteur via l'adresse IP SVM et les informations d'identification vsadmin, vérifiez si le rôle Données plus Gestion du SVM est activé. Dans ce cas, le ping vers le SVM Lif fonctionnera, mais le SSH vers le SVM Lif ne fonctionnera pas. Si oui, créez un Lif de gestion SVM uniquement et essayez de vous connecter via ce Lif de gestion SVM uniquement.
5. Si cela ne fonctionne toujours pas, créez un nouveau Lif SVM et essayez de vous connecter via ce Lif. Assurez-vous que le masque de sous-réseau est correctement défini.
6. Débogage avancé :
   a. Démarrer une trace de paquets dans ONTAP.
   b. Essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure.
   c. Attendez que l'erreur apparaisse. Arrêtez le suivi des paquets dans ONTAP.
   d. Ouvrez la trace des paquets depuis ONTAP. Il est disponible à cet endroit

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Assurez-vous qu'il existe un SYN d' ONTAP vers la boîte Agent.
.. S'il n'y a pas de SYN d' ONTAP , il s'agit d'un problème de pare-
feu dans ONTAP.
.. Ouvrez le pare-feu dans ONTAP, afin ONTAP puisse connecter la
boîte d'agent.
```

7. Si cela ne fonctionne toujours pas, veuillez consulter l'équipe réseau pour vous assurer qu'aucun pare-feu externe ne bloque la connexion d' ONTAP au boîtier Agent.
8. Si aucune des solutions ci-dessus ne résout le problème, ouvrez un dossier avec"Assistance Netapp" pour obtenir de l'aide.

{vider}

Problème : Message : « Échec de la détermination du type ONTAP pour [nom d'hôte : <adresse IP>. Raison : Erreur de connexion au système de stockage <Adresse IP> : L'hôte est inaccessible (Hôte inaccessible)"
Essayez ceci :

1. Vérifiez que l'adresse IP de gestion SVM ou l'adresse IP de gestion de cluster correcte a été fournie.
2. Connectez-vous en SSH au SVM ou au cluster auquel vous souhaitez vous connecter. Une fois connecté, assurez-vous que le nom du SVM ou du cluster est correct.

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Service.nom : audit. Motif de l'échec : serveur fpolicy externe arrêté. **Essayez ceci :**

1. Il est très probable qu'un pare-feu bloque les ports nécessaires sur la machine agent. Vérifiez que la plage de ports 35000-55000/tcp est ouverte pour que la machine agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé côté ONTAP bloquant la communication avec la machine agent.
2. Tapez la commande suivante dans la zone Agent et assurez-vous que la plage de ports est ouverte.

   ```
   sudo iptables-save | grep 3500*
   ```

   Un exemple de sortie devrait ressembler à :

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Connectez-vous à SVM, entrez les commandes suivantes et vérifiez
   qu'aucun pare-feu n'est configuré pour bloquer la communication avec
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Vérifier les commandes du pare-feu"du côté ONTAP .

3. Connectez-vous en SSH au SVM/cluster que vous souhaitez surveiller. Envoyez une requête ping à la boîte Agent à partir de la bibliothèque de données SVM (avec prise en charge des protocoles CIFS et NFS) et assurez-vous que la requête ping fonctionne :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

4. Si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affichera. Supprimez l'un des collecteurs de données via l'interface utilisateur. Redémarrez ensuite l'autre collecteur de données via l'interface utilisateur. Ensuite, le collecteur de données affichera le statut « EN COURS D'EXÉCUTION » et commencera à recevoir des événements de SVM.

   Fondamentalement, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 collecteur de données. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.

5. Dans les cas où le même SVM a été ajouté dans deux environnements de sécurité de charge de travail différents (locataires), le dernier réussira toujours. Le deuxième collecteur configurera fpolicy avec sa propre adresse IP et expulsera le premier. Ainsi, le collecteur du premier cessera de recevoir des événements et son service « audit » entrera en état d'erreur. Pour éviter cela, configurez chaque SVM sur

un seul environnement.

6. Cette erreur peut également se produire si les stratégies de service ne sont pas configurées correctement. Avec ONTAP 9.8 ou version ultérieure, pour se connecter au collecteur de sources de données, le service data-fpolicy-client est requis avec le service de données data-nfs et/ou data-cifs. De plus, le service data-fpolicy-client doit être associé aux données lif pour le SVM surveillé.

{vider}

Problème : Aucun événement n'est visible sur la page d'activité. **Essayez ceci :**

1. Vérifiez si le collecteur ONTAP est à l'état « RUNNING ». Si oui, assurez-vous que certains événements cifs sont générés sur les machines virtuelles clientes cifs en ouvrant certains fichiers.
2. Si aucune activité n'est observée, connectez-vous au SVM et entrez la commande suivante.

   ```
   <SVM>event log show -source fpolicy
   ```

   Veuillez vous assurer qu'il n'y a pas d'erreurs liées à fpolicy.

3. Si aucune activité n'est visible, veuillez vous connecter au SVM. Entrez la commande suivante :

   ```
   <SVM>fpolicy show
   ```

   Vérifiez si la politique fpolicy nommée avec le préfixe « cloudsecure_ » a été définie et si le statut est « on ». Si cette option n'est pas définie, il est fort probable que l'agent ne puisse pas exécuter les commandes dans la SVM. Veuillez vous assurer que toutes les conditions préalables décrites au début de la page ont été respectées.

{vider}

Problème : Le collecteur de données SVM est en état d'erreur et le message d'erreur est « L'agent n'a pas réussi à se connecter au collecteur » **Essayez ceci :**

1. Il est fort probable que l'agent soit surchargé et ne parvienne pas à se connecter aux collecteurs de sources de données.
2. Vérifiez combien de collecteurs de sources de données sont connectés à l'agent.
3. Vérifiez également le débit de données dans la page « Toutes les activités » de l'interface utilisateur.
4. Si le nombre d'activités par seconde est considérablement élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.

{vider}

Problème : le collecteur de données SVM affiche le message d'erreur suivant : « fpolicy.server.connectError : le nœud n'a pas pu établir de connexion avec le serveur FPolicy « 12.195.15.146 » (raison : « Sélection

expirée ») » **Essayez ceci :** le pare-feu est activé dans SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les CLI dans ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont :

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Vérifier les commandes du pare-feu"du côté ONTAP .

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : Aucune interface de données valide (rôle : données, protocoles de données : NFS ou CIFS ou les deux, état : actif) trouvée sur la SVM. **Essayez ceci :** Assurez-vous qu'il existe une interface opérationnelle (ayant un rôle de données et un protocole de données comme CIFS/NFS).

{vider}

Problème : le collecteur de données passe à l'état d'erreur, puis passe à l'état d'exécution après un certain temps, puis revient à l'état d'erreur. Ce cycle se répète. **Essayez ceci :** Cela se produit généralement dans le scénario suivant :

1. Plusieurs collecteurs de données ont été ajoutés.
2. Les collecteurs de données qui présentent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Cela signifie que 2 ou plusieurs collecteurs de données sont connectés à 1 SVM.
3. Assurez-vous qu'un seul collecteur de données se connecte à un seul SVM.
4. Supprimez les autres collecteurs de données connectés au même SVM.

{vider}

Problème : le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur SVM svmname. Motif : Valeur non valide spécifiée pour l'élément « shares-to-include » dans « fpolicy.policy.scope-modify : « Federal » **Essayez ceci :** *Les noms de partage doivent être indiqués sans guillemets. Modifiez la configuration DSC ONTAP SVM pour corriger les noms de partage.

Inclure et exclure des partages n'est pas destiné à une longue liste de noms de partages. Utilisez plutôt le filtrage par volume si vous avez un grand nombre d'actions à inclure ou à exclure.

{vider}

Problème : il existe des fpolicies existantes dans le cluster qui ne sont pas utilisées. Que faut-il faire avec ceux-ci avant l'installation de Workload Security ? **Essayez ceci :** Il est recommandé de supprimer tous les paramètres fpolicy inutilisés existants, même s'ils sont dans un état déconnecté. Workload Security créera

fpolicy avec le préfixe « cloudsecure_ ». Toutes les autres configurations fpolicy inutilisées peuvent être supprimées.

Commande CLI pour afficher la liste fpolicy :

```
 fpolicy show
Étapes pour supprimer les configurations fpolicy :
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vider}

Problème : Après l'activation de la sécurité des charges de travail, les performances ONTAP sont affectées : la latence devient sporadiquement élevée et les IOPS deviennent sporadiquement faibles. **Essayez ceci :** Lors de l'utilisation ONTAP avec Workload Security, des problèmes de latence peuvent parfois être observés dans ONTAP. Plusieurs raisons peuvent expliquer cela, comme indiqué ci-dessous :"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tous ces problèmes sont résolus dans ONTAP 9.13.1 et versions ultérieures ; il est fortement recommandé d'utiliser l'une de ces versions ultérieures.

{vider}

Problème : le collecteur de données affiche le message d'erreur : « Erreur : échec de la détermination de l'état du collecteur en 2 tentatives, essayez de redémarrer le collecteur (code d'erreur : AGENT008) ». **Essayez ceci :**

1. Sur la page Collecteurs de données, faites défiler vers la droite du collecteur de données générant l'erreur et cliquez sur le menu à 3 points. Sélectionnez *Modifier*. Saisissez à nouveau le mot de passe du collecteur de données. Enregistrez le collecteur de données en appuyant sur le bouton *Enregistrer*. Le collecteur de données redémarrera et l'erreur devrait être résolue.
2. Il se peut que la machine Agent ne dispose pas de suffisamment de CPU ou de RAM, c'est pourquoi les DSC échouent. Veuillez vérifier le nombre de collecteurs de données ajoutés à l'agent dans la machine. Si le nombre est supérieur à 20, veuillez augmenter la capacité du processeur et de la RAM de la machine Agent. Une fois le CPU et la RAM augmentés, les DSC passeront automatiquement en état d'initialisation puis en état d'exécution. Consultez le guide des tailles sur"cette page" .

{vider}

Problème : le collecteur de données génère une erreur lorsque le mode SVM est sélectionné. **Essayez ceci :** lors de la connexion en mode SVM, si l'IP de gestion du cluster est utilisée pour se connecter au lieu de l'IP de

---

gestion SVM, la connexion échouera. Assurez-vous que l'adresse IP SVM correcte est utilisée.

{vider}

Problème : le collecteur de données affiche un message d'erreur lorsque la fonction Accès refusé est activée : « Le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de fpolicy sur SVM test_svm. Motif : l'utilisateur n'est pas autorisé. **Essayez ceci :** l'utilisateur ne dispose peut-être pas des autorisations REST nécessaires à la fonctionnalité Accès refusé. Veuillez suivre les instructions sur"cette page" pour définir les autorisations.

Redémarrez le collecteur une fois les autorisations définies.

{vider}

Problème : Le collecteur est en état d'erreur avec le message : Le connecteur est en état d'erreur. Raison de l'échec : Échec de la configuration du stockage persistant sur la SVM <Nom de la SVM>. Raison : Impossible de trouver un agrégat approprié pour le volume « <volumeName> » dans le SVM « <SVM Name> ». Motif : Les informations de performance pour l'agrégat « <aggregateName> » ne sont actuellement pas disponibles. Patientez quelques minutes et réessayez la commande. Nom du service : audit. Raison de l'échec : impossible de configurer le magasin persistant sur la SVM <SVM name="">.</SVM> Reason: Unable to find a suitable aggregate for volume "<volumeName>" in SVM "<SVM Name>". Motif : Les informations sur les performances pour <aggregateName>l'agrégat « » ne sont actuellement pas disponibles.</aggregateName> Attendez quelques minutes et réessayez la commande.

Essayez ceci : Attendez quelques minutes, puis redémarrez le Collecteur.

{vider}

Si vous rencontrez toujours des problèmes, contactez les liens d'assistance mentionnés dans la page **Aide > Assistance**.

Configuration du collecteur Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP

Surveillez l'accès aux fichiers et aux utilisateurs sur votre infrastructure de stockage cloud en configurant les collecteurs de données Workload Security pour Cloud Volumes ONTAP et Amazon FSx for NetApp ONTAP. Ce guide fournit des instructions étape par étape pour déployer des agents dans AWS et les connecter à vos instances de stockage cloud.

Configuration du stockage Cloud Volumes ONTAP

Consultez la documentation OnCommand Cloud Volumes ONTAP pour configurer une instance AWS à nœud unique / HA pour héberger l'agent de sécurité de la charge de travail :https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Une fois la configuration terminée, suivez les étapes pour configurer votre SVM :https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Plateformes prises en charge

- Cloud Volumes ONTAP, pris en charge par tous les fournisseurs de services cloud disponibles, partout où ils sont disponibles. Par exemple : Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configuration de la machine agent

La machine agent doit être configurée dans les sous-réseaux respectifs des fournisseurs de services cloud. Pour en savoir plus sur l'accès au réseau, consultez les [Exigences relatives à l'agent].

Vous trouverez ci-dessous les étapes d'installation de l'agent dans AWS. Des étapes équivalentes, applicables au fournisseur de services cloud, peuvent être suivies dans Azure ou Google Cloud pour l'installation.

Dans AWS, procédez comme suit pour configurer la machine à utiliser comme agent de sécurité de charge de travail :

Suivez les étapes suivantes pour configurer la machine à utiliser comme agent de sécurité de charge de travail :

Étapes

1. Connectez-vous à la console AWS et accédez à la page EC2-Instances et sélectionnez *Lancer l'instance*.
2. Sélectionnez une AMI RHEL ou CentOS avec la version appropriée comme mentionné dans cette page :https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Sélectionnez le VPC et le sous-réseau dans lesquels réside l'instance Cloud ONTAP .
4. Sélectionnez *t2.xlarge* (4 vcpus et 16 Go de RAM) comme ressources allouées.
    a. Créez l'instance EC2.
5. Installez les packages Linux requis à l'aide du gestionnaire de packages YUM :
    a. Installez *wget* et *unzip* les packages Linux natifs.

Installer l'agent Workload Security

1. Connectez-vous en tant qu'administrateur ou propriétaire de compte à votre environnement Data Infrastructure Insights .
2. Accédez à Workload Security **Collectors** et cliquez sur l'onglet **Agents**.
3. Cliquez sur **+Agent** et spécifiez RHEL comme plate-forme cible.
4. Copiez la commande d'installation de l'agent.
5. Collez la commande d'installation de l'agent dans l'instance RHEL EC2 à laquelle vous êtes connecté. Cela installe l'agent Workload Security, fournissant tous les"Prérequis de l'agent" sont respectées.

Pour les étapes détaillées, veuillez vous référer à ce lien : https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Dépannage

Les problèmes connus et leurs résolutions sont décrits dans le tableau suivant.

Problème	Résolution

L’erreur « Sécurité de la charge de travail : échec de détermination du type ONTAP pour le collecteur de données Amazon FxSN » est affichée par le collecteur de données. Le client ne peut pas ajouter de nouveau collecteur de données Amazon FSxN dans Workload Security. La connexion au cluster FSxN sur le port 443 depuis l’agent expire. Les groupes de sécurité du pare-feu et AWS ont les règles requises activées pour permettre la communication. Un agent est déjà déployé et se trouve également dans le même compte AWS. Ce même agent est utilisé pour connecter et surveiller les périphériques NetApp restants (et ils fonctionnent tous).	Résolvez ce problème en ajoutant le segment réseau LIF fsxadmin à la règle de sécurité de l’agent. Autorisez tous les ports si vous n’êtes pas sûr des ports.

Gestion des utilisateurs

Les comptes d’utilisateurs de Workload Security sont gérés via Data Infrastructure Insights.

Data Infrastructure Insights propose quatre niveaux de compte utilisateur : propriétaire du compte, administrateur, utilisateur et invité. À chaque compte sont attribués des niveaux d’autorisation spécifiques. Un compte utilisateur disposant de privilèges d’administrateur peut créer ou modifier des utilisateurs et attribuer à chaque utilisateur l’un des rôles de sécurité de la charge de travail suivants :

Rôle	Accès à la sécurité de la charge de travail
Administrateur	Peut exécuter toutes les fonctions de sécurité de la charge de travail, y compris celles pour les alertes, l’analyse médico-légale, les collecteurs de données, les politiques de réponse automatisées et les API pour la sécurité de la charge de travail. Un administrateur peut également inviter d’autres utilisateurs, mais ne peut attribuer que des rôles de sécurité de la charge de travail.
Utilisateur	Peut afficher et gérer les alertes et consulter les analyses médico-légales. Le rôle utilisateur peut modifier l’état de l’alerte, ajouter une note, prendre des instantanés manuellement et restreindre l’accès utilisateur.
Invité	Peut afficher les alertes et les analyses médico-légales. Le rôle d’invité ne peut pas modifier l’état de l’alerte, ajouter une note, prendre des instantanés manuellement ou restreindre l’accès des utilisateurs.

Étapes

1. Connectez-vous à Workload Security
2. Dans le menu, cliquez sur **Admin > Gestion des utilisateurs**

   Vous serez redirigé vers la page de gestion des utilisateurs de Data Infrastructure Insights.

3. Sélectionnez le rôle souhaité pour chaque utilisateur.

Lors de l'ajout d'un nouvel utilisateur, sélectionnez simplement le rôle souhaité (généralement Utilisateur ou Invité).

Vous trouverez plus d'informations sur les comptes d'utilisateurs et les rôles dans Data Infrastructure Insights."Rôle de l'utilisateur" documentation.

Vérificateur de taux d'événements : Guide de dimensionnement des agents

Déterminez la taille optimale des machines Agent en mesurant les débits d'événements NFS et SMB générés par vos SVM avant de déployer les collecteurs de données. Le script Event Rate Checker vous aide à comprendre les limites de capacité (maximum 50 collecteurs de données par Agent) et garantit que votre infrastructure Agent peut gérer le volume d'événements attendu pour une détection fiable des menaces.

Exigences:

- IP de cluster
- Nom d'utilisateur et mot de passe de l'administrateur du cluster

Lors de l'exécution de ce script, aucun collecteur de données ONTAP SVM ne doit être en cours d'exécution pour le SVM pour lequel le taux d'événements est déterminé.

Mesures:

1. Installez l'agent en suivant les instructions de CloudSecure.
2. Une fois l'agent installé, exécutez le script *server_data_rate_checker.sh* en tant qu'utilisateur sudo :

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Ce script nécessite que _sshpass_ soit installé sur la machine Linux.
Il existe deux façons de l'installer :
```

   a. Exécutez la commande suivante :

```
 linux_prompt> yum install sshpass
.. Si cela ne fonctionne pas, téléchargez _sshpass_ sur la machine
Linux à partir du Web et exécutez la commande suivante :
```

```
linux_prompt> rpm -i sshpass
```

3. Fournissez les valeurs correctes lorsque vous y êtes invité. Voir ci-dessous pour un exemple.
4. L'exécution du script prendra environ 5 minutes.
5. Une fois l'exécution terminée, le script imprimera le taux d'événements à partir du SVM. Vous pouvez vérifier le taux d'événements par SVM dans la sortie de la console :

```
“Svm svm_rate is generating 100 events/sec”.
```

Chaque collecteur de données Ontap SVM peut être associé à un seul SVM, ce qui signifie que chaque collecteur de données pourra recevoir le nombre d’événements générés par un seul SVM.

Gardez à l’esprit les points suivants :

A) Utilisez ce tableau comme guide général de dimensionnement. Vous pouvez augmenter le nombre de cœurs et/ou de mémoire pour augmenter le nombre de collecteurs de données pris en charge, jusqu’à un maximum de 50 collecteurs de données :

Configuration de la machine agent	Nombre de collecteurs de données SVM	Taux maximal d’événements que la machine agent peut gérer
4 cœurs, 16 Go	10 collecteurs de données	20 000 événements/sec
4 cœurs, 32 Go	20 collecteurs de données	20 000 événements/sec

B) Pour calculer le nombre total d’événements, additionnez les événements générés pour tous les SVM de cet agent.

C) Si le script n’est pas exécuté pendant les heures de pointe ou si le trafic de pointe est difficile à prévoir, conservez une marge de taux d’événements de 30 %.

B + C doit être inférieur à A, sinon la machine Agent ne parviendra pas à surveiller.

En d’autres termes, le nombre de collecteurs de données qui peuvent être ajoutés à une seule machine agent doit être conforme à la formule ci-dessous :

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Voir lelink:concept_cs_agent_requirements.html["Exigences relatives aux
agents"] page pour les prérequis et exigences supplémentaires.
```

Exemple

Disons que nous avons trois SVMS générant des taux d’événements de 100, 200 et 300 événements par seconde, respectivement.

Nous appliquons la formule :

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

La sortie de la console est disponible sur la machine Agent dans le nom de fichier *fpolicy_stat_<SVM Name>.log* dans le répertoire de travail actuel.

Le script peut donner des résultats erronés dans les cas suivants :

- Des informations d'identification, une adresse IP ou un nom SVM incorrects sont fournis.
- Une fpolicy déjà existante avec le même nom, le même numéro de séquence, etc. donnera une erreur.
- Le script s'arrête brusquement pendant son exécution.

Un exemple d'exécution de script est présenté ci-dessous :

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
------------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

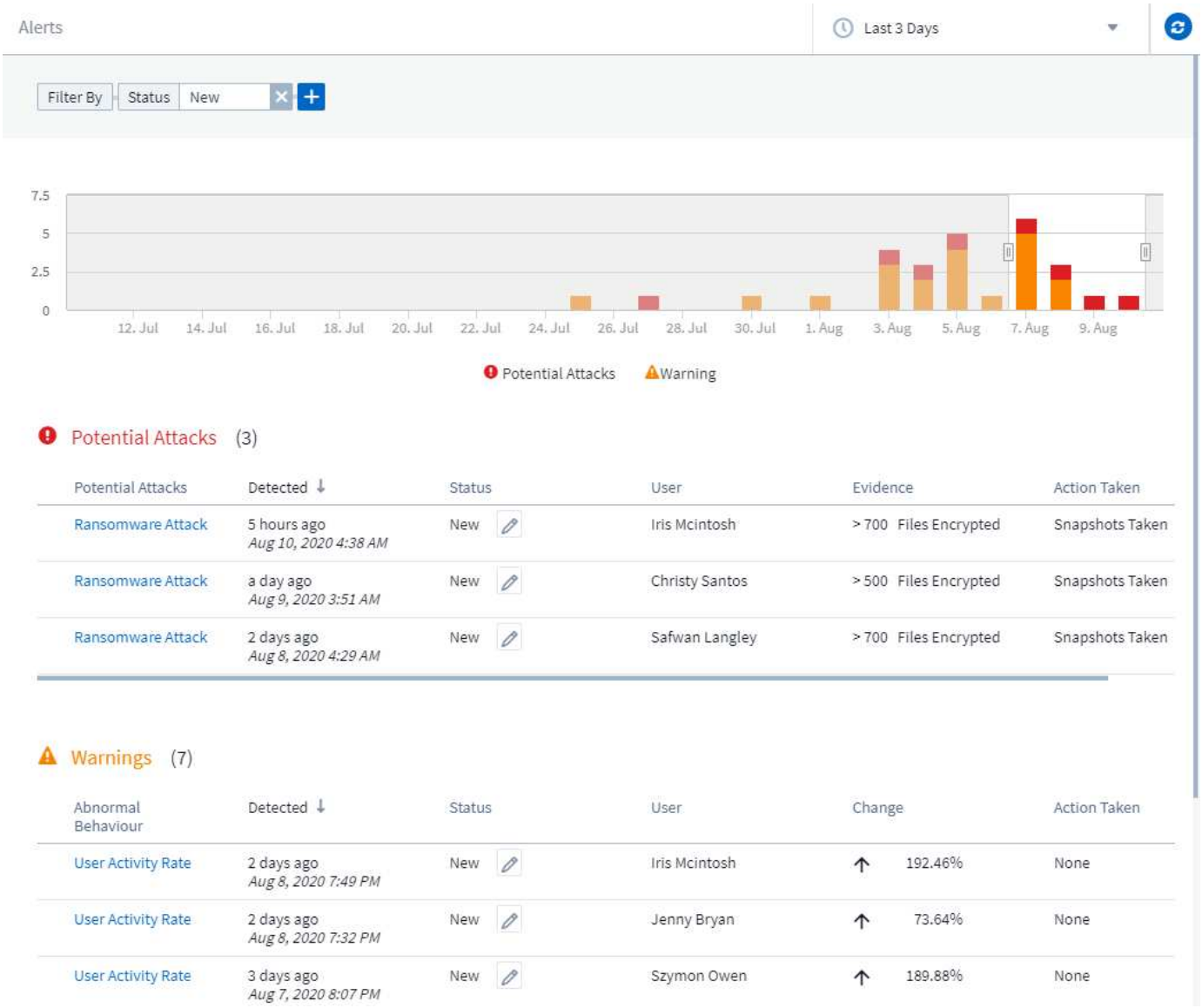
```
[root@ci-cs-data agent]#
```

Dépannage

Question	Répondre
Si j'exécute ce script sur un SVM déjà configuré pour Workload Security, utilise-t-il simplement la configuration fpolicy existante sur le SVM ou en configure-t-il un temporaire et exécute-t-il le processus ?	Le vérificateur de taux d'événements peut fonctionner correctement même pour un SVM déjà configuré pour la sécurité de la charge de travail. Il ne devrait y avoir aucun impact.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Modifiez simplement le script et modifiez le nombre maximal de SVM de 5 à n'importe quel nombre souhaité.
Si j'augmente le nombre de SVM, cela augmentera-t-il le temps d'exécution du script ?	Non. Le script s'exécutera pendant 5 minutes maximum, même si le nombre de SVM est augmenté.
Puis-je augmenter le nombre de SVM sur lesquels le script peut être exécuté ?	Oui. Vous devez modifier le script et modifier le nombre maximal de SVM de 5 à n'importe quel nombre souhaité.
Si j'augmente le nombre de SVM, cela augmentera-t-il le temps d'exécution du script ?	Non. Le script s'exécutera pendant 5 minutes maximum, même si le nombre de SVM augmente.
Que se passe-t-il si j'exécute le vérificateur de taux d'événements avec un agent existant ?	L'exécution du vérificateur de taux d'événements sur un agent déjà existant peut entraîner une augmentation de la latence sur le SVM. Cette augmentation sera de nature temporaire pendant l'exécution du vérificateur de taux d'événements.

Comprendre et examiner les alertes

La page « Alertes de sécurité des charges de travail » fournit une chronologie complète des menaces et avertissements détectés, ainsi que des outils d'investigation détaillés. Consultez les détails des alertes, gérez les mises à jour de statut, filtrez par critères et suivez les activités des utilisateurs pour enquêter efficacement sur les incidents de sécurité et y répondre.



Alerte

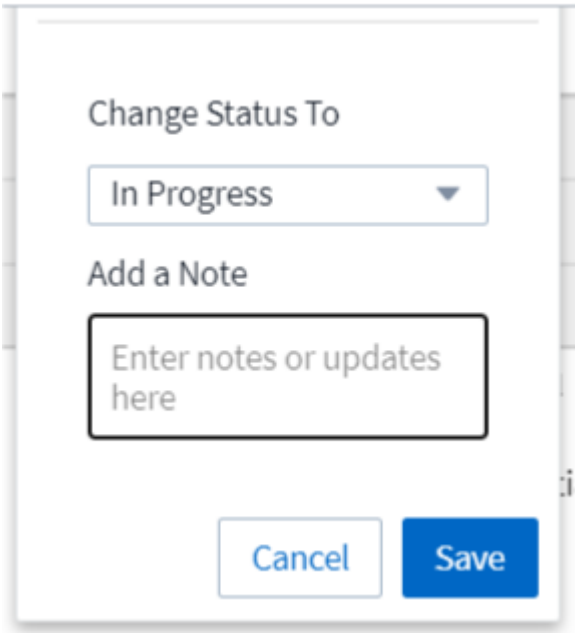
La liste des alertes affiche un graphique indiquant le nombre total d'attaques potentielles et/ou d'avertissements qui ont été émis dans la période sélectionnée, suivi d'une liste des attaques et/ou des avertissements qui se sont produits dans cette période. Vous pouvez modifier la plage horaire en ajustant les curseurs d'heure de début et d'heure de fin dans le graphique.

Les éléments suivants sont affichés pour chaque alerte :

Attaques potentielles :

- Le type d’attaque potentielle (par exemple, falsification de fichiers ou sabotage)
- La date et l’heure auxquelles l’attaque potentielle a été *détectée*
- Le *Statut* de l’alerte :
  - **Nouveau** : il s’agit de la valeur par défaut pour les nouvelles alertes.
  - **En cours** : L’alerte fait l’objet d’une enquête par un ou plusieurs membres de l’équipe.
  - **Résolu** : L’alerte a été marquée comme résolue par un membre de l’équipe.
  - **Rejeté** : l’alerte a été rejetée en tant que faux positif ou comportement attendu.

    Un administrateur peut modifier le statut de l’alerte et ajouter une note pour faciliter l’enquête.



- L’utilisateur dont le comportement a déclenché l’alerte
- *Preuve* de l’attaque (par exemple, un grand nombre de fichiers ont été chiffrés)
- L’action entreprise (par exemple, un instantané a été pris)

Avertissements :

- Le *Comportement anormal* qui a déclenché l’avertissement
- La date et l’heure auxquelles le comportement a été *détecté*
- Le *Statut* de l’alerte (Nouveau, En cours, etc.)
- L’utilisateur dont le comportement a déclenché l’alerte
- Une description du *Changement* (par exemple, une augmentation anormale de l’accès aux fichiers)
- L’action entreprise

Options de filtrage

Vous pouvez filtrer les alertes selon les critères suivants :

- Le *Statut* de l’alerte

- Texte spécifique dans la *Note*
- Le type d'*attaques/avertissements*
- L'utilisateur dont les actions ont déclenché l'alerte/l'avertissement

La page Détails de l'alerte

Vous pouvez cliquer sur un lien d'alerte sur la page de la liste des alertes pour ouvrir une page de détails pour l'alerte. Les détails de l'alerte peuvent varier selon le type d'attaque ou d'alerte. Par exemple, une page de détails sur une attaque par falsification de fichiers peut afficher les informations suivantes :

Section récapitulative :

- Type d'attaque (falsification de fichiers, sabotage) et ID d'alerte (attribué par la sécurité des charges de travail)
- Date et heure de détection de l'attaque
- Action entreprise (par exemple, un instantané automatique a été pris). L'heure de l'instantané est indiquée immédiatement sous la section récapitulative))
- Statut (Nouveau, En cours, etc.)

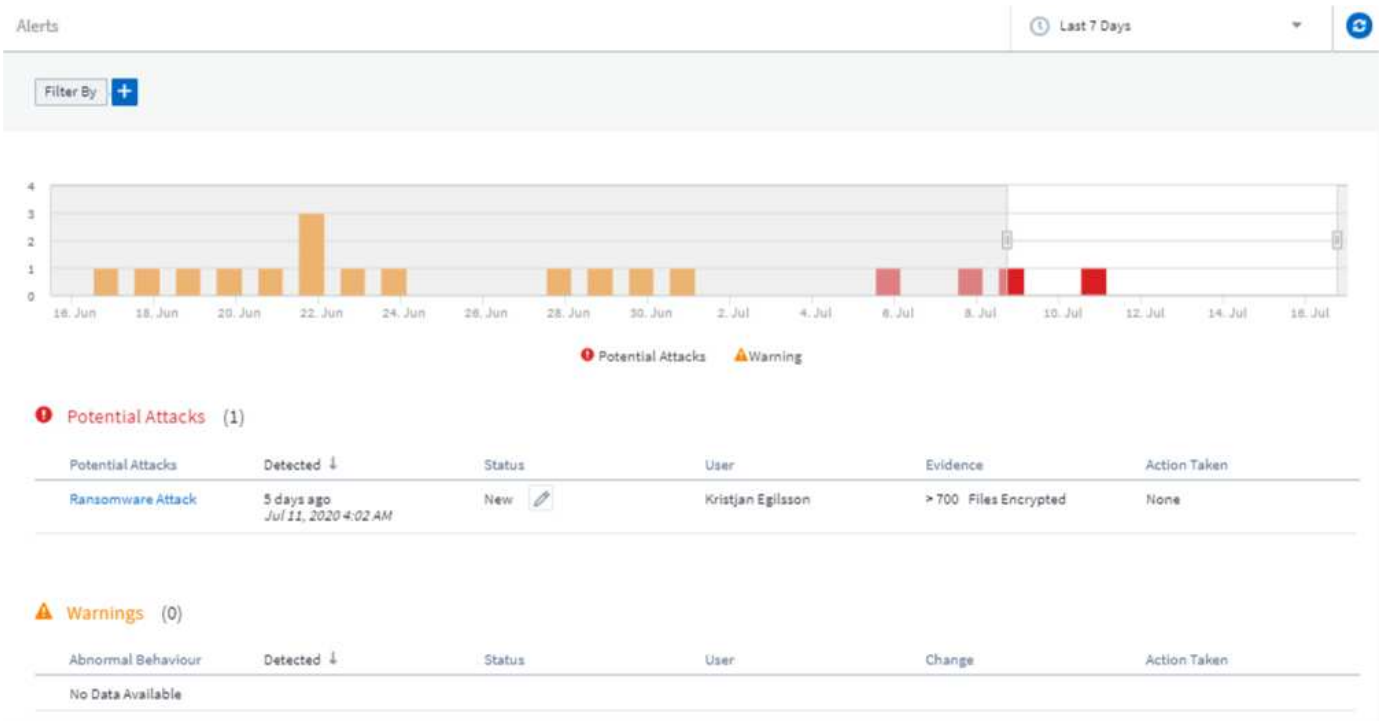
Section Résultats d'attaque :

- Nombre de volumes et de fichiers affectés
- Un résumé d'accompagnement de la détection
- Un graphique montrant l'activité du fichier pendant l'attaque

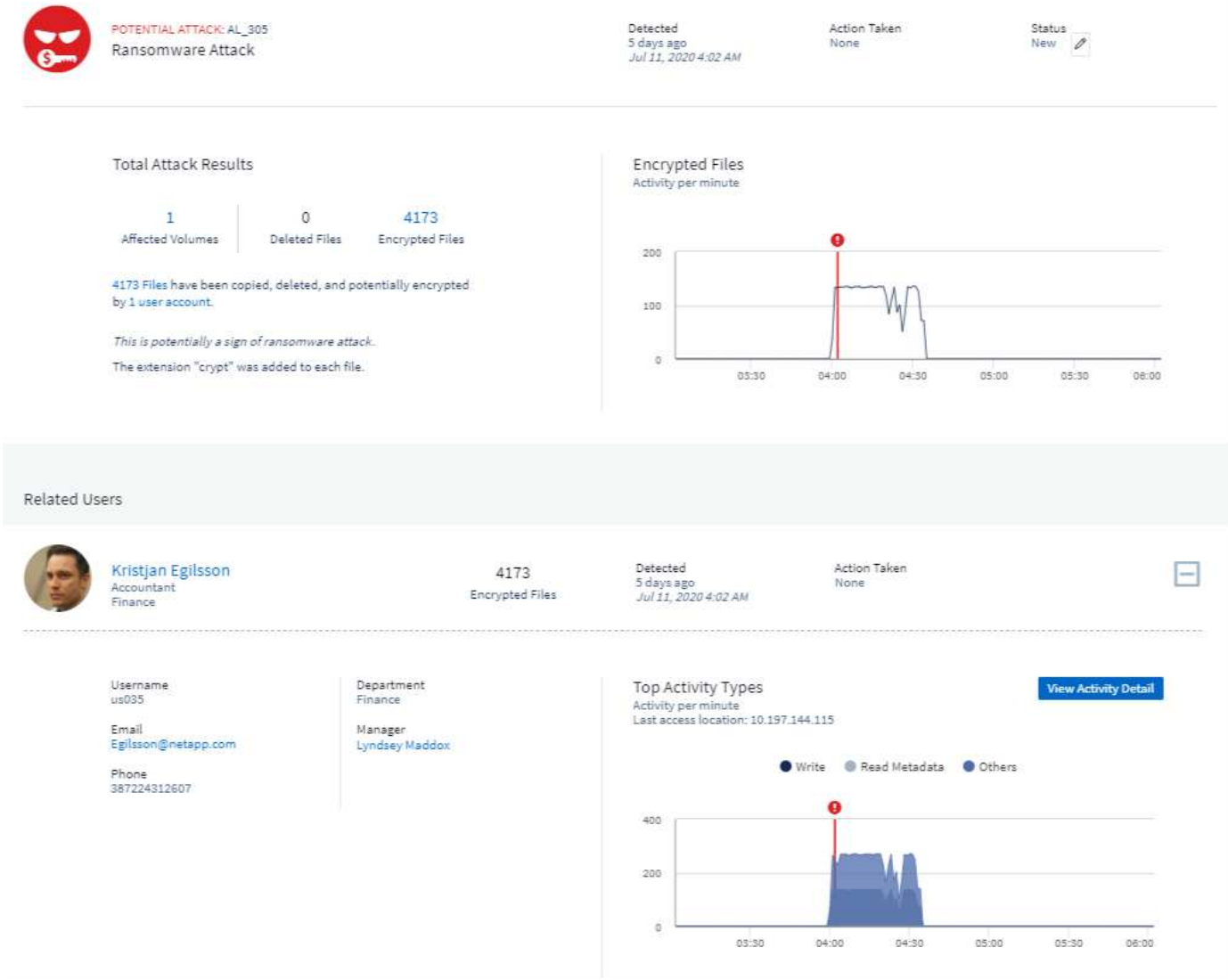
Section Utilisateurs associés :

Cette section affiche des détails sur l'utilisateur impliqué dans l'attaque potentielle, y compris un graphique de l'activité principale de l'utilisateur.

Page d'alertes (cet exemple illustre une potentielle attaque par falsification de fichiers) :



Page de détails (cet exemple illustre une attaque potentielle par falsification de fichiers) :

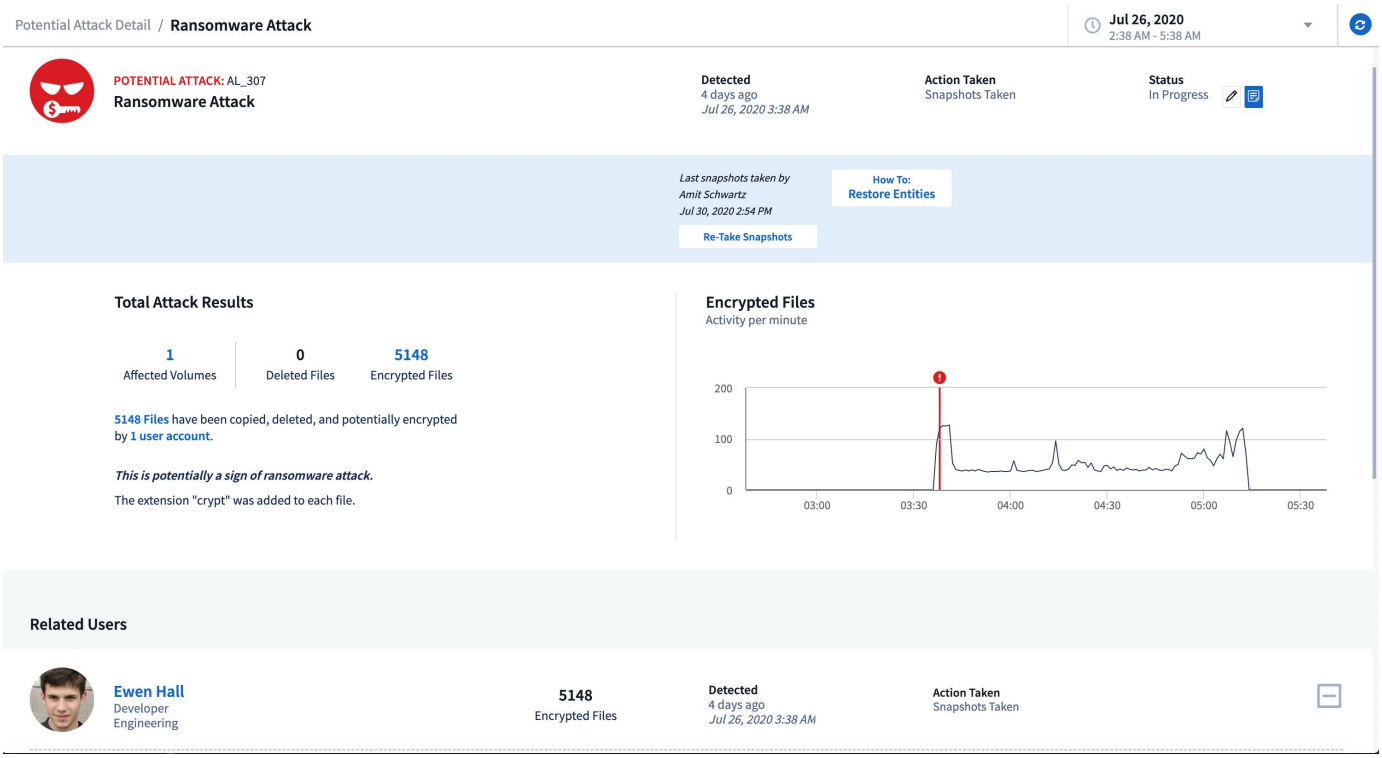


Prendre un instantané **Action**

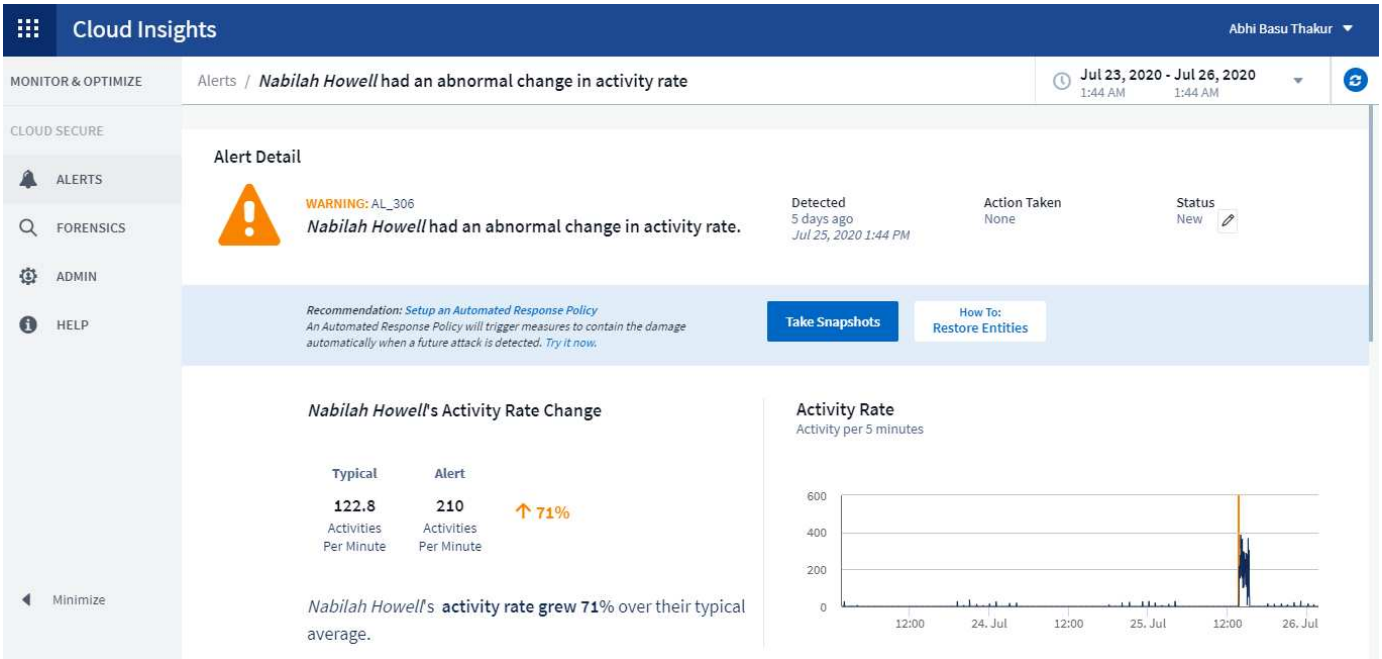
Workload Security protège vos données en prenant automatiquement un instantané lorsqu'une activité malveillante est détectée, garantissant ainsi que vos données sont sauvegardées en toute sécurité.

Vous pouvez définir "politiques de réponse automatisées" qui prennent un instantané lorsqu'une attaque par falsification de fichiers ou toute autre activité anormale de l'utilisateur est détectée. Vous pouvez également prendre une capture d'écran manuellement depuis la page d'alerte.

Capture d'écran automatique
prise :



Instantané manuel :



Notifications d’alerte

Les notifications par courrier électronique des alertes sont envoyées à une liste de destinataires d’alertes pour chaque action sur l’alerte. Pour configurer les destinataires des alertes, cliquez sur **Admin > Notifications** et saisissez une adresse e-mail pour chaque destinataire.

Politique de conservation

Les alertes et avertissements sont conservés pendant 13 mois. Les alertes et avertissements datant de plus

de 13 mois seront supprimés. Si l'environnement Workload Security est supprimé, toutes les données associées à l'environnement sont également supprimées.

Dépannage

Problème:	Essayez ceci:
Il existe une situation dans laquelle ONTAP prend des instantanés toutes les heures par jour. Les snapshots de Workload Security (WS) l'affecteront-ils ? Le snapshot WS prendra-t-il la place du snapshot horaire ? L'instantané horaire par défaut sera-t-il arrêté ?	Les instantanés de sécurité de la charge de travail n'affecteront pas les instantanés horaires. Les instantanés WS n'occuperont pas l'espace d'instantané horaire et cela devrait continuer comme avant. L'instantané horaire par défaut ne sera pas arrêté.
Que se passera-t-il si le nombre maximal de snapshots est atteint dans ONTAP?	Si le nombre maximal de snapshots est atteint, la prise de snapshots suivante échouera et Workload Security affichera un message d'erreur indiquant que le snapshot est plein. L'utilisateur doit définir des politiques d'instantanés pour supprimer les instantanés les plus anciens, sinon les instantanés ne seront pas pris. Dans ONTAP 9.3 et les versions antérieures, un volume peut contenir jusqu'à 255 copies Snapshot. Dans ONTAP 9.4 et versions ultérieures, un volume peut contenir jusqu'à 1 023 copies Snapshot. Consultez la documentation ONTAP pour plus d'informations sur"définition de la politique de suppression des instantanés" .
Workload Security n'est pas en mesure de prendre des instantanés.	Assurez-vous que le rôle utilisé pour créer des instantanés dispose du lien : https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [droits appropriés attribués]. Assurez-vous que *csrole* est créé avec les droits d'accès appropriés pour prendre des instantanés : security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Les instantanés échouent pour les alertes plus anciennes sur les SVM qui ont été supprimées de Workload Security, puis rajoutées. Pour les nouvelles alertes qui se produisent après le nouvel ajout de SVM, des instantanés sont pris.	C'est un scénario rare. Si vous rencontrez ce problème, connectez-vous à ONTAP et prenez manuellement les instantanés des alertes les plus anciennes.
Dans la page *Détails de l'alerte*, le message d'erreur « La dernière tentative a échoué » s'affiche sous le bouton *Prendre un instantané*. Le survol de l'erreur affiche « La commande d'appel de l'API a expiré pour le collecteur de données avec l'ID ».	Cela peut se produire lorsqu'un collecteur de données est ajouté à Workload Security via SVM Management IP, si le LIF du SVM est à l'état *désactivé* dans ONTAP. Activez le LIF particulier dans ONTAP et déclenchez *Prendre un instantané manuellement* à partir de Workload Security. L'action Snapshot réussira alors.

criminalistique

Forensic - Toutes les activités

La page Toutes les activités vous aide à comprendre les actions effectuées sur les entités dans l'environnement Workload Security.

Examen de toutes les données d'activité

Cliquez sur **Forensics > Forensics d'activité** et cliquez sur l'onglet **Toutes les activités** pour accéder à la page Toutes les activités. Cette page fournit un aperçu des activités de votre locataire, en mettant en évidence les informations suivantes :

- Un graphique montrant *l'historique des activités* (basé sur la plage horaire globale sélectionnée)

  Vous pouvez zoomer sur le graphique en faisant glisser un rectangle dans le graphique. La page entière sera chargée pour afficher la plage horaire zoomée. Lors d'un zoom avant, un bouton s'affiche qui permet à l'utilisateur de dézoomer.

- Une liste des données *Toutes les activités*.
- Un groupe par liste déroulante offrira la possibilité de regrouper l'activité par utilisateurs, dossiers, type d'entité, etc.
- Un bouton de chemin commun sera disponible au-dessus du tableau, en cliquant dessus, nous pourrons accéder à un panneau coulissant avec les détails du chemin de l'entité.

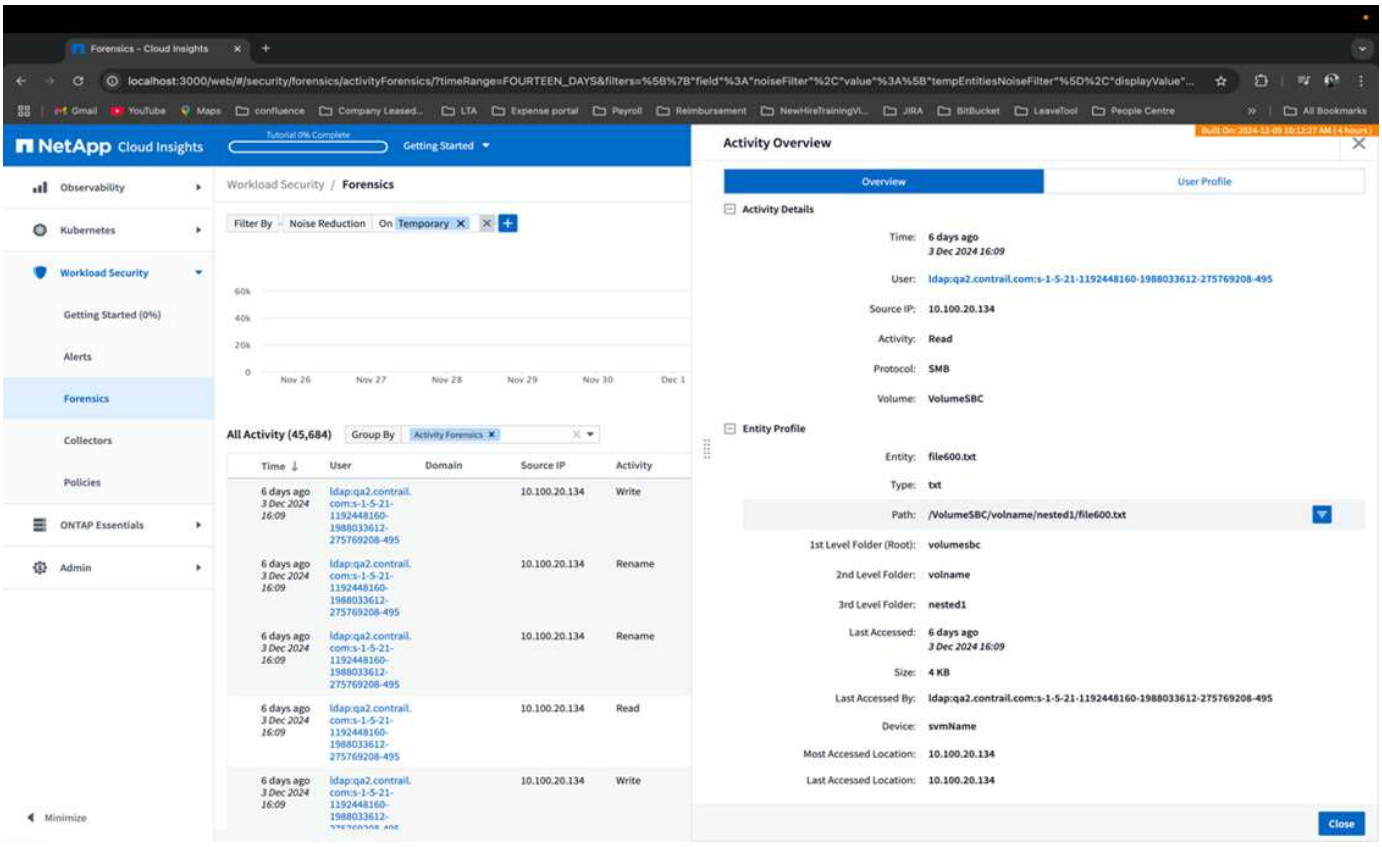
Le tableau **Toutes les activités** affiche les informations suivantes. Notez que toutes ces colonnes ne sont pas affichées par défaut. Vous pouvez sélectionner les colonnes à afficher en cliquant sur l'icône « engrenage ».

- L'**heure** à laquelle une entité a été consultée, y compris l'année, le mois, le jour et l'heure du dernier accès.
- L'**utilisateur** qui a accédé à l'entité avec un lien vers le"Informations utilisateur" comme un panneau coulissant.
- L'**activité** effectuée par l'utilisateur. Les types pris en charge sont :
  - **Modifier la propriété du groupe** - La propriété du groupe du fichier ou du dossier est modifiée. Pour plus de détails sur la propriété du groupe, veuillez consulter"ce lien."
  - **Changer de propriétaire** - La propriété du fichier ou du dossier est transférée à un autre utilisateur.
  - **Modifier l'autorisation** - L'autorisation du fichier ou du dossier est modifiée.
  - **Créer** - Créer un fichier ou un dossier.
  - **Supprimer** - Supprimer le fichier ou le dossier. Si un dossier est supprimé, les événements *delete* sont obtenus pour tous les fichiers de ce dossier et de ses sous-dossiers.
  - **Lecture** - Le fichier est lu.
  - **Lire les métadonnées** - Uniquement lors de l'activation de l'option de surveillance des dossiers. Sera généré lors de l'ouverture d'un dossier sous Windows ou de l'exécution de « ls » dans un dossier sous Linux.
  - **Renommer** - Renommer le fichier ou le dossier.
  - **Écriture** - Les données sont écrites dans un fichier.
  - **Écrire des métadonnées** - Les métadonnées du fichier sont écrites, par exemple, l'autorisation est modifiée.
  - **Autre changement** - Tout autre événement non décrit ci-dessus. Tous les événements non mappés

sont mappés au type d'activité « Autre changement ». Applicable aux fichiers et dossiers.

- Le **Chemin** est le chemin d'*entité*. Il doit s'agir soit du chemin d'entité exact (par exemple, "*/home/userX/nested1/nested2/abc.txt*") OU de la partie répertoire du chemin pour la recherche récursive (par exemple, "*/home/userX/nested1/nested2/*"). REMARQUE : les modèles de chemin d'expression régulière (par exemple, *nested*) ne sont PAS autorisés ici. Alternativement, des filtres de niveau de dossier de chemin individuel, comme mentionné ci-dessous, peuvent également être spécifiés pour le filtrage de chemin.
- Le **dossier de 1er niveau (racine)** est le répertoire racine du chemin d'entité en minuscules.
- Le **dossier de 2e niveau** est le répertoire de deuxième niveau du chemin d'entité en minuscules.
- Le **dossier de 3e niveau** est le répertoire de troisième niveau du chemin d'entité en minuscules.
- Le **dossier de 4e niveau** est le répertoire de quatrième niveau du chemin d'entité en minuscules.
- Le **Type d'entité**, y compris l'extension d'entité (c'est-à-dire de fichier) (.doc, .docx, .tmp, etc.).
- L'**Appareil** où résident les entités.
- Le **Protocole** utilisé pour récupérer les événements.
- Le **chemin d'origine** utilisé pour les événements de renommage lorsque le fichier d'origine a été renommé. Cette colonne n'est pas visible dans le tableau par défaut. Utilisez le sélecteur de colonne pour ajouter cette colonne au tableau.
- Le **Volume** où résident les entités. Cette colonne n'est pas visible dans le tableau par défaut. Utilisez le sélecteur de colonne pour ajouter cette colonne au tableau.
- Le **Nom de l'entité** est le dernier composant du chemin de l'entité ; pour le type d'entité tel que fichier, il s'agit du nom du fichier.

La sélection d'une ligne de tableau ouvre un panneau coulissant avec le profil utilisateur dans un onglet et l'aperçu de l'activité et de l'entité dans un autre onglet.



La méthode *Group by* par défaut est *Activity forensics*. Si vous sélectionnez une méthode *Group By* différente (par exemple, Type d'entité), la table *Group By* de l'entité s'affiche. Si aucune sélection n'est effectuée, *Grouper par* **tout** est affiché.

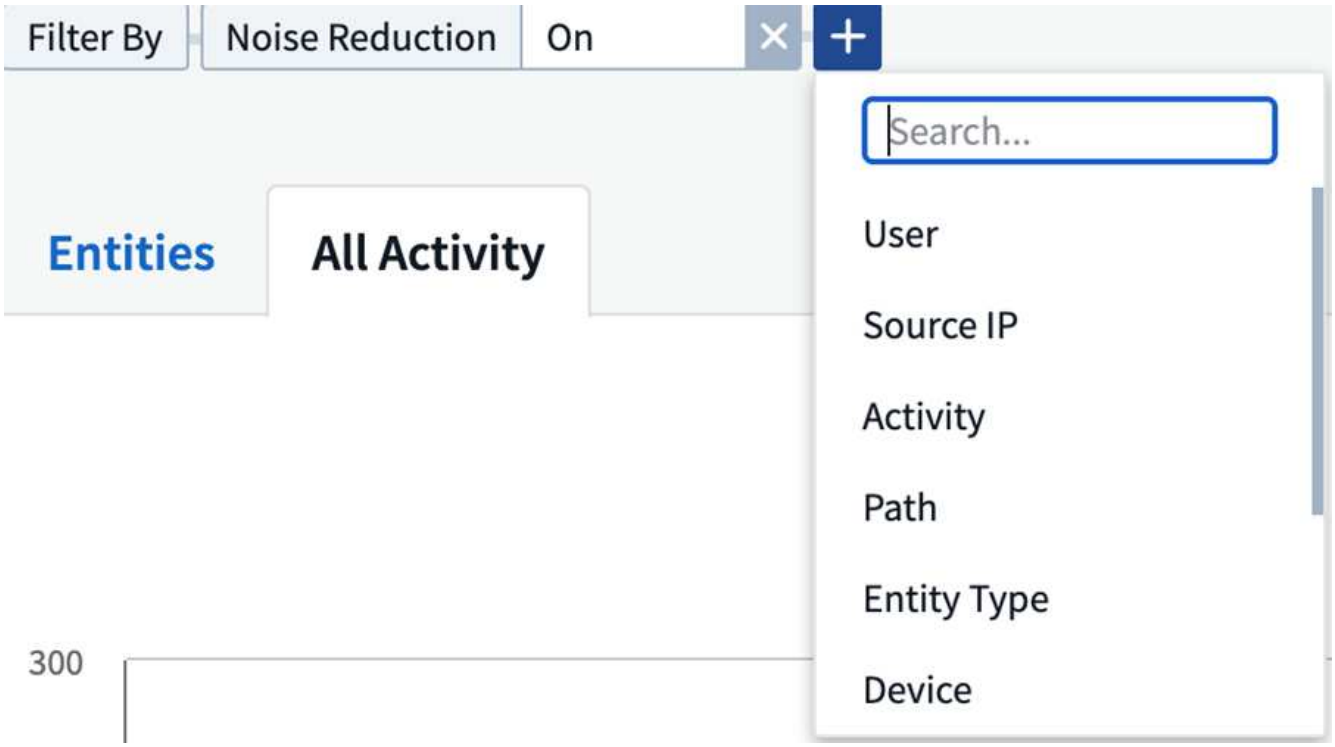
- Le nombre d'activités est affiché sous forme de lien hypertexte ; la sélection de cette option ajoutera le groupe sélectionné en tant que filtre. Le tableau d'activité sera mis à jour en fonction de ce filtre.
- Notez que si vous modifiez le filtre, modifiez la plage horaire ou actualisez l'écran, vous ne pourrez pas revenir aux résultats filtrés sans redéfinir le filtre.
- Veuillez noter que lorsque le nom de l'entité est sélectionné comme filtre, la liste déroulante Grouper par sera désactivée ; de plus, lorsque l'utilisateur est déjà sur l'écran Grouper par, le nom de l'entité comme filtre sera désactivé.

Filtrage des données d'historique des activités médico-légales

Il existe deux méthodes que vous pouvez utiliser pour filtrer les données.

- Le filtre peut être ajouté à partir du panneau coulissant. La valeur est ajoutée aux filtres appropriés dans la liste supérieure *Filtrer par*.
- Filtrer les données en saisissant dans le champ *Filtrer par* :

  Sélectionnez le filtre approprié dans le widget supérieur « Filtrer par » en cliquant sur le bouton **[+]** :



  Entrez le texte de recherche

  Appuyez sur Entrée ou cliquez en dehors de la zone de filtre pour appliquer le filtre.

Vous pouvez filtrer les données d'activité médico-légale selon les champs suivants :

- Le type **Activité**.
- **Protocole** pour récupérer les activités spécifiques au protocole.

- **Nom d'utilisateur** de l'utilisateur effectuant l'activité. Vous devez fournir le nom d'utilisateur exact à filtrer. La recherche avec un nom d'utilisateur partiel ou un nom d'utilisateur partiel préfixé ou suffixé par « * » ne fonctionnera pas.
- **Réduction du bruit** pour filtrer les fichiers créés au cours des 2 dernières heures par l'utilisateur. Il est également utilisé pour filtrer les fichiers temporaires (par exemple, les fichiers .tmp) auxquels l'utilisateur accède.
- **Domaine** de l'utilisateur effectuant l'activité. Vous devez fournir le **domaine exact** à filtrer. La recherche d'un domaine partiel, ou d'un domaine partiel préfixé ou suffixé par un caractère générique ('*'), ne fonctionnera pas. *None* peut être spécifié pour rechercher un domaine manquant.

Les champs suivants sont soumis à des règles de filtrage spéciales :

- **Type d'entité**, utilisant l'extension d'entité (fichier) - il est préférable de spécifier le type d'entité exact entre guillemets. Par exemple *"txt"*.
- **Chemin** de l'entité - Il doit s'agir soit du chemin exact de l'entité (par exemple, "*/home/userX/nested1/nested2/abc.txt*"), soit de la partie du répertoire du chemin pour la recherche récursive (par exemple, "*/home/userX/nested1/nested2/*"). REMARQUE : les modèles de chemin d'expression régulière (par exemple, *nested*) ne sont PAS autorisés ici. Les filtres de chemin de répertoire (chaîne de chemin se terminant par /) jusqu'à 4 répertoires de profondeur sont recommandés pour des résultats plus rapides. Par exemple, "*/home/userX/nested1/nested2/*". Voir le tableau ci-dessous pour plus de détails.
- Dossier de 1er niveau (racine) - répertoire racine du chemin d'entité comme filtres. Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors home OU « home » peut être utilisé.
- Dossier de 2e niveau - Répertoire de 2e niveau des filtres de chemin d'entité. Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors userX OU « userX » peut être utilisé.
- Dossier de 3e niveau – Répertoire de 3e niveau des filtres de chemin d'entité.
- Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors nested1 OU « nested1 » peut être utilisé.
- Dossier de 4e niveau - Répertoire Répertoire de 4e niveau des filtres de chemin d'entité. Par exemple, si le chemin d'accès de l'entité est /home/userX/nested1/nested2/, alors nested2 OU « nested2 » peut être utilisé.
- **Utilisateur** effectuant l'activité - il est préférable de spécifier l'utilisateur exact entre guillemets. Par exemple, *"Administrateur"*.
- **Appareil** (SVM) où résident les entités
- **Volume** où résident les entités
- Le **chemin d'origine** utilisé pour les événements de renommage lorsque le fichier d'origine a été renommé.
- **IP source** à partir de laquelle l'entité a été accédée.
  - Vous pouvez utiliser les caractères génériques * et ?. Par exemple : 10.0.0.**, 10.0?.0.10, 10.10**
  - Si une correspondance exacte est requise, vous devez fournir une adresse IP source valide entre guillemets, par exemple « 10.1.1.1 ». Les adresses IP incomplètes avec des guillemets doubles tels que « 10.1.1. », « 10.1..* », etc. ne fonctionneront pas.
- Le **Nom de l'entité** - le nom de fichier du chemin de l'entité en tant que filtres. Par exemple, si le chemin de l'entité est /home/userX/nested1/testfile.txt, le nom de l'entité est testfile.txt. Veuillez noter qu'il est recommandé de spécifier le nom exact du fichier entre guillemets ; essayez d'éviter les recherches avec caractères génériques. Par exemple, « testfile.txt ». Notez également que ce filtre de nom d'entité est recommandé pour les plages de temps plus courtes (jusqu'à 3 jours).

Les champs précédents sont soumis aux conditions suivantes lors du filtrage :

- La valeur exacte doit être entre guillemets : Exemple : « searchtext »
- Les chaînes génériques ne doivent contenir aucun guillemet : Exemple : searchtext, *searchtext*, filtrera toutes les chaînes contenant « searchtext ».
- Chaîne avec un préfixe, exemple : searchtext*, recherchera toutes les chaînes commençant par « searchtext ».

Veuillez noter que tous les champs de filtre sont sensibles à la casse. Par exemple : si le filtre appliqué est de type Entité avec une valeur comme « searchtext », il renverra des résultats avec un type Entité comme « searchtext », « SearchText », « SEARCHTEXT »

Exemples de filtres d'analyse médico-légale des activités :

Expression de filtre appliquée par l'utilisateur	Résultat attendu	Évaluation des performances	Commentaire
Chemin = "/home/userX/nested1/nested2/"	Recherche récursive de tous les fichiers et dossiers sous un répertoire donné	Rapide	Les recherches dans les répertoires jusqu'à 4 répertoires seront rapides.
Chemin = "/home/userX/nested1/"	Recherche récursive de tous les fichiers et dossiers sous un répertoire donné	Rapide	Les recherches dans les répertoires jusqu'à 4 répertoires seront rapides.
Chemin = "/home/userX/nested1/test"	Correspondance exacte où la valeur du chemin correspond à /home/userX/nested1/test	Ralentissez	La recherche exacte sera plus lente à effectuer que les recherches dans l'annuaire.
Chemin = "/home/userX/nested1/nested2/nested3/"	Recherche récursive de tous les fichiers et dossiers sous un répertoire donné	Ralentissez	Les recherches dans plus de 4 répertoires sont plus lentes.
Tout autre filtre non basé sur le chemin. Il est recommandé que les filtres de type d'utilisateur et d'entité soient entre guillemets, par exemple : Utilisateur = Administrateur ; Type d'entité = txt ;		Rapide	
Nom de l'entité = "test.log"	Correspondance exacte où le nom du fichier est test.log	Rapide	Comme c'est une correspondance exacte
Nom de l'entité = *test.log	Noms de fichiers se terminant par test.log	Lent	En raison du caractère générique, cela peut être lent.

Expression de filtre appliquée par l'utilisateur	Résultat attendu	Évaluation des performances	Commentaire
Nom de l'entité = test*.log	Les noms de fichiers commencent par test et se terminent par .log	Lent	En raison du caractère générique, cela peut être lent.
Nom de l'entité = test.lo	Noms de fichiers commençant par test.lo Par exemple : il correspondra à test.log, test.log.1, test.log1	Ralentissez	En raison du caractère générique à la fin, cela peut être lent.
Nom de l'entité = test	Noms de fichiers commençant par test	Le plus lent	En raison du caractère générique à la fin et de la valeur plus générique utilisée, cela peut être plus lent.

NOTE:

1. Le nombre d'activités affiché à côté de l'icône Toutes les activités est arrondi à 30 minutes lorsque la plage horaire sélectionnée s'étend sur plus de 3 jours. Par exemple, une plage horaire du *1er septembre 10h15 au 7 septembre 10h15* affichera le nombre d'activités du 1er septembre 10h00 au 7 septembre 10h30.
2. De même, les mesures de comptage affichées dans le graphique de l'historique des activités sont arrondies à 30 minutes lorsque la plage de temps sélectionnée s'étend sur plus de 3 jours.

Tri des données d'historique des activités médico-légales

Vous pouvez trier les données de l'historique des activités par *Heure, Utilisateur, IP source, Activité, _, _Type d'entité*, Dossier de 1er niveau (Racine), Dossier de 2e niveau, Dossier de 3e niveau et Dossier de 4e niveau. Par défaut, le tableau est trié par ordre décroissant *Time*, ce qui signifie que les données les plus récentes seront affichées en premier. Le tri est désactivé pour les champs *Device* et *Protocol*.

Guide de l'utilisateur pour les exportations asynchrones

Aperçu

La fonctionnalité Exportations asynchrones de Storage Workload Security est conçue pour gérer les exportations de données volumineuses.

Guide étape par étape : Exportation de données avec des exportations asynchrones

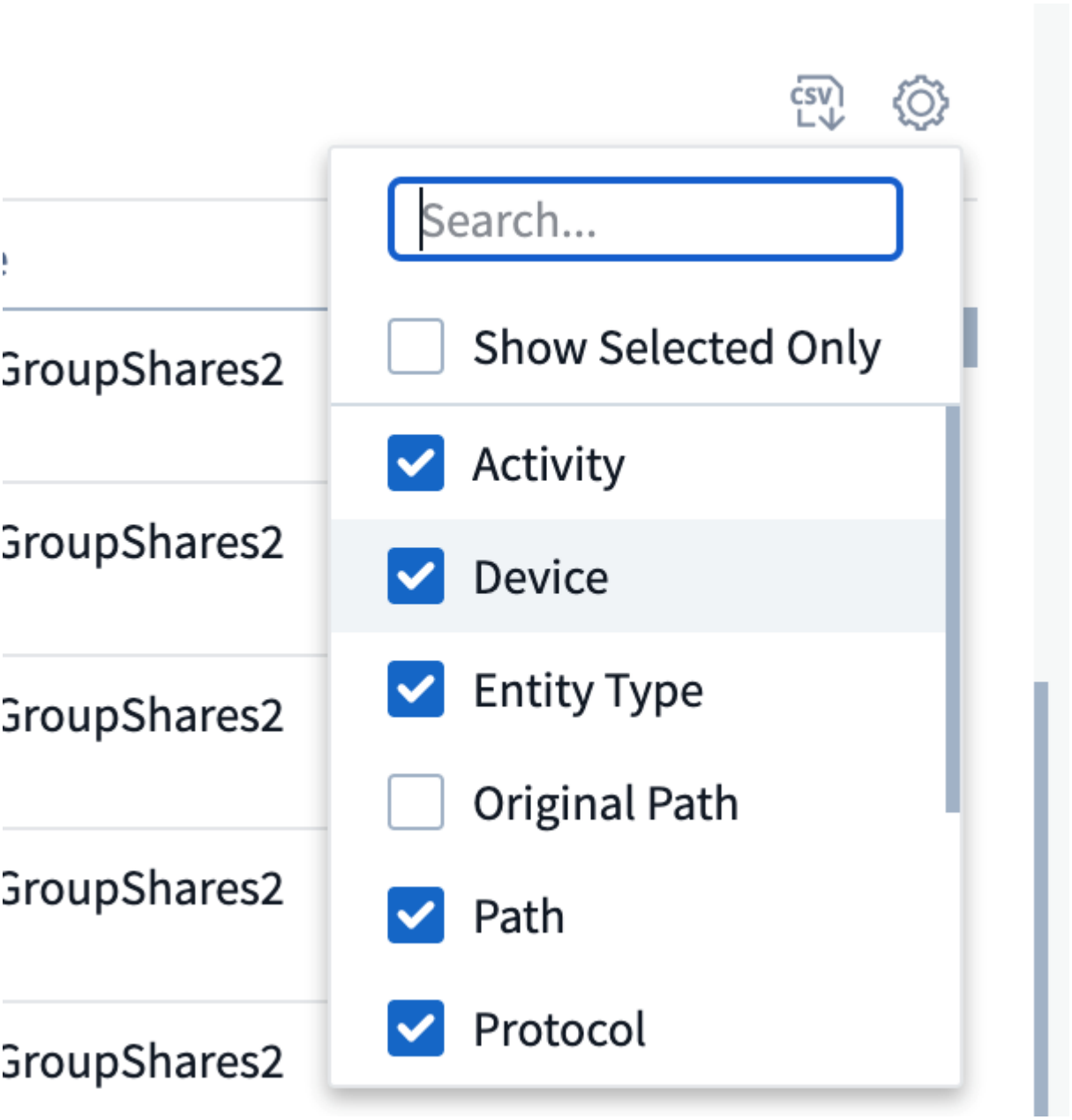
1. **Lancer l'exportation** : Sélectionnez la durée et les filtres souhaités pour l'exportation et cliquez sur le bouton Exporter.
2. **Attendez que l'exportation soit terminée** : Le temps de traitement peut varier de quelques minutes à quelques heures. Vous devrez peut-être actualiser la page d'analyse médico-légale plusieurs fois. Une fois le travail d'exportation terminé, le bouton « Télécharger le dernier fichier CSV d'exportation » sera activé.
3. **Télécharger** : Cliquez sur le bouton « Télécharger le dernier fichier d'exportation créé » pour obtenir les données exportées au format .zip. Ces données seront disponibles au téléchargement jusqu'à ce que l'utilisateur lance une autre exportation asynchrone ou que 3 jours se soient écoulés, selon la première éventualité. Le bouton restera activé jusqu'à ce qu'une autre exportation asynchrone soit lancée.

4. **Limites**:
    - Le nombre de téléchargements asynchrones est actuellement limité à 1 par utilisateur pour chaque tableau d'activités et d'analyse des activités et à 3 par locataire.
    - Les données exportées sont limitées à un maximum de 1 million d'enregistrements pour la table Activités ; tandis que pour Grouper par, la limite est d'un demi-million d'enregistrements.

Un exemple de script permettant d'extraire des données médico-légales via l'API est présent dans */opt/netapp/cloudsecure/agent/export-script/* sur l'agent. Consultez le fichier readme à cet endroit pour plus de détails sur le script.

Sélection de colonnes pour toutes les activités

Le tableau *Toutes les activités* affiche les colonnes sélectionnées par défaut. Pour ajouter, supprimer ou modifier les colonnes, cliquez sur l'icône d'engrenage à droite du tableau et sélectionnez dans la liste des colonnes disponibles.



Conservation de l'historique des activités

L'historique des activités est conservé pendant 13 mois pour les environnements Workload Security actifs.

Applicabilité des filtres dans la page médico-légale

Filtre	Ce qu'il fait	Exemple	Applicable à ces filtres	Non applicable pour ces filtres	Résultat
* (Astérisque)	vous permet de rechercher tout ce que vous voulez	Auto*03172022 Si le texte de recherche contient un trait d'union ou un trait de soulignement, indiquez l'expression entre parenthèses. Par exemple, (svm*) pour rechercher svm-123	Utilisateur, type d'entité, périphérique, volume, chemin d'accès d'origine, dossier de premier niveau, dossier de deuxième niveau, dossier de troisième niveau, dossier de quatrième niveau, nom d'entité, adresse IP source		Renvoie toutes les ressources commençant par « Auto » et se terminant par « 03172022 »
? (point d'interrogation)	vous permet de rechercher un nombre spécifique de caractères	AutoSabotageUser1_03172022 ?	Utilisateur, Type d'entité, Appareil, Volume, Dossier de 1er niveau, Dossier de 2e niveau, Dossier de 3e niveau, Dossier de 4e niveau, Nom de l'entité, IP source		renvoie AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225, etc.
OU	vous permet de spécifier plusieurs entités	AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022	Utilisateur, domaine, type d'entité, chemin d'origine, nom d'entité, adresse IP source		renvoie l'un des éléments suivants : AutoSabotageUser1_03172022 OU AutoRansomUser4_03162022

Filtre	Ce qu'il fait	Exemple	Applicable à ces filtres	Non applicable pour ces filtres	Résultat
PAS	vous permet d'exclure du texte des résultats de recherche	NOT AutoRansomUser4_03162022	Utilisateur, domaine, type d'entité, chemin d'accès d'origine, dossier de premier niveau, dossier de deuxième niveau, dossier de troisième niveau, dossier de quatrième niveau, nom d'entité, adresse IP source	Appareil	renvoie tout ce qui ne commence pas par « AutoRansomUser4_03162022 »
Aucune	recherche les valeurs NULL dans tous les champs	Aucune	Domaine		renvoie les résultats lorsque le champ cible est vide

Recherche de chemin

Les résultats de recherche avec et sans / seront différents

"/AutoDir1/AutoFile03242022"	Seule la recherche exacte fonctionne ; renvoie toutes les activités avec un chemin exact comme /AutoDir1/AutoFile03242022 (insensible à la casse)
"/AutoDir1/ "	Fonctionne ; renvoie toutes les activités avec un répertoire de 1er niveau correspondant à AutoDir1 (insensible à la casse)
"/AutoDir1/AutoFile03242022/"	Fonctionne ; renvoie toutes les activités avec un répertoire de 1er niveau correspondant à AutoDir1 et un répertoire de 2e niveau correspondant à AutoFile03242022 (insensible à la casse)
/AutoDir1/AutoFile03242022 OU /AutoDir1/AutoFile03242022	Ça ne marche pas
PAS /AutoDir1/AutoFile03242022	Ça ne marche pas
PAS /AutoDir1	Ça ne marche pas
NON /AutoFile03242022	Ça ne marche pas
*	Ça ne marche pas

Modifications de l'activité de l'utilisateur SVM racine local

Si un utilisateur SVM racine local effectue une activité, l'adresse IP du client sur lequel le partage NFS est monté est désormais prise en compte dans le nom d'utilisateur, qui sera affiché sous la forme root@<adresse-ip-du-client> dans les pages d'activité médico-légale et d'activité utilisateur.

Par exemple:

- Si SVM-1 est surveillé par Workload Security et que l'utilisateur root de ce SVM monte le partage sur un client avec l'adresse IP 10.197.12.40, le nom d'utilisateur affiché dans la page d'activité médico-légale sera *root@10.197.12.40*.
- Si le même SVM-1 est monté sur un autre client avec l'adresse IP 10.197.12.41, le nom d'utilisateur affiché dans la page d'activité médico-légale sera *root@10.197.12.41*.

*• Ceci est fait pour séparer l'activité de l'utilisateur root NFS par adresse IP. Auparavant, toute l'activité était considérée comme effectuée uniquement par l'utilisateur *root*, sans distinction d'IP.

Dépannage

Problème	Essayez ceci
Dans le tableau « Toutes les activités », sous la colonne « Utilisateur », le nom d'utilisateur est affiché comme suit : « ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817 » ou « ldap:default:80038003 »	Les raisons possibles pourraient être : 1. Aucun collecteur d'annuaire utilisateur n'a encore été configuré. Pour en ajouter un, accédez à **Sécurité de la charge de travail > Collecteurs > Collecteurs d'annuaires utilisateurs** et cliquez sur **+Collecteur d'annuaires utilisateurs**. Choisissez *Active Directory* ou *LDAP Directory Server*. 2. Un collecteur d'annuaires utilisateurs a été configuré, mais il s'est arrêté ou est dans un état d'erreur. Veuillez vous rendre dans **Collecteurs > Collecteurs du répertoire utilisateur** et vérifier le statut. Reportez-vous à la"Dépannage du collecteur d'annuaires utilisateurs" section de la documentation pour des conseils de dépannage. Après une configuration correcte, le nom sera automatiquement résolu dans les 24 heures. Si le problème n'est toujours pas résolu, vérifiez si vous avez ajouté le bon collecteur de données utilisateur. Assurez-vous que l'utilisateur fait bien partie du serveur d'annuaire Active Directory/LDAP ajouté.
Certains événements NFS ne sont pas visibles dans l'interface utilisateur.	Vérifiez les points suivants : 1. Un collecteur d'annuaires utilisateurs pour le serveur AD avec des attributs POSIX définis doit être exécuté avec l'attribut unixid activé à partir de l'interface utilisateur. 2. Tout utilisateur effectuant un accès NFS doit être visible lors d'une recherche dans la page utilisateur de l'interface utilisateur 3. Les événements bruts (événements pour lesquels l'utilisateur n'est pas encore découvert) ne sont pas pris en charge pour NFS 4. L'accès anonyme à l'exportation NFS ne sera pas surveillé. 5. Assurez-vous que la version NFS utilisée est la version 4.1 ou inférieure. (Notez que NFS 4.1 est pris en charge avec ONTAP 9.15 ou version ultérieure.)

Après avoir tapé quelques lettres contenant un caractère générique comme un astérisque (*) dans les filtres des pages Forensics *All Activity* ou *Entities*, les pages se chargent très lentement.	Un astérisque (*) dans la chaîne de recherche recherche tout. Cependant, les chaînes génériques de début telles que *<*searchTerm*>* ou *<*searchTerm*>** entraîneront une requête lente. Pour obtenir de meilleures performances, utilisez plutôt des chaînes de préfixe, au format <*searchTerm*>* (en d'autres termes, ajoutez l'astérisque (*) *après* un terme de recherche). Exemple : utilisez la chaîne *testvolume**, plutôt que **testvolume* ou **test*volume*. Utilisez une recherche de répertoire pour voir toutes les activités sous un dossier donné de manière récursive (recherche hiérarchique). Par exemple, "/path1/path2/path3/" répertoriera toutes les activités de manière récursive sous /path1/path2/path3. Vous pouvez également utiliser l'option « Ajouter au filtre » sous l'onglet Toutes les activités.
Je rencontre une erreur « La demande a échoué avec le code d'état 500/503 » lors de l'utilisation d'un filtre de chemin.	Essayez d'utiliser une plage de dates plus petite pour filtrer les enregistrements.
L'interface utilisateur médico-légale charge les données lentement lors de l'utilisation du filtre *path*.	Les filtres de chemin de répertoire (chaîne de chemin se terminant par /) jusqu'à 4 répertoires de profondeur sont recommandés pour des résultats plus rapides. Par exemple, si le chemin du répertoire est /Aaa/Bbb/Ccc/Ddd, essayez de rechercher « /Aaa/Bbb/Ccc/Ddd/ » pour charger les données plus rapidement.
L'interface utilisateur médico-légale charge les données lentement et rencontre des échecs lors de l'utilisation du filtre de nom d'entité.	Veuillez essayer avec des plages de temps plus petites et avec une recherche de valeur exacte avec des guillemets doubles. Par exemple, si entityPath est "/home/userX/nested1/nested2/nested3/testfile.txt", essayez avec "testfile.txt" comme filtre de nom d'entité.

Présentation de l'utilisateur forensique

Les informations relatives à chaque utilisateur sont fournies dans la vue d'ensemble de l'utilisateur. Utilisez ces vues pour comprendre les caractéristiques des utilisateurs, les entités associées et les activités récentes.

Profil utilisateur

Les informations du profil utilisateur incluent les coordonnées et l'emplacement de l'utilisateur. Le profil fournit les informations suivantes :

- Nom de l'utilisateur
- Adresse e-mail de l'utilisateur
- Gestionnaire des utilisateurs
- Contact téléphonique de l'utilisateur
- Localisation de l'utilisateur

Comportement de l’utilisateur

Les informations sur le comportement de l’utilisateur identifient les activités et opérations récentes effectuées par l’utilisateur. Ces informations comprennent :

- Activité récente
  - Emplacement du dernier accès
  - Graphique d’activité
  - Alertes
- Opérations des sept derniers jours
  - Nombre d’opérations

Intervalle de rafraîchissement

La liste des utilisateurs est actualisée toutes les 12 heures.

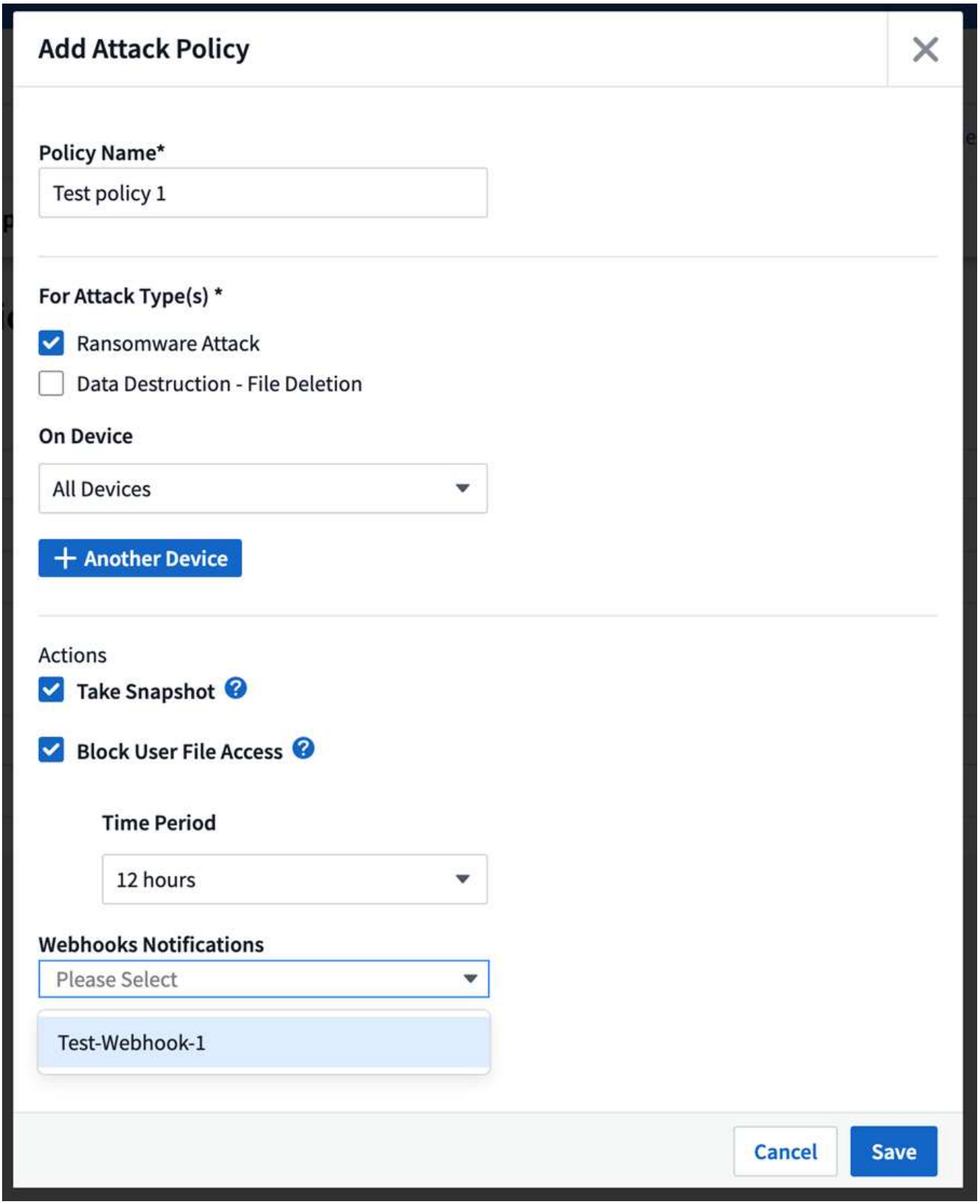
Politique de conservation

Si elle n’est pas actualisée à nouveau, la liste des utilisateurs est conservée pendant 13 mois. Après 13 mois, les données seront supprimées. Si votre environnement Workload Security est supprimé, toutes les données associées à l’environnement sont supprimées.

Politiques de réponse automatisées

Les politiques de réponse déclenchent des actions telles que la prise d’un instantané ou la restriction de l’accès des utilisateurs en cas d’attaque ou de comportement anormal des utilisateurs.

Vous pouvez définir des politiques sur des appareils spécifiques ou sur tous les appareils. Pour définir une politique de réponse, sélectionnez **Admin > Politiques de réponse automatisées** et cliquez sur le bouton **+Politique** approprié. Vous pouvez créer des politiques pour les attaques ou pour les avertissements.



Vous devez enregistrer la politique sous un nom unique.

Pour désactiver une action de réponse automatisée (par exemple, Prendre un instantané), décochez simplement l'action et enregistrez la politique.

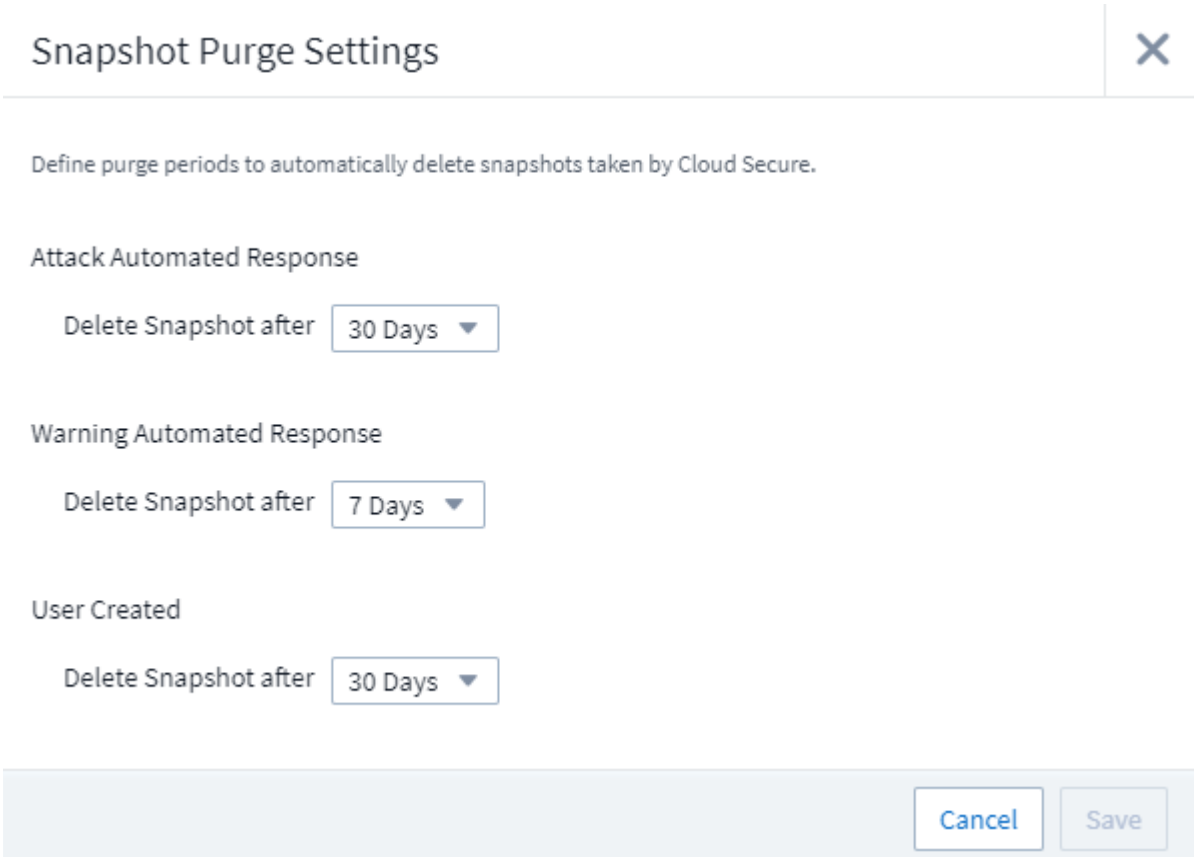
Lorsqu'une alerte est déclenchée sur les appareils spécifiés (ou tous les appareils, s'ils sont sélectionnés), la politique de réponse automatisée prend un instantané de vos données. Vous pouvez voir l'état de l'instantané sur le"Page de détails de l'alerte" .

Voir le"Restreindre l'accès des utilisateurs" page pour plus de détails sur la restriction de l'accès des utilisateurs par IP.

Vous pouvez attacher un ou plusieurs webhooks à une politique pour être averti lorsqu'une alerte est créée et qu'une action est entreprise. Il est recommandé de ne pas ajouter plus de 10 webhooks à une politique. Gardez à l'esprit que si une politique est suspendue, les notifications de webhook ne seront pas déclenchées.

Vous pouvez modifier ou suspendre une politique de réponse automatisée en choisissant l'option dans le menu déroulant de la politique.

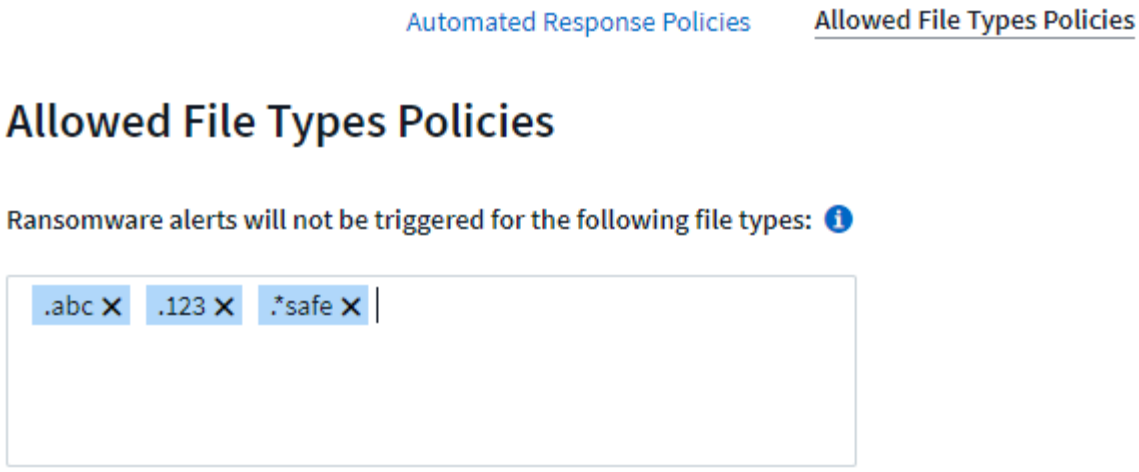
Workload Security supprimera automatiquement les instantanés une fois par jour en fonction des paramètres de purge des instantanés.



Politiques relatives aux types de fichiers autorisés

Si une attaque par falsification de fichier est détectée pour une extension de fichier connue et que des alertes sont générées sur l'écran Alertes, cette extension de fichier peut être ajoutée à une liste de types de fichiers autorisés afin d'éviter les alertes inutiles.

Accédez à **Sécurité de la charge de travail > Politiques** et accédez à l'onglet *Politiques de type de fichier autorisées*.



Une fois ajouté à la liste des *types de fichiers autorisés*, aucune alerte d'attaque par falsification de fichiers ne sera générée pour ce type de fichier autorisé. Notez que la politique relative aux *Types de fichiers autorisés* ne s'applique qu'à la détection des falsifications de fichiers.

Par exemple, si un fichier nommé *test.txt* est renommé en *test.txt.abc* et que Workload Security détecte une attaque par falsification de fichier en raison de l'extension *.abc*, l'extension *.abc* peut être ajoutée à la liste des *types de fichiers autorisés*. Après leur ajout à la liste, les attaques par falsification de fichiers ne seront plus générées contre les fichiers ayant l'extension *.abc*.

Les types de fichiers autorisés peuvent être des correspondances exactes (par exemple, « .abc ») ou des expressions (par exemple, « .**type », « .type** » ou « **type** »). Les expressions de types « .a*c », « .p*f » ne sont pas prises en charge.

Intégration avec la protection autonome contre les ransomwares ONTAP

La fonction de protection autonome ONTAP utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter et signaler de manière proactive toute activité anormale dans les fichiers pouvant indiquer des attaques malveillantes ou des modifications de données non autorisées.

Des détails supplémentaires et des exigences de licence concernant ARP peuvent être trouvés"ici" .

Workload Security s'intègre à ONTAP pour recevoir les événements ARP et fournir une couche d'analyse supplémentaire et de réponses automatiques.

Workload Security reçoit les événements ARP d' ONTAP et entreprend les actions suivantes :

1. Met en corrélation les événements de chiffrement de volume avec l'activité de l'utilisateur pour identifier qui cause les dommages.
2. Implémente des politiques de réponse automatique (si définies)
3. Fournit des capacités d'investigation médico-légale :
   - Permettre aux clients de mener des enquêtes sur les violations de données.
   - Identifiez les fichiers affectés, ce qui permet une récupération plus rapide et la réalisation d'enquêtes sur les violations de données.

Prérequis

1. Version minimale ONTAP : 9.11.1
2. Volumes compatibles ARP. Vous trouverez des détails sur l'activation d'ARP."ici" . ARP doit être activé via OnCommand System Manager. Workload Security ne peut pas activer ARP.
3. Le collecteur de sécurité de la charge de travail doit être ajouté via l'adresse IP du cluster.
4. Les informations d'identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne. En d'autres termes, les informations d'identification au niveau du cluster doivent être utilisées lors de l'ajout du SVM.

Autorisations utilisateur requises

Si vous utilisez les informations d'identification d'administration de cluster, aucune nouvelle autorisation n'est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour accorder des autorisations à Workload Security afin de collecter des informations liées à ARP à partir d' ONTAP.

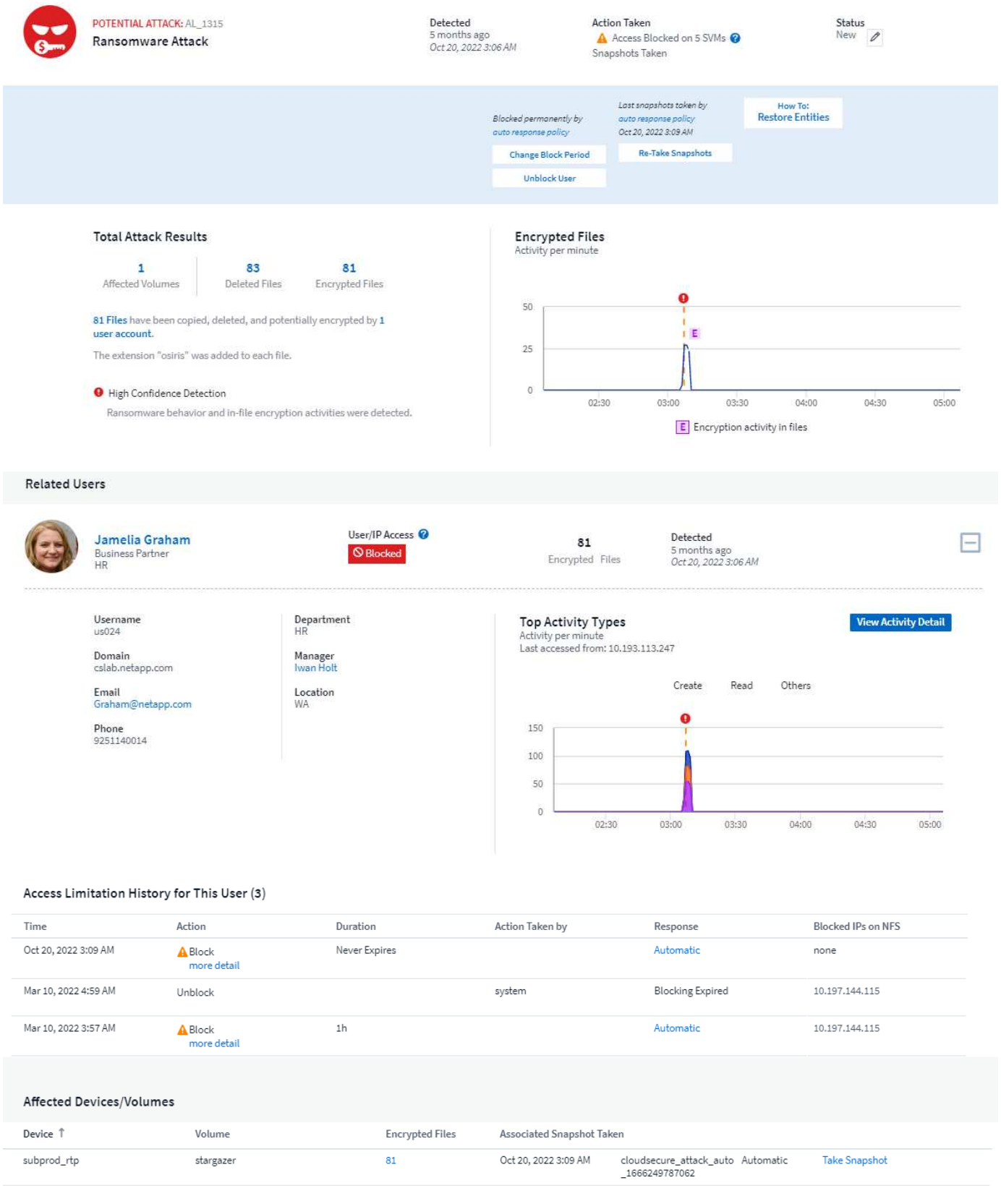
Pour *csuser* avec les informations d'identification du cluster, procédez comme suit à partir de la ligne de commande ONTAP :

```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

En savoir plus sur la configuration d'autres"Autorisations ONTAP" .

Exemple d'alerte

Un exemple d'alerte générée en raison d'un événement ARP est présenté ci-dessous :



Un bandeau de confiance élevée indique que l'attaque a démontré un comportement de falsification de fichiers ainsi que des activités de chiffrement de fichiers. Le graphique des fichiers chiffrés indique l'horodatage auquel l'activité de chiffrement du volume a été détectée par la solution ARP.

Limites

Dans le cas où un SVM n'est pas surveillé par Workload Security, mais qu'il existe des événements ARP générés par ONTAP, les événements seront toujours reçus et affichés par Workload Security. Cependant, les informations médico-légales liées à l'alerte, ainsi que la cartographie des utilisateurs, ne seront pas capturées ou affichées.

Dépannage

Les problèmes connus et leurs résolutions sont décrits dans le tableau suivant.

Problème:	Résolution:
Les alertes par e-mail sont reçues 24 heures après la détection d'une attaque. Dans l'interface utilisateur, les alertes sont affichées 24 heures avant la réception des e-mails par Data Infrastructure Insights Workload Security.	Lorsque ONTAP envoie l'événement *Ransomware Detected* à Data Infrastructure Insights Workload Security (c'est-à-dire Workload Security), l'e-mail est envoyé. L'événement contient une liste d'attaques et leurs horodatages. L'interface utilisateur de sécurité de la charge de travail affiche l'horodatage d'alerte du premier fichier attaqué. ONTAP envoie l'événement *Ransomware Detected* à Data Infrastructure Insights lorsqu'un certain nombre de fichiers sont codés. Par conséquent, il peut y avoir une différence entre le moment où l'alerte s'affiche dans l'interface utilisateur et le moment où l'e-mail est envoyé.

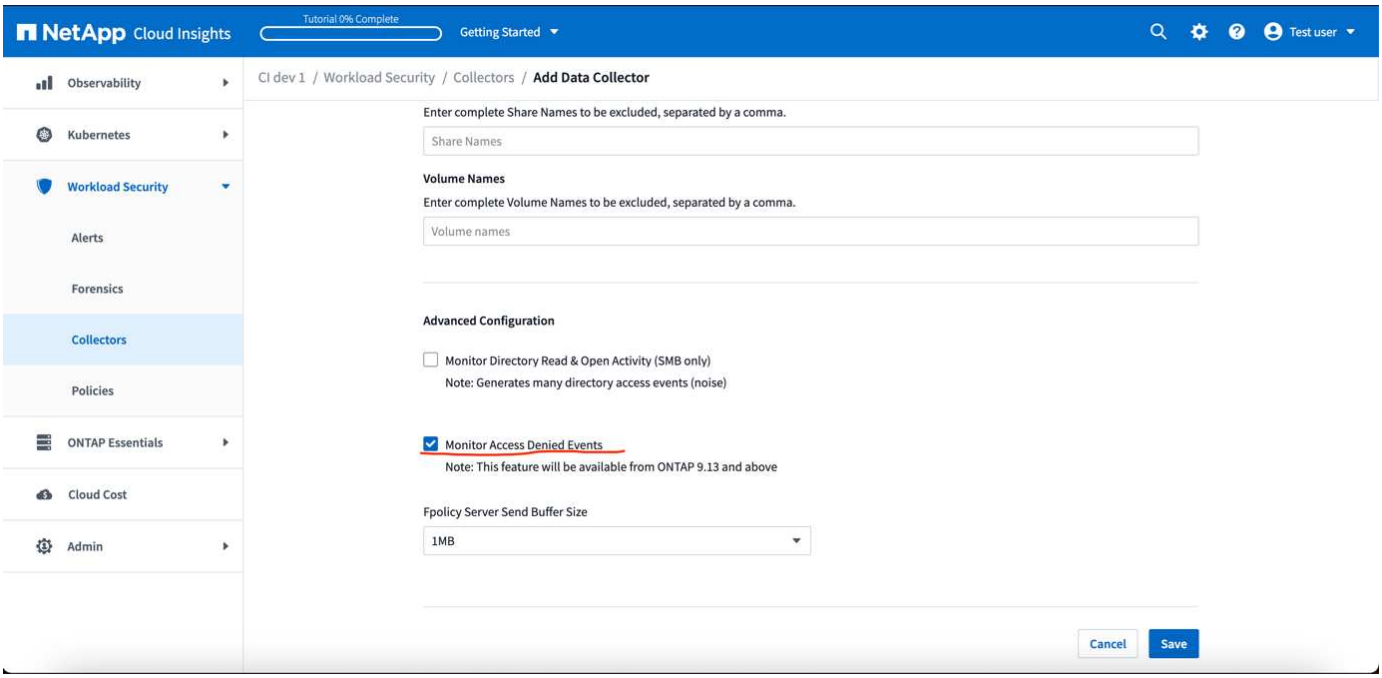
Intégration avec ONTAP Accès refusé

La fonctionnalité ONTAP Access Denied utilise l'analyse de la charge de travail dans les environnements NAS (NFS et SMB) pour détecter et avertir de manière proactive des opérations de fichiers ayant échoué (c'est-à-dire un utilisateur essayant d'effectuer une opération pour laquelle il n'a pas l'autorisation). Ces notifications d'échec d'opération de fichier, en particulier dans les cas de défaillances liées à la sécurité, contribueront davantage à bloquer les attaques internes à un stade précoce.

Data Infrastructure Insights Workload Security s'intègre à ONTAP pour recevoir les événements d'accès refusé et fournir une couche d'analyse et de réponse automatique supplémentaire.

Prérequis

- Version minimale ONTAP : 9.13.0.
- Un administrateur de sécurité de la charge de travail doit activer la fonctionnalité Accès refusé lors de l'ajout d'un nouveau collecteur ou de la modification d'un collecteur existant, en sélectionnant la case à cocher *Surveiller les événements d'accès refusé* sous Configuration avancée.



Autorisations utilisateur requises

Si le collecteur de données est ajouté à l'aide des informations d'identification d'administration du cluster, aucune nouvelle autorisation n'est nécessaire.

Si le collecteur est ajouté à l'aide d'un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l'utilisateur, suivez les étapes ci-dessous pour donner à Workload Security l'autorisation nécessaire pour s'inscrire aux événements d'accès refusé avec ONTAP.

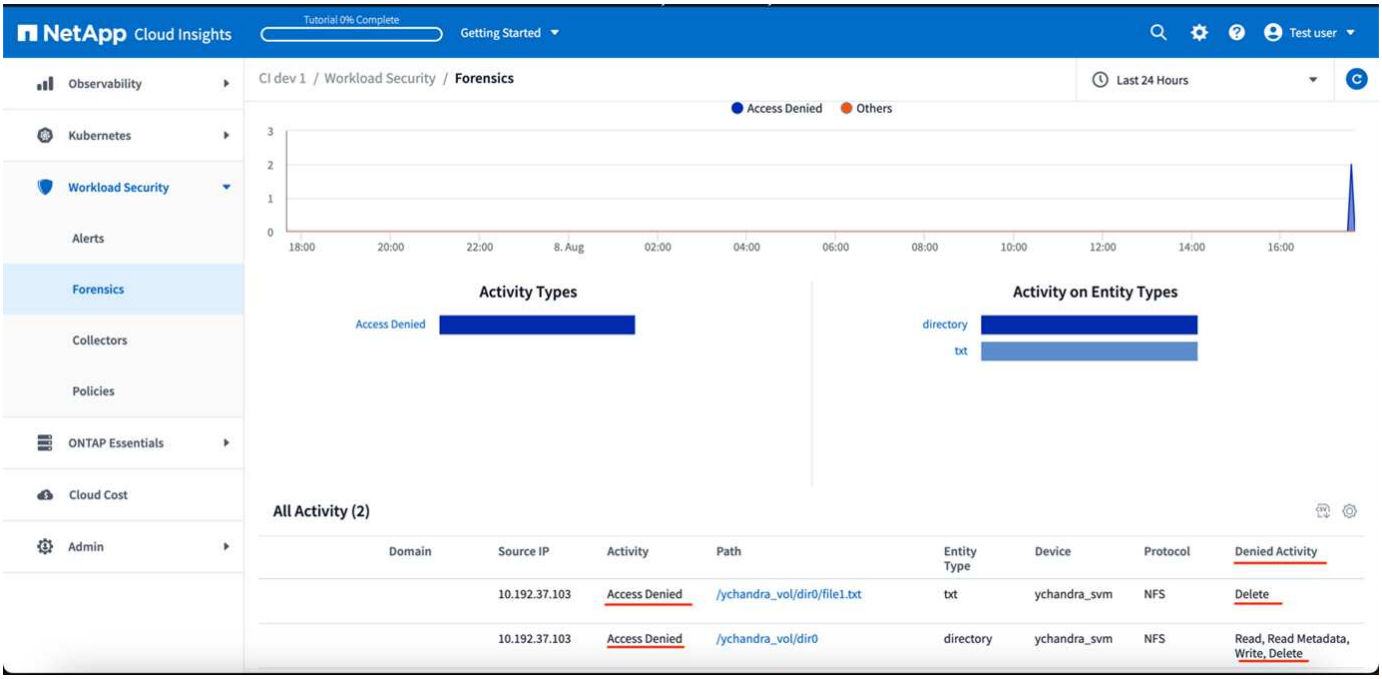
Pour csuser avec les informations d'identification *cluster*, exécutez les commandes suivantes à partir de la ligne de commande ONTAP . Notez que cette autorisation existe peut-être déjà.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Pour csuser avec les informations d'identification _SVM_, exécutez les
commandes suivantes à partir de la ligne de commande ONTAP .  Notez que
cette autorisation existe peut-être déjà.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
En savoir plus sur la configuration
d'autreslink:task_add_collector_svm.html["Autorisations ONTAP"] .
```

Événements d'accès refusé

Une fois les événements acquis à partir du système ONTAP , la page Forensics de sécurité de la charge de travail affichera les événements d'accès refusé. En plus des informations affichées, vous pouvez afficher les autorisations utilisateur manquantes pour une opération particulière en ajoutant la colonne *Activité souhaitée* au tableau à partir de l'icône d'engrenage.



Bloquer l’accès des utilisateurs pour stopper les attaques

Interrompez immédiatement les attaques détectées en bloquant l’accès des utilisateurs compromis afin d’empêcher toute nouvelle atteinte aux données ou toute exfiltration de données. La sécurité des charges de travail permet à la fois le blocage automatique via des politiques de réponse automatisées et l’intervention manuelle à partir des pages d’alerte ou de détails de l’utilisateur, vous offrant ainsi un contrôle flexible sur votre réponse de sécurité. Les restrictions d’accès s’appliquent automatiquement à tous les volumes de stockage surveillés et sont limitées dans le temps pour la restauration automatique.

L’utilisateur est directement bloqué pour SMB et l’adresse IP des machines hôtes à l’origine de l’attaque sera bloquée pour NFS. Ces adresses IP de machine ne pourront pas accéder aux machines virtuelles de stockage (SVM) surveillées par Workload Security.

Par exemple, disons que Workload Security gère 10 SVM et que la stratégie de réponse automatique est configurée pour quatre de ces SVM. Si l’attaque provient de l’une des quatre SVM, l’accès de l’utilisateur sera bloqué dans les 10 SVM. Un instantané est toujours pris sur le SVM d’origine.

S’il existe quatre SVM, dont une configurée pour SMB, une configurée pour NFS et les deux autres configurées pour NFS et SMB, toutes les SVM seront bloquées si l’attaque provient de l’une des quatre SVM.

Conditions préalables au blocage de l’accès utilisateur

Les informations d’identification au niveau du cluster sont nécessaires pour que cette fonctionnalité fonctionne.

Si vous utilisez les informations d’identification d’administration de cluster, aucune nouvelle autorisation n’est nécessaire.

Si vous utilisez un utilisateur personnalisé (par exemple, *csuser*) avec des autorisations accordées à l’utilisateur, suivez les étapes ci-dessous pour accorder des autorisations à Workload Security afin de bloquer

l'utilisateur.

Pour csuser avec les informations d'identification du cluster, procédez comme suit à partir de la ligne de commande ONTAP :

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Assurez-vous de consulter la section Autorisations du"Configuration du collecteur de données ONTAP SVM" page aussi.

Comment activer la fonctionnalité ?

- Dans Sécurité de la charge de travail, accédez à **Sécurité de la charge de travail > Politiques > Politiques de réponse automatisée**. Choisissez **+Politique d'attaque**.
- Sélectionnez (cochez) *Bloquer l'accès aux fichiers utilisateur*.

Comment configurer le blocage automatique de l'accès des utilisateurs ?

- Créez une nouvelle politique d'attaque ou modifiez une politique d'attaque existante.
- Sélectionnez les SVM sur lesquelles la politique d'attaque doit être surveillée.
- Cochez la case « Bloquer l'accès aux fichiers des utilisateurs ». La fonctionnalité sera activée lorsque cette option est sélectionnée.
- Sous « Période », sélectionnez la durée jusqu'à laquelle le blocage doit être appliqué.
- Pour tester le blocage automatique des utilisateurs, vous pouvez simuler une attaque via un"script simulé" .

Comment savoir s'il y a des utilisateurs bloqués dans le système ?

- Dans la page des listes d'alertes, une bannière en haut de l'écran sera affichée au cas où un utilisateur serait bloqué.
- En cliquant sur la bannière, vous serez redirigé vers la page « Utilisateurs », où la liste des utilisateurs bloqués peut être consultée.
- Dans la page « Utilisateurs », il y a une colonne nommée « Accès utilisateur/IP ». Dans cette colonne, l'état actuel du blocage de l'utilisateur sera affiché.

Restreindre et gérer manuellement l'accès des utilisateurs

- Vous pouvez accéder aux détails de l'alerte ou à l'écran des détails de l'utilisateur, puis bloquer ou restaurer manuellement un utilisateur à partir de ces écrans.

Historique des limitations d’accès des utilisateurs

Dans la page des détails de l’alerte et des détails de l’utilisateur, dans le panneau utilisateur, vous pouvez afficher un audit de l’historique des limitations d’accès de l’utilisateur : heure, action (bloquer, débloquer), durée, action entreprise par, manuel/automatique et adresses IP affectées pour NFS.

Comment désactiver la fonctionnalité ?

À tout moment, vous pouvez désactiver la fonctionnalité. S’il y a des utilisateurs restreints dans le système, vous devez d’abord restaurer leur accès.

- Dans Sécurité de la charge de travail, accédez à **Sécurité de la charge de travail > Politiques > Politiques de réponse automatisée**. Choisissez **+Politique d’attaque**.
- Décochez (désélectionnez) *Bloquer l’accès aux fichiers utilisateur*.

La fonctionnalité sera masquée sur toutes les pages.

Restaurer manuellement les adresses IP pour NFS

Utilisez les étapes suivantes pour restaurer manuellement toutes les adresses IP d' ONTAP si votre essai de Workload Security expire ou si l’agent/collecteur est en panne.

1. Répertoriez toutes les politiques d’exportation sur un SVM.

```
contrail-qa-fas8020:> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Supprimez les règles de toutes les stratégies sur la SVM qui ont « cloudsecure_rule » comme correspondance client en spécifiant son RuleIndex respectif. La règle de sécurité de la charge de travail sera généralement à 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Assurez-vous que la règle de sécurité de la charge de travail est
supprimée (étape facultative pour confirmer).
```

```
contrail-qa-fas8020:*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Restaurer manuellement les utilisateurs pour SMB

Utilisez les étapes suivantes pour restaurer manuellement tous les utilisateurs d' ONTAP si votre essai de Workload Security expire ou si l'agent/collecteur est en panne.

Vous pouvez obtenir la liste des utilisateurs bloqués dans Workload Security à partir de la page de la liste des utilisateurs.

1. Connectez-vous au cluster ONTAP (où vous souhaitez débloquer les utilisateurs) avec les informations d'identification *admin* du cluster. (Pour Amazon FSx, connectez-vous avec les informations d'identification FSx).
2. Exécutez la commande suivante pour répertorier tous les utilisateurs bloqués par Workload Security for SMB dans tous les SVM :

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1        -                -                Pattern: CSLAB\\US040
                                           Replacement:
2        -                -                Pattern: CSLAB\\US030
                                           Replacement:
2 entries were displayed.
```

Dans la sortie ci-dessus, 2 utilisateurs ont été bloqués (US030, US040) avec le domaine CSLAB.

1. Une fois que nous avons identifié la position à partir de la sortie ci-dessus, exécutez la commande suivante pour débloquer l'utilisateur :

```
 vserver name-mapping delete -direction win-unix -position <position>
. Confirmez que les utilisateurs sont débloqués en exécutant la
commande :
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Aucune entrée ne doit être affichée pour les utilisateurs précédemment bloqués.

Dépannage

Problème	Essayez ceci
Certains utilisateurs ne sont pas restreints, même s'il y a une attaque.	1. Assurez-vous que le collecteur de données et l'agent pour les SVM sont à l'état *Running*. Workload Security ne pourra pas envoyer de commandes si le collecteur de données et l'agent sont arrêtés. 2. Cela est dû au fait que l'utilisateur a peut-être accédé au stockage à partir d'une machine avec une nouvelle IP qui n'a pas été utilisée auparavant. La restriction s'effectue via l'adresse IP de l'hôte via lequel l'utilisateur accède au stockage. Consultez l'interface utilisateur (Détails de l'alerte > Historique des limitations d'accès pour cet utilisateur > IP affectées) pour obtenir la liste des adresses IP restreintes. Si l'utilisateur accède au stockage à partir d'un hôte dont l'adresse IP est différente des adresses IP restreintes, l'utilisateur pourra toujours accéder au stockage via l'adresse IP non restreinte. Si l'utilisateur tente d'accéder à partir des hôtes dont les adresses IP sont restreintes, le stockage ne sera pas accessible.
Cliquer manuellement sur Restreindre l'accès donne le message « Les adresses IP de cet utilisateur ont déjà été restreintes ».	L'adresse IP à restreindre est déjà restreinte pour un autre utilisateur.
La politique n'a pas pu être modifiée. Motif : non autorisé pour cette commande.	Vérifiez si vous utilisez csuser, les autorisations sont accordées à l'utilisateur comme mentionné ci-dessus.

Problème	Essayez ceci
Le blocage des utilisateurs (adresse IP) pour NFS fonctionne, mais pour SMB / CIFS, je vois un message d'erreur : « La transformation SID en DomainName a échoué. Raison du délai d'attente : le socket n'est pas établi »	Cela peut arriver si *csuser* n'a pas l'autorisation d'exécuter ssh. (Assurez-vous de la connexion au niveau du cluster, puis assurez-vous que l'utilisateur peut exécuter ssh). Le rôle *csuser* nécessite ces autorisations. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Pour *csuser* avec les informations d'identification du cluster, procédez comme suit à partir de la ligne de commande ONTAP : security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all Si *csuser* n'est pas utilisé et si l'utilisateur admin au niveau du cluster est utilisé, assurez-vous que l'utilisateur admin dispose de l'autorisation ssh sur ONTAP.
J'obtiens le message d'erreur *SID translate failed. Raison : 255 : Erreur : échec de la commande : non autorisé pour cette commandeErreur : « access-check » n'est pas une commande reconnue*, alors qu'un utilisateur aurait dû être bloqué.	Cela peut se produire lorsque *csuser* ne dispose pas des autorisations correctes. Voir "Conditions préalables au blocage de l'accès utilisateur" pour plus d'informations. Après avoir appliqué les autorisations, il est recommandé de redémarrer le collecteur de données ONTAP et le collecteur de données de l'annuaire utilisateur. Les commandes d'autorisation requises sont répertoriées ci-dessous. ---- création du rôle de connexion de sécurité -role csrole -cmddirname "règle de politique d'exportation vserver" -access all création du rôle de connexion de sécurité -role csrole -cmddirname set -access all création du rôle de connexion de sécurité -role csrole -cmddirname "session cifs vserver" -access all création du rôle de connexion de sécurité -role csrole -cmddirname "traduction d'authentification de vérification d'accès aux services vserver" -access all création du rôle de connexion de sécurité -role csrole -cmddirname "mappage de noms vserver" -access all ----

Sécurité des charges de travail : simulation de falsification de fichiers

Vous pouvez utiliser les instructions de cette page pour simuler une falsification de fichiers à des fins de test ou de démonstration de la sécurité des charges de travail à l'aide du script de simulation de falsification de fichiers inclus.

Choses à noter avant de commencer

- Le script de simulation de falsification de fichiers fonctionne uniquement sous Linux. Le script de simulation doit également générer des alertes à haute fiabilité dans le cas où l'utilisateur aurait intégré ONTAP ARP à Workload Security.
- Workload Security détectera les événements et les alertes générés avec NFS 4.1 uniquement si la version ONTAP est 9.15 ou supérieure.
- Le script est fourni avec les fichiers d'installation de l'agent Workload Security. Il est disponible sur toute machine sur laquelle un agent Workload Security est installé.
- Vous pouvez exécuter le script sur la machine de l'agent Workload Security elle-même ; il n'est pas nécessaire de préparer une autre machine Linux. Cependant, si vous préférez exécuter le script sur un autre système, copiez simplement le script et exécutez-le là-bas.
- Les utilisateurs peuvent opter pour le script Python ou Shell en fonction de leurs préférences et des exigences système.
- Le script Python nécessite des installations préalables. Si vous ne souhaitez pas utiliser Python, utilisez le script shell.

Directives :

Ce script doit être exécuté sur une SVM contenant un dossier avec un nombre substantiel de fichiers à chiffrer, idéalement 100 ou plus, y compris les fichiers dans les sous-dossiers. Assurez-vous que les fichiers ne sont pas vides.

Pour générer l'alerte, mettez temporairement le collecteur en pause avant la création des données de test. Une fois les fichiers d'échantillon générés, reprenez le collecteur et lancez le processus de cryptage.

Mesures:

Préparez le système :

Tout d'abord, montez le volume cible sur la machine. Vous pouvez monter une exportation NFS ou CIFS.

Pour monter l'exportation NFS sous Linux :

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Ne montez pas la version NFS 4.1 ; elle n'est pas prise en charge par Fpolicy.

Pour monter CIFS sous Linux :

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Activer la protection autonome contre les ransomwares ONTAP (facultatif) :

Si la version de votre cluster ONTAP est 9.11.1 ou supérieure, vous pouvez activer le service ONTAP Ransomware Protection en exécutant la commande suivante sur la console de commande ONTAP .

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Ensuite, configurez un collecteur de données :
```

1. Configurez l'agent Workload Security si ce n'est pas déjà fait.
2. Configurez un collecteur de données SVM si ce n'est pas déjà fait.
3. Assurez-vous que le protocole de montage est sélectionné lors de la configuration du collecteur de données.

Générez les fichiers d'exemple par programmation :

Avant de créer les fichiers, vous devez d'abord arrêter ou"mettre en pause le collecteur de données" traitement.

Avant d'exécuter la simulation, vous devez d'abord ajouter les fichiers à chiffrer. Vous pouvez soit copier manuellement les fichiers à crypter dans le dossier cible, soit utiliser l'un des scripts inclus pour créer les fichiers par programmation. Quelle que soit la méthode utilisée, assurez-vous qu'au moins 100 fichiers sont présents à crypter.

Si vous choisissez de créer les fichiers par programmation, vous pouvez utiliser le Shell ou Python :

Coquille:

1. Connectez-vous à la boîte Agent.
2. Montez un partage NFS ou CIFS depuis la SVM du fichier vers la machine Agent. CD dans ce dossier.
3. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) vers l'emplacement de montage cible.
4. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour créer le dossier et les fichiers du jeu de données de test :

```
 './create_dataset.sh'
. Cela créera 100 fichiers non vides avec différentes extensions dans le
dossier de montage sous un répertoire appelé « test_dataset ».
```

Python:

Script Python Prérequis :

- Installez Python (si ce n'est pas déjà fait).
  - Téléchargez Python 3.5.2 ou supérieur depuis https://www.python.org/ .
  - Pour vérifier l'installation de Python, exécutez `python --version` .
  - Le script Python a été testé sur des versions aussi anciennes que la 3.5.2.
- Installez pip s'il n'est pas déjà installé :

- Téléchargez le script get-pip.py depuis https://bootstrap.pypa.io/ .
- Installer pip en utilisant `python get-pip.py` .
- Vérifiez l'installation de pip avec `pip --version` .

- Bibliothèque PyCryptodome :
  - Le script utilise la bibliothèque PyCryptodome.
  - Installer PyCryptodome avec `pip install pycryptodome` .
  - Confirmez l'installation de PyCryptodome en exécutant `pip show pycryptodome` .

Script de création de fichier Python :

1. Connectez-vous à la boîte Agent.
2. Montez un partage NFS ou CIFS depuis la SVM du fichier vers la machine Agent. CD dans ce dossier.
3. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) vers l'emplacement de montage cible.
4. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour créer le dossier et les fichiers du jeu de données de test :

```
 'python create_dataset.py'
. Cela créera 100 fichiers non vides avec différentes extensions à
l'intérieur du dossier de montage sous un répertoire appelé
« test_dataset »
```

Reprendre le collecteur

Si vous avez mis le collecteur en pause avant de suivre ces étapes, assurez-vous de reprendre le collecteur une fois les fichiers d'exemple créés.

Générez les fichiers d'exemple par programmation :

Avant de créer les fichiers, vous devez d'abord arrêter ou"mettre en pause le collecteur de données" traitement.

Pour générer une alerte de falsification de fichier, vous pouvez exécuter le script inclus qui simulera une alerte de falsification de fichier dans Workload Security.

Coquille:

1. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) vers l'emplacement de montage cible.
2. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour crypter l'ensemble de données de test :

```
 './simulate_attack.sh'
. Cela cryptera les fichiers d'exemple créés sous le répertoire
« test_dataset ».
```

Python:

1. Copiez le script du répertoire d'installation de l'agent (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) vers l'emplacement de montage cible.
2. Veuillez noter que les prérequis Python sont installés conformément à la section Prérequis du script Python
3. Exécutez la commande suivante à l'aide des scripts dans le répertoire monté (par exemple /root/demo) pour crypter l'ensemble de données de test :

```
 'python simulate_attack.py'
. Cela cryptera les fichiers d'exemple créés sous le répertoire
« test_dataset ».
```

Générer une alerte dans Workload Security

Une fois l'exécution du script du simulateur terminée, une alerte s'affichera sur l'interface Web dans quelques minutes.

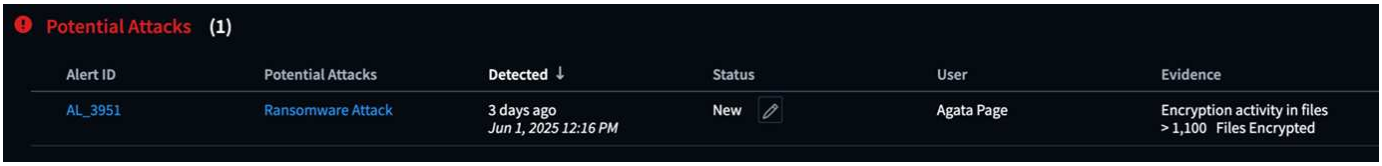
Remarque : si toutes les conditions suivantes sont remplies, une alerte de haute confiance sera générée.

1. Version ONTAP du SVM surveillée supérieure à 9.11.1
2. Protection autonome contre les ransomwares ONTAP configurée
3. Le collecteur de données de sécurité de la charge de travail est ajouté en mode Cluster.

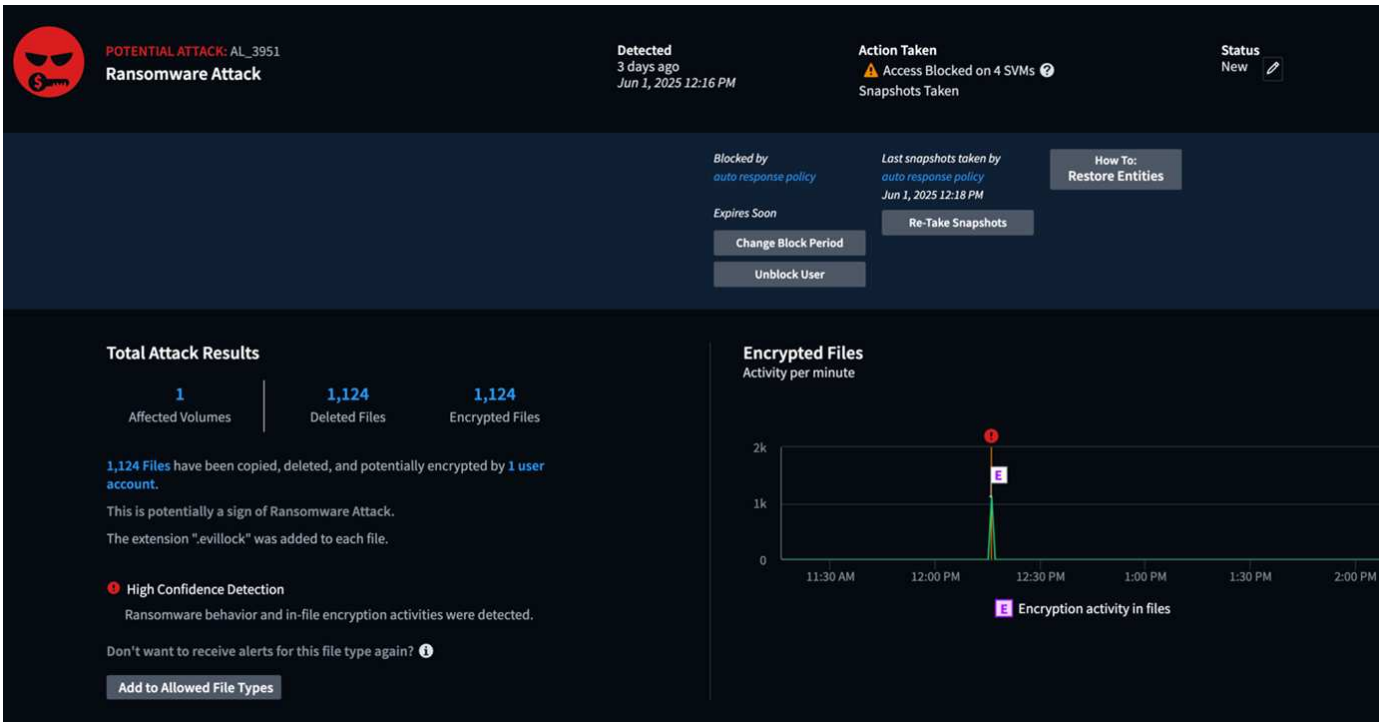
Workload Security détecte les schémas de falsification de fichiers en fonction du comportement de l'utilisateur, tandis ONTAP ARP détecte les activités de falsification de fichiers en fonction des activités de chiffrement dans les fichiers.

Si les conditions sont remplies, Workload Security marque les alertes comme alerte de haute confiance.

Exemple d'alerte de haute confiance sur la page de liste des alertes :



Exemple de détail d'alerte de haute confiance :



Déclenchement de l’alerte plusieurs fois

Workload Security analyse le comportement des utilisateurs et ne génère pas d’alertes en cas d’attaques répétées de falsification de fichiers survenant dans un délai de 24 heures pour un même utilisateur.

Pour générer une nouvelle alerte avec un utilisateur différent, veuillez suivre à nouveau les mêmes étapes (création de données de test puis cryptage des données de test).

Configuration des notifications par e-mail pour les alertes, les avertissements et l’état de santé de l’agent/collecteur de sources de données

Les notifications par e-mail vous permettent de rester informé des attaques potentielles, des alertes de sécurité et des problèmes de santé de l’infrastructure dès leur apparition. Configurez les adresses e-mail des destinataires dans les paramètres Admin > Notifications pour recevoir des alertes en temps réel adaptées aux responsabilités de chaque destinataire.

Alertes et avertissements d’attaque potentielle

Pour envoyer des notifications d’alerte d’attaque potentielle, saisissez les adresses e-mail des destinataires dans la section *Envoyer des alertes d’attaque potentielle*. Des notifications par courrier électronique sont envoyées à la liste des destinataires de l’alerte pour chaque action sur l’alerte.

Pour envoyer des notifications d’avertissement, saisissez les adresses e-mail des destinataires dans la section Envoyer des alertes d’avertissement.

Surveillance de la santé des agents et des collecteurs de données

Vous pouvez surveiller la santé des agents et des sources de données via des notifications.

Afin de recevoir des notifications dans le cas où un agent ou un collecteur de sources de données ne fonctionne pas, saisissez les adresses e-mail des destinataires dans la section *Alertes de santé de la collecte de données*.

Gardez à l'esprit les points suivants :

- Les alertes de santé ne seront envoyées qu'après que l'agent/collecteur aura cessé de signaler pendant au moins une heure.
- Une seule notification par e-mail est envoyée aux destinataires prévus au cours d'une période donnée de 24 heures, même si l'agent ou le collecteur de données est déconnecté pendant une durée plus longue.
- En cas de défaillance d'un Agent, une seule alerte sera envoyée (pas une par collecteur). L'e-mail comprendra une liste de tous les SVM concernés.
- L'échec de la collecte Active Directory est signalé comme un avertissement ; il n'a pas d'incidence sur la détection des menaces.
- La liste de configuration de mise en route inclut désormais une nouvelle phase *Configurer les notifications par e-mail*.

Notifications de mise à niveau de l'agent récepteur et du collecteur de données

- Saisissez les identifiants de messagerie dans les « Alertes de santé de collecte de données ».
- La case à cocher « Activer les notifications de mise à niveau » devient activée.
- Les notifications par e-mail de mise à niveau de l'agent et du collecteur de données sont envoyées aux identifiants de messagerie un jour avant la mise à niveau prévue.

Dépannage

Problème:	Essayez ceci :
Les identifiants de messagerie sont présents dans les « Alertes de santé du collecteur de données », mais je ne reçois pas de notifications.	Les e-mails de notification sont envoyés depuis le domaine NetApp Data Infrastructure Insights , c'est-à-dire depuis *accounts@service.cloudinsights.netapp.com*. Certaines entreprises bloquent les e-mails entrants s'ils proviennent d'un domaine externe. Assurez-vous que les notifications externes des domaines NetApp Data Infrastructure Insights sont sur liste blanche.

Notifications Webhook

Notifications de sécurité de la charge de travail à l'aide de webhooks

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte critiques ou d'avertissement à diverses applications à l'aide d'un canal webhook personnalisé.

De nombreuses applications commerciales prennent en charge les webhooks comme interface d'entrée standard, par exemple : Slack, PagerDuty, Teams et Discord. En prenant en charge un canal webhook

générique et personnalisable, Workload Security peut prendre en charge bon nombre de ces canaux de diffusion. Des informations sur la configuration des webhooks peuvent être trouvées sur les sites Web des applications respectives. Par exemple, Slack fournit"ce guide utile" .

Vous pouvez créer plusieurs canaux webhook, chaque canal ciblant un objectif différent, des applications distinctes, des destinataires différents, etc.

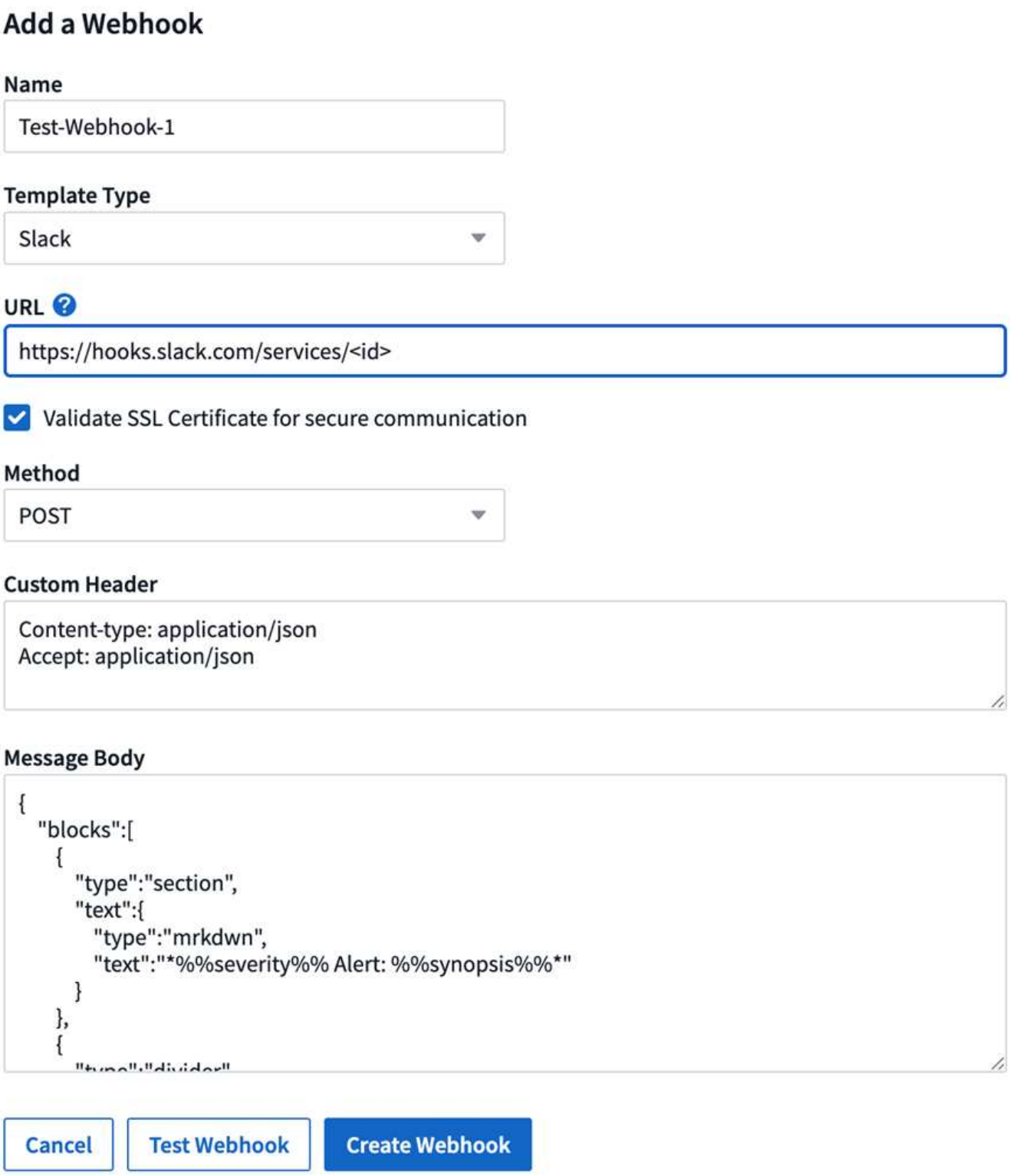
L'instance de canal webhook est composée des éléments suivants

Nom	Description
URL	URL cible du webhook, y compris le préfixe http:// ou https:// ainsi que les paramètres d'URL
Méthode	GET/POST - La valeur par défaut est POST
En-tête personnalisé	Spécifiez ici les en-têtes personnalisés
Corps du message	Mettez le corps de votre message ici
Paramètres d'alerte par défaut	Répertorie les paramètres par défaut du webhook
Paramètres et secrets personnalisés	Les paramètres et secrets personnalisés vous permettent d'ajouter des paramètres uniques et des éléments sécurisés tels que des mots de passe

Créer un webhook

Pour créer un Webhook de sécurité de charge de travail, accédez à Admin > Notifications et sélectionnez l'onglet « Webhooks de sécurité de charge de travail ». L'image suivante montre un exemple d'écran de création de webhook Slack.

Remarque : l'utilisateur doit être un administrateur de Workload Security pour créer et gérer les Webhooks de Workload Security.



- Saisissez les informations appropriées pour chacun des champs et cliquez sur « Enregistrer ».
- Vous pouvez également cliquer sur le bouton « Tester le Webhook » pour tester la connexion. Notez que cela enverra le « Corps du message » (sans substitutions) à l'URL définie selon la méthode sélectionnée.
- Les webhooks SWS comprennent un certain nombre de paramètres par défaut. De plus, vous pouvez créer vos propres paramètres ou secrets personnalisés.

Paramètres : que sont-ils et comment les utiliser ?

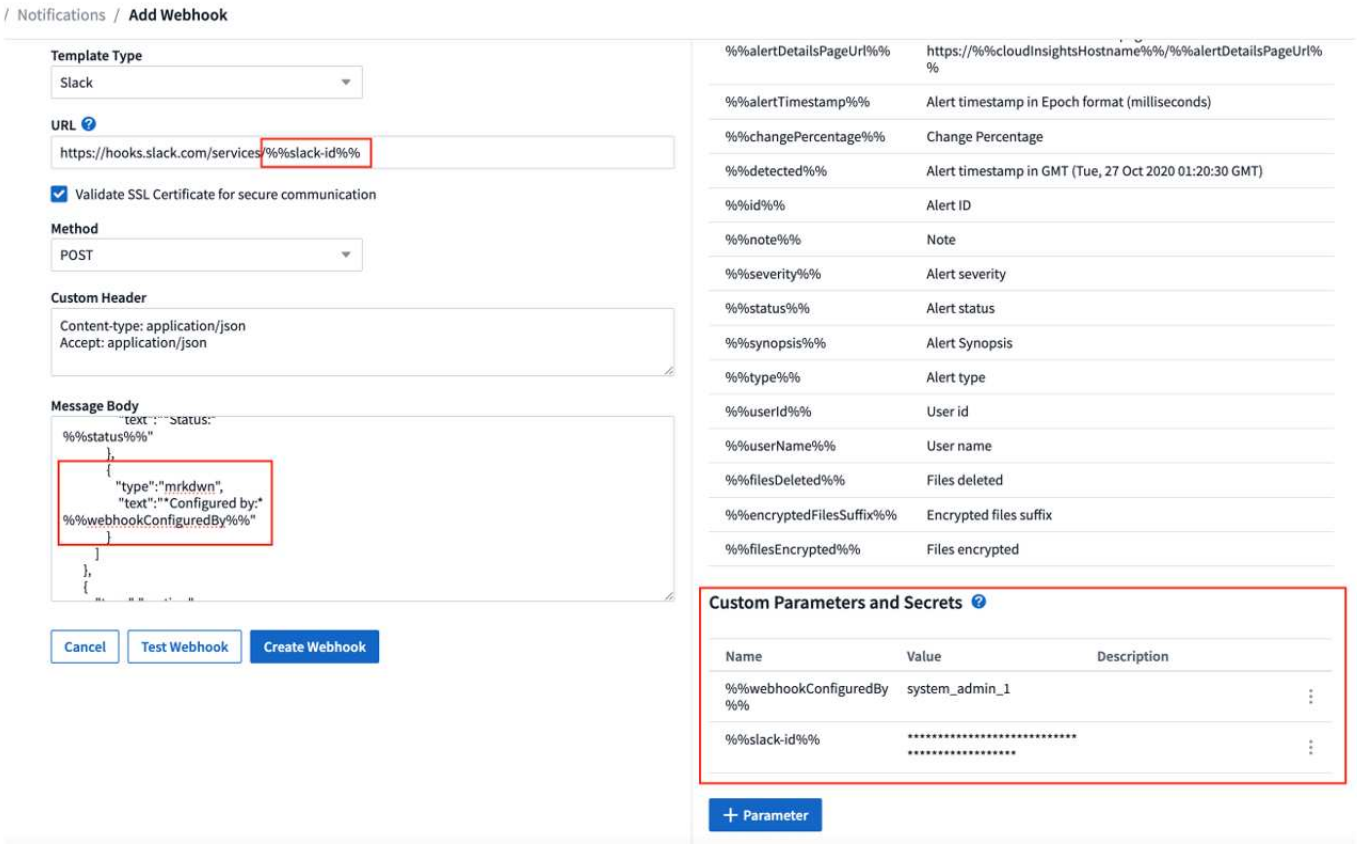
Les paramètres d'alerte sont des valeurs dynamiques renseignées par alerte. Par exemple, le paramètre *%%severity%%* sera remplacé par le type de gravité de l'alerte.

Notez que les substitutions ne sont pas effectuées lorsque vous cliquez sur le bouton « Tester le Webhook » ; le test envoie une charge utile qui affiche les espaces réservés du paramètre (*%%<param-name>%%*) mais ne les remplace pas par des données.

Paramètres et secrets personnalisés

Dans cette section, vous pouvez ajouter tous les paramètres personnalisés et/ou secrets que vous souhaitez. Un paramètre personnalisé ou un secret peut figurer dans l'URL ou le corps du message. Les secrets permettent à l'utilisateur de configurer un paramètre personnalisé sécurisé comme un mot de passe, une clé API, etc.

L'exemple d'image suivant montre comment les paramètres personnalisés sont utilisés dans la création de webhook.



Page de liste des webhooks de sécurité de la charge de travail

Sur la page de liste des Webhooks, les champs Nom, Créé par, Créé le, Statut, Sécurisé et Dernier signalement sont affichés. Remarque : la valeur de la colonne « statut » continuera de changer en fonction du résultat du dernier déclencheur de webhook. Voici quelques exemples de résultats d'état.

Statut	Description
OK	Notification envoyée avec succès.

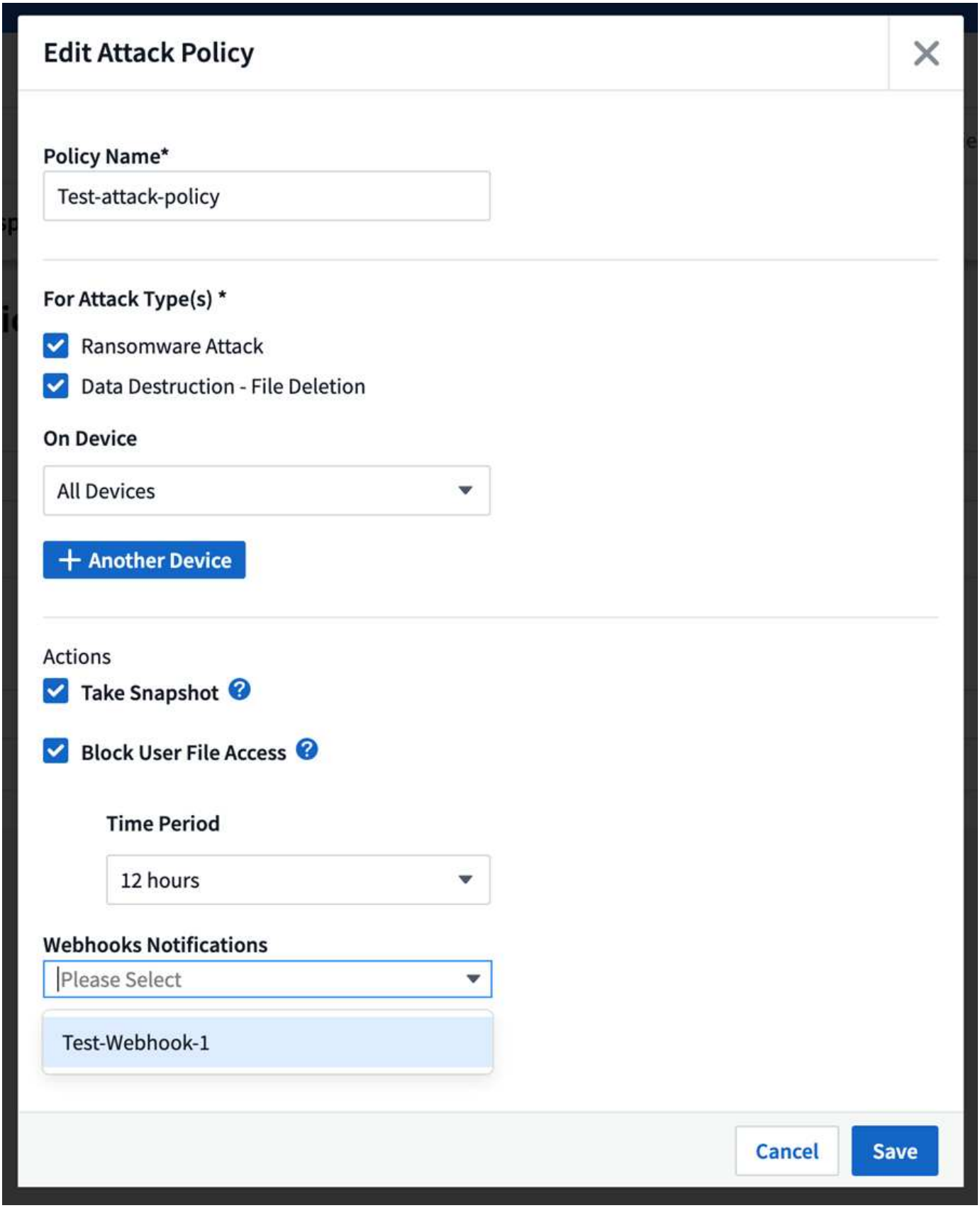
403	Interdit.
404	URL non trouvée.
400	Mauvaise demande. Vous pouvez voir ce statut s'il y a une erreur dans le corps du message, par exemple : • Json mal formaté. • Fourniture d'une valeur non valide pour les clés réservées. Par exemple, PagerDuty accepte uniquement les valeurs critiques/avertissements/erreurs/informations pour « Gravité ». Tout autre résultat peut donner un statut 400. • Erreurs de validation spécifiques à l'application. Par exemple, Slack autorise un maximum de 10 champs dans une section. L'inclusion de plus de 10 peut entraîner un statut 400.
410	La ressource n'est plus disponible

La colonne « Dernier signalement » indique l'heure à laquelle le webhook a été déclenché pour la dernière fois.

À partir de la page de liste des webhooks, les utilisateurs peuvent également modifier/dupliquer/supprimer les webhooks.

Configurer la notification Webhook dans la politique d'alerte

Pour ajouter une notification webhook à une politique d'alerte, accédez à - Sécurité de la charge de travail > Politiques - et sélectionnez une politique existante ou ajoutez une nouvelle politique. Dans la section *Actions* > liste déroulante *Notifications Webhook*, sélectionnez les webhooks requis.



Les notifications Webhook sont liées aux politiques. Lorsque l'attaque (RW/DD/WARN) se produit, l'action configurée (Prendre un instantané / blocage de l'utilisateur) sera effectuée, puis la notification webhook associée sera déclenchée.

Remarque : les notifications par e-mail sont indépendantes des politiques, elles seront déclenchées comme d'habitude.

- Si une politique est suspendue, les notifications webhook ne seront pas déclenchées.
- Plusieurs webhooks peuvent être attachés à une seule politique, mais il est recommandé de ne pas attacher plus de 5 webhooks à une politique.

Exemples de webhooks de sécurité de charge de travail

Webhooks pour"Mou"

Webhooks pour"PagerDuty" Webhooks pour"Équipes" Webhooks pour"Discorde"

Exemple de webhook de sécurité de charge de travail pour Discord

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Discord.

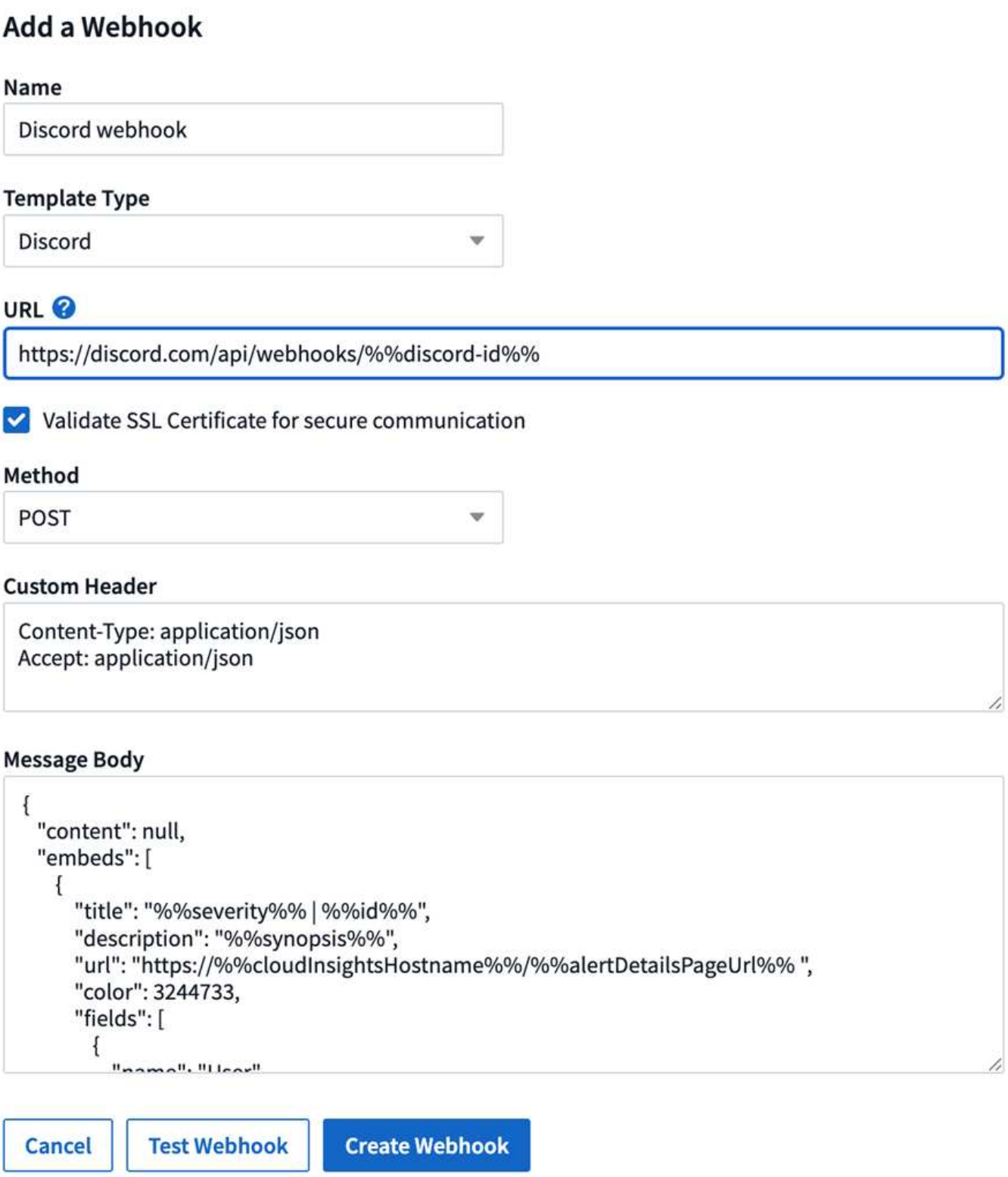
Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation Discord" pour les informations les plus récentes.

Configuration de Discord :

- Dans Discord, sélectionnez le serveur, sous Canaux texte, sélectionnez Modifier le canal (icône en forme d'engrenage)
- Sélectionnez **Intégrations > Afficher les webhooks** et cliquez sur **Nouveau webhook**
- Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook de sécurité de charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Cliquez sur « + Webhook » pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Discord**.
4. Collez l'URL Discord ci-dessus dans le champ *URL*.



Afin de tester le webhook, remplacez temporairement la valeur de l'URL dans le corps du message par n'importe quelle URL valide (telle que *https://netapp.com*), puis cliquez sur le bouton *Tester le Webhook*. Discord exige qu'une URL valide soit fournie pour que la fonctionnalité Test Webhook fonctionne.

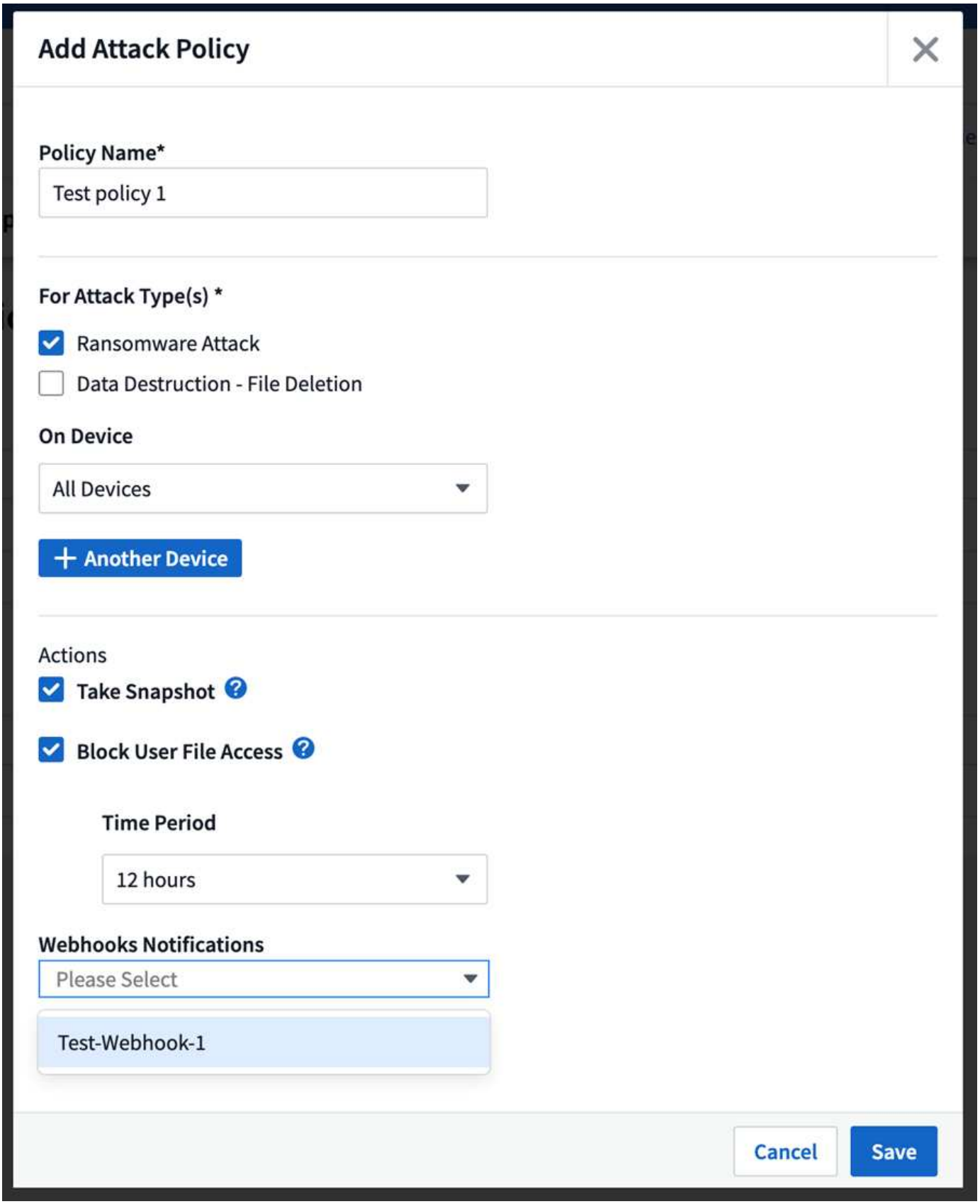
Assurez-vous de réinitialiser le corps du message une fois le test terminé.

Notifications via Webhook

Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Discord requis et enregistrez.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



Exemple de webhook de sécurité de charge de travail pour PagerDuty

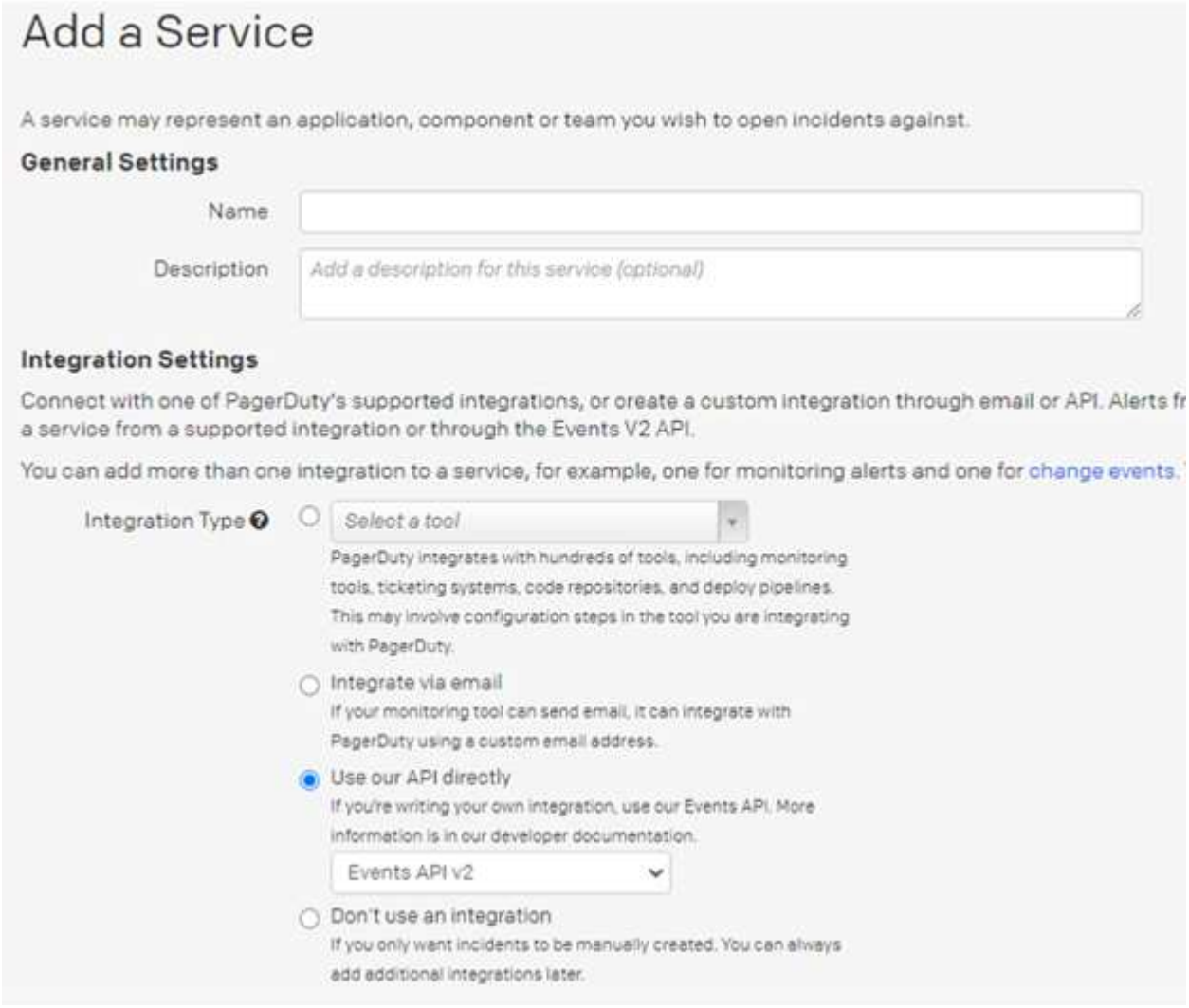
Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de

configuration de webhooks pour PagerDuty.

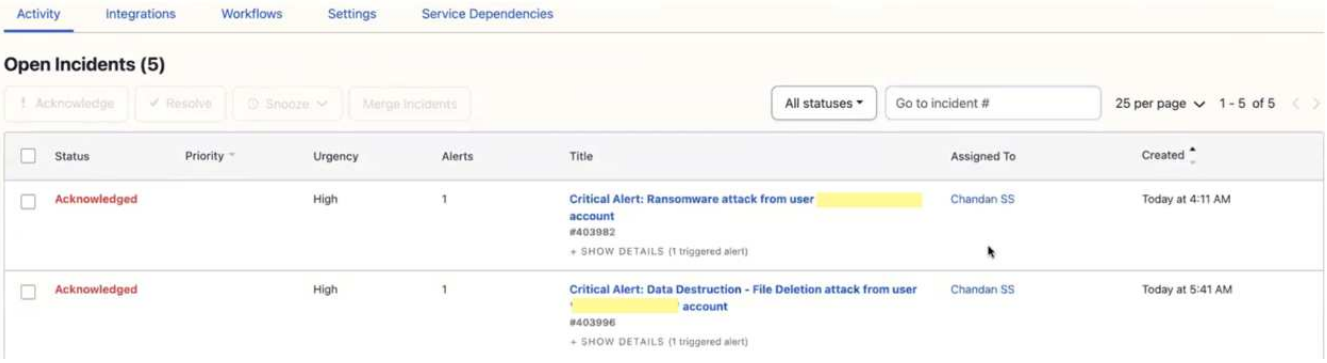
Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation de PagerDuty" pour les informations les plus récentes.

Configuration de PagerDuty :

1. Dans PagerDuty, accédez à **Services > Répertoire des services** et cliquez sur le bouton **+Nouveau service**.
2. Saisissez un *Nom* et sélectionnez *Utiliser directement notre API*. Sélectionnez *Ajouter un service*.

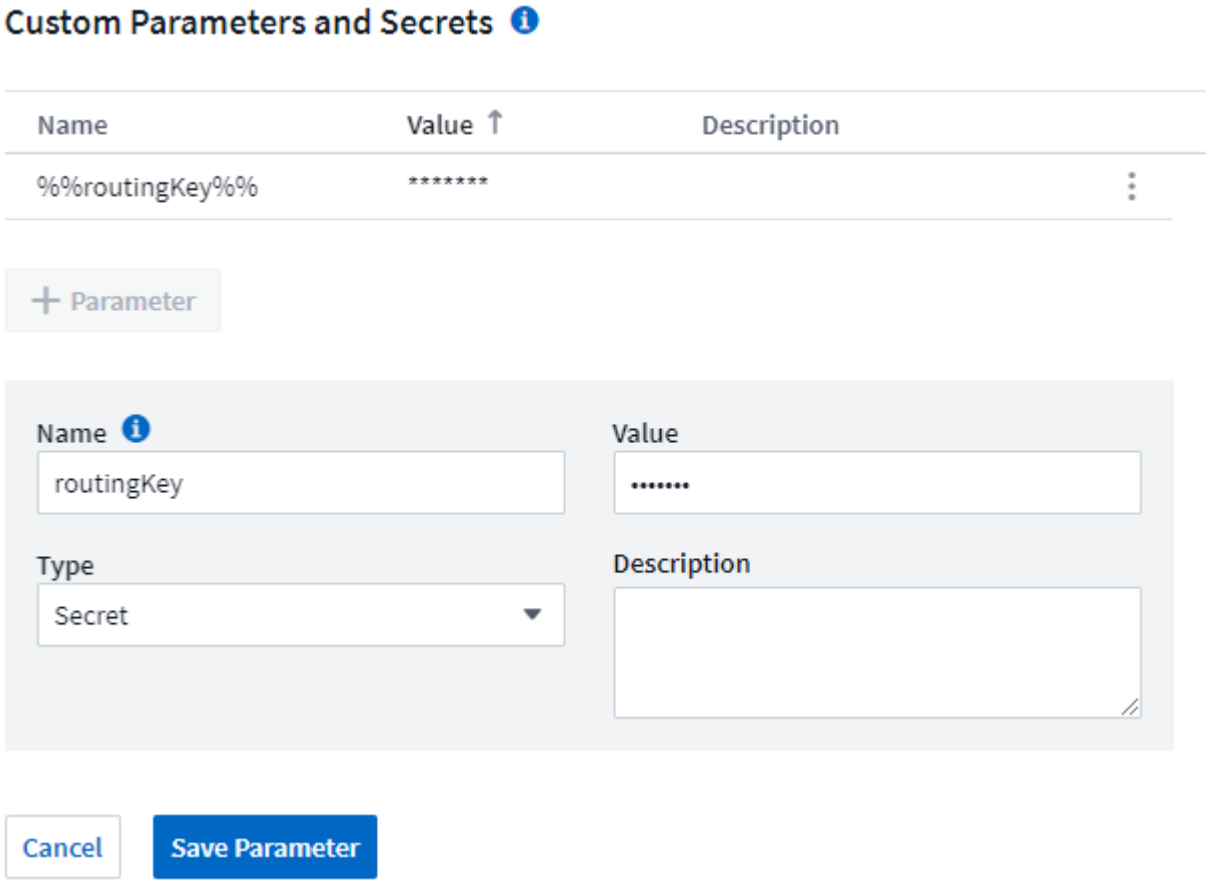


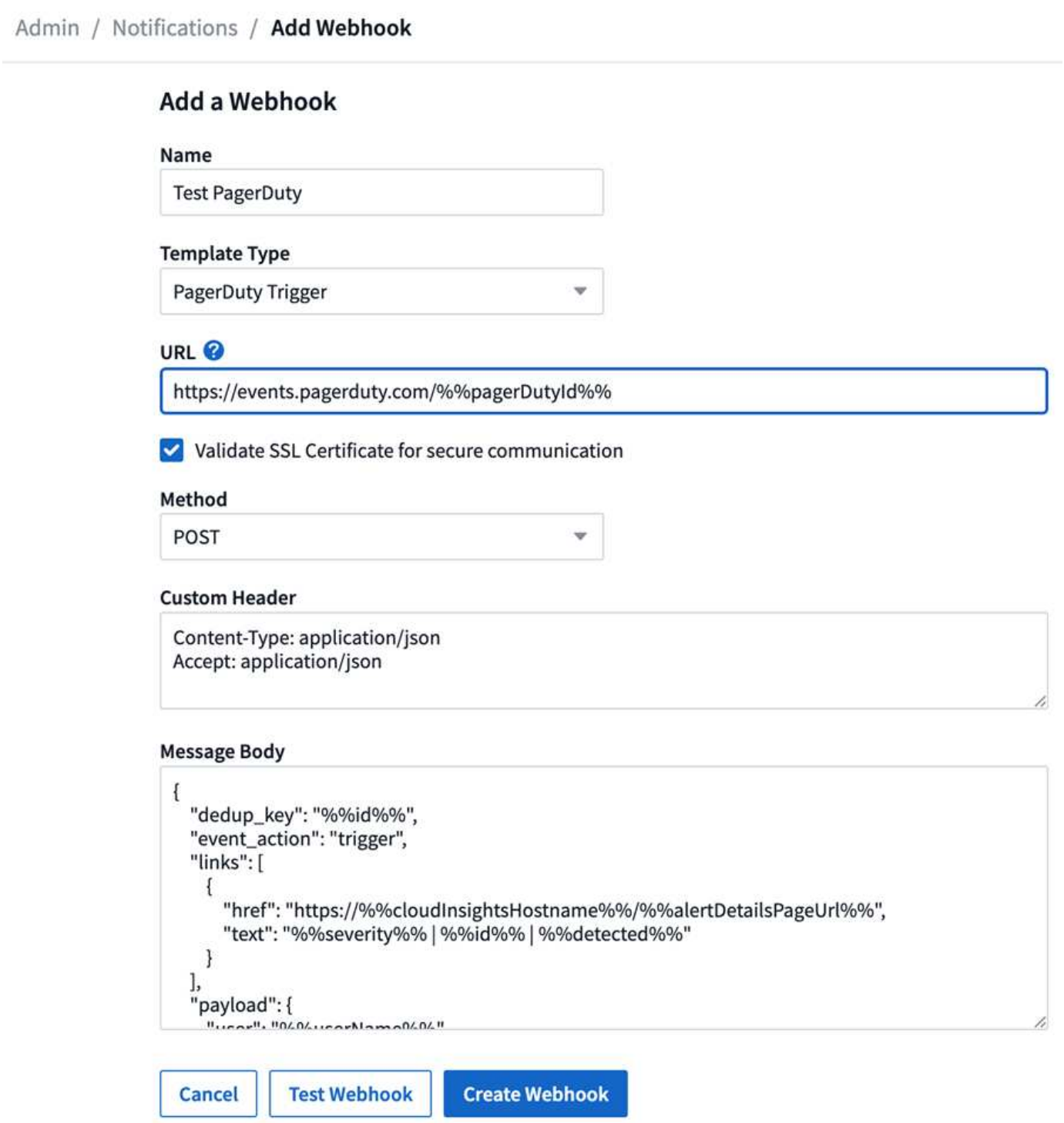
3. Sélectionnez l'onglet *Intégrations* pour voir la **Clé d'intégration**. Vous aurez besoin de cette clé lorsque vous créerez le webhook Workload Security ci-dessous.
4. Accédez à **Incidents** ou **Services** pour afficher les alertes.



Créer un Webhook PagerDuty de sécurité de charge de travail :

- Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez « + Webhook » pour créer un nouveau webhook.
- Donnez au webhook un nom significatif.
- Dans la liste déroulante *Type de modèle*, sélectionnez *Déclencheur PagerDuty*.
- Créez un secret de paramètre personnalisé nommé *routingKey* et définissez la valeur sur la clé d'intégration PagerDuty *Integration Key* créée ci-dessus.

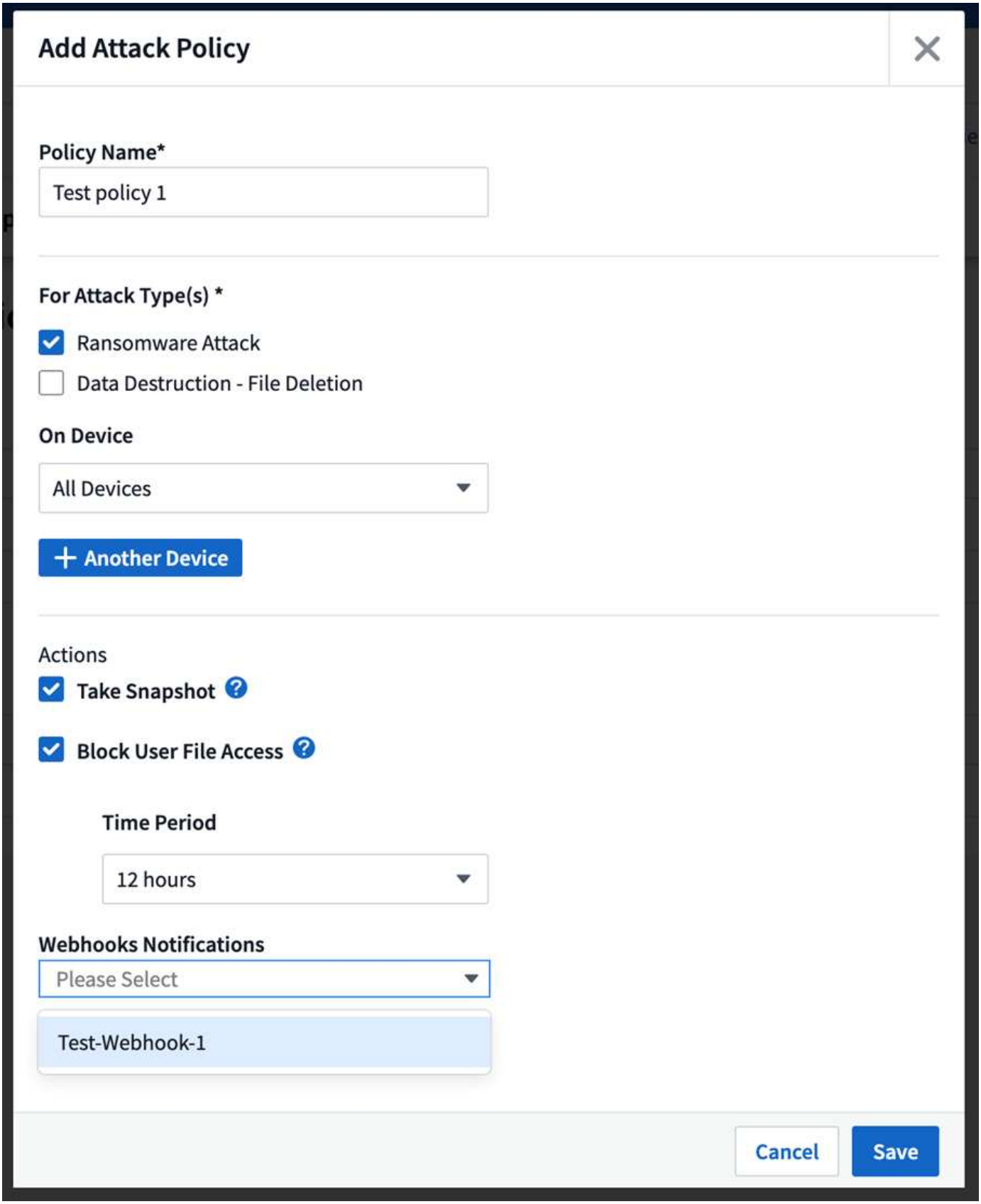




Notifications via Webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la politique doit être attachée et les actions requises.
- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks PagerDuty requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



Exemple de webhook de sécurité de charge de travail pour Slack

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Slack.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Consultez la documentation Slack pour obtenir les informations les plus récentes.

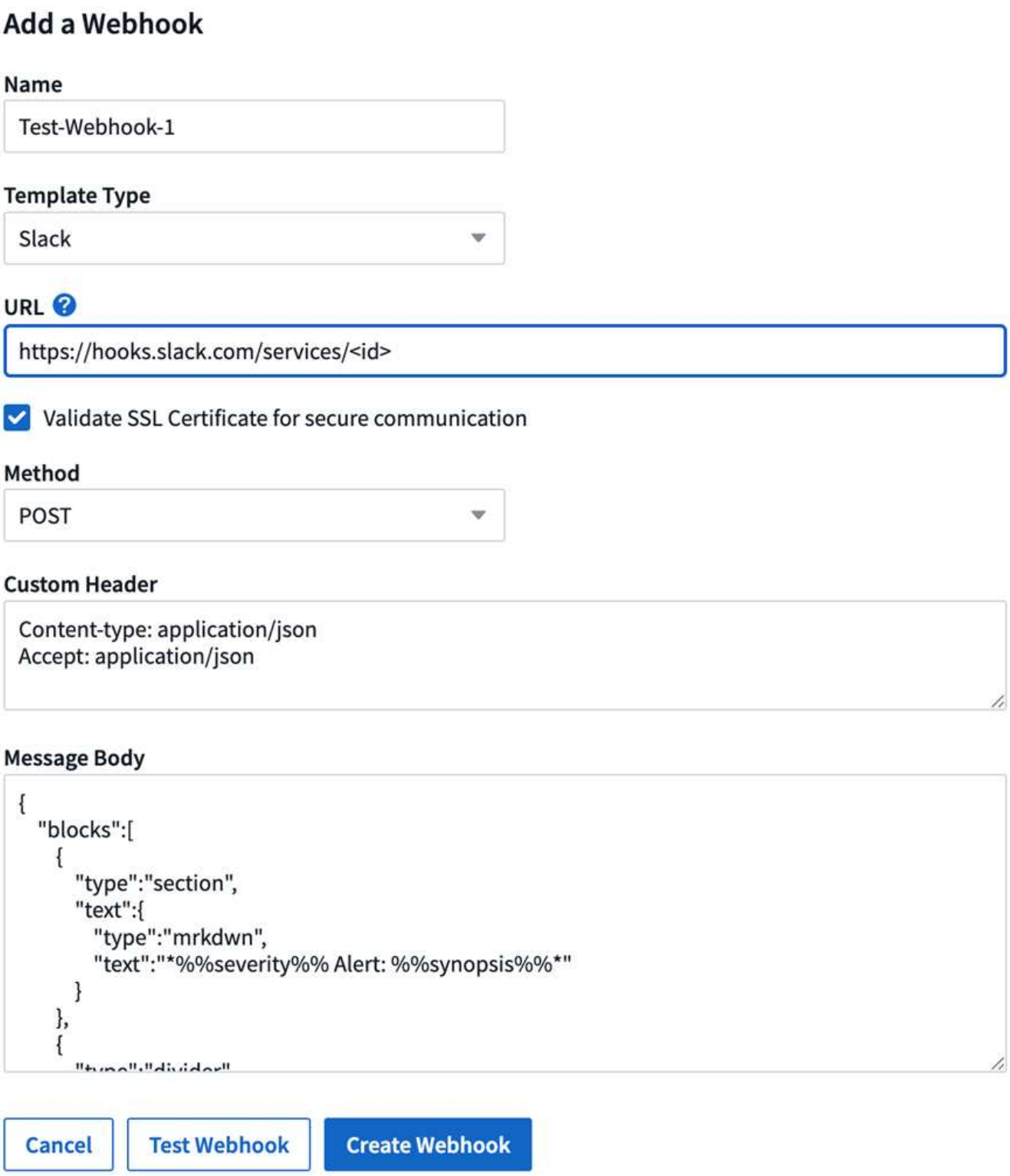
Exemple de Slack

- Aller à https://api.slack.com/apps et créez une nouvelle application. Donnez-lui un nom significatif et sélectionnez un espace de travail.

- Accédez à Webhooks entrants, cliquez sur *Activer les Webhooks entrants*, sélectionnez *Ajouter un nouveau Webhook* et sélectionnez le canal sur lequel publier.
- Copiez l'URL du Webhook. Cette URL sera fournie lors de la création d'un webhook Workload Security.

Créer un webhook Slack pour la sécurité de la charge de travail

1. Accédez à Admin > Notifications et sélectionnez l'onglet *Webhooks de sécurité de la charge de travail*. Sélectionnez _+ *Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez *Slack*.
4. Collez l'URL copiée ci-dessus.

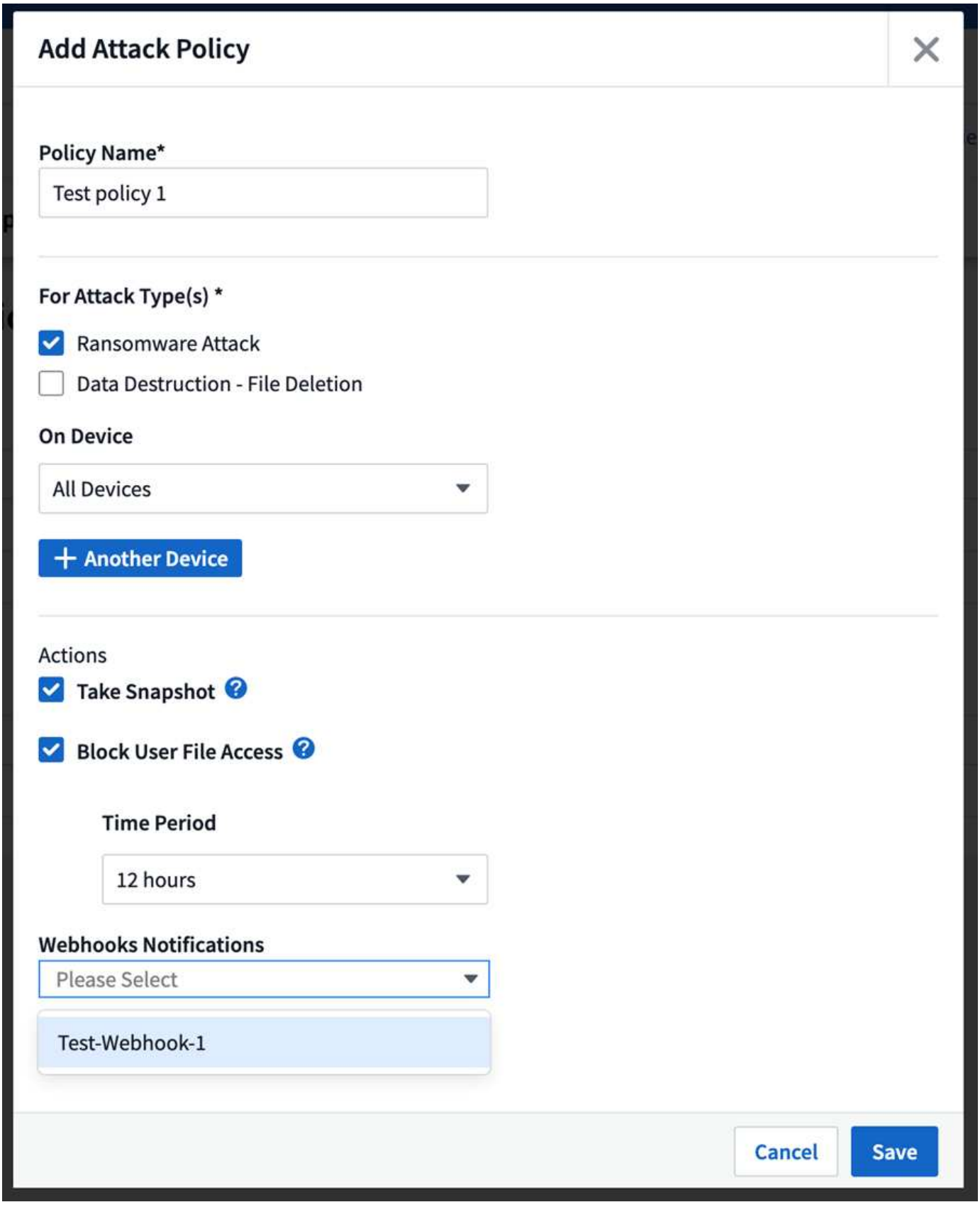


Notifications via webhook

- Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Cliquez sur *+Politique d'attaque* ou *+Politique d'avertissement*.
- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les appareils auxquels la politique doit être attachée et les actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



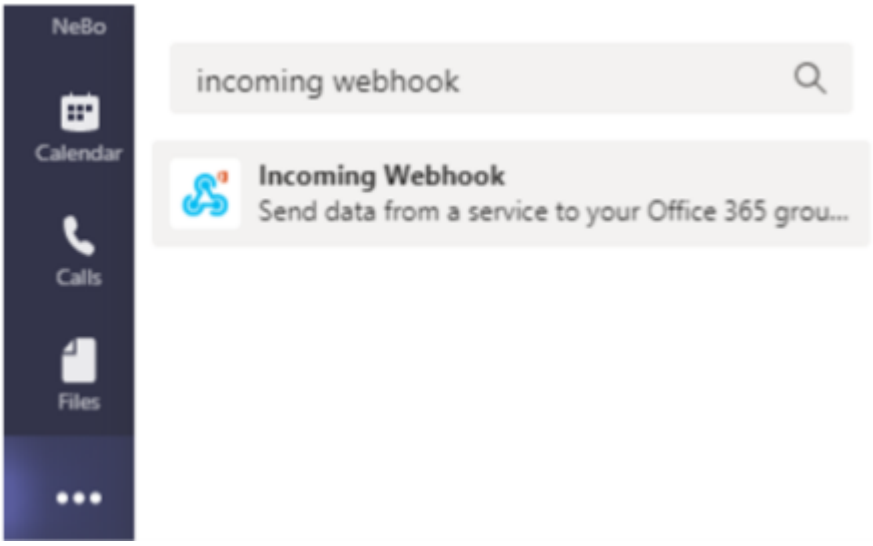
Exemple de webhook de sécurité de charge de travail pour Microsoft Teams

Les webhooks permettent aux utilisateurs d'envoyer des notifications d'alerte à diverses applications à l'aide d'un canal webhook personnalisé. Cette page fournit un exemple de configuration de webhooks pour Teams.

Cette page fait référence à des instructions de tiers, qui sont susceptibles d'être modifiées. Reportez-vous à la"Documentation des équipes" pour les informations les plus récentes.

Configuration des équipes :

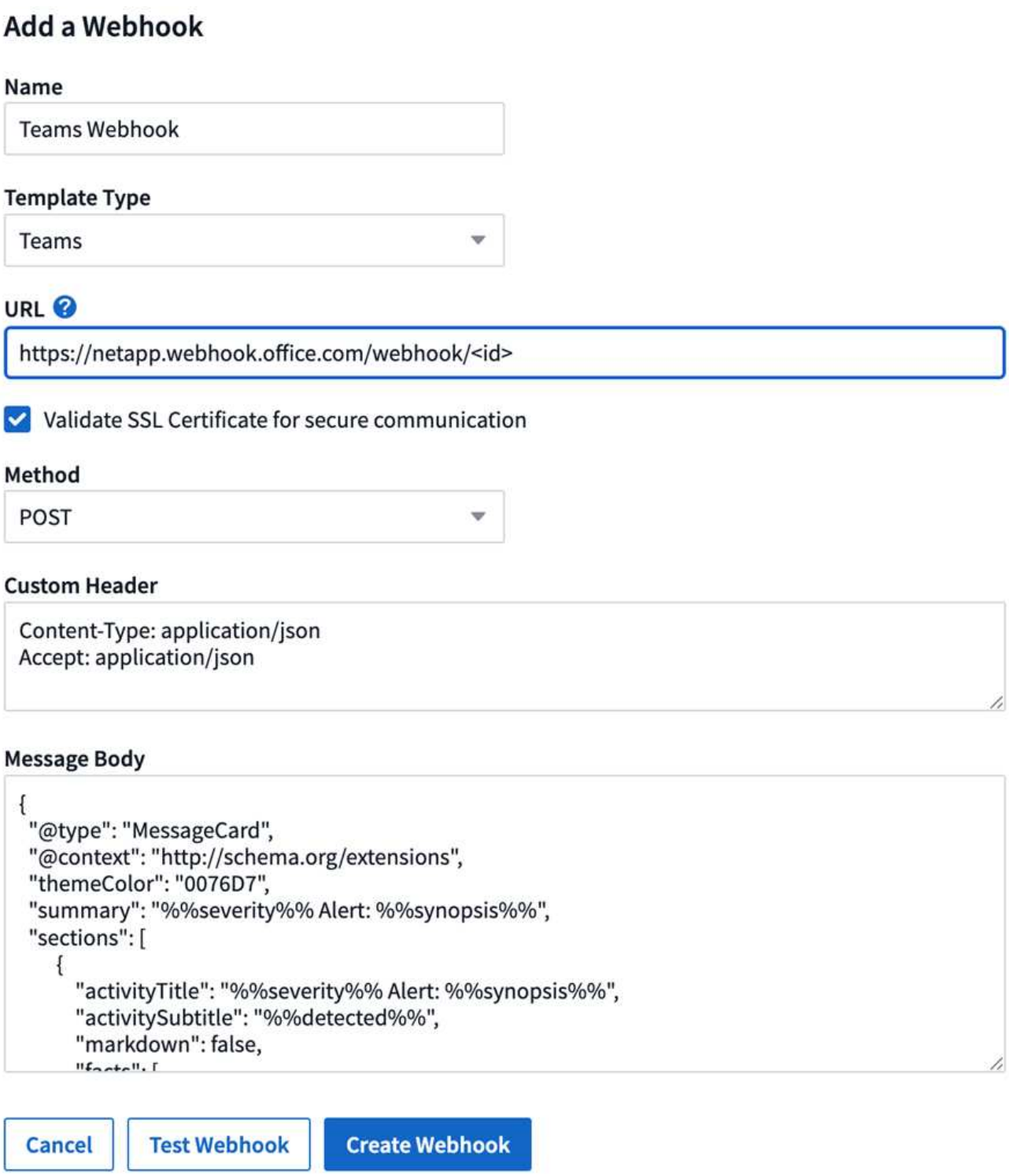
1. Dans Teams, sélectionnez le kebab et recherchez Webhook entrant.



2. Sélectionnez **Ajouter à une équipe > Sélectionner une équipe > Configurer un connecteur**.
3. Copiez l'URL du Webhook. Vous devrez coller ceci dans la configuration du webhook Workload Security.

Créer un webhook pour les équipes de sécurité de la charge de travail :

1. Accédez à Admin > Notifications et sélectionnez l'onglet *« Webhooks de sécurité de la charge de travail »*. Sélectionnez _+ *Webhook* pour créer un nouveau webhook.
2. Donnez au webhook un nom significatif.
3. Dans la liste déroulante *Type de modèle*, sélectionnez **Équipes**.



4. Collez l'URL ci-dessus dans le champ *URL*.

Étapes pour créer une notification Teams avec un modèle Adaptive Card

1. Remplacez le corps du message par le modèle suivant :

```
{
"type": "message",
"attachments": [
```

```
{
  "contentType": "application/vnd.microsoft.card.adaptive",
  "content": {
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "type": "AdaptiveCard",
    "version": "1.2",
    "body": [
      {
        "type": "TextBlock",
        "text": "%%severity%% Alert: %%synopsis%%",
        "wrap": true,
        "weight": "Bolder",
        "size": "Large"
      },
      {
        "type": "TextBlock",
        "text": "%%detected%%",
        "wrap": true,
        "isSubtle": true,
        "spacing": "Small"
      },
      {
        "type": "FactSet",
        "facts": [
          {
            "title": "User",
            "value": "%%userName%%"
          },
          {
            "title": "Attack/Abnormal Behavior",
            "value": "%%type%%"
          },
          {
            "title": "Action taken",
            "value": "%%actionTaken%%"
          },
          {
            "title": "Files encrypted",
            "value": "%%filesEncrypted%%"
          },
          {
            "title": "Encrypted files suffix",
            "value": "%%encryptedFilesSuffix%%"
          },
          {
            "title": "Files deleted",
```

```
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Si vous utilisez Power Automate Flows, les paramètres de requête dans l'URL sont au format encodé. Vous devez décoder l'URL avant de la saisir.
3. Cliquez sur « Test Webhook » pour vous assurer qu'il n'y a pas d'erreurs.
4. Enregistrez le webhook.

Notifications via Webhook

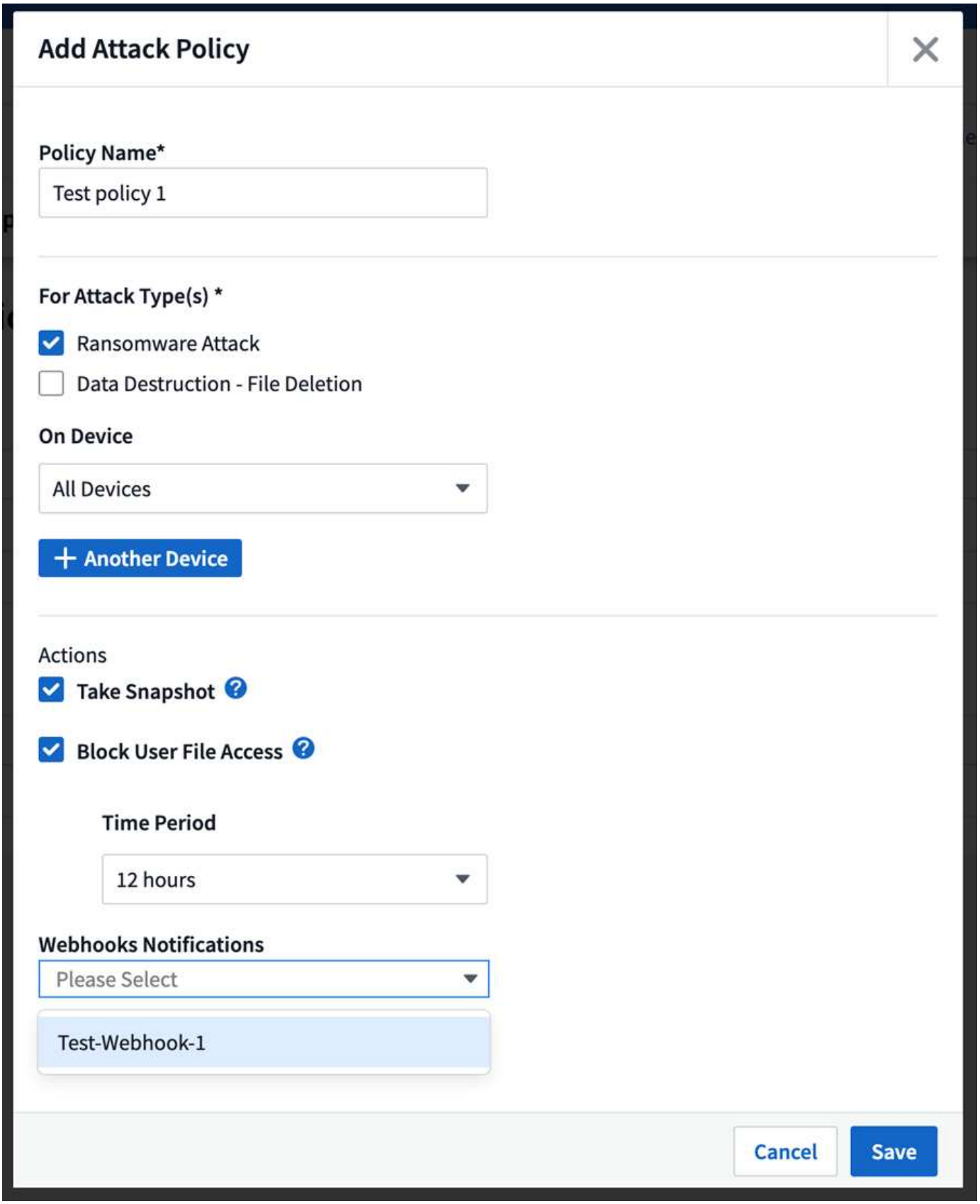
Pour notifier les événements via le webhook, accédez à *Sécurité de la charge de travail > Politiques*. Sélectionnez *+Politique d'attaque* ou *+Politique d'avertissement*.

- Saisissez un nom de politique significatif.
- Sélectionnez les types d'attaque requis, les périphériques auxquels la stratégie doit être associée et les

actions requises.

- Sous la liste déroulante *Notifications Webhooks*, sélectionnez les webhooks Teams requis. Sauvegarder la politique.

Remarque : les webhooks peuvent également être attachés à des politiques existantes en les modifiant.



API de sécurité de la charge de travail

Intégrez Workload Security à votre écosystème d'entreprise à l'aide d'une API REST

protégée par une authentification sécurisée basée sur des jetons. Récupérez les données d'activité forensique, gérez les jetons d'accès API et développez des intégrations personnalisées avec les CMDB, les systèmes de gestion des tickets et d'autres applications. La documentation Swagger interactive fournit des spécifications complètes de l'API et vous permet de tester les points de terminaison directement.

Conditions requises pour l'accès à l'API :

- Un modèle de jeton d'accès API est utilisé pour accorder l'accès.
- La gestion des jetons API est effectuée par les utilisateurs de Workload Security avec le rôle d'administrateur.

Documentation de l'API (Swagger)

Les dernières informations sur l'API sont disponibles en vous connectant à Workload Security et en accédant à **Admin > Accès API**. Cliquez sur le lien **Documentation API**. La documentation de l'API est basée sur Swagger, qui fournit une brève description et des informations d'utilisation de l'API et vous permet de l'essayer sur votre locataire.

Si vous appelez l'API Forensics Activity, utilisez l'API cloudsecure_forensics.activities.**v2**. Si vous effectuez plusieurs appels à cette API, assurez-vous que les appels se produisent de manière séquentielle et non en parallèle. Plusieurs appels parallèles peuvent entraîner l'expiration du délai d'attente de l'API.

Jetons d'accès API

Avant d'utiliser l'API Workload Security, vous devez créer un ou plusieurs **jetons d'accès API**. Les jetons d'accès accordent des autorisations de lecture. Vous pouvez également définir l'expiration de chaque jeton d'accès.

Pour créer un jeton d'accès :

- Cliquez sur **Admin > Accès API**
- Cliquez sur **+Jeton d'accès API**
- Entrez **Nom du jeton**
- Spécifiez **Expiration du jeton**

Votre jeton ne sera disponible que pour la copie dans le presse-papiers et l'enregistrement pendant le processus de création. Les jetons ne peuvent pas être récupérés après leur création, il est donc fortement recommandé de copier le jeton et de l'enregistrer dans un endroit sûr. Vous serez invité à cliquer sur le bouton Copier le jeton d'accès API avant de pouvoir fermer l'écran de création de jeton.

Vous pouvez désactiver, activer et révoquer les jetons. Les jetons désactivés peuvent être activés.

Les jetons accordent un accès général aux API du point de vue du client, en gérant l'accès aux API dans le cadre de leur propre locataire.

L'application reçoit un jeton d'accès après qu'un utilisateur s'est authentifié et a autorisé l'accès avec succès, puis transmet le jeton d'accès comme identifiant lorsqu'il appelle l'API cible. Le jeton transmis informe l'API

que le porteur du jeton a été autorisé à accéder à l'API et à effectuer des actions spécifiques en fonction de la portée qui a été accordée lors de l'autorisation.

L'en-tête HTTP où le jeton d'accès est transmis est **X-CloudInsights-ApiKey:**

Par exemple, utilisez ce qui suit pour récupérer les ressources de stockage :

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Où _<API_Access_Token>_ est le jeton que vous avez enregistré lors de la
création de la clé d'accès API et _<Workload Security Tenant>_ est l'URL
du locataire de votre environnement Workload Security.
```

Des informations détaillées peuvent être trouvées dans le lien *Documentation API* sous **Admin > Accès API**.

Script pour extraire des données via l'API

Les agents Workload Security incluent un script d'exportation pour faciliter les appels parallèles à l'API v2 en divisant la plage horaire demandée en lots plus petits.

Le script se trouve dans */opt/netapp/cloudsecure/agent/export-script*. Un fichier README dans le même répertoire fournit des instructions d'utilisation.

Voici un exemple de commande pour appeler le script :

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

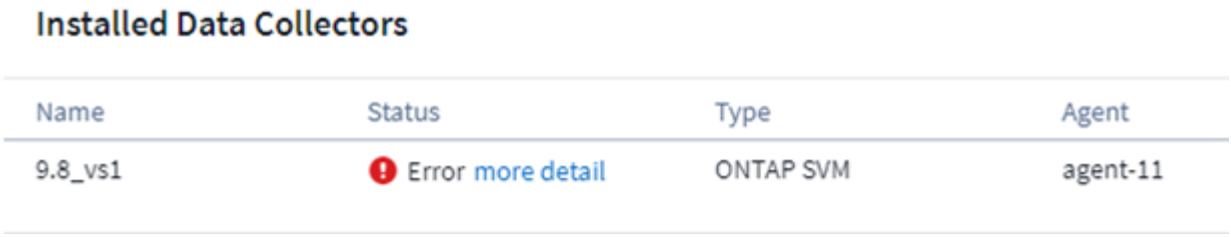
Paramètres clés : - `--iteration_interval 12` : Divise la plage horaire demandée en intervalles de 12 heures. - `--num_workers 3` : Récupère ces intervalles en parallèle à l'aide de 3 threads.

Dépannage du collecteur de données ONTAP SVM

Workload Security utilise des collecteurs de données pour collecter les données d'accès aux fichiers et aux utilisateurs à partir des appareils. Vous trouverez ici des conseils pour résoudre les problèmes liés à ce collecteur.

Voir le"Configuration du collecteur SVM" page pour obtenir des instructions sur la configuration de ce collecteur.

En cas d'erreur, vous pouvez cliquer sur *plus de détails* dans la colonne *Statut* de la page Collecteurs de données installés pour obtenir des détails sur l'erreur.



Les problèmes connus et leurs résolutions sont décrits ci-dessous.

Problème : le collecteur de données s'exécute pendant un certain temps et s'arrête après un temps aléatoire, échouant avec : « Message d'erreur : le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : serveur fpolicy externe surchargé. **Essayez ceci :** le taux d'événements d' ONTAP était bien supérieur à ce que la boîte d'agent peut gérer. La connexion a donc été interrompue.

Vérifiez le trafic de pointe dans CloudSecure lorsque la déconnexion s'est produite. Vous pouvez le vérifier à partir de la page **CloudSecure > Analyse forensique des activités > Toutes les activités**.

Si le trafic agrégé de pointe est supérieur à ce que l'Agent Box peut gérer, reportez-vous à la page du vérificateur de taux d'événements pour savoir comment dimensionner le déploiement du collecteur dans une Agent Box.

Si l'agent a été installé dans la boîte Agent avant le 4 mars 2021, exécutez les commandes suivantes dans la boîte Agent :

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Redémarrez le collecteur à partir de l'interface utilisateur après le redimensionnement.

{vider}

Problème : le collecteur signale le message d'erreur : « Aucune adresse IP locale trouvée sur le connecteur pouvant atteindre les interfaces de données du SVM ». **Essayez ceci :** cela est probablement dû à un problème de réseau côté ONTAP . Veuillez suivre ces étapes :

1. Assurez-vous qu'il n'y a pas de pare-feu sur le LIF de données SVM ou sur le LIF de gestion qui bloque la connexion depuis le SVM.
2. Lors de l'ajout d'un SVM via une adresse IP de gestion de cluster, assurez-vous que la durée de vie des données et la durée de vie de gestion du SVM sont pingables à partir de la machine virtuelle de l'agent. En cas de problème, vérifiez la passerelle, le masque de réseau et les routes du lif.

   Vous pouvez également essayer de vous connecter au cluster via ssh à l'aide de l'adresse IP de gestion du cluster et d'envoyer une requête ping à l'adresse IP de l'agent. Assurez-vous que l'adresse IP de l'agent est pingable :

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

3. Si vous avez essayé de vous connecter via l'IP du cluster et que cela ne fonctionne pas, essayez de vous connecter directement via l'IP SVM. Veuillez consulter ci-dessus les étapes de connexion via l'IP SVM.
4. Lors de l'ajout du collecteur via l'adresse IP SVM et les informations d'identification vsadmin, vérifiez si le rôle Données plus Gestion du SVM est activé. Dans ce cas, le ping vers le SVM Lif fonctionnera, mais le SSH vers le SVM Lif ne fonctionnera pas. Si oui, créez un Lif de gestion SVM uniquement et essayez de vous connecter via ce Lif de gestion SVM uniquement.
5. Si cela ne fonctionne toujours pas, créez un nouveau Lif SVM et essayez de vous connecter via ce Lif. Assurez-vous que le masque de sous-réseau est correctement défini.
6. Débogage avancé :
   a. Démarrer une trace de paquets dans ONTAP.
   b. Essayez de connecter un collecteur de données au SVM à partir de l'interface utilisateur CloudSecure.
   c. Attendez que l'erreur apparaisse. Arrêtez le suivi des paquets dans ONTAP.
   d. Ouvrez la trace des paquets depuis ONTAP. Il est disponible à cet endroit

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Assurez-vous qu'il existe un SYN d' ONTAP vers la boîte Agent.
.. S'il n'y a pas de SYN d' ONTAP , il s'agit d'un problème de pare-
feu dans ONTAP.
.. Ouvrez le pare-feu dans ONTAP, afin ONTAP puisse connecter la
boîte d'agent.
```

7. Si cela ne fonctionne toujours pas, veuillez consulter l'équipe réseau pour vous assurer qu'aucun pare-feu externe ne bloque la connexion d' ONTAP au boîtier Agent.
8. Si aucune des solutions ci-dessus ne résout le problème, ouvrez un dossier avec"Assistance Netapp" pour obtenir de l'aide.

{vider}

Problème : Message : « Échec de la détermination du type ONTAP pour [nom d'hôte : <adresse IP>. Raison : Erreur de connexion au système de stockage <Adresse IP> : L'hôte est inaccessible (Hôte inaccessible)"
Essayez ceci :

1. Vérifiez que l'adresse IP de gestion SVM ou l'adresse IP de gestion de cluster correcte a été fournie.
2. Connectez-vous en SSH au SVM ou au cluster auquel vous souhaitez vous connecter. Une fois connecté, assurez-vous que le nom du SVM ou du cluster est correct.

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Service.nom : audit. Motif de l'échec : serveur fpolicy externe arrêté. **Essayez ceci :**

1. Il est très probable qu'un pare-feu bloque les ports nécessaires sur la machine agent. Vérifiez que la plage de ports 35000-55000/tcp est ouverte pour que la machine agent se connecte à partir du SVM. Assurez-vous également qu'aucun pare-feu n'est activé côté ONTAP bloquant la communication avec la machine agent.
2. Tapez la commande suivante dans la zone Agent et assurez-vous que la plage de ports est ouverte.

   ```
   sudo iptables-save | grep 3500*
   ```

   Un exemple de sortie devrait ressembler à :

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Connectez-vous à SVM, entrez les commandes suivantes et vérifiez
   qu'aucun pare-feu n'est configuré pour bloquer la communication avec
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Vérifier les commandes du pare-feu"du côté ONTAP .

3. Connectez-vous en SSH au SVM/cluster que vous souhaitez surveiller. Envoyez une requête ping à la boîte Agent à partir de la bibliothèque de données SVM (avec prise en charge des protocoles CIFS et NFS) et assurez-vous que la requête ping fonctionne :

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si le ping n'est pas possible, assurez-vous que les paramètres réseau dans ONTAP sont corrects, afin que la machine de l'agent soit pingable.

4. Si un seul SVM est ajouté deux fois à un locataire via 2 collecteurs de données, cette erreur s'affichera. Supprimez l'un des collecteurs de données via l'interface utilisateur. Redémarrez ensuite l'autre collecteur de données via l'interface utilisateur. Ensuite, le collecteur de données affichera le statut « EN COURS D'EXÉCUTION » et commencera à recevoir des événements de SVM.

   Fondamentalement, dans un locataire, 1 SVM ne doit être ajouté qu'une seule fois, via 1 collecteur de données. 1 SVM ne doit pas être ajouté deux fois via 2 collecteurs de données.

5. Dans les cas où le même SVM a été ajouté dans deux environnements de sécurité de charge de travail différents (locataires), le dernier réussira toujours. Le deuxième collecteur configurera fpolicy avec sa propre adresse IP et expulsera le premier. Ainsi, le collecteur du premier cessera de recevoir des événements et son service « audit » entrera en état d'erreur. Pour éviter cela, configurez chaque SVM sur

un seul environnement.

6. Cette erreur peut également se produire si les stratégies de service ne sont pas configurées correctement. Avec ONTAP 9.8 ou version ultérieure, pour se connecter au collecteur de sources de données, le service data-fpolicy-client est requis avec le service de données data-nfs et/ou data-cifs. De plus, le service data-fpolicy-client doit être associé aux données lif pour le SVM surveillé.

{vider}

Problème : Aucun événement n'est visible sur la page d'activité. **Essayez ceci :**

1. Vérifiez si le collecteur ONTAP est à l'état « RUNNING ». Si oui, assurez-vous que certains événements cifs sont générés sur les machines virtuelles clientes cifs en ouvrant certains fichiers.
2. Si aucune activité n'est observée, connectez-vous au SVM et entrez la commande suivante.

   ```
   <SVM>event log show -source fpolicy
   ```

   Veuillez vous assurer qu'il n'y a pas d'erreurs liées à fpolicy.

3. Si aucune activité n'est visible, veuillez vous connecter au SVM. Entrez la commande suivante :

   ```
   <SVM>fpolicy show
   ```

   Vérifiez si la politique fpolicy nommée avec le préfixe « cloudsecure_ » a été définie et si le statut est « on ». Si cette option n'est pas définie, il est fort probable que l'agent ne puisse pas exécuter les commandes dans la SVM. Veuillez vous assurer que toutes les conditions préalables décrites au début de la page ont été respectées.

{vider}

Problème : Le collecteur de données SVM est en état d'erreur et le message d'erreur est « L'agent n'a pas réussi à se connecter au collecteur » **Essayez ceci :**

1. Il est fort probable que l'agent soit surchargé et ne parvienne pas à se connecter aux collecteurs de sources de données.
2. Vérifiez combien de collecteurs de sources de données sont connectés à l'agent.
3. Vérifiez également le débit de données dans la page « Toutes les activités » de l'interface utilisateur.
4. Si le nombre d'activités par seconde est considérablement élevé, installez un autre agent et déplacez certains des collecteurs de sources de données vers le nouvel agent.

{vider}

Problème : le collecteur de données SVM affiche le message d'erreur suivant : « fpolicy.server.connectError : le nœud n'a pas pu établir de connexion avec le serveur FPolicy « 12.195.15.146 » (raison : « Sélection

expirée ») » **Essayez ceci :** le pare-feu est activé dans SVM/Cluster. Le moteur fpolicy ne peut donc pas se connecter au serveur fpolicy. Les CLI dans ONTAP qui peuvent être utilisées pour obtenir plus d'informations sont :

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Vérifier les commandes du pare-feu"du côté ONTAP .

{vider}

Problème : Message d'erreur : « Le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : Aucune interface de données valide (rôle : données, protocoles de données : NFS ou CIFS ou les deux, état : actif) trouvée sur la SVM. **Essayez ceci :** Assurez-vous qu'il existe une interface opérationnelle (ayant un rôle de données et un protocole de données comme CIFS/NFS).

{vider}

Problème : le collecteur de données passe à l'état d'erreur, puis passe à l'état d'exécution après un certain temps, puis revient à l'état d'erreur. Ce cycle se répète. **Essayez ceci :** Cela se produit généralement dans le scénario suivant :

1. Plusieurs collecteurs de données ont été ajoutés.
2. Les collecteurs de données qui présentent ce type de comportement auront 1 SVM ajouté à ces collecteurs de données. Cela signifie que 2 ou plusieurs collecteurs de données sont connectés à 1 SVM.
3. Assurez-vous qu'un seul collecteur de données se connecte à un seul SVM.
4. Supprimez les autres collecteurs de données connectés au même SVM.

{vider}

Problème : le connecteur est dans un état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration (politique sur SVM svmname. Motif : Valeur non valide spécifiée pour l'élément « shares-to-include » dans « fpolicy.policy.scope-modify : « Federal » **Essayez ceci :** *Les noms de partage doivent être indiqués sans guillemets. Modifiez la configuration DSC ONTAP SVM pour corriger les noms de partage.

Inclure et exclure des partages n'est pas destiné à une longue liste de noms de partages. Utilisez plutôt le filtrage par volume si vous avez un grand nombre d'actions à inclure ou à exclure.

{vider}

Problème : il existe des fpolicies existantes dans le cluster qui ne sont pas utilisées. Que faut-il faire avec ceux-ci avant l'installation de Workload Security ? **Essayez ceci :** Il est recommandé de supprimer tous les paramètres fpolicy inutilisés existants, même s'ils sont dans un état déconnecté. Workload Security créera

fpolicy avec le préfixe « cloudsecure_ ». Toutes les autres configurations fpolicy inutilisées peuvent être supprimées.

Commande CLI pour afficher la liste fpolicy :

```
 fpolicy show
Étapes pour supprimer les configurations fpolicy :
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vider}

Problème : Après l'activation de la sécurité des charges de travail, les performances ONTAP sont affectées : la latence devient sporadiquement élevée et les IOPS deviennent sporadiquement faibles. **Essayez ceci :** Lors de l'utilisation ONTAP avec Workload Security, des problèmes de latence peuvent parfois être observés dans ONTAP. Plusieurs raisons peuvent expliquer cela, comme indiqué ci-dessous :"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tous ces problèmes sont résolus dans ONTAP 9.13.1 et versions ultérieures ; il est fortement recommandé d'utiliser l'une de ces versions ultérieures.

{vider}

Problème : le collecteur de données affiche le message d'erreur : « Erreur : échec de la détermination de l'état du collecteur en 2 tentatives, essayez de redémarrer le collecteur (code d'erreur : AGENT008) ». **Essayez ceci :**

1. Sur la page Collecteurs de données, faites défiler vers la droite du collecteur de données générant l'erreur et cliquez sur le menu à 3 points. Sélectionnez *Modifier*. Saisissez à nouveau le mot de passe du collecteur de données. Enregistrez le collecteur de données en appuyant sur le bouton *Enregistrer*. Le collecteur de données redémarrera et l'erreur devrait être résolue.
2. Il se peut que la machine Agent ne dispose pas de suffisamment de CPU ou de RAM, c'est pourquoi les DSC échouent. Veuillez vérifier le nombre de collecteurs de données ajoutés à l'agent dans la machine. Si le nombre est supérieur à 20, veuillez augmenter la capacité du processeur et de la RAM de la machine Agent. Une fois le CPU et la RAM augmentés, les DSC passeront automatiquement en état d'initialisation puis en état d'exécution. Consultez le guide des tailles sur"cette page" .

{vider}

Problème : le collecteur de données génère une erreur lorsque le mode SVM est sélectionné. **Essayez ceci :** lors de la connexion en mode SVM, si l'IP de gestion du cluster est utilisée pour se connecter au lieu de l'IP de

gestion SVM, la connexion échouera. Assurez-vous que l'adresse IP SVM correcte est utilisée.

{vider}

Problème : le collecteur de données affiche un message d'erreur lorsque la fonction Accès refusé est activée : « Le connecteur est en état d'erreur. Nom du service : audit. Motif de l'échec : échec de la configuration de fpolicy sur SVM test_svm. Motif : l'utilisateur n'est pas autorisé. **Essayez ceci :** l'utilisateur ne dispose peut-être pas des autorisations REST nécessaires à la fonctionnalité Accès refusé. Veuillez suivre les instructions sur"cette page" pour définir les autorisations.

Redémarrez le collecteur une fois les autorisations définies.

{vider}

Problème : Le collecteur est en état d'erreur avec le message : Le connecteur est en état d'erreur. Raison de l'échec : Échec de la configuration du stockage persistant sur la SVM <Nom de la SVM>. Raison : Impossible de trouver un agrégat approprié pour le volume « <volumeName> » dans le SVM « <SVM Name> ». Motif : Les informations de performance pour l'agrégat « <aggregateName> » ne sont actuellement pas disponibles. Patientez quelques minutes et réessayez la commande. Nom du service : audit. Raison de l'échec : impossible de configurer le magasin persistant sur la SVM <SVM name="">.</SVM> Reason: Unable to find a suitable aggregate for volume "<volumeName>" in SVM "<SVM Name>". Motif : Les informations sur les performances pour <aggregateName>l'agrégat « » ne sont actuellement pas disponibles.</aggregateName> Attendez quelques minutes et réessayez la commande.

Essayez ceci : Attendez quelques minutes, puis redémarrez le Collecteur.

{vider}

Si vous rencontrez toujours des problèmes, contactez les liens d'assistance mentionnés dans la page **Aide > Assistance**.

Dépannage

Dépannage des problèmes généraux Data Infrastructure Insights

Vous trouverez ici des suggestions pour résoudre les problèmes liés à Data Infrastructure Insights.

Voir aussi"Dépannage des problèmes d'unité d'acquisition Linux" et"Dépannage des problèmes liés à l'unité d'acquisition Windows" .

Problèmes de connexion

Problème:	Essayez ceci :
Data Infrastructure Insights se déconnecte automatiquement toutes les 6 heures	Cela est dû à la désactivation des cookies tiers du navigateur. Les utilisateurs peuvent configurer leur navigateur pour activer tous les cookies tiers ou utiliser une liste d'exceptions plus restreinte pour activer uniquement ceux destinés à Data Infrastructure Insights. Exemple : Ouvrez les paramètres de votre navigateur. Sélectionnez l'option « Autoriser tous les cookies ». **OU** Sélectionnez « Bloquer les cookies tiers » et ajoutez des exceptions pour *[*.]auth0.com* et *[*.]netapp.com*. Microsoft Edge suit le même format pour les exceptions que Chrome. Dans Firefox, les exceptions de cookies sont simplement désignées par *auth0.com* et *netapp.com*.
J'ai un compte Console mais je n'arrive pas à me connecter.	Ouvrir un ticket depuis https://mysupport.netapp.com/site/help . Sélectionnez la catégorie console.netapp.com > Problèmes de compte/connexion » ou console.netapp.com > Problèmes de fédération ». Ceux-ci sont spécifiquement destinés aux problèmes ou questions liés à la console. Pour tous les autres problèmes d'assistance technique Data Infrastructure Insights , contactez"Prise en charge de NetApp" .
J'ai été invité à Data Infrastructure Insights mais je reçois un message « non autorisé ».	Vérifiez que vous avez créé un compte Console ou que votre organisation utilise la connexion SSO avec Console. Vérifiez que l'adresse e-mail de votre profil de console correspond à l'adresse e-mail indiquée dans votre e-mail de bienvenue Data Infrastructure Insights . Si l'e-mail ne correspond pas, demandez une nouvelle invitation avec la bonne adresse e-mail.

Problème:	Essayez ceci :
Je me suis déconnecté de la console et j'ai été automatiquement déconnecté de Data Infrastructure Insights.	L'authentification unique (SSO) sur NetApp Cloud Services déconnecte toutes les sessions Data Infrastructure Insights . Si vous avez accès à plusieurs comptes Data Infrastructure Insights , la déconnexion de l'un d'eux entraîne la déconnexion de toutes les sessions actives. Connectez-vous à nouveau pour accéder à votre compte.
J'ai été automatiquement déconnecté après plusieurs jours.	Les comptes NetApp Cloud nécessitent une réauthentification tous les quelques jours (le paramètre actuel de la console est de 7 jours). Connectez-vous à nouveau pour accéder à votre compte.
Je reçois un message d'erreur « plus autorisé à me connecter ».	Contactez l'administrateur de votre compte pour vérifier l'accès à Data Infrastructure Insights. Vérifiez que l'adresse e-mail de votre profil de console correspond à l'adresse e-mail indiquée dans votre e-mail de bienvenue Data Infrastructure Insights
Autres erreurs de connexion	Essayez le mode navigation privée dans Chrome ou effacez l'historique du navigateur, les cookies et le cache. Essayez avec un autre profil de navigateur (par exemple Chrome - ajouter une personne).

Autres questions

Question:	Répondre:
Mes quotas stricts Qtree s'affichent correctement dans les requêtes, mais mes quotas souples s'affichent comme la capacité totale du volume. Est-ce correct ?	Seuls les quotas stricts, définis manuellement ou via Trident, s'afficheront comme quotas définis ; si aucun quota strict n'est spécifié, la capacité Qtree sera la capacité du volume interne.
J'ai un quota souple et un quota dur définis manuellement dans le même Qtree, mais la capacité totale affichée est le quota dur ; est-ce correct ?	Oui, si un quota strict est spécifié, il sera affiché comme capacité totale.
Lorsque je saisis l'heure de planification d'un rapport Cognos, il m'arrive parfois d'obtenir un « m » supplémentaire dans l'heure de planification. Par exemple, si j'entre l'heure sous la forme « 02:15 PM », un caractère supplémentaire peut être ajouté : « 02:15 PMM » (ou PMm). Lorsque je clique à l'extérieur, cela change l'heure à « 2 h 15 ». Je peux enregistrer le rapport, mais lorsque je rouvre le rapport enregistré, l'heure de planification apparaît comme AM (c'est-à-dire matin), que j'aie entré AM ou PM dans l'heure de planification.	Saisissez à nouveau l'heure programmée en veillant à ne pas saisir les caractères « AM » ou « PM » complets ; il suffit de taper « A » pour « AM » ou « P » pour « PM ». Si le caractère supplémentaire ne s'affiche pas, l'heure programmée sera correctement définie.

Ressources

Des conseils de dépannage supplémentaires peuvent être trouvés dans le"Base de connaissances NetApp" (connexion d'assistance requise).

Des informations d'assistance supplémentaires peuvent être trouvées dans Data Infrastructure Insights"Support" page.

Si vous disposez d'un abonnement Data Infrastructure Insights actif, vous pouvez utiliser ces options d'assistance :

"Téléphone" "Ticket d'assistance"

Pour plus d'informations, consultez le "Documentation d'assistance sur les Data Infrastructure Insights" .

Dépannage des problèmes d'unité d'acquisition sous Linux

Vous trouverez ici des suggestions pour résoudre les problèmes liés aux unités d'acquisition sur un serveur Linux.

Problème:	**Essayez ceci :**
Le statut AU sur la page **Observabilité > Collecteurs** dans l'onglet **Unités d'acquisition** affiche « Certificat expiré » ou « Certificat révoqué ».	Cliquez sur le menu à droite de l'AU et sélectionnez **Restaurer la connexion**. Suivez les instructions pour restaurer votre unité d'acquisition : 1. Arrêtez le service Unité d'acquisition (AU). Vous pouvez cliquer sur le bouton *Copier la commande d'arrêt* pour copier rapidement la commande dans le presse-papiers, puis coller cette commande dans une invite de commande sur la machine de l'unité d'acquisition. 2. Créez un fichier nommé « token » dans le dossier */var/lib/netapp/cloudinsights/acq/conf* sur l'AU. 3. Cliquez sur le bouton *Copier le jeton* et collez ce jeton dans le fichier que vous avez créé. 4. Redémarrez le service AU. Cliquez sur le bouton *Copier la commande de redémarrage* et collez la commande dans une invite de commande sur l'AU.
Autorisation refusée lors du démarrage du service serveur de l'unité d'acquisition	Lorsque l'AU est installé sur SELINUX, SE doit être défini sur le mode *permissif*. Le mode *Enforcing* n'est pas pris en charge. Après avoir défini SELINUX en mode permissif, redémarrez le service AU.
Les exigences du serveur ne sont pas satisfaites	Assurez-vous que votre serveur d'unité d'acquisition ou votre machine virtuelle répond"exigences"
Les exigences du réseau ne sont pas satisfaites	Assurez-vous que votre serveur/VM d'unité d'acquisition peut accéder à votre environnement Data Infrastructure Insights (<environment-name>.c01.cloudinsights.netapp.com) via une connexion SSL sur le port 443. Essayez les commandes suivantes : *ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com* Notez que le port 443 doit être ouvert « sortant » de l'AU vers Data Infrastructure Insights.

Le serveur proxy n'est pas configuré correctement	Vérifiez vos paramètres proxy et désinstallez/réinstallez le logiciel de l'unité d'acquisition si nécessaire pour entrer les paramètres proxy corrects. 1. Essayez « curl ». Reportez-vous aux informations/documentations « man curl » concernant les proxys : --preproxy, --proxy-* (il s'agit d'un caractère générique « * » car curl prend en charge de nombreux paramètres de proxy). 2. Essayez "wget". Consultez la documentation pour les options proxy.
L'installation de l'unité d'acquisition a échoué dans Data Infrastructure Insights avec des erreurs d'informations d'identification lors du démarrage du service d'acquisition (et visible dans le fichier acq.log).	Cela peut être dû à l'inclusion de caractères spéciaux dans les informations d'identification du proxy. Désinstallez l'AU (*sudo cloudinsights-uninstall.sh*) et réinstallez-le sans utiliser de caractères spéciaux.
Linux : bibliothèque manquante / fichier introuvable	Assurez-vous que votre serveur/VM d'unité d'acquisition Linux dispose de toutes les bibliothèques nécessaires. Par exemple, vous devez avoir la bibliothèque *unzip* installée sur le serveur. Pour installer la bibliothèque *unzip*, exécutez la commande **sudo yum install unzip** avant d'exécuter le script d'installation de l'unité d'acquisition
Problèmes d'autorisation	Assurez-vous d'être connecté en tant qu'utilisateur avec les autorisations *sudo*
L'acquisition ne fonctionne pas :	Récupérez le fichier acq.log depuis /opt/netapp/cloudinsights/acq/logs (Linux) Redémarrez le service d'acquisition : sudo cloudinsights-service.sh restart acquisition
Problèmes de collecte de données :	Envoyez un rapport d'erreur depuis la page de destination du collecteur de données en cliquant sur le bouton « Envoyer un rapport d'erreur »
Statut : Échec du battement de cœur	L'unité d'acquisition (AU) envoie un battement de cœur à Data Infrastructure Insights toutes les 60 secondes pour renouveler son bail. Si l'appel de pulsation échoue en raison d'un problème de réseau ou d'une absence de réponse de Data Infrastructure Insights, la durée de bail de l'AU n'est pas mise à jour. Lorsque la durée du bail de l'AU expire, Data Infrastructure Insights affiche le statut « Échec du battement de cœur ». Étapes de dépannage : vérifiez la connexion réseau entre le serveur de l'unité d'acquisition et CloudInsights. Vérifiez si le service Unité d'acquisition est en cours d'exécution. Si le service n'est pas en cours d'exécution, démarrez-le. Consultez le journal de l'unité d'acquisition (/var/log/netapp/cloudinsights/acq/acq.log) pour voir s'il y a des erreurs.

Je vois un message « Erreur de pulsation : »	Cette erreur peut se produire en cas d'interruption du réseau entraînant une interruption de la communication entre l'unité d'acquisition et l'environnement Data Infrastructure Insights pendant plus d'une minute. Vérifiez que la connexion entre l'AU et Data Infrastructure Insights est stable et active.
Lors de la réinstallation de l'unité d'acquisition, je vois « ValueError : contexte de fichier pour /opt/netapp/cloudinsights(/.*) ? déjà défini ».	Sur un système avec SELinux, ce message d'erreur peut apparaître après `cloudinsights-uninstall.sh -p` a été exécuté et l'unité d'acquisition doit être réinstallée. Exécution de la commande `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` devrait corriger le problème et supprimer le message.

Considérations sur les proxys et les pare-feu

Si votre organisation nécessite l'utilisation d'un proxy pour l'accès à Internet, vous devrez peut-être comprendre le comportement du proxy de votre organisation et rechercher certaines exceptions pour que Data Infrastructure Insights fonctionne. Gardez à l'esprit les points suivants :

- Tout d'abord, votre organisation bloque-t-elle l'accès par défaut et autorise-t-elle uniquement l'accès à des sites Web/domaines spécifiques par exception ? Si tel est le cas, vous devrez ajouter le domaine suivant à la liste des exceptions :

  ```
  *.cloudinsights.netapp.com
  ```

  Votre unité d'acquisition Data Infrastructure Insights , ainsi que vos interactions dans un navigateur Web avec Data Infrastructure Insights, seront toutes dirigées vers des hôtes portant ce nom de domaine.

- Deuxièmement, certains proxys tentent d'effectuer une inspection TLS/SSL en se faisant passer pour des sites Web Data Infrastructure Insights avec des certificats numériques non générés par NetApp. Le modèle de sécurité de l'unité d'acquisition Data Infrastructure Insights est fondamentalement incompatible avec ces technologies. Vous aurez également besoin du nom de domaine ci-dessus, exclu de cette fonctionnalité, pour que l'unité d'acquisition de Data Infrastructure Insights puisse se connecter avec succès à Data Infrastructure Insights et faciliter la découverte de données.

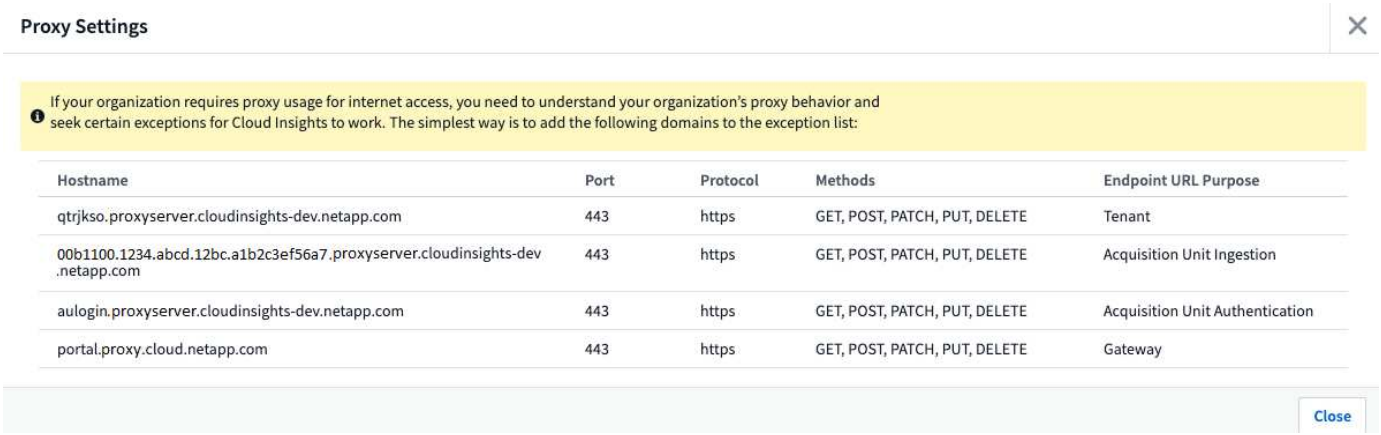
Dans le cas où le proxy est configuré pour l'inspection du trafic, l'environnement Data Infrastructure Insights doit être ajouté à une liste d'exceptions dans la configuration du proxy. Le format et la configuration de cette liste d'exceptions varient en fonction de votre environnement proxy et de vos outils, mais en général, vous devez ajouter les URL des serveurs Data Infrastructure Insights à cette liste d'exceptions afin de permettre à l'AU de communiquer correctement avec ces serveurs.

La manière la plus simple de procéder consiste à ajouter le domaine Data Infrastructure Insights lui-même à la liste des exceptions :

```
 *.cloudinsights.netapp.com
Dans le cas où le proxy n'est pas configuré pour l'inspection du trafic,
une liste d'exceptions peut être requise ou non.  Si vous ne savez pas si
vous devez ajouter Data Infrastructure Insights à une liste d'exceptions,
ou si vous rencontrez des difficultés lors de l'installation ou de
l'exécution de Data Infrastructure Insights en raison de la configuration
du proxy et/ou du pare-feu, contactez votre équipe d'administration de
proxy pour configurer la gestion de l'interception SSL par le proxy.
```

Affichage des points de terminaison proxy

Vous pouvez afficher vos points de terminaison proxy en cliquant sur le lien **Paramètres proxy** lors du choix d'un collecteur de données lors de l'intégration, ou sur le lien sous *Paramètres proxy* sur la page **Aide > Assistance**. Un tableau comme celui-ci s'affiche. Si vous disposez de Workload Security dans votre environnement, les URL des points de terminaison configurés seront également affichées dans cette liste.



Ressources

Des conseils de dépannage supplémentaires peuvent être trouvés dans le"Base de connaissances NetApp" (connexion d'assistance requise).

Des informations d'assistance supplémentaires peuvent être trouvées dans Data Infrastructure Insights"Support" page.

Dépannage des problèmes d'unité d'acquisition sous Windows

Vous trouverez ici des suggestions pour résoudre les problèmes liés aux unités d'acquisition sur un serveur Windows.

Problème:	Essayez ceci :

Le statut AU sur la page **Observabilité > Collecteurs** dans l'onglet **Unités d'acquisition** affiche « Certificat expiré » ou « Certificat révoqué ».	Cliquez sur le menu à droite de l'AU et sélectionnez **Restaurer la connexion**. Suivez les instructions pour restaurer votre unité d'acquisition : 1. Arrêtez le service Unité d'acquisition (AU). Vous pouvez cliquer sur le bouton *Copier la commande d'arrêt* pour copier rapidement la commande dans le presse-papiers, puis coller cette commande dans une invite de commande sur la machine de l'unité d'acquisition. 2. Créez un fichier nommé « token » dans le dossier *c:\Program Files\ Cloud Insights\Acquisition Unit\conf* sur l'AU. 3. Cliquez sur le bouton *Copier le jeton* et collez ce jeton dans le fichier que vous avez créé. 4. Redémarrez le service AU. Cliquez sur le bouton *Copier la commande de redémarrage* et collez la commande dans une invite de commande sur l'AU.
Les exigences du serveur ne sont pas satisfaites	Assurez-vous que votre serveur d'unité d'acquisition ou votre machine virtuelle répond"exigences"
Les exigences du réseau ne sont pas satisfaites	Assurez-vous que votre serveur/VM d'unité d'acquisition peut accéder à votre environnement Data Infrastructure Insights (<environment-name>.c01.cloudinsights.netapp.com) via une connexion SSL sur le port 443. Essayez les commandes suivantes : *ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com* Notez que le port 443 doit être ouvert « sortant » de l'AU vers Data Infrastructure Insights.
Le serveur proxy n'est pas configuré correctement	Vérifiez vos paramètres proxy et désinstallez/réinstallez le logiciel de l'unité d'acquisition si nécessaire pour entrer les paramètres proxy corrects. 1. Essayez « curl ». Reportez-vous aux informations/documentations « man curl » concernant les proxys : --preproxy, --proxy-* (il s'agit d'un caractère générique « * » car curl prend en charge de nombreux paramètres de proxy). 2. Essayez "wget". Consultez la documentation pour les options proxy.
L'installation de l'unité d'acquisition a échoué dans Data Infrastructure Insights avec des erreurs d'informations d'identification lors du démarrage du service d'acquisition (et visible dans le fichier acq.log).	Cela peut être dû à l'inclusion de caractères spéciaux dans les informations d'identification du proxy. Désinstallez l'AU (*sudo cloudinsights-uninstall.sh*) et réinstallez-le sans utiliser de caractères spéciaux.
Problèmes d'autorisation	Assurez-vous d'être connecté en tant qu'utilisateur avec des autorisations d'administrateur

L'acquisition ne fonctionne pas	Vous pouvez trouver des informations dans le fichier acq.log dans le dossier *<répertoire d'installation>\Cloud Insights\Acquisition Unit\log*. Redémarrer l'acquisition via les services Windows
Problèmes de collecte de données	Envoyez un rapport d'erreur depuis la page de destination du collecteur de données en cliquant sur le bouton « Envoyer un rapport d'erreur »
Statut : Échec du battement de cœur	L'unité d'acquisition (AU) envoie un battement de cœur à Data Infrastructure Insights toutes les 60 secondes pour renouveler son bail. Si l'appel de pulsation échoue en raison d'un problème de réseau ou d'une absence de réponse de Data Infrastructure Insights, la durée de bail de l'AU n'est pas mise à jour. Lorsque la durée du bail de l'AU expire, Data Infrastructure Insights affiche le statut « Échec du battement de cœur ». Étapes de dépannage : * Vérifiez la connexion réseau entre le serveur de l'unité d'acquisition et CloudInsights. * Vérifiez si le service Unité d'acquisition est en cours d'exécution. Si le service n'est pas en cours d'exécution, démarrez-le. * Vérifiez le journal de l'unité d'acquisition (<Répertoire d'installation>:\Program Files\ Cloud Insights\Acquisition Unit\log\acq.log) pour voir s'il y a des erreurs.
Je vois un message « Erreur de battement de cœur : »	Cette erreur peut se produire en cas d'interruption du réseau entraînant une interruption de la communication entre l'unité d'acquisition et l'environnement Data Infrastructure Insights pendant plus d'une minute. Vérifiez que la connexion entre l'AU et Data Infrastructure Insights est stable et active.

Considérations sur les proxys et les pare-feu

Si votre organisation nécessite l'utilisation d'un proxy pour l'accès à Internet, vous devrez peut-être comprendre le comportement du proxy de votre organisation et rechercher certaines exceptions pour que Data Infrastructure Insights fonctionne. Gardez à l'esprit les points suivants :

- Tout d'abord, votre organisation bloque-t-elle l'accès par défaut et autorise-t-elle uniquement l'accès à des sites Web/domaines spécifiques par exception ? Si tel est le cas, vous devrez ajouter le domaine suivant à votre liste d'exceptions :

  ```
  *.cloudinsights.netapp.com
  ```

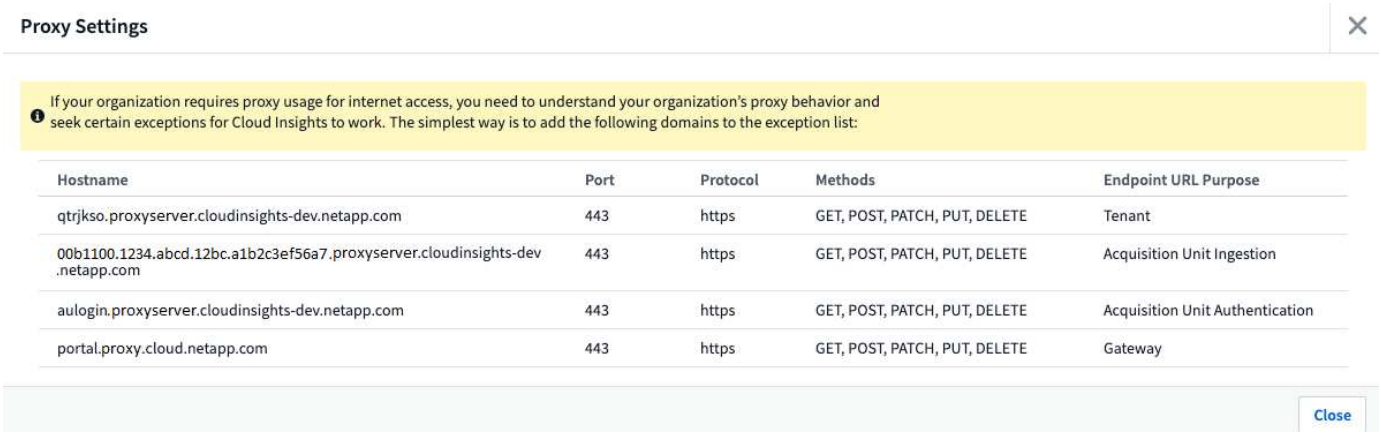
  Votre unité d'acquisition Data Infrastructure Insights , ainsi que vos interactions dans un navigateur Web avec Data Infrastructure Insights, seront toutes dirigées vers des hôtes portant ce nom de domaine.

- Deuxièmement, certains proxys tentent d'effectuer une inspection TLS/SSL en se faisant passer pour des sites Web Data Infrastructure Insights avec des certificats numériques non générés par NetApp. Le modèle de sécurité de l'unité d'acquisition Data Infrastructure Insights est fondamentalement incompatible avec ces technologies. Vous aurez également besoin du nom de domaine ci-dessus, exclu de cette

fonctionnalité, pour que l'unité d'acquisition de Data Infrastructure Insights puisse se connecter avec succès à Data Infrastructure Insights et faciliter la découverte de données.

Affichage des points de terminaison proxy

Vous pouvez afficher vos points de terminaison proxy en cliquant sur le lien **Paramètres proxy** lors du choix d'un collecteur de données lors de l'intégration, ou sur le lien sous *Paramètres proxy* sur la page **Aide > Assistance**. Un tableau comme celui-ci s'affiche. Si vous disposez de Workload Security dans votre environnement, les URL des points de terminaison configurés seront également affichées dans cette liste.



Ressources

Des conseils de dépannage supplémentaires peuvent être trouvés dans le"Base de connaissances NetApp" (connexion d'assistance requise).

Des informations d'assistance supplémentaires peuvent être trouvées dans Data Infrastructure Insights"Support" page.

Recherche sur un collecteur de données en échec

Si un collecteur de données présente un message d'échec et un impact élevé ou moyen, vous devez rechercher ce problème à l'aide de la page de résumé du collecteur de données avec ses informations liées.

Utilisez les étapes suivantes pour déterminer la cause des collecteurs de données défaillants. Les messages d'échec du collecteur de données s'affichent dans le menu **Admin** et sur la page **Collecteurs de données installés**.

Étapes

1. Cliquez sur **Admin** > **Collecteurs de données** > **Collecteurs de données installés**.
2. Cliquez sur le nom lié du collecteur de données défaillant pour ouvrir la page Résumé.
3. Sur la page Résumé, consultez la zone Commentaires pour lire les notes qui pourraient avoir été laissées par un autre ingénieur qui pourrait également enquêter sur cette panne.
4. Notez tous les messages de performance.
5. Déplacez le pointeur de votre souris sur les segments du graphique de la chronologie des événements pour afficher des informations supplémentaires.
6. Sélectionnez un message d'erreur pour un périphérique et affichez-le sous la chronologie des événements,

puis cliquez sur l’icône Détails de l’erreur qui s’affiche à droite du message.

Les détails de l’erreur incluent le texte du message d’erreur, les causes les plus probables, les informations utilisées et les suggestions de ce qui peut être essayé pour corriger le problème.

7. Dans la zone Appareils signalés par ce collecteur de données, vous pouvez filtrer la liste pour afficher uniquement les appareils qui vous intéressent, et vous pouvez cliquer sur le lien **Nom** d’un appareil pour afficher la page d’actif de cet appareil.
8. Lorsque vous revenez à la page de résumé du collecteur de données, vérifiez la zone **Afficher les modifications récentes** au bas de la page pour voir si des modifications récentes auraient pu causer le problème.

Matrice de support du collecteur de Data Infrastructure Insights

La matrice de prise en charge des collecteurs de données fournit une référence pour les collecteurs de données pris en charge par Data Infrastructure Insights , y compris les informations sur les fournisseurs et les modèles.

Stockage HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 7200 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7400c HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400c HP_3PAR 7440c HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 HP_3PAR 8440 InServ F200 InServ F400 InServ T400 InServ T800 InServ V400 InServ V800	3.1.1 (MU1) 3.1.2 (MU3) 3.1.3 (MU1) 3.1.3 (MU2) 3.2.1 (MU2) 3.2.1 (MU3) 3.2.1 (MU5) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 3.3.1 (MU1) 3.3.1 (MU2) 3.3.1 (MU3) 3.3.1 (MU5) 3.3.2 (MU1) 4.3.1 4.3.3 4.4.1 Type de version : Version avec support standard 4.5.15 Type de version : Version avec support étendu 4.5.18 Type de version : Version avec support étendu 4.5.21 Type de version : Version avec support étendu 4.5.24 Type de version : Version avec support étendu 4.5.7 Type de version : Version avec support étendu 4.6.1 Type de version : Version de support étendu 9.5.15 Type de version : Version de support étendu 9.5.8 Type de version : Version de support étendu 9.6.1 Type de version : Version de support étendu

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					stockage ?
		Capacité écrite	Mis en œuvre	SSH	Capacité totale
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Carte des volumes	LUN	Mis en œuvre	SSH	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	SSH	
		Port de stockage	Mis en œuvre	SSH	
		Type	Écart	SSH	
	Masque de volume	Initiateur	Mis en œuvre	SSH	
		Contrôleur de protocole	Mis en œuvre	SSH	
		Port de stockage	Mis en œuvre	SSH	
		Type	Écart	SSH	
	Volume Réf.	Nom	Mis en œuvre	SSH	
		IP de stockage	Mis en œuvre	SSH	
	Alias WWN	Alias d’hôte	Mis en œuvre	SSH	
		Type d’objet	Mis en œuvre	SSH	
		Source	Mis en œuvre	SSH	
		WWN	Mis en œuvre	SSH	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Ratio de blocage partiel	Mis en œuvre	SMI-S	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		ID du serveur	Mis en œuvre	SMI-S	
		Débit de lecture	Mis en œuvre	SMI-S	
		Débit total	Mis en œuvre	SMI-S	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	SMI-S	
		Écriture en attente	Mis en œuvre	SMI-S	écriture totale en attente

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
3Par SMI-S	SMI-S	HTTP/HTTPS	5988/5989		true	true	true	true
CLI 3Par	SSH	SSH	22		true	FAUX	true	true

Amazon AWS EC2

Modèles et versions pris en charge par ce collecteur de données : Versions d’API :

- 01/10/2014

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Disque de machine virtuelle	OID	Mis en œuvre	HTTPS	
		OID du disque virtuel	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		OID de la machine virtuelle	Mis en œuvre	HTTPS	
	Hôte	Système d’exploitation hôte	Mis en œuvre	HTTPS	
		adresses IP	Mis en œuvre	HTTPS	
		Fabricant	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		OID	Mis en œuvre	HTTPS	
	Informations	Description de l’API	Mis en œuvre	HTTPS	
		Nom de l’API	Mis en œuvre	HTTPS	
		Version de l’API	Mis en œuvre	HTTPS	
		Nom de la source de données	Mis en œuvre	HTTPS	Informations
		Date	Mis en œuvre	HTTPS	
		ID de l’expéditeur	Mis en œuvre	HTTPS	
		Clé d’origine	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	
	machine virtuelle	Utilisation totale du processeur	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		diskIops.total	Mis en œuvre	HTTPS	
		Écriture des IOPS sur disque	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d'écriture	Mis en œuvre	HTTPS	
		Débit de lecture du disque	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	débit total du disque en lecture
		Débit d'écriture du disque	Mis en œuvre	HTTPS	
		Débit de lecture IP	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit IP total
		ipThroughput.écriture	Mis en œuvre	HTTPS	
	Machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API EC2	HTTPS	HTTPS	443		true	true	true	true

Amazon AWS S3

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
S3	01/08/2010

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					les disques de rechange)
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Piscine de stockage	Inclure dans la capacité de l'eau chaude sanitaire	Mis en œuvre	HTTPS	Un moyen pour ACQ de contrôler quels pools de stockage sont intéressants dans DWH Capacity
		Nom	Mis en œuvre	HTTPS	
		Capacité du disque physique (Mo)	Mis en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe de raid	Mis en œuvre	HTTPS	indique si ce pool de stockage est un groupe RAID
		Rapport brut/utilisable	Mis en œuvre	HTTPS	ratio de conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance	Volume interne	Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		Total des objets	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API S3	HTTPS	HTTPS	443		true	true	true	true

Azure NetApp Files

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles
2019-06-01 2024-07-01	Azure NetApp Files

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S’agit-il d’un périphérique de virtualisation de stockage ?
		Commentaire	Écart	HTTPS	état : commentaire en texte libre décrivant le SVM

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre		
	Disque de pool de stockage	Lecture des IOP	Mis en œuvre		Nombre d’IOP en lecture sur le disque
		Les IOP écrivent	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit d’écriture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Total des IOP	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Azure Netapp Files	HTTPS	HTTPS	443		true	true	true	true

Commutateurs Fibre Channel Brocade

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
176,51 183,0 Brocade 200E Brocade 300E Brocade 4024 Intégré Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480 Intégré Brocade 6505 Brocade 6510 Brocade 6520 Brocade 6546 Brocade 6547 Intégré Brocade 6548 Brocade 6558 Brocade 7800 Brocade 7810 Commutateur d'extension Brocade 7840 Brocade DCX Brocade DCX-4S Backbone Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade M5424 Intégré Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v6.2.2b v6.2.2f v6.2.2g v6.4.1b v6.4.2a v6.4.3 v6.4.3d v6.4.3f3 v7.0.1 v7.0.1b v7.0.2 v7.0.2b1 v7.0.2c v7.0.2e v7.0.2e1 v7.1.0a v7.1.0b v7.2.0a v7.2.0d v7.2.1 v7.2.1c v7.2.1c1 v7.2.1d v7.3.0a v7.3.0c v7.3.1 v7.3.1c v7.3.1d v7.3.2a v7.4.0a v7.4.1 v7.4.1d v7.4.1e v7.4.2 v7.4.2a v7.4.2a4 v7.4.2c v7.4.2d v7.4.2e v7.4.2f v7.4.2g v7.4.2g_cvr_824494_01 v7.4.2h v7.4.2j1 v8.0.2c v8.0.2d v8.0.2f v8.1.0b v8.1.1a v8.1.2a v8.1.2d v8.1.2f v8.1.2g v8.1.2h v8.1.2j v8.1.2k v8.2.0 v8.2.0a v8.2.0a1 v8.2.0b v8.2.1 v8.2.1a v8.2.1c v8.2.1d v8.2.2a v8.2.2b v8.2.2c v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3a1 v8.2.3a_cvr_855776_01 v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v8.2.3e2 v9.0.0a v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1 v9.1.1a v9.1.1b v9.1.1b_lw v9.1.1c v9.1.1d v9.1.1d1 v9.1.1d2 v9.1.1d2_lw v9.1.1d5 v9.2.0a v9.2.0b v9.2.0b1_lw v9.2.0c v9.2.0c1 v9.2.1a v9.2.1a1 v9.2.2

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		WWN	Mis en œuvre	SSH	
	Zone	Nom de la zone	Mis en œuvre	SSH	
		Type	Ecart	SSH	
	Membre de la zone	WWN	Mis en œuvre	SSH	
	Capacités de zonage	Configuration active	Mis en œuvre	SSH	
		Nom de la configuration	Mis en œuvre	SSH	
		Comportement de zonage par défaut	Mis en œuvre	SSH	
		WWN	Mis en œuvre	SSH	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Perte de synchronisation			perte de synchronisation
		Erreur de port,	Mis en œuvre	SNMP	Délai d'expiration
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		transmission			
		Nombre total d'erreurs de port	Mis en œuvre	SNMP	Nombre total d'erreurs de port
		ID du serveur	Mis en œuvre	SNMP	
		Taux de trame du trafic	Mis en œuvre	SNMP	
		Taux de trame du trafic total	Mis en œuvre	SNMP	
		Taux de trame du trafic	Mis en œuvre	SNMP	
		Taille moyenne du cadre	Mis en œuvre	SNMP	Taille moyenne des trames de trafic
		Cadres TX	Mis en œuvre	SNMP	taille moyenne de la trame du trafic
		Taux de trafic reçu	Mis en œuvre	SNMP	
		Taux de trafic total	Mis en œuvre	SNMP	
		Taux de transmission du trafic	Mis en œuvre	SNMP	
		Utilisation du trafic reçu	Mis en œuvre	SNMP	
		Utilisation totale du trafic	Mis en œuvre	SNMP	Utilisation totale du trafic
		Utilisation de la transmission du trafic	Mis en œuvre	SNMP	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
SNMP Brocade	SNMP	SNMPv1, SNMPv2, SNMPv3	161		true	true	true	true
Brocade SSH	SSH	SSH	22		FAUX	FAUX	true	true
Configuration de l'assistant de source de données	Saisie manuelle				true	true	true	true

Conseiller réseau Brocade HTTP

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
14.4.3 14.4.4	Brocade 6520 Brocade DCX 8510-4 Brocade G620 Brocade X6-8 EMC Connectrix DS-6510B	v7.3.0b v7.4.1b v8.2.3c1 v9.0.1e1

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		WWN	Mis en œuvre	HTTP/S	
	Zone	Nom de la zone	Mis en œuvre	HTTP/S	
	Membre de la zone	Type	Mis en œuvre	HTTP/S	
		WWN	Mis en œuvre	HTTP/S	
	Capacités de zonage	Configuration active	Mis en œuvre	HTTP/S	
		Nom de la configuration	Mis en œuvre	HTTP/S	
		WWN	Mis en œuvre	HTTP/S	
performance	port	Crédit BB zéro transmis	Mis en œuvre	HTTP/S	Crédit BB zéro transmis
		Crédit BB zéro total	Mis en œuvre	HTTP/S	Crédit BB zéro total
		BB Crédit Zéro Ms Transmis	Mis en œuvre	HTTP/S	BB Crédit Zéro Ms Transmis

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST de Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

Brocade FOS REST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
183,0 184,0 190,0 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7810 Commutateur d'extension Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v8.2.2a v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v9.0.0b v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1a v9.1.1b v9.1.1c v9.1.1c3 v9.1.1d v9.1.1d1 v9.1.1d1_lw v9.1.1d2 v9.1.1d3_cvr_861742_01 v9.2.0a v9.2.0b v9.2.0b1 v9.2.0b_cvr_857687_01 v9.2.0c v9.2.0c3 v9.2.1 v9.2.1a v9.2.1b v9.2.2

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
780					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		WWN	Mis en œuvre	HTTPS	
	Zone	Nom de la zone	Mis en œuvre	HTTPS	
	Membre de la zone	Type	Ecart	HTTPS	
		WWN	Mis en œuvre	HTTPS	
	Capacités de zonage	Configuration active	Mis en œuvre	HTTPS	
		Nom de la configuration	Mis en œuvre	HTTPS	
		Comportement de zonage par défaut	Mis en œuvre	HTTPS	
		WWN	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Perte de synchronisation			perte de synchronisation
		Nombre total d'erreurs de port	Mis en œuvre	HTTPS	Nombre total d'erreurs de port
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		ID du serveur	Mis en œuvre	HTTPS	
		Taux de trame du trafic	Mis en œuvre	HTTPS	
		Taux de trame du trafic total	Mis en œuvre	HTTPS	
		Taux de trame du trafic	Mis en œuvre	HTTPS	
		Taille moyenne du cadre	Mis en œuvre	HTTPS	Taille moyenne des trames de trafic
		Cadres TX	Mis en œuvre	HTTPS	taille moyenne de la trame du trafic
		Taux de trafic reçu	Mis en œuvre	HTTPS	
		Taux de trafic total	Mis en œuvre	HTTPS	
		Taux de transmission du trafic	Mis en œuvre	HTTPS	
		Utilisation du trafic reçu	Mis en œuvre	HTTPS	
		Utilisation totale du trafic	Mis en œuvre	HTTPS	Utilisation totale du trafic
		Utilisation de la transmission du trafic	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Brocade FOS	HTTPS		443		true	true	true	true

Commutateurs Cisco MDS et Nexus Fabric

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
DS-C9124-2-K9 DS-C9124-K9 DS-C9132T-K9 DS-C9148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148T-K9 DS-C9148V-K9 DS-C9220I-K9 DS-C9222I-K9 DS-C9250I-K9 DS-C9396S-K9 DS-C9396T-K9 DS-C9396V-K9 DS-C9506 DS-C9509 DS-C9513 DS-C9706 DS-C9710 DS-C9718 DS-HP-8GFC-K9 DS-HP-FC-K9 N5K-C5548UP N5K-C5596UP N5K-C5696Q UCS-FI-6248UP UCS-FI-6296UP UCS-FI-6332 UCS-FI-6332-16UP UCS-FI-64108 UCS-FI-6454	3,3(1c) 4,1(3a) 4,2(1a) 5,0(1a) 5,0(3)N2(3.11e) 5,0(3)N2(4.01d) 5,0(3)N2(4.13i) 5,0(3)N2(4.21e) 5,0(3)N2(4.21j) 5,0(3)N2(4,21k) 5,0(3)N2(4,22c) 5,0(3)N2(4,23f) 5,0(3)N2(4,23g) 5,0(3)N2(4,34a) 5,0(8) 5,2(2d) 5,2(8) 5,2(8a) 5,2(8b) 5.2(8c) 5,2(8d) 5,2(8f) 5,2(8g) 5,2(8h) 5,2(8i) 6,2(11) 6,2(11b) 6,2(11c) 6,2(13) 6,2(13a) 6,2(15) 6,2(17) 6,2(19) 6,2(21) 6,2(23) 6,2(25) 6,2(27) 6,2(29) 6,2(31) 6,2(33) 6,2(5a) 6,2(7) 6,2(9) 6,2(9a) 6,2(9b) 7,0(3)N2(4.04e) 7,0(3)N2(4.13b) 7,0(3)N2(4,13g) 7,3(0)D1(1) 7,3(1)DY(1) 7,3(13)N1(1) 7,3(8)N1(1) 8,1(1) 8,1(1a) 8,2(1) 8,2(2) 8,3(1) 8,3(2) 8,4(1) 8.4(1a) 8.4(2) 8.4(2a) 8.4(2b) 8.4(2c) 8.4(2d) 8.4(2e) 8.4(2f) 8.5(1) 9.2(1a) 9.2(2) 9.3(1) 9.3(2) 9.3(2a) 9.3(5)I42(1b) 9.3(5)I42(1g) 9.3(5)I42(1j) 9.3(5)I42(1k) 9.3(5)I42(3f) 9.3(5)I43(4b) 9.4(1) 9.4(1a) 9.4(2) 9.4(2a) 9.4(3)

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		commutateur			
		Type	Écart	SNMP	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		VSAN active	Mis en œuvre	SNMP	
		WWN	Mis en œuvre	SNMP	
	Inconnu	Conducteur	Mis en œuvre	SNMP	
		Micrologiciel	Mis en œuvre	SNMP	
		Généré	Mis en œuvre	SNMP	
		Fabricant	Mis en œuvre	SNMP	
		Modèle	Mis en œuvre	SNMP	
		Nom	Mis en œuvre	SNMP	
		WWN	Mis en œuvre	SNMP	
	Alias WWN	Alias d’hôte	Mis en œuvre	SNMP	
		Type d’objet	Mis en œuvre	SNMP	
		Source	Mis en œuvre	SNMP	
		WWN	Mis en œuvre	SNMP	
	Zone	Nom de la zone	Mis en œuvre	SNMP	
		Type de zone	Mis en œuvre	SNMP	
	Membre de la zone	Type	Écart	SNMP	
		WWN	Mis en œuvre	SNMP	
	Capacités de zonage	Configuration active	Mis en œuvre	SNMP	
		Nom de la configuration	Mis en œuvre	SNMP	
		Comportement de zonage par défaut	Mis en œuvre	SNMP	
		Contrôle de fusion	Mis en œuvre	SNMP	
		WWN	Mis en œuvre	SNMP	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		de la transmission			port
		Nombre total d'erreurs de port	Mis en œuvre	SNMP	Nombre total d'erreurs de port
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		ID du serveur	Mis en œuvre	SNMP	
		Taux de trame du trafic	Mis en œuvre	SNMP	
		Taux de trame du trafic total	Mis en œuvre	SNMP	
		Taux de trame du trafic	Mis en œuvre	SNMP	
		Taille moyenne du cadre	Mis en œuvre	SNMP	Taille moyenne des trames de trafic
		Cadres TX	Mis en œuvre	SNMP	taille moyenne de la trame du trafic
		Taux de trafic reçu	Mis en œuvre	SNMP	
		Taux de trafic total	Mis en œuvre	SNMP	
		Taux de transmission du trafic	Mis en œuvre	SNMP	
		Utilisation du trafic reçu	Mis en œuvre	SNMP	
		Utilisation totale du trafic	Mis en œuvre	SNMP	Utilisation totale du trafic
		Utilisation de la transmission du trafic	Mis en œuvre	SNMP	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Cisco SNMP	SNMP	SNMPv1 (inventaire uniquement), SNMPv2, SNMPv3	161		true	true	true	true

Cohésion

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Nœud de calcul C4000 C4600 C5036 C5066 C6025 C6035 C6055 CX8405 PXG1 UCS-C240M5H10 ROBO virtuel	6.8.1_u1_version-20221022_6f58ed2a 6.8.2_u1_version-20240509_a5da4644 7.1.2_u2_version-20240925_66722648 7.1.2_u3_version-20241231_bb47fe77 7.2.1_version-20241114_794eae46 7.2.2_version-20250228_63e93ccf

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					utilisable en capacité brute
		Statut	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Activation de stockage	Mis en œuvre		
		Provisionnement léger pris en charge	Mis en œuvre		Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre		
		Capacité totale utilisée	Mis en œuvre		Capacité totale en Mo
		Type	Écart		
		Virtuel	Mis en œuvre		S’agit-il d’un périphérique de virtualisation de stockage ?
		Crypté	Mis en œuvre		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance	Stockage	Échec de la capacité brute	Mis en œuvre		
		Capacité brute	Mis en œuvre		
		Capacité brute de réserve	Mis en œuvre		Capacité brute des disques de rechange (somme de tous les disques de rechange)
		Capacité des pools de stockage	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Clé	Mis en œuvre		
		Latence de lecture	Mis en œuvre		
		Latence totale	Mis en œuvre		
		Latence d'écriture	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		
		Utilisation totale	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Cohesity	HTTPS	HTTPS	443		true	true	true	true

EMC Celerra (SSH)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
NSX VG8 VNX5200 VNX5300 VNX5400 VNX5500	5.5.38-1 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.9-155

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					en Mo
		Instantané de la capacité utilisée	Mis en œuvre	SSH	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Attribut de stockage	Mis en œuvre	SSH	
		Provisionnement léger pris en charge	Mis en œuvre	SSH	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	SSH	
		Capacité totale utilisée	Mis en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtuel	Mis en œuvre	SSH	S'agit-il d'un périphérique de virtualisation de stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Celerra CLI	SSH	SSH			true	FAUX	true	true

EMC CLARiiON (NaviCLI)

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
6,26 6,28 7,32 7,33	CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600	04.28.000.5.710 05.32.000.5.206 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.008.5.119 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266 05.33.021.5.322 3.26.40.5.029

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Cible réplica	Mis en œuvre	CLI	
		ID du pool de stockage	Mis en œuvre	CLI	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Provisionnement léger	Mis en œuvre	CLI	
		Type	Écart	CLI	
		UUID	Mis en œuvre	CLI	
		Capacité utilisée	Mis en œuvre	CLI	
	Carte des volumes	LUN	Mis en œuvre	CLI	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	CLI	
		Port de stockage	Mis en œuvre	CLI	
		Type	Écart	CLI	
	Masque de volume	Initiateur	Mis en œuvre	CLI	
		Contrôleur de protocole	Mis en œuvre	CLI	
		Port de stockage	Mis en œuvre	CLI	
		Type	Écart	CLI	
	Membre du volume	Capacité	Mis en œuvre	CLI	Instantané Capacité utilisée en Mo
		Nom	Mis en œuvre	CLI	
		Rang	Mis en œuvre	CLI	
		Capacité brute totale	Mis en œuvre	CLI	Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre	CLI	Niveau de redondance
		ID du pool de stockage	Mis en œuvre	CLI	
		Capacité utilisée	Mis en œuvre	CLI	
	Alias WWN	Alias d'hôte	Mis en œuvre	CLI	
		propriété intellectuelle	Mis en œuvre	CLI	
		Type d'objet	Mis en œuvre	CLI	
		Source	Mis en œuvre	CLI	
		WWN	Mis en œuvre	CLI	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Utilisation de la lecture	Mis en œuvre	CLI	
		Utilisation totale	Mis en œuvre	CLI	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation Écriture	Mis en œuvre	CLI	
	Volume	Taux de réussite du cache en lecture	Mis en œuvre	CLI	
		Taux de réussite du cache total	Mis en œuvre	CLI	
		Taux de réussite du cache en écriture	Mis en œuvre	CLI	
		Capacité brute	Mis en œuvre	CLI	
		Capacité totale	Mis en œuvre	CLI	
		Capacité utilisée	Mis en œuvre	CLI	
		Ratio de capacité utilisée	Mis en œuvre	CLI	
		Lecture des IOP	Mis en œuvre	CLI	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	CLI	
		Les IOP écrivent	Mis en œuvre	CLI	
		Latence de lecture	Mis en œuvre	CLI	
		Latence totale	Mis en œuvre	CLI	
		Latence d'écriture	Mis en œuvre	CLI	
		Ratio de blocage partiel	Mis en œuvre	CLI	
		Débit de lecture	Mis en œuvre	CLI	
		Débit total	Mis en œuvre	CLI	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	CLI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Navi CLI	CLI		6389,2162,2163,443(HTTPS)/80(HTTP)		true	true	true	FAUX

Domaine de données EMC (SSH)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
DD VE DD2500 DD3300 DD4200 DD6300 DD6400 DD6800 DD6900 DD7200 DD9300 DD9400 DD9410 DD9500 DD9800 DD990 DD9900 DD9910	6.0.2.30-606339 6.1.2.051-633576 6.1.2.20-606786 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.20-1023227 7.10.1.0-1042928 7.10.1.1-1049892 7.10.1.10-1068159 7.10.1.15-1078832 7.10.1.20-1090468 7.10.1.30-1105324 7.10.1.40-1126469 7.10.1.50-1146826 7.11.0.0-1035502 7.13.0.20-1082704 7.2.0.20-658029 7.2.0.60-682124 7.2.0.70-686759 7.2.0.90-692270 7.7.4.0-1017976 7.7.5.1-1040473 7.7.5.11-1046187 7.7.5.25-1078970 7.7.5.30-1091295 8.0.0.10-1097914 8.1.0.10-1127744

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
830					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Rapport brut/utilisable	Mis en œuvre	SSH	ratio de conversion de la capacité brute
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		ID du pool de stockage	Mis en œuvre	SSH	
		Provisionnement léger pris en charge	Mis en œuvre	SSH	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	SSH	
		Capacité totale utilisée	Mis en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtuel	Mis en œuvre	SSH	S'agit-il d'un périphérique de virtualisation de stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Interface de ligne de commande du domaine de données	SSH	SSH	22		true	true	true	true

CEM ECS

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
ECS	3.6.1.3 3.6.2.1 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.6 3.8.0.1 3.8.0.2 3.8.0.3 3.8.0.4 3.8.0.5 3.8.0.6 3.8.1.1 3.8.1.2 3.8.1.3

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		nœud utilisable en Mo			
		Utilisation de la capacité du nœud utilisée en Mo	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Piscine de stockage	Inclure dans la capacité de l'eau chaude sanitaire	Mis en œuvre	HTTPS	Un moyen pour ACQ de contrôler quels pools de stockage sont intéressants dans DWH Capacity
		Nom	Mis en œuvre	HTTPS	
		Capacité du disque physique (Mo)	Mis en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe de raid	Mis en œuvre	HTTPS	indique si ce pool de stockage est un groupe RAID
		Rapport brut/utilisable	Mis en œuvre	HTTPS	ratio de conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	
	Disque de pool de stockage	Capacité provisionnée	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité de dépassement d'engagement	Mis en œuvre	HTTPS	Présenté comme une série chronologique
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST EMC ECS	HTTPS	HTTPS	443		true	true	true	true

Dell EMC Isilon et PowerScale Rest

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
A100 A200 A2000 A300 A3000 F200 F600 F800 F900 H400 H500 H5600 H600 H700 NL410 S210 X210 X410	9.1.0.10 9.1.0.6 9.1.0.9 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.13 9.2.1.19 9.2.1.4 9.2.1.9 9.4.0.11 9.4.0.13 9.4.0.14 9.4.0.15 9.4.0.16 9.4.0.17 9.4.0.18 9.5.0.3 9.5.0.5 9.5.0.6 9.5.0.7 9.5.0.8 9.5.1.0 9.5.1.1 9.5.1.2 9.7.1.0 9.7.1.2 9.7.1.3 9.7.1.4 9.7.1.5 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.1.0.4 v8.1.2.0 v9.0.0.0

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					RAID
		Rapport brut/utilisable	Mis en œuvre	HTTPS	ratio de conversion de la capacité brute
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Instantané de la capacité allouée	Écart	HTTPS	Capacité allouée aux snapshots en Mo
		Instantané de la capacité utilisée	Mis en œuvre	HTTPS	
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d’écriture	Mis en œuvre	HTTPS	Mo/s

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST EMC Isilon et PowerScale	HTTPS		443		true	true	true	true

Dell EMC Isilon / PowerScale (CLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
A200 H400 H500 NL400 NL410 S210 Traceback (dernier appel le plus récent) : X200 X400 X410	9.1.0.18 9.1.0.19 9.2.1.12 9.2.1.13 9.2.1.15 9.4.0.17 9.5.0.3 9.5.0.6 9.5.0.8 9.7.1.2 9.8.0.2 v7.2.0.5 v7.2.1.3 v7.2.1.6 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.0.1.1 v8.1.2.0

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					léger pour la couche de volume située au-dessus de lui
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité totale allouée	Mis en œuvre	SSH	
		Capacité totale utilisée	Mis en œuvre	SSH	Capacité totale en Mo
		Type	Écart	SSH	
		Virtuel	Mis en œuvre	SSH	S’agit-il d’un périphérique de virtualisation de stockage ?

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mis en œuvre	SSH	
		Utilisation totale	Mis en œuvre	SSH	
	Disque de pool de stockage	Capacité totale	Mis en œuvre	SSH	
		Ratio de capacité utilisée	Mis en œuvre	SSH	
		Capacité totale de données	Mis en œuvre	SSH	
		Capacité provisionnée	Mis en œuvre	SSH	
		Capacité de données utilisées	Mis en œuvre	SSH	
		Capacité utilisée	Mis en œuvre	SSH	
		Capacité brute	Mis en œuvre	SSH	
		Ratio de capacité de dépassement d'engagement	Mis en œuvre	SSH	Présenté comme une série chronologique
		Instantané de la capacité utilisée	Mis en œuvre	SSH	
		Capacité réservée aux instantanés	Mis en œuvre	SSH	
		Instantané du ratio de capacité utilisée	Mis en œuvre	SSH	Présenté comme une série chronologique

API de gestion utilisées par ce collecteur de données :

API	**Protocole utilisé**	**Protocole de couche de transport utilisé**	**Ports entrants utilisés**	**Ports sortants utilisés**	**Prend en charge l'authentification**	**Nécessite uniquement des informations d'identification en « lecture seule »**	**Prend en charge le cryptage**	**Compatible avec le pare-feu (ports statiques)**
Isilon SSH	SSH	SSH	22		true	FAUX	true	true

EMC PowerStore REST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5200T PowerStore 9000T PowerStore 9200T	2.1.0.1 2.1.1.0 3.2.0.1 3.2.1.0 3.2.1.1 3.5.0.1 3.5.0.2 3.6.0.0 3.6.1.0 3.6.1.1 3.6.1.2 3.6.1.3 3.6.1.4 4.0.0.1 4.0.0.2 4.0.1.0

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Masque de volume	Initiateur	Mis en œuvre		
		Contrôleur de protocole	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart		
	Alias WWN	Alias d’hôte	Mis en œuvre		
		Type d’objet	Mis en œuvre		
		Source	Mis en œuvre		
		WWN	Mis en œuvre		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre		
	Volume	Capacité brute	Mis en œuvre		
		Capacité totale	Mis en œuvre		
		Capacité utilisée	Mis en œuvre		
		Ratio de capacité utilisée	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Clé	Mis en œuvre		
		Latence de lecture	Mis en œuvre		
		Latence totale	Mis en œuvre		
		Latence d’écriture	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST EMC PowerStore	HTTPS	HTTPS	443		true	true	true	true

EMC RecoverPoint (HTTP)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Point de récupération	5.1.SP4.P1(h.89) 5.1.SP4.P2(h.101) 5.1.SP4.P3(h.109) 5.1.SP4.P4(h.97) 5.1.SP4.P5(h.138)

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					les disques de rechange)
		Virtuel	Mis en œuvre	HTTPS	S’agit-il d’un périphérique de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Nœud de stockage	Taille de la mémoire	Écart	HTTPS	mémoire de l’appareil en Mo
		Modèle	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		Nombre de processeurs	Mis en œuvre	HTTPS	processeur de l’appareil
		Numéro de série	Mis en œuvre	HTTPS	
		État	Mis en œuvre	HTTPS	texte libre décrivant l’état de l’appareil
		UUID	Mis en œuvre	HTTPS	
		Version	Mis en œuvre	HTTPS	version du logiciel
	Synchronisation du stockage	Mode	Mis en œuvre	HTTPS	
		Énumération des modes	Mis en œuvre	HTTPS	
		Stockage source	Mis en œuvre	HTTPS	
		Volume source	Mis en œuvre	HTTPS	
		État	Mis en œuvre	HTTPS	texte libre décrivant l’état de l’appareil
		Énumération d’état	Mis en œuvre	HTTPS	
		Stockage cible	Mis en œuvre	HTTPS	
		Volume cible	Mis en œuvre	HTTPS	
		Technologie	Mis en œuvre	HTTPS	technologie qui modifie l’efficacité du stockage

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST RecoverPoint	HTTPS	HTTPS	443		true	true	true	true

EMC ScaleIO et PowerFlex REST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
ScaleIO	R3_5.1201.101 R3_6.1000.134

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S’agit-il d’un

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					préformatées de stockage ?
	Volume	Capacité	Mis en œuvre	HTTPS	Instantané Capacité utilisée en Mo
		Chemin de jonction	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		Capacité brute totale	Mis en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la matrice)
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		IP de l’hôte	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance	Stockage	Échec de la capacité brute	Mis en œuvre		
		Capacité brute	Mis en œuvre		
		Capacité brute de réserve	Mis en œuvre		Capacité brute des disques de rechange (somme de tous les disques de rechange)
		Capacité des pools de stockage	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Clé	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST EMC ScaleIO et PowerFlex	HTTPS	HTTPS	443		true	true	true	true

Interface de ligne de commande EMC Symmetrix

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
V10.0.0.0 V10.0.1.1 V10.1.0.0 V10.1.0.1 V10.1.0.3 V10.1.0.5 V10.2.0.0 V8.3.0.6 V8.4.0.7 V8.4.0.9 V9.1.0.5 V9.1.0.6 V9.2.1.0 V9.2.2.0 V9.2.3.0 V9.2.3.1 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.8	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5876.286.194(16F40000) version 115 5876.309.196(16F40000) version 153 5876.309.196(16F40000) version 162 5876.309.196(16F40000) version 94 5977.1151.1151(17590000) version 45 5977.1151.1151(17590000) version 60 5977.1151.1151(17590000) version 9 5978.711.711(175A0000) version 320 5978.711.711(175A0000) version 335 5978.711.711(175A0000) version 365 5978.711.711(175A0000) version 416 5978.711.711(175A0000) version 436 5978.711.711(175A0000) version 438 5978.711.711(175A0000) version 448 5978.711.711(175A0000) version 484 5978.711.711(175A0000) version 542 5978.711.711(175A0000) version 581 5978.714.714(175A0000) version 1 5978.714.714(175A0000) version 101 5978.714.714(175A0000) version 108 5978.714.714(175A0000) version 117 5978.714.714(175A0000) version 137 5978.714.714(175A0000) version 145 5978.714.714(175A0000) version 34 5978.714.714(175A0000) version 49 5978.714.714(175A0000) version 53 5978.714.714(175A0000) version 79

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	masque de volume	Initiateur	Mis en œuvre		
	volume	Contrôleur de protocole	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mis en œuvre		
		Type	Écart		
	Membre du volume	Hiérarchisation automatique	Mis en œuvre		indique si ce pool de stockage participe à la hiérarchisation automatique avec d'autres pools
		Capacité	Mis en œuvre		Instantané Capacité utilisée en Mo
		Cylindres	Mis en œuvre		
		Nom	Mis en œuvre		
		Rang	Mis en œuvre		
		Capacité brute totale	Mis en œuvre		Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre		Niveau de redondance
		ID du pool de stockage	Mis en œuvre		
		UUID	Mis en œuvre		
	Volume Réf.	Nom	Mis en œuvre		
		IP de stockage	Mis en œuvre		
	Alias WWN	Alias d'hôte	Mis en œuvre		
		Type d'objet	Mis en œuvre		
		Source	Mis en œuvre		
		WWN	Mis en œuvre		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Écriture en attente	Mis en œuvre		attente
	Volume	Taux de réussite du cache en lecture	Mis en œuvre		
		Taux de réussite du cache total	Mis en œuvre		
		Taux de réussite du cache en écriture	Mis en œuvre		
		Capacité brute	Mis en œuvre		
		Capacité totale	Mis en œuvre		
		Capacité utilisée	Mis en œuvre		
		Capacité écrite	Mis en œuvre		
		Ratio de capacité utilisée	Mis en œuvre		
		Ratio de capacité écrit	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Clé	Mis en œuvre		
		Latence de lecture	Mis en œuvre		
		Latence totale	Mis en œuvre		
		Latence d'écriture	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		
		Écriture en attente	Mis en œuvre		écriture totale en attente

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
symcli	CLI		2707		true	true	true	true
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		true	FAUX	FAUX	true

Dell Unisphere REST

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
V10.0.0.5 V10.0.1.5 V10.1.0.1 V10.1.0.5 V10.1.0.6 V10.1.0.8 V10.2.0.1 V10.2.0.2 V9.2.3.15 V9.2.3.20 V9.2.3.22 V9.2.3.4 V9.2.4.1 V9.2.4.10 V9.2.4.11 V9.2.4.12 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.9	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX200K VMAX250F VMAX400K VMAX450F VMAX950F	5977.1131.1131 construction 615 5977.1151.1151 construction 60 construction 60 5978.711.711 construction 205 5978.711.711 construction 335 construction 335 5978.711.711 construction 365 5978.711.711 construction 416 5978.711.711 construction 436 construction 436 5978.711.711 construction 438 5978.711.711 construction 448 5978.711.711 construction 471 5978.711.711 construction 484 5978.711.711 construction 484 construction 484 5978.711.711 build 542 5978.711.711 build 542 build 542 5978.711.711 build 581 5978.711.711 build 75 5978.711.711 build 8 build 8 5978.714.711 build 49 5978.714.714 build 1 build 1 5978.714.714 build 101 build 101 5978.714.714 build 108 5978.714.714 build 117 5978.714.714 build 117 build 117 5978.714.714 build 131 build 131 5978.714.714 build 137 5978.714.714 build 137 build 137 5978.714.714 build 145 5978.714.714 build 149 build 149 5978.714.714 build 34 5978.714.714 build 49 5978.714.714 build 49 build 49 5978.714.714 build 79 5978.714.714 build 79 build 79 6079.175.0 build 161 build 161 6079.175.0 build 259 build 259 6079.225.0 build 127 build 127 6079.225.0 build 216 build 216 6079.225.0 build 218 build 218 6079.225.0 build 291 build 291 6079.225.0 build 331 build 331 6079.225.0 build 86 build 86 6079.275.0 build 221 build 221

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					stockage ?
		Capacité écrite	Mis en œuvre	HTTPS	Capacité totale
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Pourcentage de capacité effectivement utilisée	Mis en œuvre	HTTPS	
		Compression activée	Mis en œuvre	HTTPS	
		groupes de stockage	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Alias WWN	Alias d’hôte	Mis en œuvre	HTTPS	
		Type d’objet	Mis en œuvre	HTTPS	
		Source	Mis en œuvre	HTTPS	
		WWN	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Volume	Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit d’écriture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence d’écriture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Total des IOP	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Économies totales de compression	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API Dell Unisphere	HTTPS	HTTPS	443		true	true	true	true

EMC VNX (SSH)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
VNX5300 VNX5500 VNX5700	05.32.000.5.216 05.32.000.5.221 05.32.000.5.249 7.1.76-4 7.1.80-3

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Port de stockage	Mis en œuvre	SSH	
		Contrôleur de protocole	Mis en œuvre	SSH	
		Type	Écart	SSH	
	Masque de volume	Port de stockage	Mis en œuvre	SSH	
		Initiateur	Mis en œuvre	SSH	
		Contrôleur de protocole	Mis en œuvre	SSH	
		Type	Écart	SSH	
	Membre du volume	Nom	Mis en œuvre	SSH	
		ID du pool de stockage	Mis en œuvre	SSH	
		Rang	Mis en œuvre	SSH	
		Capacité	Mis en œuvre	SSH	Instantané Capacité utilisée en Mo
		Capacité brute totale	Mis en œuvre	SSH	Capacité brute totale (somme de tous les disques de la matrice)
		Capacité utilisée	Mis en œuvre	SSH	
		Redondance	Mis en œuvre	SSH	Niveau de redondance
	Alias WWN	Source	Mis en œuvre	SSH	
		Alias d'hôte	Mis en œuvre	SSH	
		WWN	Mis en œuvre	SSH	
		Type d'objet	Mis en œuvre	SSH	
		propriété intellectuelle	Mis en œuvre	SSH	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
960					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité provisionnée	Mis en œuvre	SSH	
		Ratio de	Mis en œuvre	SSH	Présenté comme

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Capacité de provisionnement d'engagement			
	Volume	Latence totale	Mis en œuvre	SSH	
		Ratio de blocage partiel	Mis en œuvre	SSH	
		Latence de lecture	Mis en œuvre	SSH	
		Les IOP écrivent	Mis en œuvre	SSH	
		Débit de lecture	Mis en œuvre	SSH	
		Total des IOP	Mis en œuvre	SSH	
		Latence d'écriture	Mis en œuvre	SSH	
		Lecture des IOP	Mis en œuvre	SSH	Nombre d'IOP en lecture sur le disque
		Taux de réussite du cache en lecture	Mis en œuvre	SSH	
		Taux de réussite du cache total	Mis en œuvre	SSH	
		Taux de réussite du cache en écriture	Mis en œuvre	SSH	
		Débit d'écriture	Mis en œuvre	SSH	
		Débit total	Mis en œuvre	SSH	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
VNX SSH et CLI	SSH	SSH	22		true	FAUX	true	true

EMC VNXe et Unity Unisphere (CLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Unity 300 Unity 300F Unity 350F Unity 380 Unity 380F Unity 400 Unity 400F Unity 450F Unity 480 Unity 480F Unity 500 Unity 550F Unity 600F Unity 650F Unity 680F Unity 880 Unity 880F UnityVSA VNXe3200	3.1.17.10229825 4.1.2.9257522 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.3.1.0.6.028 5.4.0.0.5.094 5.4.1.0.5.006

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Volume cible	Mis en œuvre	HTTPS	
		Technologie	Mis en œuvre	HTTPS	technologie qui
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Capacité	Mis en œuvre	HTTPS	Instantané Capacité utilisée en Mo
		Chemin de jonction	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		Capacité brute totale	Mis en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la matrice)
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Volume	Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Interface de ligne de commande VNXe et Unisphere	HTTPS	HTTPS	443		true	true	true	true

EMC VPLEX

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
VPLEX	6.2.0.04.00.07 6.2.0.07.00.02 6.2.1.0.0.519

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Capacité totale allouée	Mis en œuvre	HTTP/S	
		Capacité totale utilisée	Mis en œuvre	HTTP/S	Capacité totale en Mo
		Type	Écart	HTTP/S	
		Virtuel	Mis en œuvre	HTTP/S	S’agit-il d’un périphérique de virtualisation de stockage ?
	Volume	Capacité	Mis en œuvre	HTTP/S	Instantané Capacité utilisée en Mo
		Nom	Mis en œuvre	HTTP/S	
		Capacité brute totale	Mis en œuvre	HTTP/S	Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre	HTTP/S	Niveau de redondance
		ID du pool de stockage	Mis en œuvre	HTTP/S	
		Provisionnement léger	Mis en œuvre	HTTP/S	
		UUID	Mis en œuvre	HTTP/S	
		Virtuel	Mis en œuvre	HTTP/S	S’agit-il d’un périphérique de virtualisation de stockage ?
	Carte des volumes	LUN	Mis en œuvre	HTTP/S	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTP/S	
		Port de stockage	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Masque de volume	Initiateur	Mis en œuvre	HTTP/S	
		Contrôleur de protocole	Mis en œuvre	HTTP/S	
		Port de stockage	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	SSH	
	Volume	Capacité brute	Mis en œuvre	SSH	
		Capacité totale	Mis en œuvre	SSH	
		Total des IOP	Mis en œuvre	SSH	
		Clé	Mis en œuvre	SSH	
		Latence de lecture	Mis en œuvre	SSH	
		Latence totale	Mis en œuvre	SSH	
		Latence d’écriture	Mis en œuvre	SSH	
		ID du serveur	Mis en œuvre	SSH	
		Débit de lecture	Mis en œuvre	SSH	
		Débit total	Mis en œuvre	SSH	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	SSH	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Interface de ligne de commande EMC VPLEX	SSH	SSH	22		true	true	true	true
API EMC VPLEX	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

EMC XtremIO (HTTP)

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
6.2.1 6.3.2 6.3.3 6.4.0 6.4.1 6.4.2	1 brique et 125 To 1 brique et 24 To 1 brique et 31 To 1 brique et 8 To 1 x 10 To 1 x 20 To 1 x 40 To 2 briques et 83 To 3 briques et 146 To 3 briques et 251 To 3 briques et 283 To 4 briques et 628 To 4 briques et 754 To 4 x 20 To 6 x 40 To	4.0.27-1 4.0.31-11 6.3.3-8_X2 6.4.0-36_hotfix_2_X2

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
990					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Volume cible	Mis en œuvre	HTTPS	
		Technologie	Mis en œuvre	HTTPS	technologie qui définit l'efficacité du stockage
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Capacité	Mis en œuvre	HTTPS	Instantané Capacité utilisée en Mo
		Taille du disque	Mis en œuvre	HTTPS	liste séparée par des virgules des tailles de disque (Go)
		Vitesse du disque	Mis en œuvre	HTTPS	liste séparée par des virgules des vitesses de disque (tr/min)
		Type de disque	Pas disponible	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		Capacité brute totale	Mis en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre	HTTPS	Niveau de redondance
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Volume	Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d’écriture	Mis en œuvre	HTTPS	
		Ratio de blocage partiel	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST EMC XtremIO	HTTPS	HTTPS	443		true	true	true	true

NetApp Série E

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
2660 2680 2702 2704 2800B 2804 2806 3000 4000 5486 5488 5504 5564 5600 5700 5700B 6000 7999	08.40.60.01 08.80.00.00 7.84.46.0 8.20.16.0 8.20.27.0 8.20.30.0 8.20.8.0 8.25.14.0 8.25.6.0 8.40.0.1 8.40.20.0 8.40.30.4 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.30.5 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0 8.75.0.1 8.75.1.0 8.80.0.0 8.80.1.0 8.81.0.3 8.81.1.0 8.81.2.0 8.81.3.0 8.90.0.0

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Type	Écart	RMI	
		Virtuel	Mis en œuvre	RMI	S’agit-il d’un périphérique de virtualisation de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Capacité	Mis en œuvre	RMI	Instantané Capacité utilisée en Mo
		Type de disque	Pas disponible	RMI	
		Nom	Mis en œuvre	RMI	
		Capacité brute totale	Mis en œuvre	RMI	Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre	RMI	Niveau de redondance
		ID du pool de stockage	Mis en œuvre	RMI	
		Provisionnement léger	Mis en œuvre	RMI	
		Type	Écart	RMI	
		UUID	Mis en œuvre	RMI	
		Capacité utilisée	Mis en œuvre	RMI	
		Virtuel	Mis en œuvre	RMI	S’agit-il d’un périphérique de virtualisation de stockage ?
		Capacité écrite	Mis en œuvre	RMI	Capacité totale écrite sur ce volume par un hôte en Mo
	Carte des volumes	LUN	Mis en œuvre	RMI	Nom du lun backend
		Port de stockage	Mis en œuvre	RMI	
		Type	Écart	RMI	
	Masque de volume	Initiateur	Mis en œuvre	RMI	
		Port de stockage	Mis en œuvre	RMI	
		Type	Écart	RMI	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1010					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Utilisation de la lecture	Mis en œuvre	RMI	
		Utilisation totale	Mis en œuvre	RMI	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation Écriture	Mis en œuvre	RMI	
	Volume	Taux de réussite du cache en lecture	Mis en œuvre	RMI	
		Taux de réussite du cache total	Mis en œuvre	RMI	
		Taux de réussite du cache en écriture	Mis en œuvre	RMI	
		Capacité brute	Mis en œuvre	RMI	
		Capacité totale	Mis en œuvre	RMI	
		Capacité utilisée	Mis en œuvre	RMI	
		Capacité écrite	Mis en œuvre	RMI	
		Ratio de capacité utilisée	Mis en œuvre	RMI	
		Ratio de capacité écrit	Mis en œuvre	RMI	
		Lecture des IOP	Mis en œuvre	RMI	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	RMI	
		Les IOP écrivent	Mis en œuvre	RMI	
		Latence de lecture	Mis en œuvre	RMI	
		Latence totale	Mis en œuvre	RMI	
		Latence d'écriture	Mis en œuvre	RMI	
		Débit de lecture	Mis en œuvre	RMI	
		Débit total	Mis en œuvre	RMI	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	RMI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API SANtricity	RMI	TCP			true	true	FAUX	FAUX

Stockage pur FlashBlade REST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
FlashBlade FlashBlade//S200	Pureté//FB 4.1.5 Pureté//FB 4.3.0 Pureté//FB 4.3.11 Pureté//FB 4.3.6 Pureté//FB 4.4.3

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1016					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		brut/utilisable			conversion de la capacité utilisable en capacité brute
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Attribut de la capacité utilisée	Mis en œuvre	HTTPS	
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S’agit-il d’un périphérique de virtualisation de stockage ?

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1024					

		Espace d'économie de compression	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Économies de compression	Mis en œuvre	HTTPS	
	Stockage	Échec de la capacité brute	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Capacité brute de réserve	Mis en œuvre	HTTPS	Capacité brute des disques de rechange (somme de tous les disques de rechange)
		Capacité des pools de stockage	Mis en œuvre	HTTPS	
		Autres IOP	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d'écriture	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API FlashBlade de stockage pur	HTTPS	HTTPS	443		true	true	true	true

Google Cloud Compute

Modèles et versions pris en charge par ce collecteur de données : Versions d'API :

- v1

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Disque de machine virtuelle	OID	Mis en œuvre	HTTPS	
		OID du disque virtuel	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		OID de la machine virtuelle	Mis en œuvre	HTTPS	
	Hôte	Système d’exploitation hôte	Mis en œuvre	HTTPS	
		adresses IP	Mis en œuvre	HTTPS	
		Fabricant	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		OID	Mis en œuvre	HTTPS	
	Informations	Description de l’API	Mis en œuvre	HTTPS	
		Nom de l’API	Mis en œuvre	HTTPS	
		Version de l’API	Mis en œuvre	HTTPS	
		Nom de la source de données	Mis en œuvre	HTTPS	Informations
		Date	Mis en œuvre	HTTPS	
		ID de l’expéditeur	Mis en œuvre	HTTPS	
		Clé d’origine	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance	machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Utilisation totale du processeur	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		diskIops.total	Mis en œuvre	HTTPS	
		Écriture des IOPS sur disque	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Débit de lecture du disque	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	débit total du disque en lecture
		Débit d'écriture du disque	Mis en œuvre	HTTPS	
		Débit de lecture IP	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit IP total
		ipThroughput.écriture	Mis en œuvre	HTTPS	
		Utilisation totale de la mémoire	Mis en œuvre	HTTPS	
		swapRate.inRate	Mis en œuvre	HTTPS	
		Taux de swap	Mis en œuvre	HTTPS	
		Taux de swap total	Mis en œuvre	HTTPS	
		Planifier le temps d'attente	Mis en œuvre	HTTPS	Temps d'attente pour être programmé en pourcentage
	Machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST de la plateforme de calcul Google	HTTPS		443		true	true	true	true

Volumes Netapp de Google Cloud

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1032					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					pool de stockage est un groupe RAID
Produit	**Catégorie**	**Capacité/ Attributs**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité de données allouée	Écart	HTTPS	capacité allouée aux données
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité du disque physique (Mo)	Mis en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Rapport brut/utilisable	Mis en œuvre	HTTPS	ratio de conversion de la capacité utilisable en capacité brute
			Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1038					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Clé	Mis en œuvre	HTTPS	
	Disque de pool de stockage	Espace de stockage d'objets utilisé	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Total des IOP	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Capacité totale de données	Mis en œuvre	HTTPS	
		Capacité provisionnée	Mis en œuvre	HTTPS	
		Capacité de données utilisées	Mis en œuvre	HTTPS	
		Débit d'écriture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Ratio de capacité de dépassement d'engagement	Mis en œuvre	HTTPS	Présenté comme une série chronologique

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST de la plateforme de calcul Google	HTTPS		443		true	true	true	true

HDS HCP (HTTPS)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Plateforme de contenu Hitachi	9.6.2.37 9.6.3.33 9.7.2.27 9.7.3.14

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1042					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
performance	Stockage	Échec de la capacité brute	Mis en œuvre		
		Capacité brute	Mis en œuvre		
		Capacité brute de réserve	Mis en œuvre		Capacité brute des disques de rechange (somme de tous les disques de rechange)
		Capacité des pools de stockage	Mis en œuvre		
		Clé	Mis en œuvre		
		ID du serveur	Mis en œuvre		
	Données du nœud de stockage	Clé	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		
		Utilisation totale	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST HDS HCP	HTTPS	HTTPS	9090		true	true	true	true

Gestionnaire de périphériques HiCommand

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
7.6.1 8.0 8.7.1 8.7.3 8.7.6 8.8.3	DF850MH DF850S HM800 HM850 P9500 RAID800 VSP5000 XP24000 XP8	0983/AH 0984/BH 0985/BS 0986/AH 0988/HS DKC:60-08-22 DKC:60-08-65 DKC:70-06-43 DKC:80-06-80-00/02 DKC:80-06-91-00/00 DKC:80-06-96-00/00 DKC:83-05-46-60/00 DKC:83-05-50-60/00 DKC:83-05-53-60/00 DKC:88-08-08-60/00 DKC:88-08-10-60/00 DKC : 88-08-12-60/00 DKC:88-08-13-60/00 DKC:88-08-13-60/01 DKC:90-08-81-00/00 DKC:90-09-21-00/00 DKC:90-09-23-00/00 DKC:90-09-24-00/00 DKC:90-09-24-00/01 DKC:90-09-25 SVP:60-08-21/00 SVP:60-08-54/00 SVP:70-06-30/00 SVP:80-06-76/02 SVP:80-06-86/00 SVP:80-06-91/00 SVP:83-05-50-60/00 SVP:83-05-54-60/00 SVP:83-05-57-60/00 SVP:88-08-10-60/00 SVP:88-08-12-60/00 SVP:88-08-14-60/00 SVP:88-08-15-60/00 SVP:90-08-81/00 SVP:90-09-21/00 SVP:90-09-23/00 SVP:90-09-24/00 SVP:90-09-25/00

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Source de la réplique	Mis en œuvre	API XML HDS	
		Cible réplica	Mis en œuvre	API XML HDS	
		ID du pool de stockage	Mis en œuvre	API XML HDS	
		Provisionnement léger	Mis en œuvre	API XML HDS	
		Type	Écart	API XML HDS	
		Capacité utilisée	Mis en œuvre	API XML HDS	
	Carte des volumes	LUN	Mis en œuvre	API XML HDS	Nom du lun backend
		Masquage obligatoire	Mis en œuvre	API XML HDS	
		Contrôleur de protocole	Mis en œuvre	API XML HDS	
		Port de stockage	Mis en œuvre	API XML HDS	
	Masque de volume	Initiateur	Mis en œuvre	API XML HDS	
		Contrôleur de protocole	Mis en œuvre	API XML HDS	
		Port de stockage	Mis en œuvre	API XML HDS	
	Membre du volume	Capacité	Mis en œuvre	API XML HDS	Instantané Capacité utilisée en Mo
		Cylindres	Mis en œuvre	API XML HDS	
		Nom	Mis en œuvre	API XML HDS	
		Rang	Mis en œuvre	API XML HDS	
		Capacité brute totale	Mis en œuvre	API XML HDS	Capacité brute totale (somme de tous les disques de la matrice)
		ID du pool de stockage	Mis en œuvre	API XML HDS	
		Capacité utilisée	Mis en œuvre	API XML HDS	
	Alias WWN	Alias d’hôte	Mis en œuvre	API XML HDS	
		Type d’objet	Mis en œuvre	API XML HDS	
		Source	Mis en œuvre	API XML HDS	
		WWN	Mis en œuvre	API XML HDS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1056					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mis en œuvre	Exportation/CLI	
		Utilisation totale	Mis en œuvre	Exportation/CLI	
	Volume	Latence totale	Mis en œuvre	Exportation/CLI	
		Lecture des IOP	Mis en œuvre	Exportation/CLI	Nombre d'IOP en lecture sur le disque
		Latence de lecture	Mis en œuvre	Exportation/CLI	
		Taux de réussite du cache en lecture	Mis en œuvre	Exportation/CLI	
		Les IOP écrivent	Mis en œuvre	Exportation/CLI	
		Taux de réussite du cache total	Mis en œuvre	Exportation/CLI	
		Taux de réussite du cache en écriture	Mis en œuvre	Exportation/CLI	
		Débit de lecture	Mis en œuvre	Exportation/CLI	
		Débit d'écriture	Mis en œuvre	Exportation/CLI	
		Débit total	Mis en œuvre	Exportation/CLI	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Total des IOP	Mis en œuvre	Exportation/CLI	
		Latence d'écriture	Mis en œuvre	Exportation/CLI	
		Capacité totale	Mis en œuvre	Exportation/CLI	
		Capacité brute	Mis en œuvre	Exportation/CLI	
		Capacité utilisée	Mis en œuvre	Exportation/CLI	
		Ratio de capacité utilisée	Mis en œuvre	Exportation/CLI	
	Volume	Clé	Mis en œuvre	Exportation/CLI	
		ID du serveur	Mis en œuvre	Exportation/CLI	
		Capacité totale	Mis en œuvre	Exportation/CLI	
		Capacité brute	Mis en œuvre	Exportation/CLI	
		Capacité utilisée	Mis en œuvre	Exportation/CLI	
		Ratio de capacité utilisée	Mis en œuvre	Exportation/CLI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Utilitaire d'exportation (USPV) / SNM CLI (AMS)	Exportation/CLI				FAUX	FAUX	FAUX	FAUX
API XML du gestionnaire de périphériques HiCommand	API XML HDS	HTTP/HTTPS	2001		true	true	true	true

Centre d'opérations Hitachi

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
VSP 5100 VSP 5500 VSP 5600 VSP 5600H VSP E1090 VSP E590 VSP E790 VSP E790H VSP F1500 VSP F400 VSP F900 VSP G1000 VSP G1500 VSP G600 VSP G800 VSP G900 XP8	80-06-91-00/00:01-71-03/02 80-06-94-00/00:01-70-03/04 80-06-96-00/00:01-71-03/02 80-06-96-00/00:01-76-03/03 83-05-49-40/01:01-69-03/02 83-05-49-60/01:01-65-03/05 83-05-49-60/01:01-69-03/02 83-05-51-40/00:01-70-03/04 83-05-51-40/00:01-71-03/02 83-05-51-40/00:01-76-03/03 88-08-08-60/00:01-65-03/05 88-08-08-60/00:01-70-03/04 88-08-11-60/00:01-65-03/05 88-08-11-60/00:01-70-03/04 88-08-13-60/00:01-65-03/05 88-08-13-60/01:01-65-03/05 88-08-13-60/01:01-70-03/04 88-08-13-60/01:01-71-03/02 88-08-13-60/01:01-76-03/03 90-08-82-00/00:01-65-03/05 90-08-82:01.70.04 90-09-01-00/01:01-65-03/05 90-09-22-00/00:01-65-03/05 90-09-22-00/00:01-70-03/04 90-09-22-00/00:01-71-03/02 90-09-24-00/01:01-65-03/05 90-09-24-00/01:01-71-03/02 90-09-24-00/01:01-76-03/03 90-09-24:01.65.05 90-09-25-00/00:01-76-03/03 90-09-25:01.70.04 90-09-26-00/00:01-65-03/05 90-09-26-00/00:01-71-03/02 90-09-26-00/00:01-76-03/03 93-07-01-80/00:01-70-03/04 93-07-22-40/00:01-65-03/05 93-07-22-40/00:01-69-03/02 93-07-22-80/00:01-70-03/04 93-07-22-80/00:01-71-03/02 93-07-23-80/00:01-71-03/02 93-07-23-80/01:01-71-03/02 93-07-24-40/00:01-76-03/03 93-07-24-80/00:01-70-03/04 null:null

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Volume cible	Mis en œuvre		
		Technologie	Mis en œuvre		technologie qui
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Capacité	Mis en œuvre		Instantané Capacité utilisée en Mo
		Chemin de jonction	Mis en œuvre		
		Nom	Mis en œuvre		
		Type de protection	Mis en œuvre		
		Capacité brute totale	Mis en œuvre		Capacité brute totale (somme de tous les disques de la matrice)
		ID du pool de stockage	Mis en œuvre		
		Provisionnement léger	Mis en œuvre		
		Type	Écart		
		Capacité utilisée	Mis en œuvre		
		Compression activée	Mis en œuvre		
	Carte des volumes	LUN	Mis en œuvre		Nom du lun backend
		Masquage obligatoire	Mis en œuvre		
		Contrôleur de protocole	Mis en œuvre		
		Port de stockage	Mis en œuvre		
		Type	Écart		
	Masque de volume	Initiateur	Mis en œuvre		
		Contrôleur de protocole	Mis en œuvre		
		Port de stockage	Mis en œuvre		
		Type	Écart		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Taux de réussite du cache en lecture	Mis en œuvre		
		Taux de réussite du cache total	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Clé	Mis en œuvre		
		Latence de lecture	Mis en œuvre		
		Latence totale	Mis en œuvre		
		Latence d'écriture	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST du centre d'opérations Hitachi	HTTPS	HTTPS	443		true	true	true	true

HDS HNAS (CLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Fichier 34 G600 G800 HNAS 4060 HNAS 4080 HNAS 4100 N800	14.6.7520.04 14.7.7623.07 14.9.7916.07 15.1.8030.03 15.1.8030.05 15.2.8128.05 15.2.8128.07 15.2.8128.09 15.3.8224.02

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité totale allouée	Mis en œuvre	SSH	
		Capacité totale utilisée	Mis en œuvre	SSH	Capacité totale en Mo
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	SSH	
		Virtuel	Mis en œuvre	SSH	S'agit-il d'un périphérique de virtualisation de stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Interface de ligne de commande HDS HNAS	SSH	SSH	22		true	true	true	true

Stockage HPE Nimble/Alletra 6000

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
v1	5050 6070 AF1000 AF20Q AF40 AF60 AF80 CS1000 CS300 CS3000 CS500 HF20 HF20C HF20H HF40 HF60	5.0.8.0-677726-opt 5.2.1.1100-1027043-opt 5.2.1.400-796142-opt 5.2.1.700-882343-opt 5.2.1.800-930936-opt 6.0.0.400-991061-opt 6.0.0.500-1005932-opt 6.1.1.200-1020304-opt 6.1.1.300-1028597-opt 6.1.2.300-1042680-opt 6.1.2.400-1048557-opt 6.1.2.500-1053701-opt 6.1.2.502-1057650-opt 6.1.2.600-1064273-opt

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1088					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart	HTTPS	
	Alias WWN	Alias d'hôte	Mis en œuvre	HTTPS	
		Type d'objet	Mis en œuvre	HTTPS	
		Source	Mis en œuvre	HTTPS	
		WWN	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1096					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Volume	Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Économies totales de compression	Mis en œuvre	HTTPS	
		Espace d’économie de compression	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d’écriture	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST HP Nimble	HTTPS	HTTPS	5392		true	FAUX	true	true

Huawei OceanStor (REST/HTTPS)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
18800 V5 2600 V3 5310 V5 5500 V3 5500 V5 5800 V3 6800 V3 Dorado 18000 V6 NVMe Dorado 3000 V6 Dorado 5000 V3 Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V500R007C60 Kunpeng V500R007C61 V500R007C71 Kunpeng V600R003C00 V600R005C11 V600R005C26 V600R005C27

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Capacité	Mis en œuvre	HTTPS	Instantané Capacité utilisée en Mo
		Chemin de jonction	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		Capacité brute totale	Mis en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre	HTTPS	Niveau de redondance
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Volume	Taux de réussite du cache en lecture	Mis en œuvre	HTTPS	
		Taux de réussite du cache total	Mis en œuvre	HTTPS	
		Taux de réussite du cache en écriture	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d’écriture	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Huawei OceanStor	HTTPS	HTTPS	8088		true	true	true	true
API REST des performances de Huawei OceanStor	HTTPS	HTTPS	8088		true	FAUX	true	true

IBM Cleversafe

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		UUID	Mis en œuvre	HTTPS	
		Version	Mis en œuvre	HTTPS	version du logiciel
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Adresses IP de gestion	Mis en œuvre	HTTPS	
	Piscine de stockage	Inclure dans la capacité de l'eau chaude sanitaire	Mis en œuvre	HTTPS	Un moyen pour ACQ de contrôler quels pools de stockage sont intéressants dans DWH Capacity
		Nom	Mis en œuvre	HTTPS	
		Capacité du disque physique (Mo)	Mis en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe de raid	Mis en œuvre	HTTPS	indique si ce pool de stockage est un groupe RAID
		Rapport brut/utilisable	Mis en œuvre	HTTPS	ratio de conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST IBM Cleversafe	HTTPS	HTTPS	443		true	true	true	true

IBM DS 8K (DSCLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
2107-951 2107-961 2107-993 2107-994 2107-996 2107-A05	- 7.10.1.8 7.6.31.4250 7.7.51.1400 7.9.32.101 7.9.33.132 7.9.33.95 7.9.40.251 7.9.41.65

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1126					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
	Masque de volume	Initiateur	Mis en œuvre	DSNI	
		Contrôleur de protocole	Mis en œuvre	DSNI	
		Port de stockage	Mis en œuvre	DSNI	
	Alias WWN	Alias d’hôte	Mis en œuvre	DSNI	
		Système d’exploitation hôte	Mis en œuvre	DSNI	
		Type d’objet	Mis en œuvre	DSNI	
		Source	Mis en œuvre	DSNI	
		WWN	Mis en œuvre	DSNI	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité brute	Mis en œuvre	DSNI	
		Capacité utilisée	Mis en œuvre	DSNI	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Ratio de capacité utilisée	Mis en œuvre	DSNI	
	Volume	Taux de réussite du cache en lecture	Mis en œuvre	DSNI	
		Taux de réussite du cache total	Mis en œuvre	DSNI	
		Taux de réussite du cache en écriture	Mis en œuvre	DSNI	
		Capacité brute	Mis en œuvre	DSNI	
		Capacité totale	Mis en œuvre	DSNI	
		Capacité utilisée	Mis en œuvre	DSNI	
		Ratio de capacité utilisée	Mis en œuvre	DSNI	
		Lecture des IOP	Mis en œuvre	DSNI	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	DSNI	
		Les IOP écrivent	Mis en œuvre	DSNI	
		Clé	Mis en œuvre	DSNI	
		Latence de lecture	Mis en œuvre	DSNI	
		Latence totale	Mis en œuvre	DSNI	
		Latence d'écriture	Mis en œuvre	DSNI	
		ID du serveur	Mis en œuvre	DSNI	
		Débit de lecture	Mis en œuvre	DSNI	
		Débit total	Mis en œuvre	DSNI	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	DSNI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Configuration de l'assistant de source de données	Saisie manuelle				true	true	true	true
Interface de ligne de commande IBM DS	DSNI	DSNI			true	true	true	true

IBM PowerVM (SSH)

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Nom	Mis en œuvre	SSH	
		OID	Mis en œuvre	SSH	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type de plate-forme	Mis en œuvre	SSH	
	Informations	Nom de la source de données	Mis en œuvre	SSH	Informations
		Date	Mis en œuvre	SSH	
		ID de l'expéditeur	Mis en œuvre	SSH	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Accès SSH à la console de gestion du matériel IBM	SSH	SSH	22		true	FAUX	true	true

IBM SVC (CLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
2072-12F 2072-12G 2072-224 2072-24C 2072-24E 2072-24F 2072-24G 2072-2N4 2072-324 2072-3H4 2072-3N2 2072-3N4 2072-92F 2072-92G 2076-124 2076-12F 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2076-AF6 2076- AFF 2077-24F 2077-24G 2077-424 2077-4H4 2078-12F 2078-12G 2078-224 2078-24C 2078-24F 2078-24G 2078-324 2078-424 2078-4H4 2078-92G 2078-AF3 4657-24G 4657-924 4662-12G 4662-24G 4662-6H2 4666-AH8 4666-UH8 4680-24H 4680-2P4 4680-3P4 4680-92H 4983-AH8 9843-AE2 9843-AE3 9846-AG8 9848-AF7 9848-AF8 9848-AG8 9848-UG8 SERVICE	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.7.1.8 7.8.1.11 7.8.1.12 7.8.1.13 7.8.1.14 7.8.1.16 7.8.1.5 7.8.1.6 7.8.1.7 7.8.1.8 8.2.1.10 8.2.1.8 8.2.1.9 8.3.1.10 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.8 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.13 8.4.0.15 8.4.0.2 8.4.0.5 8.4.0.6 8.4.0.9 8.4.2.0 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.13 8.5.0.14 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.6.0.0 8.6.0.2 8.6.0.3 8.6.0.4 8.6.0.5 8.7.0.0 8.7.0.1 8.7.0.2 8.7.0.3

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1142					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité utilisée	Mis en œuvre	SSH	
		Virtuel	Mis en œuvre	SSH	S’agit-il d’un volume de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité écrite	Mis en œuvre	SSH	Capacité totale écrite sur ce volume par un hôte en Mo
		Compression activée	Mis en œuvre	SSH	
		Crypté	Mis en œuvre	SSH	
	Carte des volumes	LUN	Mis en œuvre	SSH	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	SSH	
		Port de stockage	Mis en œuvre	SSH	
	Masque de volume	Initiateur	Mis en œuvre	SSH	
		Contrôleur de protocole	Mis en œuvre	SSH	
		Port de stockage	Mis en œuvre	SSH	
		Type	Écart	SSH	
	Alias WWN	Alias d’hôte	Mis en œuvre	SSH	
		Type d’objet	Mis en œuvre	SSH	
		Source	Mis en œuvre	SSH	
		WWN	Mis en œuvre	SSH	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Utilisation de la lecture	Mis en œuvre	SSH	
		Utilisation totale	Mis en œuvre	SSH	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation Écriture	Mis en œuvre	SSH	
	Volume	Taux de réussite du cache en lecture	Mis en œuvre	SSH	
		Taux de réussite du cache total	Mis en œuvre	SSH	
		Taux de réussite du cache en écriture	Mis en œuvre	SSH	
		Capacité brute	Mis en œuvre	SSH	
		Capacité totale	Mis en œuvre	SSH	
		Capacité utilisée	Mis en œuvre	SSH	
		Capacité écrite	Mis en œuvre	SSH	
		Ratio de capacité utilisée	Mis en œuvre	SSH	
		Ratio de capacité écrit	Mis en œuvre	SSH	
		Lecture des IOP	Mis en œuvre	SSH	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	SSH	
		Les IOP écrivent	Mis en œuvre	SSH	
		Latence de lecture	Mis en œuvre	SSH	
		Latence totale	Mis en œuvre	SSH	
		Latence d'écriture	Mis en œuvre	SSH	
		Débit de lecture	Mis en œuvre	SSH	
		Débit total	Mis en œuvre	SSH	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	SSH	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Interface de ligne de commande IBM SVC	SSH	SSH	22		true	FAUX	true	true

IBM XIV et A9000 (XIVCLI)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
A14	10.2.4.e

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1156					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		(Mo)			logique définie lors des opérations de
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Nom	Mis en œuvre	XIVe CLI	nt du volume
		ID du pool de stockage	Mis en œuvre	XIVe CLI	
		Type	Écart	XIVe CLI	
		Type de disque	Pas disponible	XIVe CLI	
		Groupe de disques	Mis en œuvre	XIVe CLI	Type de groupe de disques
		Provisionnement léger	Mis en œuvre	XIVe CLI	
		Capacité	Mis en œuvre	XIVe CLI	Instantané Capacité utilisée en Mo
		Capacité brute totale	Mis en œuvre	XIVe CLI	Capacité brute totale (somme de tous les disques de la matrice)
		Capacité utilisée	Mis en œuvre	XIVe CLI	
		Redondance	Mis en œuvre	XIVe CLI	Niveau de redondance
		Compression activée	Mis en œuvre	XIVe CLI	
	Carte des volumes	LUN	Mis en œuvre	XIVe CLI	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	XIVe CLI	
	Masque de volume	Initiateur	Mis en œuvre	XIVe CLI	
		Contrôleur de protocole	Mis en œuvre	XIVe CLI	
	Alias WWN	Source	Mis en œuvre	XIVe CLI	
		Alias d'hôte	Mis en œuvre	XIVe CLI	
		WWN	Mis en œuvre	XIVe CLI	
		Type d'objet	Mis en œuvre	XIVe CLI	
		Système d'exploitation hôte	Mis en œuvre	XIVe CLI	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Interface de ligne de commande IBM DS	DSNI	DSNI			true	true	true	true
Interface de ligne de commande IBM XIV	XIVe CLI	TCP	7778		true	FAUX	true	FAUX

Infinidat Infinibox (HTTP)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
F4303 F6230 F6240	6.0.20.40 6.0.31.0 7.1.14.0 7.1.15.0 7.3.20.90 8.1.0.280

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1162					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Alias WWN	Alias d'hôte	Mis en œuvre	HTTPS	
		Type d'objet	Mis en œuvre	HTTPS	
		Source	Mis en œuvre	HTTPS	
		WWN	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Infinidat	HTTPS	HTTPS	443		true	true	true	true

Microsoft Azure Compute

Modèles et versions pris en charge par ce collecteur de données : Versions d'API :

- 01/06/2018

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Disque de machine virtuelle	OID	Mis en œuvre	HTTPS	
		OID du disque virtuel	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		OID de la machine virtuelle	Mis en œuvre	HTTPS	
	Hôte	Système d’exploitation hôte	Mis en œuvre	HTTPS	
		adresses IP	Mis en œuvre	HTTPS	
		Fabricant	Mis en œuvre	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		OID	Mis en œuvre	HTTPS	
	Informations	Description de l’API	Mis en œuvre	HTTPS	
		Nom de l’API	Mis en œuvre	HTTPS	
		Version de l’API	Mis en œuvre	HTTPS	
		Nom de la source de données	Mis en œuvre	HTTPS	Informations
		Date	Mis en œuvre	HTTPS	
		ID de l’expéditeur	Mis en œuvre	HTTPS	
		Clé d’origine	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	
	machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Utilisation totale du processeur	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		diskIops.total	Mis en œuvre	HTTPS	
		Écriture des IOPS sur disque	Mis en œuvre	HTTPS	
		Débit de lecture du disque	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	débit total du disque en lecture
		Débit d'écriture du disque	Mis en œuvre	HTTPS	
		Débit de lecture IP	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit IP total
		ipThroughput.écriture	Mis en œuvre	HTTPS	
	Machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST de calcul Microsoft Azure	HTTPS	HTTPS	443		true	true	true	true

Microsoft Hyper-V

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Processeurs	Mis en œuvre	WMI	
		Capacité provisionnée	Mis en œuvre	WMI	
		Capacité utilisée	Mis en œuvre	WMI	
	Disque de machine virtuelle	OID	Mis en œuvre	WMI	
		OID du disque virtuel	Mis en œuvre	WMI	
		OID de la machine virtuelle	Mis en œuvre	WMI	
	Hôte	Nombre de processeurs hôtes	Mis en œuvre	WMI	
		Vitesse du processeur hôte	Mis en œuvre	WMI	
		Domaine hôte	Mis en œuvre	WMI	
		Mémoire installée par l'hôte	Mis en œuvre	WMI	
		Modèle d'hôte	Mis en œuvre	WMI	
		Nombre de cartes réseau	Mis en œuvre	WMI	
		Vitesse de la carte réseau	Mis en œuvre	WMI	
		adresses IP	Mis en œuvre	WMI	
		Fabricant	Mis en œuvre	WMI	
		Nom	Mis en œuvre	WMI	
		OID	Mis en œuvre	WMI	
		Type de plate-forme	Mis en œuvre	WMI	
	Nœud ISCSI	Alias d'hôte	Mis en œuvre	WMI	
		Nom du nœud	Mis en œuvre	WMI	
		OID	Mis en œuvre	WMI	
		Type	Écart	WMI	
	Informations	Nom de la source de données	Mis en œuvre	WMI	Informations
		Date	Mis en œuvre	WMI	
		ID de l'expéditeur	Mis en œuvre	WMI	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	Gestion WS	
	machine virtuelle	Capacité totale	Mis en œuvre	Gestion WS	
		Capacité utilisée	Mis en œuvre	Gestion WS	
		Ratio de capacité utilisée	Mis en œuvre	Gestion WS	
		Utilisation totale du processeur	Mis en œuvre	Gestion WS	
		Lecture des IOP	Mis en œuvre	Gestion WS	Nombre d’IOP en lecture sur le disque
		diskIops.total	Mis en œuvre	Gestion WS	
		Écriture des IOPS sur disque	Mis en œuvre	Gestion WS	
		Latence totale	Mis en œuvre	Gestion WS	
		Débit de lecture du disque	Mis en œuvre	Gestion WS	
		Débit de lecture	Mis en œuvre	Gestion WS	débit total du disque en lecture
		Débit d’écriture du disque	Mis en œuvre	Gestion WS	
		Débit de lecture IP	Mis en œuvre	Gestion WS	
		Débit total	Mis en œuvre	Gestion WS	Débit IP total
		ipThroughput.écriture	Mis en œuvre	Gestion WS	
	Machine virtuelle	Capacité totale	Mis en œuvre	Gestion WS	
		Capacité utilisée	Mis en œuvre	Gestion WS	
		Ratio de capacité utilisée	Mis en œuvre	Gestion WS	
		Clé	Mis en œuvre	Gestion WS	
		ID du serveur	Mis en œuvre	Gestion WS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
PowerShell	Gestion WS	HTTP	5985		true	FAUX	FAUX	true
WMI	WMI	WMI	135		true	FAUX	true	true

Mode NetApp 7

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
1,12 1,17 1,19 1,20 1,21	FAS2040 FAS2220 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS3140 FAS3160 FAS3250 FAS3270 FAS6240 FAS6250 FAS8020 FAS8040 FAS8060 N6070 N6240 N6270	8.1.1 7-Mode 8.1.4P9D18 7-Mode 8.2.2 7-Mode 8.2.3 7-Mode 8.2.3P2 7-Mode 8.2.3P3 7-Mode 8.2.4 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.4P6 7-Mode 8.2.5 7-Mode 8.2.5P3 7-Mode 8.2.5P4 7-Mode 8.2.5P5 7-Mode 8.2P3 7-Mode 8.2P4 7-Mode Data ONTAP version 7.3.3 Data ONTAP version 8.2.5 7-Mode Data ONTAP version 8.2.5P1 7-Mode

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Carte des volumes	LUN	Mis en œuvre		Nom du lun backend
		Contrôleur de protocole	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type	Écart		
	Masque de volume	Initiateur	Mis en œuvre		
		Contrôleur de protocole	Mis en œuvre		
		Port de stockage	Mis en œuvre		
		Type	Écart		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Débit d’écriture	Mis en œuvre		
		Utilisation de la lecture	Mis en œuvre		
		Utilisation totale	Mis en œuvre		
		Utilisation Écriture	Mis en œuvre		
	Volume	Capacité brute	Mis en œuvre		
		Capacité totale	Mis en œuvre		
		Capacité utilisée	Mis en œuvre		
		Ratio de capacité utilisée	Mis en œuvre		
		Lecture de la densité IO	Mis en œuvre		
		Densité IO totale	Mis en œuvre		
		Densité d’E/S d’écriture	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Latence de lecture	Mis en œuvre		
		Latence totale	Mis en œuvre		
		Latence d’écriture	Mis en œuvre		
		Ratio de blocage partiel	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre		
		Écriture en attente	Mis en œuvre		écriture totale en attente

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
Mode ZAPI NetApp 7	ZAPI	ZAPI			true	true	true	true

REST NetApp Série E

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
2800B 2806 5700	08.71.03.00 08.73.00.00 08.74.02.00 08.75.00.00 08.75.00.01 08.80.00.00 08.81.00.03 08.81.02.00 08.81.03.00 08.90.00.00

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Crypté	Mis en œuvre	HTTPS	
	Volume	Capacité	Mis en œuvre	HTTPS	Instantané Capacité utilisée en Mo
		Type de disque	Pas disponible	HTTPS	
		Nom	Mis en œuvre	HTTPS	
		Capacité brute totale	Mis en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la matrice)
		Redondance	Mis en œuvre	HTTPS	Niveau de redondance
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
		Crypté	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture) en Mo/s
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d’écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l’authentification	Nécessite uniquement des informations d’identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST NetApp série E	HTTPS	HTTPS	443		true	true	true	true

Amazon FSx for NetApp ONTAP

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
FSx pour ONTAP	Data ONTAP

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1220					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Pool de stockage de machine virtuelle lRef	ID du pool de stockage	Mis en œuvre	HTTPS	
Produit	**Catégorie** Catégorie du volume de la machine virtuelle	**Fonctionnalité/ Attribut** Fonctionnalité	**Statut** Mis en œuvre	**Protocole utilisé** HTTPS	**Informations supplémentaires**
	Volume	Capacité	Mis en œuvre	HTTPS	Instantané Capacité utilisée en Mo
		Groupe de disques	Mis en œuvre	HTTPS	Type de groupe de disques
		Chemin de jonction	Mis en œuvre	HTTPS	
		Dernière heure d'accès connue	Mis en œuvre	HTTPS	Dernier accès connu au volume
		Nom	Mis en œuvre	HTTPS	
		Identifiant Qtree	Mis en œuvre	HTTPS	identifiant unique du qtree
		Capacité brute totale	Mis en œuvre	HTTPS	Capacité brute totale (somme de tous les disques de la matrice)
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Crypté	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Ratio de capacité de dépassement d'engagement	Mis en œuvre	HTTPS	Présenté comme une série chronologique
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Attribut de la capacité utilisée	Mis en œuvre	HTTPS	
		Capacité réservée aux instantanés	Mis en œuvre	HTTPS	
	Machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

Data ONTAP en cluster NetApp ONTAP 8.1.1+

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
AFF-A150 AFF-A1K AFF-A20 AFF-A200 AFF-A220 AFF-A250 AFF-A300 AFF -A320 AFF-A400 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C60 AFF-C80 AFF-C800 AFF AFF8040 AFF8060 AFF8080 ASA-A250 ASA-A400 ASA-A800 ASA-A900 ASA-C250 ASA-C400 ASA-C800 CDvM100 CDvM200 DM5000H DM7100F FAS2240-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS2820 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• 8.2.3P4 • 8.2.3P5 • 8.3.1P2 • 8.3.2 • 8.3.2P12 • 8.3.2P5 • 9.0.0 • 9.1.0 • 9.1.0P1 • 9.1.0P11 • 9.1.0P15 • 9.1.0P17 • 9.1.0P19 • 9.1.0P2 • 9.1.0P20 • 9.1.0P3 • 9.1.0P6 • 9.1.0P7 • 9.1.0P8 • 9.1.0P9 • 9.10.0 • 9.10.1 • 9.10.1P1 • 9.10.1P10 • 9.10.1P11 • 9.10.1P12 • 9.10.1P13 • 9.10.1P14 • 9.10.1P15 • 9.10.1P16 • 9.10.1P17 • 9.10.1P18 • 9.10.1P19 • 9.10.1P2 • 9.10.1P20 • 9.10.1P3 9.10.1P4 9.10.1P5

Produits pris en charge par ce collecteur de données :

-
- 9.10.1P6
- 9.10.1P7
- 9.10.1P8
- 9.10.1P9
- 9.11.0P1
- 9.11.1
- 9.11.1P1
- 9.11.1P10
- 9.11.1P11
- 9.11.1P12
- 9.11.1P13
- 9.11.1P14
- 9.11.1P15
- 9.11.1P16
- 9.11.1P17
- 9.11.1P18
- 9.11.1P2
- 9.11.1P3
- 9.11.1P4
- 9.11.1P5
- 9.11.1P6
- 9.11.1P7
- 9.11.1P8
- 9.11.1P9
- 9.12.1
- 9.12.1P1
- 9.12.1P10
- 9.12.1P11
- 9.12.1P12
- 9.12.1P13
- 9.12.1P14
- 9.12.1P15
- 9.12.1P16
- 9.12.1P17
- 9.12.1P2
- 9.12.1P3

9.12.1P4

9.12.1P5

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation			• 9.12.1P7 • 9.12.1P8 • 9.12.1P9 • 9.13.0 • 9.13.0P1 • 9.13.0P3 • 9.13.1 • 9.13.1D1 • 9.13.1P1 • 9.13.1P10 • 9.13.1P11 • 9.13.1P12 • 9.13.1P13 • 9.13.1P14 • 9.13.1P2 • 9.13.1P3 • 9.13.1P4 • 9.13.1P5 • 9.13.1P6 • 9.13.1P7 • 9.13.1P8 • 9.13.1P9 • 9.14.0 • 9.14.0P1 • 9.14.0P2 • 9.14.1 • 9.14.1P1 • 9.14.1P10 • 9.14.1P11 • 9.14.1P2 • 9.14.1P4 • 9.14.1P5 • 9.14.1P6 • 9.14.1P7 • 9.14.1P8 9.14.1P8D5 9.14.1P9		
1246					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
			• 9.15.0P2 • 9.15.1 • 9.15.1P1 • 9.15.1P2 • 9.15.1P2D2 • 9.15.1P3 • 9.15.1P4 • 9.15.1P5 • 9.15.1P6 • 9.15.1P7 • 9.15.1P7D4 • 9.15.1P8 • 9.16.1 • 9.16.1P1 • 9.17.1 • 9.2.0P3 • 9.2.0P4 • 9.3.0P15 • 9.3.0P18 • 9.3.0P20 • 9.3.0P21 • 9.3.0P6 • 9.3.0P7 • 9.3.0P8 • 9.4.0 • 9.4.0P2 • 9.4.0P5 • 9.5.0 • 9.5.0P1 • 9.5.0P10 • 9.5.0P14 • 9.5.0P16 • 9.5.0P17 • 9.5.0P18 • 9.5.0P19 9.5.0P2 9.5.0P3		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
			• 9.5.0P7 • 9.5.0P9 • 9.6.0 • 9.6.0P11 • 9.6.0P18 • 9.6.0P2 • 9.6.0P3 • 9.6.0P5 • 9.7.0 • 9.7.0P10 • 9.7.0P11 • 9.7.0P12 • 9.7.0P13 • 9.7.0P14 • 9.7.0P15 • 9.7.0P16 • 9.7.0P17 • 9.7.0P18 • 9.7.0P19 • 9.7.0P20 • 9.7.0P21 • 9.7.0P22 • 9.7.0P23 • 9.7.0P4 • 9.7.0P5 • 9.7.0P6 • 9.7.0P7 • 9.7.0P8 • 9.7.0P9 • 9.8.0 • 9.8.0P1 • 9.8.0P10 • 9.8.0P11 • 9.8.0P12 • 9.8.0P13 9.8.0P14 9.8.0P15		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
			• 9.8.0P17 • 9.8.0P18 • 9.8.0P19 • 9.8.0P2 • 9.8.0P20 • 9.8.0P21 • 9.8.0P3 • 9.8.0P4 • 9.8.0P6 • 9.8.0P7 • 9.8.0P8 • 9.8.0P9 • 9,0 • 9,1 • 9.9.1P10 • 9.9.1P11 • 9.9.1P12 • 9.9.1P13 • 9.9.1P14 • 9.9.1P15 • 9.9.1P16 • 9.9.1P17 • 9.9.1P18 • 9.9.1P19 • 9.9.1P2 • 9.9.1P20 • 9.9.1P3 • 9.9.1P6 • 9.9.1P7 • 9.9.1P9		

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					périphérique de virtualisation de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Crypté	Mis en œuvre	HTTPS	
		Limite QoS IOPS	Mis en œuvre	HTTPS	
		Limite de qualité de service (MBPS)	Mis en œuvre	HTTPS	
		Limite Qos brute	Mis en œuvre	HTTPS	
		QoS - Politique	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Machine virtuelle	Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
	Volume	Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Lecture de la densité IO	Mis en œuvre	HTTPS	
		Densité IO totale	Mis en œuvre	HTTPS	
		Densité d'E/S d'écriture	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d'écriture	Mis en œuvre	HTTPS	
		Ratio de blocage partiel	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

ASA

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
ASA-A1K ASA-A20 ASA-A90	NetApp Release 9.16.1 : Sam. 18 janv. 19:31:15 UTC 2025 NetApp Release 9.16.1RC1 : Lun. 4 nov. 10:39:46 UTC 2024

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1282					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Contrôleur de protocole	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
performance	Disque	Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	
		Utilisation de la lecture	Mis en œuvre	HTTPS	
		Utilisation totale	Mis en œuvre	HTTPS	
		Utilisation Écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API NetApp ASA	HTTPS	HTTPS	443		true	true	true	true

NetApp ONTAP REST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
AFF-A150 AFF-A220 AFF-A250 AFF-A300 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF-A250 ASA-A400 ASA-A800 ASA-C250 ASA-C800 ASA FAS2720 FAS2750 FAS2820 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• NetApp Release 9.14.1P10 : jeu. 28 nov. 2024, 12:32:16 UTC • NetApp Release 9.14.1P11 : mer. 22 janv. 2025, 11:55:28 UTC • NetApp Release 9.14.1P1 : jeu. 15 févr. 2024, 00:45:21 UTC • NetApp Release 9.14.1P4 : jeu. 18 avr. 2024, 15:59:10 UTC • NetApp Release 9.14.1P5 : sam. 18 mai 2024, 19:42:16 UTC • NetApp Release 9.14.1P6 : mar. 18 juin 2024, 16:11:44 UTC • NetApp Release 9.14.1P7 : jeu. 1er août 2024, 03:07:44 UTC • Version NetApp 9.14.1P8 : ven. 13 sept. 2024, 07:12:27 UTC • NetApp Release 9.14.1P9 : lun. 21 oct. 2024, 18:04:05 UTC • NetApp Release 9.15.1 : jeu. 4 juil. 2024, 12:21:07 UTC • NetApp Release 9.15.1P1 : mar. 30 juil. 2024, 05:15:49 UTC • NetApp Release 9.15.1P2 : mar. 27 août 2024, 16:35:16 UTC • NetApp Release 9.15.1P3 : mer. 25 sept. 2024, 22:33:44 UTC • NetApp Release 9.15.1P4 : dim. 27 oct. 2024, 20:15:53 UTC • Version NetApp 9.15.1P5 : dim. 24 nov. 2024, 16:31:37 UTC • NetApp Release 9.15.1P6 : mer. 4 déc. 01:42:39 UTC 2024 • Version NetApp 9.15.1P7 : sam. 18 janv. 2025, 21:34:02 UTC • NetApp Release 9.15.1RC2 : lun. 24 juin 2024, 04:49:55 UTC • NetApp Release 9.16.1 : sam. 18 janv. 2025, 19:31:15 UTC • NetApp Release 9.16.1P1 : ven. 14 févr. 2025, 03:53:50 UTC • NetApp Release 9.16.1RC1 : lun. 4 nov. 2024, 10:39:46 UTC • NetApp Release Clawhammer__9.14.1 : sam. 18 mai 2024 09:23:49 UTC • NetApp Release Cloudstream__9.16.1 : lun. 4 nov. 05:51:46 UTC 2024

Produits pris en charge par ce collecteur de données :

-
- NetApp Release Cloudstream__9.16.1 : jeu. 13 mars 2025 20:55:54 UTC
- NetApp Release Electricjellyfish__9.17.1 : lun. 3 mars 2025 05:57:49 UTC
- NetApp Release Electricjellyfish__9.17.1 : dim. 9 mars 2025 05:56:14 UTC
- NetApp Release Electricjellyfish__9.17.1 : dim. 16 mars 2025 04:54:53 UTC
- NetApp Release Electricjellyfish__9.17.1 : mar. 28 janv. 2025 11:48:14 UTC
- NetApp Release Electricjellyfish__9.17.1 : mar. 18 mars 2025 04:59:54 UTC
- NetApp Release Electricjellyfish__9.17.1 : mer. 12 mars 2025 04:42:03 UTC
- NetApp Release Mightysquirrel__9.15.1 : ven. 24 mai 2024 05:03:10 UTC
- NetApp Release Mightysquirrel__9.15.1 : sam. 18 janv. 2025 11:39:42 UTC
- NetApp publie Tropicallightning__9.18.0 : ven. 21 févr. 2025, 14:02:58 UTC
- NetApp Release Tropicallightning__9.18.0 : lun. 17 févr. 08:18:14 UTC 2025
- NetApp Release Tropicallightning__9.18.0 : jeu. 20 févr. 08:11:55 UTC 2025
- NetApp Release Tropicallightning__9.18.0 : jeu. 27 févr. 04:15:40 UTC 2025
- NetApp publie Tropicallightning__9.18.0 : mar. 18 févr. 2025, 14:00:54 UTC
- NetApp Release Tropicallightning__9.18.0 : mer. 26 févr. 08:19:21 UTC 2025
- NetApp Release Tropicallightning__9.18.0 : mer. 29 janv. 08:34:06 UTC 2025

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Crypté	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Clé	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité attribuée aux instantanés	Mis en œuvre	HTTPS	
		Instantané de la capacité utilisée	Mis en œuvre	HTTPS	
		Instantané du ratio de capacité utilisée	Mis en œuvre	HTTPS	Présenté comme une série chronologique

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST NetApp ONTAP	HTTPS	HTTPS	443		true	true	true	true

NetApp SolidFire 8.1+

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF4805 SF9605 SF9608 H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 SF19210 SF38410 SF4805 SF9605 SF9608	11.1.0.72 11.7.0.76 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1318					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		IOPS en rafale de qualité de service	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Limite QoS IOPS	Mis en œuvre	HTTPS	
		QOS Min IOPS	Mis en œuvre	HTTPS	
		QoS - Politique	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Masquage obligatoire	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1326					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mis en œuvre	HTTPS	
		Utilisation totale	Mis en œuvre	HTTPS	
	Volume	Capacité brute	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Économies totales de compression	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d'écriture	Mis en œuvre	HTTPS	
		Ratio de blocage partiel	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	
		Utilisation totale	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST SolidFire	HTTPS	HTTPS	443		true	true	true	true

NetApp StorageGRID (HTTPS)

Modèles et versions pris en charge par ce collecteur de données :

Versions API	Modèles	Versions du micrologiciel
3,2 3,3 3,4 3,5 4,0 4,1	Webscale	11.4.0 11.5.0.11 11.5.0.6 11.5.0.7 11.5.0.9 11.6.0 11.6.0.10 11.6.0.11 11.6.0.12 11.6.0.13 11.6.0.14 11.6.0.15 11.6.0.16 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0 11.7.0.11 11.7.0.12 11.7.0.13 11.7.0.3 11.7.0.4 11.7.0.5 11.7.0.6 11.7.0.8 11.7.0.9 11.8.0 11.8.0.1 11.8.0.2 11.8.0.3 11.8.0.5 11.8.0.6 11.8.0.7 11.8.0.8 11.8.0.9 11.9.0 11.9.0.1 11.9.0.2 11.9.0.3 11.9.0.4

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
		Utilisation de la capacité des nœuds	Mis en œuvre	HTTPS	
		Métadonnées utilisées en Mo	Mis en œuvre	HTTPS	
		Nom du site	Mis en œuvre	HTTPS	
	Piscine de stockage	Inclure dans la capacité de l'eau chaude sanitaire	Mis en œuvre	HTTPS	Un moyen pour ACQ de contrôler quels pools de stockage sont intéressants dans DWH Capacity
		Nom	Mis en œuvre	HTTPS	
		Capacité du disque physique (Mo)	Mis en œuvre	HTTPS	utilisé comme capacité brute pour le pool de stockage
		Groupe de raid	Mis en œuvre	HTTPS	indique si ce pool de stockage est un groupe RAID
		Rapport brut/utilisable	Mis en œuvre	HTTPS	ratio de conversion de la capacité utilisable en capacité brute
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S'agit-il d'un périphérique de virtualisation de stockage ?

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre		
	Données du nœud de stockage	Clé	Mis en œuvre		
		Métadonnées autorisées sur l’utilisation de la capacité des nœuds	Mis en œuvre		
		Utilisation totale de la capacité des nœuds	Mis en œuvre		
		Utilisation de la capacité du nœud utilisable	Mis en œuvre		
		Utilisation de la capacité du nœud	Mis en œuvre		
		Utilisation de la capacité du nœud Métadonnées utilisées	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre		
	Disque de pool de stockage	Capacité provisionnée	Mis en œuvre		
		Capacité brute	Mis en œuvre		
		Capacité totale	Mis en œuvre		
		Capacité utilisée	Mis en œuvre		
		Ratio de capacité de dépassement d’engagement	Mis en œuvre		Présenté comme une série chronologique
		Ratio de capacité utilisée	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST StorageGrid	HTTPS	HTTPS	443		true	FAUX	true	true

Stockage Nutanix (REST)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
NX-3170-G7 NX-8155-G7 HPE DX380 12LFF G11 HPE DX380-24 G10 HPE DX385-12 Gen10 Plus NX-3060-G6 NX-3060-G7 NX-3060-G8 NX-3155G-G7 NX-3155G-G8 NX-3170-G6 NX-8035-G8 NX-8150-G7 NX-8150-G8 NX-8155-G8 XF3070 XF8050-Core	5.20.1.1 6.10 6.10.1 6.5.3.7 6.5.4 6.5.5.1 6.5.5.7 6.5.6 6.5.6.5 6.5.6.6 6.5.6.7 6.7.1.6 7.0

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		UUID	Mis en œuvre	HTTPS	
	Carte des volumes	LUN	Mis en œuvre	HTTPS	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Masque de volume	Initiateur	Mis en œuvre	HTTPS	
		Contrôleur de protocole	Mis en œuvre	HTTPS	
		Port de stockage	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
					(lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Disque de pool de stockage	Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d’écriture	Mis en œuvre	HTTPS	
	Volume	Latence totale	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d’IOP en lecture sur le disque
		Latence de lecture	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit d’écriture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Total des IOP	Mis en œuvre	HTTPS	
		Latence d’écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Nutanix	HTTPS	HTTPS	443		true	true	true	true

OpenStack (API REST / SSH)

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		hôte			
		adresses IP	Mis en œuvre	HTTPS	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Nom	Mis en œuvre	HTTPS	
		OID	Mis en œuvre	HTTPS	
	Nœud ISCSI	Alias d'hôte	Mis en œuvre	HTTPS	
		Nom du nœud	Mis en œuvre	HTTPS	
		OID	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
	Informations	Nom de la source de données	Mis en œuvre	HTTPS	Informations
		Date	Mis en œuvre	HTTPS	
		ID de l'expéditeur	Mis en œuvre	HTTPS	
		Clé d'origine	Mis en œuvre	HTTPS	
performance	Hôte	Utilisation totale du processeur	Mis en œuvre		
		Clé	Mis en œuvre		
		Utilisation totale de la mémoire	Mis en œuvre		
		ID du serveur	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST OpenStack	HTTPS	HTTPS	443		true	FAUX	true	true
OpenStack SSH	SSH	SSH	22		true	FAUX	true	true

Oracle ZFS (HTTPS)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
Stockage Sun ZFS 7120 Stockage Sun ZFS 7320 Stockage Sun ZFS 7330 Stockage Sun ZFS 7335 Stockage Sun ZFS 7350 Stockage Sun ZFS 7370 Stockage Sun ZFS 7390 Stockage Sun ZFS 7420	1-1.1 1-1.2 1-1.3 1-1.34 1-1.4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.7.29 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.37 2013.06.05.8.44 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.56 2013.06.05.8.6 2013.06.05.8.61 2013.06.05.8.65 2013.06.05.8.7 2013.06.05.8.72 2013.06.05.8.74 2013.06.05.8.76

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1364					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité utilisée	Mis en œuvre	HTTP/S	
		Virtuel	Mis en œuvre	HTTP/S	S’agit-il d’un périphérique de stockage ?
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Carte des volumes	LUN	Mis en œuvre	HTTP/S	Nom du lun backend
		Masquage obligatoire	Mis en œuvre	HTTP/S	
		Contrôleur de protocole	Mis en œuvre	HTTP/S	
		Port de stockage	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Masque de volume	Initiateur	Mis en œuvre	HTTP/S	
		Contrôleur de protocole	Mis en œuvre	HTTP/S	
		Port de stockage	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					Mo/s
		Utilisation totale	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
	Données du nœud de stockage	Taux de réussite du cache total	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Clé	Mis en œuvre		
		ID du serveur	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		
		Utilisation totale	Mis en œuvre		
	Disque de pool de stockage	Total des IOP	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Oracle ZFS	HTTP/HTTPS	HTTP/HTTPS	215		true	true	true	true

Baie Flash de stockage pure (HTTP)

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
DFSC1 FA-450 FA-C40R3 FA-C50R4 FA-C60 FA-C60R3 FA-C70R4 FA-C90R4 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X20R4 FA-X50R2 FA-X50R3 FA-X50R4 FA-X70R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4 FA-XL130 FA-XL170 FA-m20 FA-m20r2 FA-m50 FA-m70 FA-m70r2 OXYGÈNE	5.3.14 5.3.20 6.1.10 6.1.14 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.2.10 6.3.10 6.3.11 6.3.12 6.3.13 6.3.14 6.3.15 6.3.16 6.3.17 6.3.18 6.3.3 6.3.6 6.3.7 6.3.9 6.4.10 6.4.2 6.4.3 6.4.7 6.4.8 6.4.9 6.5.0 6.5.1 6.5.2 6.5.3 6.5.4 6.5.5 6.5.6 6.5.7 6.5.8 6.5.9 6.6.10 6.6.11 6.6.5 6.6.6 6.6.7 6.7.0 6.7.1 6.8.1 6.8.2 6.8.3

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Capacité écrite	Mis en œuvre	HTTP/S	Capacité totale écrite sur ce volume par un hôte en Mo
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Authentification activée	Mis en œuvre	HTTP/S	
	Carte des volumes	LUN	Mis en œuvre	HTTP/S	Nom du lun backend
		Contrôleur de protocole	Mis en œuvre	HTTP/S	
		Port de stockage	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Masque de volume	Initiateur	Mis en œuvre	HTTP/S	
		Contrôleur de protocole	Mis en œuvre	HTTP/S	
		Port de stockage	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Alias WWN	Alias d’hôte	Mis en œuvre	HTTP/S	
		Type d’objet	Mis en œuvre	HTTP/S	
		Source	Mis en œuvre	HTTP/S	
		WWN	Mis en œuvre	HTTP/S	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Instantané de la capacité utilisée	Mis en œuvre		
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
	Volume	Capacité brute	Mis en œuvre		
		Capacité totale	Mis en œuvre		
		Capacité utilisée	Mis en œuvre		
		Ratio de capacité utilisée	Mis en œuvre		
		Lecture des IOP	Mis en œuvre		Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre		
		Les IOP écrivent	Mis en œuvre		
		Latence de lecture	Mis en œuvre		
		Latence totale	Mis en œuvre		
		Latence d'écriture	Mis en œuvre		
		Débit de lecture	Mis en œuvre		
		Débit total	Mis en œuvre		Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre		

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST de stockage pur	HTTP/HTTPS	HTTP/HTTPS	80/443		true	true	true	true

Red Hat RHV (REST)

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					
1392					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Disque de machine virtuelle	OID	Mis en œuvre	HTTP/S	
		OID du disque virtuel	Mis en œuvre	HTTP/S	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Attribut de machine virtuelle	Mis en œuvre	HTTP/S	
	Hôte	Nombre de processeurs hôtes	Mis en œuvre	HTTP/S	
		Vitesse du processeur hôte	Mis en œuvre	HTTP/S	
		Mémoire installée par l'hôte	Mis en œuvre	HTTP/S	
		Modèle d'hôte	Mis en œuvre	HTTP/S	
		Nombre de cartes réseau	Mis en œuvre	HTTP/S	
		Vitesse de la carte réseau	Mis en œuvre	HTTP/S	
		adresses IP	Mis en œuvre	HTTP/S	
		Fabricant	Mis en œuvre	HTTP/S	
		Nom	Mis en œuvre	HTTP/S	
		OID	Mis en œuvre	HTTP/S	
		Type de plate-forme	Mis en œuvre	HTTP/S	
	Nœud ISCSI	Nom du nœud	Mis en œuvre	HTTP/S	
		OID	Mis en œuvre	HTTP/S	
		Type	Écart	HTTP/S	
	Informations	Nom de la source de données	Mis en œuvre	HTTP/S	Informations
		Date	Mis en œuvre	HTTP/S	
		ID de l'expéditeur	Mis en œuvre	HTTP/S	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST Red Hat RHEV	HTTPS	HTTPS	443		true	true	true	true

Stockage Rubrik

Modèles et versions pris en charge par ce collecteur de données : Versions du micrologiciel :

- 8.1.3-p12-25506
- 8.1.3-p13-25544
- 8.1.3-p2-24912
- 9.0.3-p10-25744
- 9.0.3-p5-25595
- 9.0.3-p6-25611
- 9.1.1-27527
- 9.1.2-27824
- 9.1.2-p1-27870
- 9.1.2-p1-27870_HP1473894
- 9.1.3-p1-28075
- 9.1.3-p8-28434
- 9.2.2-p1-29213
- 9.2.3-29313
- 9.2.3-p1-29368

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					léger pour la couche de volume située au-dessus de lui
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S’agit-il d’un périphérique de virtualisation de stockage ?
		Pourcentage de capacité effectivement utilisée	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1402					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

					écriture sur tous les disques) en Mo/s
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Débit d'écriture	Mis en œuvre	HTTPS	
		Utilisation totale	Mis en œuvre	HTTPS	
	Disque de pool de stockage	Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit d'écriture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Total des IOP	Mis en œuvre	HTTPS	
		Capacité totale	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
		Autre capacité utilisée	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Ratio de capacité utilisée	Mis en œuvre	HTTPS	
		Capacité de données utilisées	Mis en œuvre	HTTPS	
		Instantané de la capacité utilisée	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST de stockage Rubrik	HTTPS	HTTPS	443		true	true	true	true

Magasin de données VAST

Modèles et versions pris en charge par ce collecteur de données :

Modèles	Versions du micrologiciel
VA2437096 Données VAST	Version de build : release-5.0.0-sp24-1389206 Version de build : release-5.0.0-sp24-1389206 Version de build : release-5.0.0-sp70-1532643 Version de build : release-5.1.0-sp50-1578267 Version de build : release-5.1.0-sp51-hf3-1643358 Version de build : release-5.1.0-sp56-1630237 Version de build : release-5.1.0-sp56-hf10-1682647 Version de build : release-5.1.0-sp56-hf14-1700467 Version du système : 5.0.0.94 Version du système : 5.0.0.133 Version du système : 5.0.0.94 Version du système : 5.1.0.210 Version du système : 5.1.0.231

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Instantané de la capacité allouée	Écart	HTTPS	Capacité allouée aux snapshots en Mo
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Instantané de la capacité utilisée	Mis en œuvre	HTTPS	
		ID du pool de stockage	Mis en œuvre	HTTPS	
		Provisionnement léger pris en charge	Mis en œuvre	HTTPS	Si ce volume interne prend en charge le provisionnement léger pour la couche de volume située au-dessus de lui
		Capacité totale allouée	Mis en œuvre	HTTPS	
		Capacité totale utilisée	Mis en œuvre	HTTPS	Capacité totale en Mo
		Type	Écart	HTTPS	
		Virtuel	Mis en œuvre	HTTPS	S’agit-il d’un périphérique de virtualisation de stockage ?
		Crypté	Mis en œuvre	HTTPS	
	Machine virtuelle de stockage	Capacité allouée (Mo)	Mis en œuvre	HTTPS	Capacité allouée aux snapshots
		Commentaire	Mis en œuvre	HTTPS	
		Clé de guidage	Mis en œuvre	HTTPS	Clé unique mondiale de la machine virtuelle de stockage
		Nom	Mis en œuvre	HTTPS	
		Type	Écart	HTTPS	
		UUID	Mis en œuvre	HTTPS	
		Capacité utilisée	Mis en œuvre	HTTPS	
	Référence du volume interne de la machine virtuelle	ID du volume interne	Mis en œuvre	HTTPS	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance	Stockage	Échec de la capacité brute	Mis en œuvre	HTTPS	
		Capacité brute	Mis en œuvre	HTTPS	
		Capacité brute de réserve	Mis en œuvre	HTTPS	Capacité brute des disques de rechange (somme de tous les disques de rechange)
		Capacité des pools de stockage	Mis en œuvre	HTTPS	
		Lecture de la densité IO	Mis en œuvre	HTTPS	
		Densité IO totale	Mis en œuvre	HTTPS	
		Densité d'E/S d'écriture	Mis en œuvre	HTTPS	
		Autres IOP	Mis en œuvre	HTTPS	
		Lecture des IOP	Mis en œuvre	HTTPS	Nombre d'IOP en lecture sur le disque
		Total des IOP	Mis en œuvre	HTTPS	
		Les IOP écrivent	Mis en œuvre	HTTPS	
		Clé	Mis en œuvre	HTTPS	
		Latence de lecture	Mis en œuvre	HTTPS	
		Latence totale	Mis en œuvre	HTTPS	
		Latence d'écriture	Mis en œuvre	HTTPS	
		ID du serveur	Mis en œuvre	HTTPS	
		Débit de lecture	Mis en œuvre	HTTPS	
		Débit total	Mis en œuvre	HTTPS	Débit total moyen du disque (lecture et écriture sur tous les disques) en Mo/s
		Débit d'écriture	Mis en œuvre	HTTPS	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API VAST DataStore	HTTPS	HTTPS	443		true	true	true	true

Centre virtuel NetApp HCI

Modèles et versions pris en charge par ce collecteur de données : Versions d'API :

- VMware vCenter Server 6.7.0 build-10244857
- VMware vCenter Server 7.0.3 build-20395099

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Nœud ISCSI	Alias d’hôte	Mis en œuvre	Services Web	
		Nom du nœud	Mis en œuvre	Services Web	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		OID	Mis en œuvre	Services Web	
		Type	Écart	Services Web	
	Informations	Description de l’API	Mis en œuvre	Services Web	
		Nom de l’API	Mis en œuvre	Services Web	
		Version de l’API	Mis en œuvre	Services Web	
		Nom de l’API client	Mis en œuvre	Services Web	
		Version de l’API client	Mis en œuvre	Services Web	
		Nom de la source de données	Mis en œuvre	Services Web	Informations
		Date	Mis en œuvre	Services Web	
		ID de l’expéditeur	Mis en œuvre	Services Web	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		swapRate.inRate	Mis en œuvre	Services Web	
		Débit d'écriture du disque	Mis en œuvre	Services Web	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Utilisation totale du processeur	Mis en œuvre	Services Web	
		Planifier le temps d'attente	Mis en œuvre	Services Web	Temps d'attente pour être programmé en pourcentage
		diskIops.total	Mis en œuvre	Services Web	
		Taux de swap total	Mis en œuvre	Services Web	
		Débit de lecture	Mis en œuvre	Services Web	débit total du disque en lecture

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST VMware	Services Web	HTTP/HTTPS	80/443		true	true	true	true

VMware Cloud sur AWS

Modèles et versions pris en charge par ce collecteur de données : Versions d'API :

- VMware vCenter Server 7.0.3 build-21477706
- VMware vCenter Server 7.0.3 build-24322018
- VMware vCenter Server 8.0.0 build-22877852
- VMware vCenter Server 8.0.1 build-22161730
- VMware vCenter Server 8.0.1 build-23525738
- VMware vCenter Server 8.0.3 build-24322831

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Nom	Mis en œuvre	Services Web	
		OID	Mis en œuvre	Services Web	
Produit	**Catégorie**	**Fonctionnalité/ Attribut**	**Statut**	**Protocole utilisé**	**Informations supplémentaires**
		Type de plate-forme	Mis en œuvre	Services Web	
	Informations	Description de l’API	Mis en œuvre	Services Web	
		Nom de l’API	Mis en œuvre	Services Web	
		Version de l’API	Mis en œuvre	Services Web	
		Nom de l’API client	Mis en œuvre	Services Web	
		Version de l’API client	Mis en œuvre	Services Web	
		Nom de la source de données	Mis en œuvre	Services Web	Informations
		Date	Mis en œuvre	Services Web	
		ID de l’expéditeur	Mis en œuvre	Services Web	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance	Hôte	Utilisation totale du processeur	Mis en œuvre	Services Web	
		Lecture des IOP	Mis en œuvre	Services Web	Nombre d'IOP en lecture sur le disque
		diskIops.total	Mis en œuvre	Services Web	
		Écriture des IOPS sur disque	Mis en œuvre	Services Web	
		Latence de lecture	Mis en œuvre	Services Web	
		Latence totale	Mis en œuvre	Services Web	
		Latence d'écriture	Mis en œuvre	Services Web	
		Débit de lecture du disque	Mis en œuvre	Services Web	
		Débit de lecture	Mis en œuvre	Services Web	débit total du disque en lecture
		Débit d'écriture du disque	Mis en œuvre	Services Web	
		Débit de lecture IP	Mis en œuvre	Services Web	
		Débit total	Mis en œuvre	Services Web	Débit IP total
		ipThroughput.écriture	Mis en œuvre	Services Web	
		Clé	Mis en œuvre	Services Web	
		Utilisation totale de la mémoire	Mis en œuvre	Services Web	
		ID du serveur	Mis en œuvre	Services Web	
		swapRate.inRate	Mis en œuvre	Services Web	
		Taux de swap	Mis en œuvre	Services Web	
		Taux de swap total	Mis en œuvre	Services Web	

API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST VMware	Services Web	HTTP/HTTPS	80/443		true	true	true	true

VMware vSphere (services Web)

Modèles et versions pris en charge par ce collecteur de données : Versions d'API :

- VMware ESXi 6.0.0 build-10474991
- VMware ESXi 6.0.0 build-10719132
- VMware ESXi 6.0.0 build-13635687
- VMware ESXi 6.0.0 build-2494585
- VMware ESXi 6.0.0 build-3620759
- VMware ESXi 6.0.0 build-5050593
- VMware ESXi 6.0.0 build-5224934
- VMware ESXi 6.0.0 build-9239799
- VMware ESXi 6.5.0 build-5310538
- VMware ESXi 7.0.3 build-20036589
- VMware ESXi 7.0.3 build-20328353
- VMware ESXi 8.0.0 build-21203435
- VMware ESXi 8.0.1 build-21495797
- VMware vCenter Server 5.0.0 build-623373
- VMware vCenter Server 5.5.0 build-1750787
- VMware vCenter Server 5.5.0 build-2442329
- VMware vCenter Server 5.5.0 build-3252642
- VMware vCenter Server 5.5.0 build-6516310
- VMware vCenter Server 5.5.0 build-9911218
- VMware vCenter Server 6.0.0 build-13638472
- VMware vCenter Server 6.0.0 build-14510545
- VMware vCenter Server 6.0.0 build-2776511
- VMware vCenter Server 6.0.0 build-3634793
- VMware vCenter Server 6.0.0 build-5183551
- VMware vCenter Server 6.0.0 build-9313458

- VMware vCenter Server 6.5.0 build-10964411
- VMware vCenter Server 6.5.0 build-12863991
- VMware vCenter Server 6.5.0 build-15259038
- VMware vCenter Server 6.5.0 build-17994927
- VMware vCenter Server 6.5.0 build-18499837
- VMware vCenter Server 6.5.0 build-18711281
- VMware vCenter Server 6.5.0 build-20510539
- VMware vCenter Server 6.5.0 build-22499743
- VMware vCenter Server 6.5.0 build-5973321
- VMware vCenter Server 6.7.0 build-10244857
- VMware vCenter Server 6.7.0 build-11727113
- VMware vCenter Server 6.7.0 build-14070654
- VMware vCenter Server 6.7.0 build-14792544
- VMware vCenter Server 6.7.0 build-15679289
- VMware vCenter Server 6.7.0 build-17137232
- VMware vCenter Server 6.7.0 build-17137327
- VMware vCenter Server 6.7.0 build-18010560
- VMware vCenter Server 6.7.0 build-18010599
- VMware vCenter Server 6.7.0 build-18485185
- VMware vCenter Server 6.7.0 build-18831049
- VMware vCenter Server 6.7.0 build-19299595
- VMware vCenter Server 6.7.0 build-19832280
- VMware vCenter Server 6.7.0 build-20504301
- VMware vCenter Server 6.7.0 build-20504362
- VMware vCenter Server 6.7.0 build-22509751
- VMware vCenter Server 6.7.0 build-24323669
- VMware vCenter Server 6.7.0 build-8170161
- VMware vCenter Server 7.0.2 build-17958471
- VMware vCenter Server 7.0.2 build-18356314
- VMware vCenter Server 7.0.2 build-18455184
- VMware vCenter Server 7.0.2 build-22781136
- VMware vCenter Server 7.0.3 build-18778458
- VMware vCenter Server 7.0.3 build-19234570
- VMware vCenter Server 7.0.3 build-19480866
- VMware vCenter Server 7.0.3 build-19717403
- VMware vCenter Server 7.0.3 build-20150588
- VMware vCenter Server 7.0.3 build-20395099

- VMware vCenter Server 7.0.3 build-20845200
- VMware vCenter Server 7.0.3 build-20990077
- VMware vCenter Server 7.0.3 build-21290409
- VMware vCenter Server 7.0.3 build-21477706
- VMware vCenter Server 7.0.3 build-21784236
- VMware vCenter Server 7.0.3 build-21958406
- VMware vCenter Server 7.0.3 build-22357613
- VMware vCenter Server 7.0.3 build-22837322
- VMware vCenter Server 7.0.3 build-23085514
- VMware vCenter Server 7.0.3 build-23788036
- VMware vCenter Server 7.0.3 build-24026615
- VMware vCenter Server 7.0.3 build-24201990
- VMware vCenter Server 7.0.3 build-24322018
- VMware vCenter Server 8.0.0 build-20519528
- VMware vCenter Server 8.0.0 build-20920323
- VMware vCenter Server 8.0.0 build-21216066
- VMware vCenter Server 8.0.0 build-21457384
- VMware vCenter Server 8.0.1 build-21560480
- VMware vCenter Server 8.0.1 build-21815093
- VMware vCenter Server 8.0.1 build-21860503
- VMware vCenter Server 8.0.1 build-22088981
- VMware vCenter Server 8.0.1 build-22368047
- VMware vCenter Server 8.0.1 build-24005165
- VMware vCenter Server 8.0.2 build-22385739
- VMware vCenter Server 8.0.2 build-22617221
- VMware vCenter Server 8.0.2 build-23319993
- VMware vCenter Server 8.0.2 build-23504390
- VMware vCenter Server 8.0.2 build-23929136
- VMware vCenter Server 8.0.2 build-24321653
- VMware vCenter Server 8.0.3 build-24022515
- VMware vCenter Server 8.0.3 build-24091160
- VMware vCenter Server 8.0.3 build-24262322
- VMware vCenter Server 8.0.3 build-24305161
- VMware vCenter Server 8.0.3 build-24322831

Produits pris en charge par ce collecteur de données :

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
fondation					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

	Nœud ISCSI	Alias d’hôte	Mis en œuvre	Services Web	
		Nom du nœud	Mis en œuvre	Services Web	
		OID	Mis en œuvre	Services Web	
		Type	Écart	Services Web	
	Informations	Description de l’API	Mis en œuvre	Services Web	
		Nom de l’API	Mis en œuvre	Services Web	
		Version de l’API	Mis en œuvre	Services Web	
		Nom de l’API client	Mis en œuvre	Services Web	
		Version de l’API client	Mis en œuvre	Services Web	
		Nom de la source de données	Mis en œuvre	Services Web	Informations
		Date	Mis en œuvre	Services Web	
		ID de l’expéditeur	Mis en œuvre	Services Web	

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires
performance					
1444					

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

Produit	Catégorie	Fonctionnalité/ Attribut	Statut	Protocole utilisé	Informations supplémentaires

		Débit d'écriture du disque	Mis en œuvre	Services Web	
		Débit de lecture	Mis en œuvre	Services Web	

Produit	Catégorie	Fonctionnalité/ Attribut IP	Statut	Protocole utilisé	Informations supplémentaires
		Débit total	Mis en œuvre	Services Web	Débit IP total
		ipThroughput.écriture	Mis en œuvre	Services Web	
		Utilisation totale de la mémoire	Mis en œuvre	Services Web	
		swapRate.inRate	Mis en œuvre	Services Web	
		Taux de swap	Mis en œuvre	Services Web	
		Taux de swap total	Mis en œuvre	Services Web	
		Planifier le temps d'attente	Mis en œuvre	Services Web	Temps d'attente pour être programmé en pourcentage

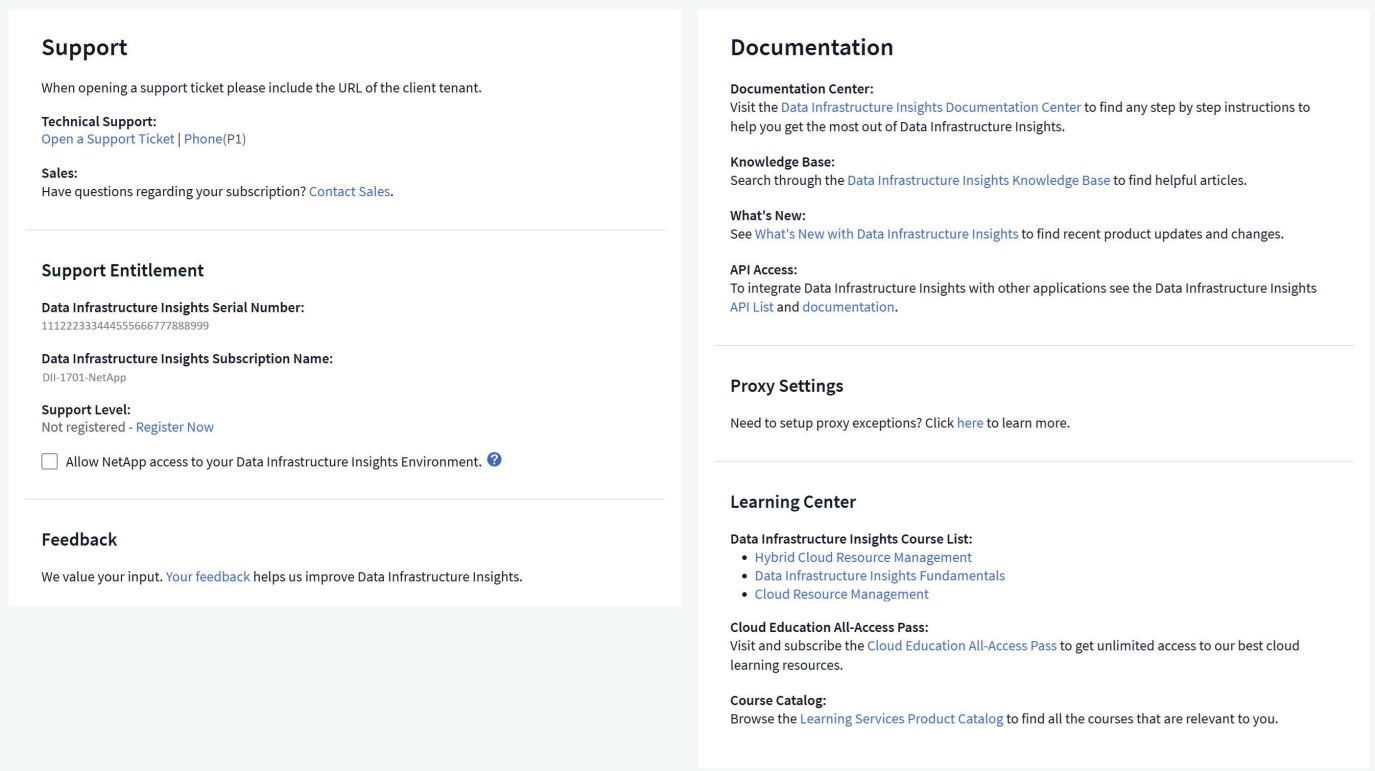
API de gestion utilisées par ce collecteur de données :

API	Protocole utilisé	Protocole de couche de transport utilisé	Ports entrants utilisés	Ports sortants utilisés	Prend en charge l'authentification	Nécessite uniquement des informations d'identification en « lecture seule »	Prend en charge le cryptage	Compatible avec le pare-feu (ports statiques)
API REST VMware	Services Web	HTTP/HTTPS	80/443		true	true	true	true

Référence et support

Demande d’assistance

Vous pouvez accéder aux options d’assistance disponibles dans Data Infrastructure Insights en sélectionnant **Aide > Assistance**.



Activation du droit d’assistance

Data Infrastructure Insights propose un libre-service et une assistance par e-mail lorsqu’il est exécuté en mode d’essai. Une fois que vous avez souscrit au service, il est fortement recommandé d’activer le droit d’assistance. L’activation du droit d’assistance vous permet d’accéder au support technique via le système de billetterie Web et par téléphone. Le mode d’assistance par défaut est le libre-service jusqu’à ce que l’enregistrement soit terminé. Voirdétails ci-dessous.

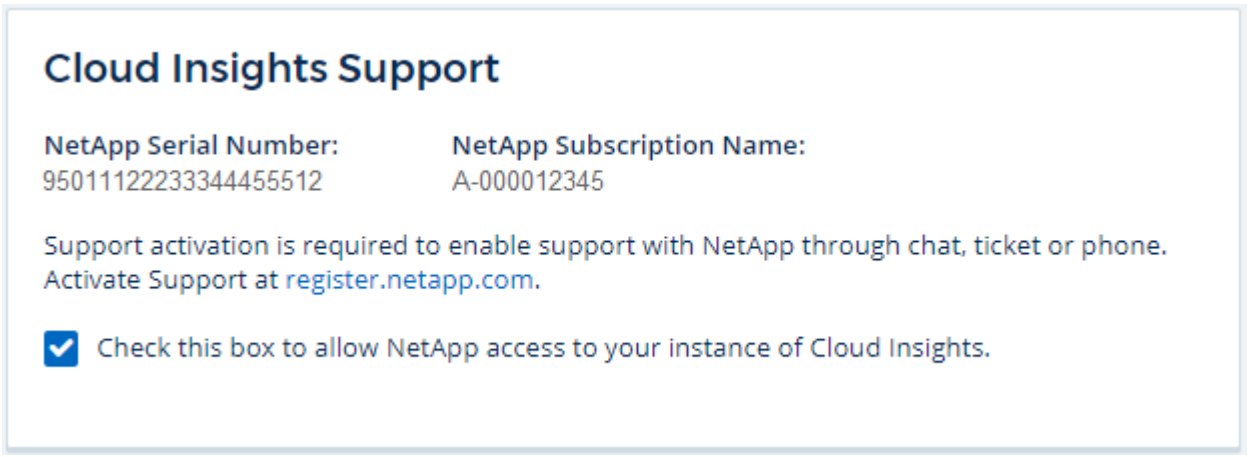
Au cours du processus d’abonnement initial, votre instance Data Infrastructure Insights générera un numéro de série NetApp à 20 chiffres commençant par « 950 ». Ce numéro de série NetApp représente l’abonnement Data Infrastructure Insights associé à votre compte. Vous devez enregistrer le numéro de série NetApp pour activer le droit de support. Nous proposons deux options d’inscription au support :

1. Utilisateur disposant d’un compte SSO NetApp Support Site (NSS) préexistant (par exemple, client NetApp actuel)
2. Nouveau client NetApp sans compte SSO NetApp Support Site (NSS) préexistant

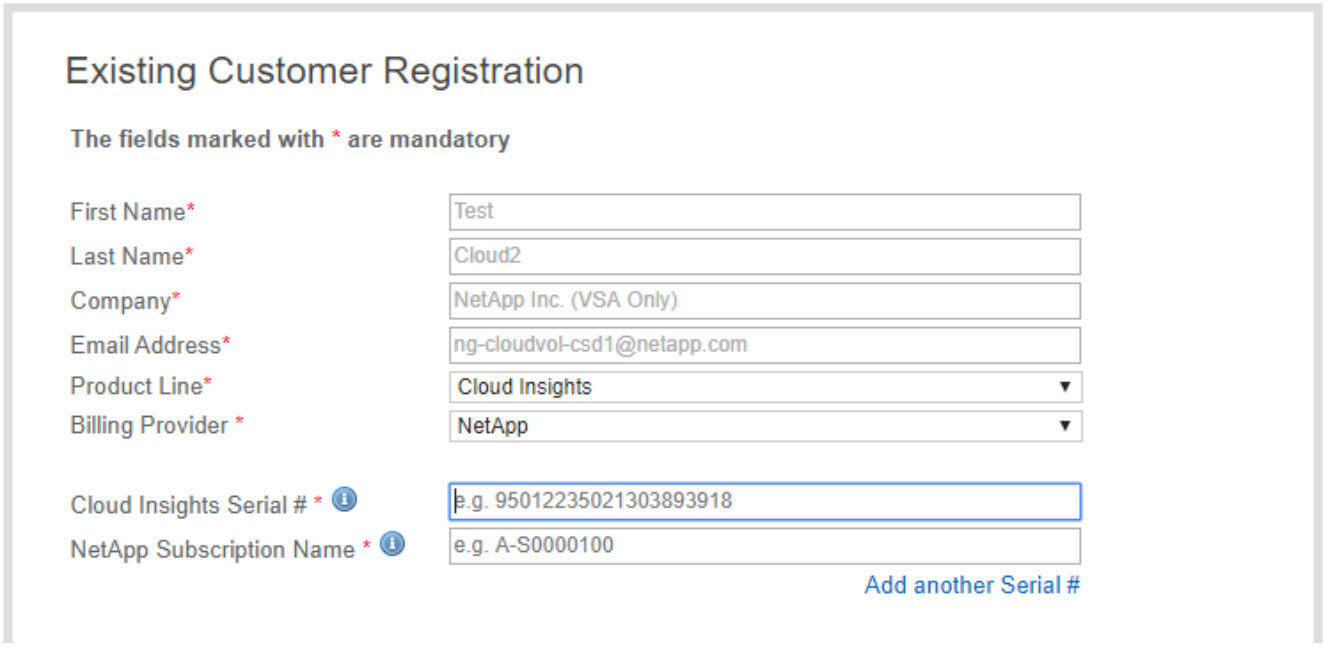
Option 1 : Étapes pour un utilisateur disposant d’un compte SSO NetApp Support Site (NSS) préexistant

Étapes

1. Accédez au site Web d'inscription NetApp https://register.netapp.com
2. Sélectionnez « Je suis déjà inscrit en tant que client NetApp » et choisissez *Data Infrastructure Insights* comme gamme de produits. Sélectionnez votre fournisseur de facturation (NetApp ou AWS) et indiquez votre numéro de série et votre nom d'abonnement NetApp ou votre identifiant client AWS en vous référant au menu « Aide > Support » dans l'interface utilisateur de Data Infrastructure Insights :



3. Remplissez le formulaire d'inscription du client existant et cliquez sur **Soumettre**.



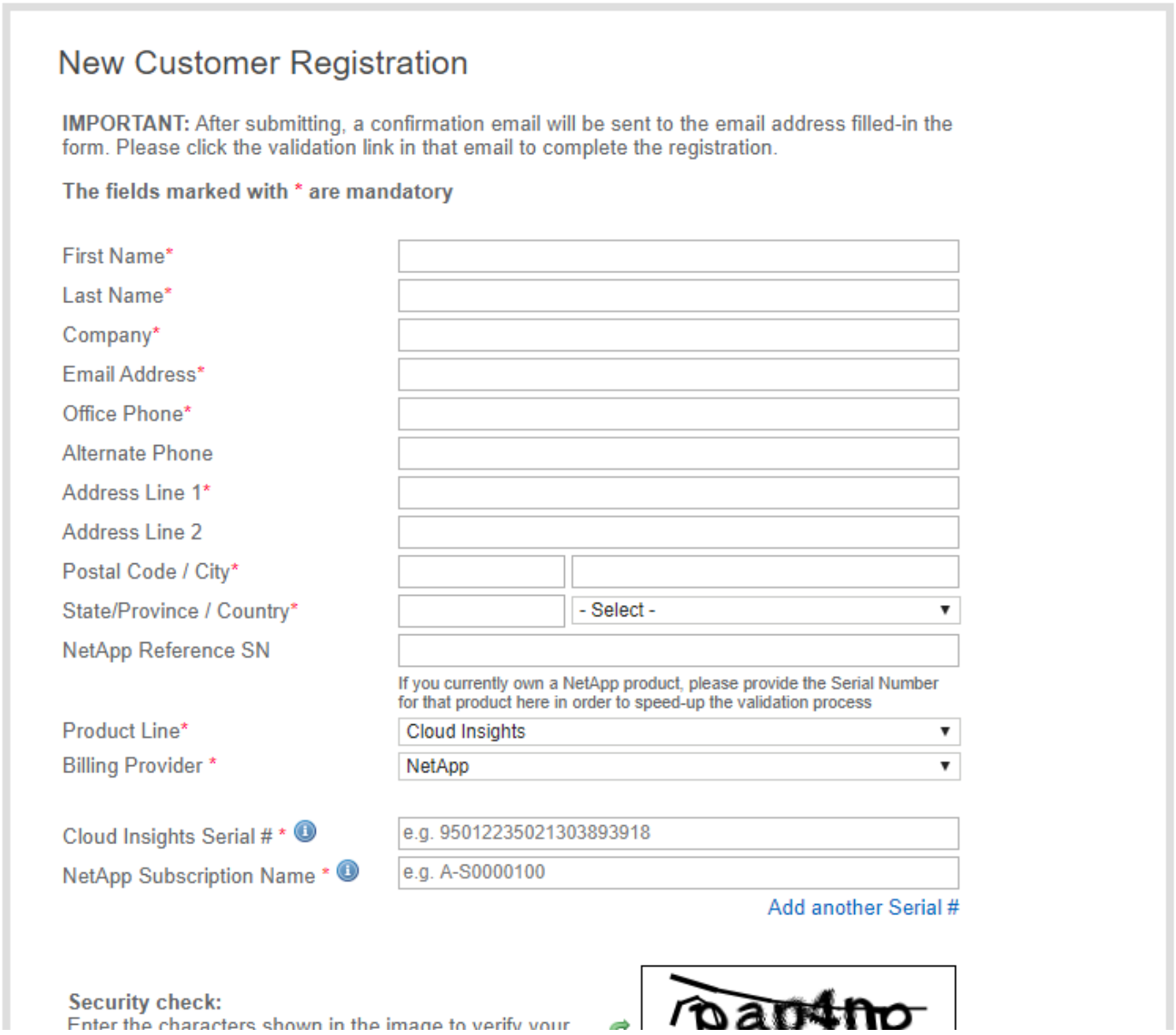
4. Si aucune erreur ne se produit, l'utilisateur sera dirigé vers une page « Inscription soumise avec succès ». L'adresse e-mail associée au nom d'utilisateur NSS SSO utilisé pour l'enregistrement recevra un e-mail dans quelques minutes indiquant « votre produit est désormais éligible au support ».
5. Il s'agit d'un enregistrement unique pour le numéro de série NetApp de Data Infrastructure Insights .

Option 2 : Étapes pour un nouveau client NetApp sans compte SSO NetApp Support Site (NSS) préexistant

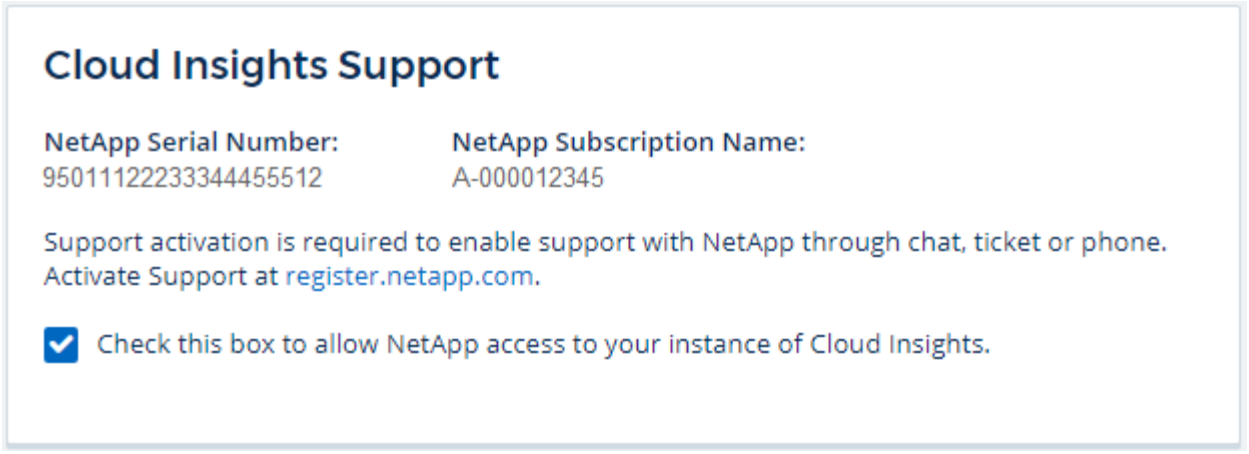
Étapes

1. Accédez au site Web d'inscription NetApp https://register.netapp.com
2. Sélectionnez « Je ne suis pas un client NetApp enregistré » et complétez les informations requises dans

l'exemple de formulaire ci-dessous :



1. Sélectionnez *Data Infrastructure Insights* comme gamme de produits. Sélectionnez votre fournisseur de facturation (NetApp ou AWS) et indiquez votre numéro de série et votre nom d'abonnement NetApp ou votre identifiant client AWS en vous référant au menu « Aide > Support » dans l'interface utilisateur de Data Infrastructure Insights :



2. Si aucune erreur ne se produit, l'utilisateur sera dirigé vers une page « Inscription soumise avec succès ». L'adresse e-mail associée au nom d'utilisateur NSS SSO utilisé pour l'enregistrement recevra un e-mail dans quelques heures indiquant « votre produit est désormais éligible au support ».
3. En tant que nouveau client NetApp , vous devrez également créer un compte utilisateur NetApp Support Site (NSS) pour les futures inscriptions et accéder au portail d'assistance pour l'assistance technique et la billetterie Web. Ce lien se trouve à https://mysupport.netapp.com/eservice/public/now.do . Vous pouvez fournir votre numéro de série Data Infrastructure Insights nouvellement enregistré pour accélérer le processus.
4. Il s'agit d'un enregistrement unique pour le numéro de série NetApp de Data Infrastructure Insights .

Obtenir des informations d'assistance

NetApp fournit un support pour Data Infrastructure Insights de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24h/24 et 7j/7, telles que des articles de la base de connaissances (KB) ou la communauté NetApp . Pour les utilisateurs abonnés à Data Infrastructure Insights, le support technique est disponible par téléphone ou par ticket Web. Un compte SSO NetApp Support Site (NSS) est requis pour les tickets Web ainsi que pour la gestion des cas.

Assistance en libre-service :

Ces options d'assistance sont disponibles en mode d'essai et sont disponibles gratuitement 24h/24 et 7j/7 :

- * https://kb.netapp.com/Cloud/ncds/nds/dii/dii_kbs [Base de connaissances]*

  En cliquant sur les liens de cette section, vous accédez à la base de connaissances NetApp , où vous pouvez rechercher des articles pertinents, des procédures et bien plus encore.

- *"Documentation" *

  En cliquant sur le lien Documentation, vous accédez à ce centre de documentation.

- *"Communauté" *

  En cliquant sur le lien de la communauté, vous accédez à la communauté NetApp Data Infrastructure Insights , où vous pouvez vous connecter avec vos pairs et vos experts.

Il existe également un lien pour fournir**"Retour"** pour nous aider à améliorer Data Infrastructure Insights.

Assistance aux abonnements

Outre les options d'auto-assistance ci-dessus, si vous disposez d'un abonnement Data Infrastructure Insights ou d'une assistance payante pour les produits ou services NetApp surveillés, vous pouvez travailler avec un ingénieur de support NetApp pour résoudre votre problème.

> Vous devez vous inscrire pour pouvoiractiver le support pour les produits NetApp Cloud. Pour vous inscrire, rendez-vous sur le site de NetApp"Enregistrement de l'assistance aux services de données cloud" .

Il est fortement recommandé de cocher la case pour autoriser un ingénieur de support NetApp à accéder à votre locataire Data Infrastructure Insights pendant votre session de support. Cela permettra à l'ingénieur de résoudre le problème et de vous aider à le résoudre rapidement. Lorsque votre problème est résolu ou que votre session d'assistance est terminée, vous pouvez décocher la case.

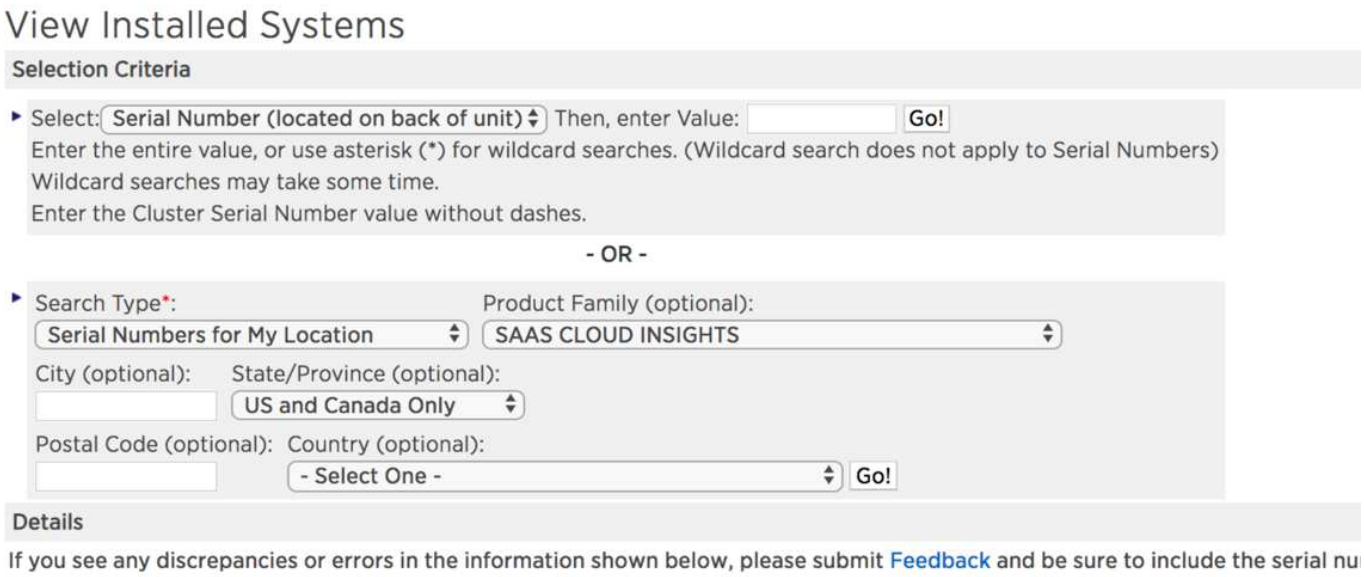
Vous pouvez demander de l'aide par l'une des méthodes suivantes. Vous devez disposer d'un abonnement Data Infrastructure Insights actif pour utiliser ces options d'assistance :

- **"Téléphone"**
- **"Ticket d'assistance"**

Vous pouvez également demander une assistance commerciale en cliquant sur le lien **Contacter le service commercial**.

Votre numéro de série Data Infrastructure Insights est visible dans le service à partir du menu **Aide > Support**. Si vous rencontrez des problèmes pour accéder au service et avez déjà enregistré un numéro de série auprès de NetApp , vous pouvez également consulter votre liste de numéros de série Data Infrastructure Insights à partir du site de support NetApp comme suit :

- Connectez-vous à mysupport.netapp.com
- Dans l'onglet Produits > Mes produits, utilisez la famille de produits « SaaS Data Infrastructure Insights» pour localiser tous vos numéros de série enregistrés :



Matrice de support du collecteur de Data Infrastructure Insights

Vous pouvez afficher ou télécharger des informations et des détails sur les collecteurs de données pris en charge dans le* Matrice de prise en charge du collecteur de Data Infrastructure Insights *, role= .

Centre d'apprentissage

Quel que soit votre abonnement, **Aide > Support** renvoie vers plusieurs offres de cours NetApp University pour vous aider à tirer le meilleur parti de Data Infrastructure Insights. Découvrez-les !

Référence du collecteur de données - Infrastructure

Référence spécifique au fournisseur

Les rubriques de cette section fournissent des informations de référence spécifiques au fournisseur. Dans la plupart des cas, la configuration d'un collecteur de données est simple. Dans certains cas, vous pouvez avoir besoin d'informations ou de commandes supplémentaires pour configurer correctement le collecteur de données.

Cliquez sur un **fournisseur** dans le menu de gauche pour voir les informations concernant leurs collecteurs de données.

Configuration du collecteur de données Amazon EC2

Data Infrastructure Insights utilise le collecteur de données Amazon EC2 pour acquérir des données d'inventaire et de performances à partir d'instances EC2.

Exigences

Pour collecter des données à partir des appareils Amazon EC2, vous devez disposer des informations suivantes :

- Vous devez posséder l'un des éléments suivants :
  - Le **rôle IAM** pour votre compte cloud Amazon EC2, si vous utilisez l'authentification par rôle IAM. Le rôle IAM s'applique uniquement si votre unité d'acquisition est installée sur une instance AWS.
  - L'ID **Clé d'accès IAM** et la clé d'accès secrète de votre compte cloud Amazon EC2, si vous utilisez l'authentification par clé d'accès IAM.
- Vous devez avoir le privilège « liste d'organisation »
- Port 443 HTTPS
- Les instances EC2 peuvent être signalées comme une machine virtuelle ou (moins naturellement) comme un hôte. Les volumes EBS peuvent être signalés à la fois comme un disque virtuel utilisé par la machine virtuelle et comme un magasin de données fournissant la capacité du disque virtuel.

Les clés d'accès se composent d'un ID de clé d'accès (par exemple, AKIAIOSFODNN7EXAMPLE) et d'une clé d'accès secrète (par exemple, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Vous utilisez des clés d'accès pour signer les demandes programmatiques que vous envoyez à EC2 si vous utilisez les SDK Amazon EC2, REST ou les opérations API de requête. Ces clés sont fournies avec votre contrat Amazon.

Configuration

Saisissez les données dans les champs du collecteur de données conformément au tableau ci-dessous :

Champ	Description
Région AWS	Choisissez la région AWS
Rôle IAM	À utiliser uniquement lors de l'acquisition sur un AU dans AWS. Voir ci-dessous pour plus d'informations surRôle IAM .
ID de clé d'accès AWS IAM	Saisissez l'ID de clé d'accès AWS IAM. Obligatoire si vous n'utilisez pas le rôle IAM.
Clé d'accès secrète AWS IAM	Saisissez la clé d'accès secrète AWS IAM. Obligatoire si vous n'utilisez pas le rôle IAM.
Je comprends qu'AWS me facture les demandes d'API	Cochez cette case pour vérifier que vous avez bien compris qu'AWS vous facture les demandes d'API effectuées par le sondage Data Infrastructure Insights .

Configuration avancée

Champ	Description
Inclure des régions supplémentaires	Spécifiez les régions supplémentaires à inclure dans le sondage.
Rôle inter-comptes	Rôle permettant d'accéder aux ressources dans différents comptes AWS.
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60
Choisissez « Exclure » ou « Inclure » pour appliquer le filtre aux machines virtuelles par balises	Spécifiez s'il faut inclure ou exclure les machines virtuelles par balises lors de la collecte de données. Si « Inclure » est sélectionné, le champ Clé de balise ne peut pas être vide.
Clés et valeurs de balises sur lesquelles filtrer les machines virtuelles	Cliquez sur **+ Filtrer la balise** pour choisir les machines virtuelles (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs qui correspondent aux clés et aux valeurs des balises sur la machine virtuelle. La clé de balise est obligatoire, la valeur de balise est facultative. Lorsque la valeur de balise est vide, la machine virtuelle est filtrée tant qu'elle correspond à la clé de balise.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 1800
Espace de noms des métriques de l'agent CloudWatch	Espace de noms dans EC2/EBS à partir duquel collecter des données. Notez que si les noms des métriques par défaut dans cet espace de noms sont modifiés, Data Infrastructure Insights peut ne pas être en mesure de collecter ces données renommées. Il est recommandé de laisser les noms de métriques par défaut.

Clé d'accès IAM

Les clés d'accès sont des informations d'identification à long terme pour un utilisateur IAM ou l'utilisateur racine du compte AWS. Les clés d'accès sont utilisées pour signer des requêtes programmatiques à l'AWS CLI ou à l'API AWS (directement ou à l'aide du SDK AWS).

Les clés d'accès se composent de deux parties : un identifiant de clé d'accès et une clé d'accès secrète. Lorsque vous utilisez l'authentification *IAM Access Key* (par opposition à l'authentification *IAM Role*), vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour l'authentification des demandes. Pour plus d'informations, consultez la documentation Amazon sur"Clés d'accès" .

Rôle IAM

Lorsque vous utilisez l'authentification *IAM Role* (par opposition à l'authentification par clé d'accès IAM), vous devez vous assurer que le rôle que vous créez ou spécifiez dispose des autorisations appropriées nécessaires pour accéder à vos ressources.

Par exemple, si vous créez un rôle IAM nommé *InstanceEc2ReadOnly*, vous devez configurer la stratégie pour accorder l'autorisation d'accès à la liste en lecture seule EC2 à toutes les ressources EC2 pour ce rôle IAM. De plus, vous devez accorder l'accès STS (Security Token Service) afin que ce rôle soit autorisé à assumer des rôles sur plusieurs comptes.

Après avoir créé un rôle IAM, vous pouvez l'attacher lorsque vous créez une nouvelle instance EC2 ou toute instance EC2 existante.

Après avoir attaché le rôle IAM *InstanceEc2ReadOnly* à une instance EC2, vous pourrez récupérer les informations d'identification temporaires via les métadonnées d'instance par nom de rôle IAM et les utiliser pour accéder aux ressources AWS par n'importe quelle application exécutée sur cette instance EC2.

Pour plus d'informations, consultez la documentation Amazon sur"Rôles IAM" .

Remarque : le rôle IAM ne peut être utilisé que lorsque l'unité d'acquisition s'exécute dans une instance AWS.

Mappage des balises Amazon aux annotations Data Infrastructure Insights

Le collecteur de données Amazon EC2 inclut une option qui vous permet de renseigner les annotations Data Infrastructure Insights avec des balises configurées sur EC2. Les annotations doivent être nommées exactement comme les balises EC2. Data Infrastructure Insights renseignera toujours les annotations de type texte portant le même nom et fera de son mieux pour renseigner les annotations d'autres types (nombre, booléen, etc.). Si votre annotation est d'un type différent et que le collecteur de données ne parvient pas à la renseigner, il peut être nécessaire de supprimer l'annotation et de la recréer en tant que type de texte.

Notez qu'AWS est sensible à la casse, tandis que Data Infrastructure Insights n'est pas sensible à la casse. Ainsi, si vous créez une annotation nommée « OWNER » dans Data Infrastructure Insights et des balises nommées « OWNER », « Owner » et « owner » dans EC2, toutes les variantes EC2 de « owner » seront mappées à l'annotation « OWNER » de Cloud Insight.

Inclure des régions supplémentaires

Dans la section **Configuration avancée** d'AWS Data Collector, vous pouvez définir le champ **Inclure des régions supplémentaires** pour inclure des régions supplémentaires, séparées par une virgule ou un point-virgule. Par défaut, ce champ est défini sur ***us-.**, qui collecte toutes les régions AWS américaines. Pour collecter sur *toutes* les régions, définissez ce champ sur **.***. Si le champ **Inclure des régions supplémentaires** est vide, le collecteur de données collectera les données sur les actifs spécifiés dans le champ **Région AWS** comme spécifié dans la section **Configuration**.

Collecte à partir des comptes enfants AWS

Data Infrastructure Insights prend en charge la collecte de comptes enfants pour AWS au sein d'un seul collecteur de données AWS. La configuration de cette collection est effectuée dans l'environnement AWS :

- Vous devez configurer chaque compte enfant pour qu'il dispose d'un rôle AWS qui permet à l'ID de compte principal d'accéder aux détails EC2 à partir du compte enfant.
- Chaque compte enfant doit avoir le nom de rôle configuré comme la même chaîne.
- Saisissez cette chaîne de nom de rôle dans la section **Configuration avancée** de Data Infrastructure Insights AWS Data Collector, dans le champ **Rôle inter-comptes**.
- Le compte sur lequel le collecteur est installé doit disposer des privilèges *administrateur d'accès délégué*. Voir le"Documentation AWS" pour plus d'informations.

Meilleure pratique : il est fortement recommandé d'attribuer la stratégie AWS prédéfinie *AmazonEC2ReadOnlyAccess* au compte principal EC2. De plus, l'utilisateur configuré dans la source de données doit avoir au moins la politique prédéfinie *AWSOrganizationsReadOnlyAccess* attribuée, afin d'interroger AWS.

Veuillez consulter les éléments suivants pour obtenir des informations sur la configuration de votre environnement afin de permettre à Data Infrastructure Insights de collecter des données à partir des comptes enfants AWS :

"Tutoriel : Déléguer l'accès aux comptes AWS à l'aide des rôles IAM"

"Configuration AWS : fournir l'accès à un utilisateur IAM dans un autre compte AWS dont vous êtes propriétaire"

"Création d'un rôle pour déléguer des autorisations à un utilisateur IAM"

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Amazon FSx for NetApp ONTAP

Ce collecteur de données acquiert des données d'inventaire et de performances à partir d' Amazon FSx for NetApp ONTAP. Ce collecteur de données sera mis à disposition progressivement dans toutes les régions de service Data Infrastructure Insights . Contactez votre commercial si vous ne voyez pas l'icône de ce collecteur dans votre environnement Data Infrastructure Insights .

Ce collecteur Data Infrastructure Insights nécessite un utilisateur ONTAP avec un rôle *Filesystem-Scoped*. Veuillez consulter l'AWS"Rôles et règles" documentation sur les options disponibles. À l'heure actuelle, AWS ne prend en charge qu'un seul type de rôle d'utilisateur avec l'étendue du système de fichiers, à savoir *fsxadmin*. Il s'agit du rôle approprié à utiliser pour le collecteur Data Infrastructure Insights . L'utilisateur doit également avoir ces trois applications qui lui sont attribuées : http, ontapi, ssh.

Terminologie

Data Infrastructure Insights acquiert les données d'inventaire et de performances du collecteur de données FSx- NetApp . Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Cluster	Stockage
LUN	Volume
Volume	Volume interne

Terminologie FSx- NetApp

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources de stockage FSx- NetApp . Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – Une liste délimitée par des virgules des noms de modèles uniques et discrets au sein de ce cluster.
- Fournisseur – AWS
- Numéro de série – Le numéro de série de la matrice.
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données.
- Capacité brute – somme de base 2 de tout le stockage SSD attribué au système de fichiers FSx.
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes internes individuels.
- Débit – agrégé à partir de volumes internes. Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire.

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire.
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Agrégat » ou de « Groupe RAID ».
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs.
- IOPS – la somme des IOPS de tous les volumes alloués sur ce pool de stockage.
- Débit – le débit total de tous les volumes alloués sur ce pool de stockage.

Exigences

Les exigences suivantes sont requises pour configurer et utiliser ce collecteur de données :

- Vous devez avoir accès à un compte avec le rôle « fsxadmin », avec trois applications qui lui sont

attribuées : ssh, ontapi, http

- Les détails du compte incluent le nom d'utilisateur et le mot de passe.
- Exigences du port : 443

Configuration

Champ	Description
IP de gestion NetApp	Adresse IP ou nom de domaine complet du cluster NetApp
Nom d'utilisateur	Nom d'utilisateur pour le cluster NetApp
Mot de passe	Mot de passe pour le cluster NetApp

Mesures avancées

Ce collecteur de données collecte les mesures avancées suivantes à partir du stockage FSx pour NetApp ONTAP :

- politique f
- nfsv3
- nfsv3:nœud
- nfsv4
- nfsv4_1
- nfsv4_1 : nœud
- nfsv4:nœud
- groupe_de_politiques
- qtree
- volume
- volume_de_charge_de_travail

Notez que les commandes CLI et API FSx récupèrent certaines valeurs de capacité que Data Infrastructure Insights ZAPI ne collecte pas. Par conséquent, certaines valeurs de capacité (telles que celles des pools de stockage) peuvent être différentes dans Data Infrastructure Insights de ce qu'elles sont sur FSx lui-même.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Recevez une réponse HTTP 401 ou un code d'erreur ZAPI 13003 et ZAPI renvoie « Privilèges insuffisants » ou « non autorisé pour cette commande »	Vérifiez le nom d'utilisateur et le mot de passe, ainsi que les privilèges/autorisations de l'utilisateur.
ZAPI renvoie « le rôle du cluster n'est pas cluster_mgmt LIF »	AU doit communiquer avec l'IP de gestion du cluster. Vérifiez l'IP et changez-la si nécessaire

Problème:	Essayez ceci:
La commande ZAPI échoue après une nouvelle tentative	AU a un problème de communication avec le cluster. Vérifiez le réseau, le numéro de port et l'adresse IP. L'utilisateur doit également essayer d'exécuter une commande à partir de la ligne de commande à partir de la machine AU.
AU n'a pas réussi à se connecter à ZAPI via HTTP	Vérifiez si le port ZAPI accepte le texte en clair. Si AU tente d'envoyer du texte en clair à un socket SSL, la communication échoue.
La communication échoue avec SSLException	AU tente d'envoyer SSL à un port en texte clair sur un fichier. Vérifiez si le port ZAPI accepte SSL ou utilisez un autre port.
Erreurs de connexion supplémentaires : la réponse ZAPI contient le code d'erreur 13001, « la base de données n'est pas ouverte ». Le code d'erreur ZAPI est 60 et la réponse contient « l'API ne s'est pas terminée à temps ». La réponse ZAPI contient « initialize_session() a renvoyé un environnement NULL ». Le code d'erreur ZAPI est 14007 et la réponse contient « le nœud n'est pas sain ».	Vérifiez le réseau, le numéro de port et l'adresse IP. L'utilisateur doit également essayer d'exécuter une commande à partir de la ligne de commande à partir de la machine AU.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données de calcul Azure

Data Infrastructure Insights utilise le collecteur de données de calcul Azure pour acquérir des données d'inventaire et de performances à partir d'instances de calcul Azure.

Exigences

Vous avez besoin des informations suivantes pour configurer ce collecteur de données.

- Exigence de port : 443 HTTPS
- URI de redirection Azure OAuth 2.0 (login.microsoftonline.com)
- IP REST de gestion Azure (management.azure.com)
- Adresse IP du gestionnaire de ressources Azure (management.core.windows.net)
- ID d'application du principal de service Azure (client) (rôle de lecteur requis)
- Clé d'authentification du principal du service Azure (mot de passe utilisateur)
- Vous devez configurer un compte Azure pour la découverte de Data Infrastructure Insights .

  Une fois le compte correctement configuré et l'application enregistrée dans Azure, vous disposerez des informations d'identification requises pour découvrir l'instance Azure avec Data Infrastructure Insights. Le lien suivant décrit comment configurer le compte pour la découverte.https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal[]

Configuration

Saisissez les données dans les champs du collecteur de données conformément au tableau ci-dessous :

Champ	Description
ID d'application du principal de service Azure (client) (rôle de lecteur requis)	ID de connexion à Azure. Nécessite un accès au rôle de lecteur.
ID de locataire Azure	ID de locataire Microsoft
Clé d'authentification du principal du service Azure	Clé d'authentification de connexion
Je comprends que Microsoft me facture les demandes d'API	Cochez cette case pour vérifier que vous avez bien compris que Microsoft vous facture les demandes d'API effectuées par le sondage Insight.

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60
Choisissez « Exclure » ou « Inclure » pour appliquer le filtre aux machines virtuelles par balises	Spécifiez s'il faut inclure ou exclure les machines virtuelles par balises lors de la collecte de données. Si « Inclure » est sélectionné, le champ Clé de balise ne peut pas être vide.
Clés et valeurs de balises sur lesquelles filtrer les machines virtuelles	Cliquez sur **+ Filtrer la balise** pour choisir les machines virtuelles (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs qui correspondent aux clés et aux valeurs des balises sur la machine virtuelle. La clé de balise est obligatoire, la valeur de balise est facultative. Lorsque la valeur de balise est vide, la machine virtuelle est filtrée tant qu'elle correspond à la clé de balise.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Broadcom

Collecteur de données Brocade Network Advisor

Data Infrastructure Insights utilise le collecteur de données Brocade Network Advisor pour acquérir des données d'inventaire et de performances à partir des commutateurs Brocade .

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Brocade Network Advisor. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la

plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Changer	Changer
Port	Port
Tissu virtuel, tissu physique	Tissu
Commutateur logique	Commutateur logique

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les éléments suivants sont requis pour configurer ce collecteur de données :

- L'unité d'acquisition Data Infrastructure Insights initiera des connexions au port TCP 443 sur le serveur BNA. Le serveur BNA doit exécuter la version 14.2.1 ou supérieure.
- Adresse IP du serveur Brocade Network Advisor
- Nom d'utilisateur et mot de passe d'un compte administrateur
- Exigence de port : HTTP/HTTPS 443

Configuration

Champ	Description
Adresse IP du serveur Brocade Network Advisor	Adresse IP du serveur Network Advisor
Nom d'utilisateur	Nom d'utilisateur pour le commutateur
Nom d'utilisateur	Nom d'utilisateur administrateur
Mot de passe	Mot de passe administrateur

Configuration avancée

Champ	Description
Type de connexion	HTTPS (port par défaut 443) ou HTTP (port par défaut 80)
Remplacer le port de connexion	Si vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Mot de passe	Mot de passe pour le commutateur
Intervalle d'interrogation de l'inventaire (min)	La valeur par défaut est 40
Rapport sur la passerelle d'accès	Cochez cette case pour inclure les appareils en mode passerelle d'accès
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 1800

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Recevez un message indiquant que plusieurs nœuds sont connectés au port Access Gateway ou que le collecteur de données ne parvient pas à détecter le périphérique Access Gateway.	Vérifiez que le périphérique NPV fonctionne correctement et que tous les WWN connectés sont attendus. N'acquérez pas directement le dispositif NPV. Au lieu de cela, l'acquisition du commutateur de structure principal collectera les données du périphérique NPV.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données du commutateur FC Brocade

Data Infrastructure Insights utilise la source de données Brocade FC Switch (SSH) pour découvrir l'inventaire des périphériques de commutation Brocade ou renommés exécutant le micrologiciel Factored Operating System (FOS) 4.2 et versions ultérieures. Les appareils en modes commutateur FC et passerelle d'accès sont pris en charge.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données Brocade FC Switch. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Changer	Changer
Port	Port
Tissu virtuel, tissu physique	Tissu
Zone	Zone
Commutateur logique	Commutateur logique
Volume virtuel	Volume
Zone LSA	Zone IVR

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- L'unité d'acquisition Data Infrastructure Insights (AU) initiera des connexions au port TCP 22 sur les commutateurs Brocade pour collecter des données d'inventaire. L'AU initiera également des connexions au port UDP 161 pour la collecte de données de performances.

- Il doit y avoir une connectivité IP à tous les commutateurs de la structure. Si vous cochez la case Découvrir tous les commutateurs de la structure, Data Infrastructure Insights identifie tous les commutateurs de la structure ; cependant, il a besoin d'une connectivité IP à ces commutateurs supplémentaires pour les découvrir.
- Le même compte est nécessaire à l'échelle mondiale sur tous les commutateurs de la structure. Vous pouvez utiliser PuTTY (émulateur de terminal open source) pour confirmer l'accès.
- Les ports 161 et 162 doivent être ouverts à tous les commutateurs de la structure pour l'interrogation des performances SNMP.
- Chaîne de communauté SNMP en lecture seule

Configuration

Champ	Description
Changer d'adresse IP	Adresse IP ou nom de domaine complet du serveur EFC
Nom d'utilisateur	Nom d'utilisateur pour le commutateur
Mot de passe	Mot de passe pour le commutateur
SNMP	Version SNMP
Chaîne de communauté SNMP	Chaîne de communauté SNMP en lecture seule utilisée pour accéder au commutateur
Nom d'utilisateur SNMP	Nom d'utilisateur SNMP
Mot de passe SNMP	Mot de passe SNMP

Configuration avancée

Champ	Description
Nom du tissu	Nom du tissu à signaler par le collecteur de données. Laissez vide pour signaler le nom du tissu comme WWN.
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 15.
Appareils exclus	Liste séparée par des virgules des identifiants d'appareils à exclure de l'interrogation
Domaines d'administration actifs	Sélectionnez si vous utilisez des domaines d'administration
Récupérer les données MPR	Sélectionnez cette option pour acquérir les données de routage de votre routeur multiprotocole.
Activer le piégeage	Sélectionnez cette option pour activer l'acquisition lors de la réception d'un trap SNMP du périphérique. Si vous sélectionnez Activer le piégeage, vous devez également activer SNMP.
Temps minimum entre les pièges (sec)	Temps minimum entre les tentatives d'acquisition déclenchées par des pièges. La valeur par défaut est 10.

Champ	Description
Découvrez tous les commutateurs du fabric	Sélectionnez pour découvrir tous les commutateurs du fabric
Privilégier les HBA plutôt que les alias de zone	Choisissez de privilégier les alias HBA ou de zone
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est 300.
Protocole d'authentification SNMP	Protocole d'authentification SNMP (SNMP v3 uniquement)
Mot de passe de confidentialité SNMP	Mot de passe de confidentialité SNMP (SNMP v3 uniquement)
Nouvelles tentatives SNMP	Nombre de tentatives de nouvelle tentative SNMP

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
L'acquisition de l'inventaire de la source de données Brocade échoue avec l'erreur : <date> <heure> ERREUR [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Erreur 2 sur 2 : <nom de la source de données> [Erreur interne] - Impossible de générer le modèle pour le périphérique <IP>. Erreur lors de la détection de l'invite ([Nom du périphérique <nom>] : Impossible de générer le modèle pour le périphérique <IP>. Erreur lors de la détection de l'invite)	Le problème peut être dû au fait que le commutateur Brocade met trop de temps à renvoyer une invite, dépassant le délai d'expiration par défaut de 5 secondes. Dans les paramètres de configuration avancée du collecteur de données dans Data Infrastructure Insights, essayez d'augmenter le *Délai d'attente de la bannière SSH (sec)* à une valeur plus élevée.
Erreur : « Data Infrastructure Insights a reçu un rôle de châssis non valide »	Vérifiez que l'utilisateur configuré dans cette source de données dispose de l'autorisation de rôle de châssis.
Erreur : « Adresse IP du châssis incompatible »	En règle générale, DII ne prend PAS en charge la traduction d'adresses réseau ou la traduction d'adresses de port entre l'unité d'acquisition et les périphériques. DII peut détecter que le nom d'hôte/l'adresse IP dans la configuration du collecteur ne correspond à aucune des adresses que l'appareil pense avoir.
Recevez un message indiquant que plusieurs nœuds sont connectés au port Access Gateway	Vérifiez que le périphérique NPV fonctionne correctement et que tous les WWN connectés sont attendus. N'acquérez pas directement le dispositif NPV. Au lieu de cela, l'acquisition du commutateur de structure principal collectera les données du périphérique NPV.

Problème:	Essayez ceci:
Erreur : ….Nombre maximal de sessions à distance pour la connexion…	FOS a des limites différentes pour le nombre de sessions SSH simultanées prises en charge par rôle d'utilisateur. La session SSH de DII sur cet appareil est rejetée lors de la connexion pour violation de ces limites. Cela peut être un signe que vous avez des collectionneurs en double qui découvrent le même actif, ce qui doit être évité.

Performances

Problème:	Essayez ceci:
La collecte des performances échoue avec le message « Délai d'attente expiré lors de l'envoi de la requête SNMP ».	Selon les variables de requête et la configuration du commutateur, certaines requêtes peuvent dépasser le délai d'expiration par défaut. "En savoir plus" .
La collecte des performances échoue avec… Des doublons de lignes ont été trouvés dans la table SNMP…	DII a détecté de mauvaises réponses SNMP. Vous utilisez probablement FOS 8.2.3e. Effectuez une mise à niveau vers la version 8.2.3e2 ou supérieure.
Les collectes de performances échouent avec… Nom d'utilisateur inconnu…	Vous avez configuré votre collecteur DII avec une valeur « Nom d'utilisateur SNMP » qui n'est pas insérée dans l'un des emplacements utilisateur SNMPv3. La simple création d'un utilisateur sur Brocade FOS ne l'active PAS nécessairement en tant qu'utilisateur SNMPv3 - vous devez le placer dans l'un des emplacements utilisateur v3.
Les collectes de performances échouent avec… Niveau de sécurité non pris en charge…	Vous avez configuré votre collecteur DII pour utiliser SNMPv3, mais avec des paramètres de cryptage (alias confidentialité) et/ou d'autorisation qui ne sont pas activés sur l'appareil en question.
La collecte des performances échoue avec… Le mot de passe de confidentialité vide n'est autorisé que pour le protocole de confidentialité AUCUN	Vous avez configuré votre collecteur DII pour utiliser SNMPv3, avec un protocole de cryptage, également appelé protocole de confidentialité (AES, etc.), mais vous avez une valeur « Mot de passe de confidentialité SNMP » vide, donc DII ne peut pas négocier les flux de données SNMPv3 chiffrés avec cet appareil.
La collecte des performances échoue avec …..VF:nn, erreur : aucun accès…	Vous avez configuré votre collecteur DII pour utiliser SNMPv3 sur un périphérique avec plusieurs Virtual Fabrics activés, mais l'utilisateur SNMPv3 n'a PAS de droits pour VF NN. DII ne prend pas en charge la découverte partielle d'un actif physique. Vous devez toujours accorder à DII l'accès à tous les 128 VF possibles de manière proactive, car DII tentera toujours de récupérer les données de performances pour tout VF existant sur un périphérique physique donné.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Brocade FOS REST

Data Infrastructure Insights utilise le collecteur Brocade FOS REST pour découvrir l'inventaire et les performances des périphériques de commutation Brocade exécutant le micrologiciel FabricOS (FOS) 8.2 et versions ultérieures. Veuillez noter que les premières versions de FOS 8.2 peuvent contenir des bugs d'API REST ; il est fortement recommandé d'exécuter la dernière version de FOS possible prise en charge par votre plateforme.

Remarque : le niveau « utilisateur » par défaut de FOS n'est pas suffisamment puissant pour que Data Infrastructure Insights puisse visualiser tous les aspects logiques d'un périphérique. Nous avons besoin d'un compte utilisateur avec le « rôle de châssis » activé, ainsi que des autorisations sur toutes les structures virtuelles configurées sur un commutateur.

Voici un exemple de la manière dont vous pouvez créer un compte utilisateur « à privilèges minimaux » pour l'utilisation de Data Infrastructure Insights dans une session SSH sur un périphérique FOS :

userConfig --add NetAppCIUser -r utilisateur -l 1-128 -c utilisateur -p Qwerty!

Cela créera un utilisateur « NetAppCIUser » avec un mot de passe « Qwerty! ». Cet utilisateur a le rôle « utilisateur » (-r) sur les 128 structures virtuelles possibles (-l). Cet utilisateur dispose en outre du rôle « Châssis » requis (-c) avec un accès de niveau utilisateur attribué.

Par défaut, ce collecteur tentera de découvrir tous les périphériques FOS qui font partie de toutes les structures dont le commutateur fait partie.

Remarque : l'utilisateur en lecture seule par défaut de FOS, « user », n'a PAS d'autorisations d'affichage sur tous les Virtual Fabrics, ni d'autorisations de « rôle de châssis ». Cela signifie que vous aurez peu de chances de réussir en utilisant « utilisateur » avec Data Infrastructure Insights, qui doit comprendre à la fois la configuration physique et logique du périphérique FOS.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Brocade FOS REST. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Changer	Changer
Port	Port
Tissu virtuel, tissu physique	Tissu
Zone	Zone
Commutateur logique	Commutateur logique
Zone LSA	Zone IVR

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Il doit y avoir une connectivité TCP vers tous les commutateurs de la structure. Ce type de collecteur de données essaiera de manière transparente HTTP et HTTPS pour chaque périphérique de la structure. Si vous sélectionnez la case à cocher *Découvrir tous les commutateurs de la structure*, Data Infrastructure Insights identifie tous les commutateurs de la structure ; cependant, il a besoin d'une connectivité TCP à ces commutateurs supplémentaires pour les découvrir.
- Le même compte est nécessaire à l'échelle mondiale sur tous les commutateurs de la structure. Vous pouvez utiliser l'interface Web de l'appareil pour confirmer l'accès.

Configuration

Champ	Description
Changer d'adresse IP	Adresse IP ou nom de domaine complet du commutateur FOS
Nom d'utilisateur	Nom d'utilisateur pour le commutateur
Mot de passe	Mot de passe pour le commutateur

Configuration avancée

Champ	Description
Appareils exclus	Liste séparée par des virgules des adresses IPv4 des périphériques à exclure de l'interrogation.
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 60.
Découvrez tous les commutateurs du fabric	Sélectionnez pour découvrir tous les commutateurs du tissu.
Privilégier les HBA plutôt que les alias de zone	Choisissez de privilégier les alias HBA ou de zone.
Type de connexion	HTTP ou HTTPS.
Notez que ce paramètre modifie uniquement le protocole que CI tente d'utiliser en premier par périphérique - CI tentera automatiquement le protocole opposé si la valeur par défaut échoue	Remplacer le port TCP
Spécifiez un port si vous n'utilisez pas le port par défaut.	Intervalle d'interrogation des performances (sec)

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
La fonctionnalité Test m'avertit qu'un protocole est inaccessible	Un périphérique Brocade FOS 8.2+ donné ne voudra communiquer que sur HTTP ou HTTPS. Si un commutateur dispose d'un certificat numérique installé, le commutateur renverra des erreurs HTTP si l'on tente de communiquer avec lui avec HTTP non chiffré plutôt qu'avec HTTPS. La fonction de test tente la communication avec HTTP et HTTPS. Si le test vous indique qu'un protocole réussit, vous pouvez enregistrer le collecteur en toute sécurité et ne pas vous inquiéter de l'échec de l'autre protocole. Le collecteur tentera les deux protocoles pendant la collecte et échouera uniquement si aucun ne fonctionne.
Erreur : l'inventaire échoue avec l'erreur 401 Non autorisé… Clé de session non valide…	Il s'agit d'un bug distinct dans certaines versions très anciennes de 8.2 FOS, comme 8.2.1c, qui ne prennent PAS correctement en charge l'authentification de base HTTP. Mise à niveau vers une version ultérieure 8.2 ou 9.*
Erreur : « Data Infrastructure Insights a reçu un rôle de châssis non valide »	Vérifiez que l'utilisateur configuré dans cette source de données dispose de l'autorisation de rôle de châssis.
Erreur : « Adresse IP du châssis incompatible »	Modifiez la configuration de la source de données pour utiliser l'adresse IP du châssis.
L'inventaire échoue avec une erreur 403 Forbidden	Il peut s'agir simplement d'informations d'identification erronées ou cela peut indiquer que vous essayez d'utiliser un rôle insuffisamment puissant. N'oubliez pas que les utilisateurs de niveau « utilisateur » n'ont PAS le droit « Rôle de châssis » requis ni l'accès à la vue aux structures virtuelles non par défaut.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données des commutateurs Cisco MDS Fabric

Data Infrastructure Insights utilise le collecteur de données Cisco MDS Fabric Switches pour découvrir l'inventaire des commutateurs Cisco MDS Fabric ainsi qu'une variété de commutateurs Cisco Nexus FCoE sur lesquels le service FC est activé.

De plus, vous pouvez découvrir de nombreux modèles d'appareils Cisco fonctionnant en mode NPV avec ce collecteur de données.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données du commutateur Cisco FC. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Changer	Changer
Port	Port
VSAN	Tissu
Zone	Zone
Commutateur logique	Commutateur logique
Entrée du serveur de noms	Entrée du serveur de noms
Zone de routage inter-VSAN (IVR)	Zone IVR

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Une adresse IP d'un commutateur dans la structure ou de commutateurs individuels
- Découverte du châssis, pour permettre la découverte de la structure
- Si vous utilisez SNMP V2, chaîne de communauté en lecture seule
- Le port 161 est utilisé pour accéder à l'appareil

Configuration

Champ	Description
Commutateur IP Cisco	Adresse IP ou nom de domaine complet du commutateur
Version SNMP	Sélectionnez V1, V2 ou V3. La version V2 ou ultérieure est requise pour l'acquisition des performances.
Chaîne de communauté SNMP	Chaîne de communauté SNMP en lecture seule utilisée pour accéder au commutateur (non applicable pour SNMP v3)
Nom d'utilisateur	Nom d'utilisateur pour le commutateur (SNMP v3 uniquement)
Mot de passe	Mot de passe utilisé pour le commutateur (SNMPv3 uniquement)

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les interrogations d'inventaire (par défaut 40 minutes)
Protocole d'authentification SNMP	Protocole d'authentification SNMP (SNMPv3 uniquement)

Champ	Description
Protocole de confidentialité SNMP	Protocole de confidentialité SNMP (SNMPv3 uniquement)
Mot de passe de confidentialité SNMP	Mot de passe de confidentialité SNMP
Nouvelles tentatives SNMP	Nombre de tentatives de nouvelle tentative SNMP
Délai d'expiration SNMP (ms)	Délai d'expiration SNMP (par défaut 5000 ms)
Activer le piégeage	Sélectionnez pour activer le piégeage. Si vous activez le piégeage, vous devez également activer les notifications SNMP.
Temps minimum entre les pièges (sec)	Temps minimum entre les tentatives d'acquisition déclenchées par des traps (par défaut 10 secondes)
Découvrez tous les commutateurs Fabric	Sélectionnez pour découvrir tous les commutateurs du fabric
Appareils exclus	Liste séparée par des virgules des adresses IP des appareils à exclure de l'interrogation
Appareils inclus	Liste séparée par des virgules des adresses IP des appareils à inclure dans l'interrogation
Vérifier le type d'appareil	Sélectionnez cette option pour accepter uniquement les appareils qui s'annoncent explicitement comme des appareils Cisco
Premier type d'alias	Fournir une première préférence pour la résolution de l'alias. Choisissez parmi les options suivantes : **Device Alais** Il s'agit d'un nom convivial pour un WWN de port (pWWN) qui peut être utilisé dans toutes les commandes de configuration, selon les besoins. Tous les commutateurs de la famille Cisco MDS 9000 prennent en charge les services d'alias de périphériques distribués (alias de périphériques). **Aucun** Ne signalez aucun alias. **Description du port** Une description pour aider à identifier le port dans une liste de ports. **Alias de zone (tous)** Un nom convivial pour un port qui peut être utilisé uniquement pour la configuration active. C'est la valeur par défaut.
Deuxième type d'alias	Fournir une deuxième préférence pour la résolution de l'alias
Troisième type d'alias	Fournir une troisième préférence pour la résolution de l'alias
Activer la prise en charge du mode proxy SANTap	Sélectionnez si votre commutateur Cisco utilise SANTap en mode proxy. Si vous utilisez EMC RecoverPoint, vous utilisez probablement SANTap.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance (par défaut 300 secondes)

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : Échec de la détection du châssis – aucun commutateur n'a été détecté	• Envoyez une requête ping à l'appareil avec l'adresse IP configurée • Connectez-vous à l'appareil à l'aide de l'interface graphique utilisateur Cisco Device Manager • Connectez-vous à l'appareil à l'aide de la CLI • Essayez d'exécuter la marche SNMP
Erreur : le périphérique n'est pas un commutateur Cisco MDS	• Assurez-vous que l'adresse IP de la source de données configurée pour l'appareil est correcte. • Connectez-vous à l'appareil à l'aide de l'interface graphique utilisateur Cisco Device Manager. • Connectez-vous à l'appareil à l'aide de l'interface de ligne de commande.
Erreur : Data Infrastructure Insights ne parvient pas à obtenir le WWN du commutateur.	Il se peut qu'il ne s'agisse pas d'un commutateur FC ou FCoE et qu'il ne soit donc pas pris en charge. Assurez-vous que l'IP/FQDN configuré dans la source de données est vraiment un commutateur FC/FCoE.
Erreur : plusieurs nœuds connectés au port du commutateur NPV ont été détectés	Désactiver l'acquisition directe du commutateur NPV
Erreur : impossible de se connecter au commutateur	• Assurez-vous que l'appareil est en marche • Vérifiez l'adresse IP et le port d'écoute • Envoyez une requête ping à l'appareil • Connectez-vous à l'appareil à l'aide de l'interface graphique utilisateur Cisco Device Manager • Connectez-vous à l'appareil à l'aide de la CLI • Exécutez la marche SNMP

Performances

Problème:	Essayez ceci:
Erreur : l'acquisition des performances n'est pas prise en charge par SNMP v1	• Modifier la source de données et désactiver les performances du commutateur • Modifier la source de données et la configuration du commutateur pour utiliser SNMP v2 ou supérieur

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Cohesity SmartFiles

Ce collecteur basé sur l'API REST acquerra un cluster Cohesity, découvrira les « vues » (en tant que volumes internes Data Infrastructure Insights), les différents nœuds, ainsi que collectera des mesures de performances.

Configuration

Champ	Description
IP du cluster Cohesity	Adresse IP du cluster Cohesity
Nom d'utilisateur	Nom d'utilisateur pour le cluster Cohesity
Mot de passe	Mot de passe utilisé pour le cluster Cohesity

Configuration avancée

Champ	Description
Port TCP	Port utilisé pour la communication TCP avec le cluster Cohesity
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.
Intervalle de sondage des performances (min)	Intervalle entre les sondages de performance. La valeur par défaut est de 900 secondes.

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Dell

Collecteur de données Dell EMC série XC

Data Infrastructure Insights utilise ce collecteur de données pour découvrir les informations d'inventaire et de performances des baies de stockage Dell EMC série XC.

Configuration

Champ	Description
Adresse IP externe de Prism	Adresse IP du serveur XC
Nom d'utilisateur	Nom d'utilisateur pour le serveur XC
Mot de passe	Mot de passe utilisé pour le serveur XC

Configuration avancée

Champ	Description
Port TCP	Port utilisé pour la communication TCP avec le serveur XC
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.
Intervalle de sondage des performances (min)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Dell EMC

Collecteur de données DELL EMC Data Domain

Ce collecteur de données collecte des informations d'inventaire et de performances à partir des systèmes de stockage de déduplication DELL EMC Data Domain. Pour configurer ce collecteur de données, vous devez suivre des instructions de configuration et des recommandations d'utilisation spécifiques.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Data Domain. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Tableau	Stockage
Port FC	Port
Système de fichiers	Volume interne
Quota	Quota
Partage NFS et CIFS	Partage de fichiers

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous avez besoin des informations suivantes pour configurer ce collecteur de données :

- Adresse IP du périphérique Data Domain
- Nom d'utilisateur et mot de passe en lecture seule pour le stockage Data Domain
- Port SSH 22

Configuration

Champ	Description
adresse IP	L'adresse IP ou le nom de domaine complet de la baie de stockage Data Domain
Nom d'utilisateur	Le nom d'utilisateur pour la baie de stockage Data Domain

Champ	Description
Mot de passe	Le mot de passe de la baie de stockage Data Domain

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20.
Port SSH	Port de service SSH

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données EMC ECS

Ce collecteur de données acquiert les données d'inventaire et de performances des systèmes de stockage EMC ECS. Pour la configuration, le collecteur de données nécessite une adresse IP ou un nom d'hôte du cluster ECS ainsi qu'un nom d'utilisateur et un mot de passe.

Dell EMC ECS est mesuré à un taux différent entre les To bruts et les unités gérées. Chaque 40 To de capacité ECS non formatée est facturé 1"Unité gérée (UG)" .

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données ECS. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Cluster	Stockage
Locataire	Piscine de stockage
Seau	Volume interne
Disque	Disque

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Une adresse IP ou un nom d'hôte du cluster ECS
- Un nom d'utilisateur et un mot de passe pour le système ECS
- Port 4443 (HTTPS). Nécessite une connectivité sortante au port TCP 4443 sur le système ECS.

Configuration

Champ	Description
Hôte ECS	Adresse IP ou nom de domaine complet du système ECS
Port hôte ECS	Port utilisé pour la communication avec l'hôte ECS
Identifiant utilisateur ECS	Identifiant utilisateur pour ECS
Mot de passe	Mot de passe utilisé pour ECS

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 360 minutes.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : l'authentification de l'utilisateur a échoué.	Assurez-vous que vos informations d'identification pour cet appareil sont correctes.

Performances

Problème:	Essayez ceci:
Erreur : les données collectées ne sont pas suffisantes.	* Vérifiez l'horodatage de la collecte dans le fichier journal et modifiez l'intervalle d'interrogation en conséquence * Attendez plus longtemps
Erreur : l'intervalle d'interrogation des performances est trop grand.	Vérifiez l'horodatage de la collecte dans le fichier journal ${logfile} et modifiez l'intervalle d'interrogation en conséquence

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Dell EMC PowerScale

Data Infrastructure Insights utilise le collecteur de données SSH Dell EMC PowerScale (anciennement Isilon) pour acquérir des données d'inventaire et de performances à partir du stockage NAS évolutif PowerScale.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante

utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Conduire	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Système de fichiers	Volume interne

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous avez besoin des informations suivantes pour configurer ce collecteur de données :

- Autorisations d'administrateur sur le stockage PowerScale
- Adresse IP du cluster PowerScale
- Accès SSH au port 22

Configuration

Champ	Description
adresse IP	L'adresse IP ou le nom de domaine complet du cluster PowerScale
Nom d'utilisateur	Nom d'utilisateur pour le cluster PowerScale
Mot de passe	Mot de passe utilisé pour le cluster PowerScale

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est 300.
Port SSH	Port de service SSH. La valeur par défaut est 22.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Informations de connexion non valides » avec le message d'erreur « Les commandes non activées pour l'administration basée sur les rôles nécessitent un accès utilisateur root »	* Vérifiez que l'utilisateur dispose des autorisations nécessaires pour exécuter les commandes suivantes sur le périphérique : > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Vérifiez que les informations d'identification utilisées dans l'assistant correspondent aux informations d'identification du périphérique
« Erreur interne » avec les messages d'erreur « L'exécution de la commande <Votre commande> a échoué avec l'autorisation : <Votre autorisation actuelle>. Problème d'autorisation d'exécution de la commande Sudo »	Vérifiez que l'utilisateur dispose des autorisations sudo pour exécuter la commande suivante sur l'appareil

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données REST Dell EMC Isilon / PowerScale

Data Infrastructure Insights utilise le collecteur de données REST Dell EMC Isilon / PowerScale pour acquérir des données d'inventaire et de performances à partir du stockage Dell EMC Isilon ou PowerScale. Ce collecteur prend en charge les tableaux exécutant OneFS 8.0.0+.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Conduire	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Système de fichiers OneFS	Volume interne
Système de fichiers OneFS	Piscine de stockage
Qtree	Qtree

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous avez besoin des informations suivantes pour configurer ce collecteur de données :

- Un compte utilisateur et un mot de passe. Ce compte n'a PAS besoin d'être administrateur/root, mais vous DEVEZ accorder un nombre substantiel de privilèges en lecture seule à votre compte de service - voir le

tableau ci-dessous

- Adresse IP / Nom de domaine complet du cluster Dell EMC Isilon / PowerScale
- Accès HTTPS au port 8080
- Cluster Isilon / PowerScale exécutant OneFS 8.0.0 ou supérieur

Nom du privilège	Description	r(lecture) ou rw (lecture+écriture)
ISI_PRIV_LOGIN_PAPI	API de la plateforme	r
ISI_PRIV_SYS_TIME	Durée	r
ISI_PRIV_AUTH	Authentification	r
RÔLE_PRIV_ISI	Privilège	r
APPAREILS_PRIVÉS_ISI	Appareils	r
ISI_PRIV_EVENT	Événement	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
RÉSEAU_PRIVÉ_ISI	Réseau	r
ISI_PRIV_NFS	NFS	r
ISI_PRIV_PAPI_CONFIG	Configurer l'API de la plateforme	r
ISI_PRIV_QUOTA	Quota	r
Piscines intelligentes privées ISI	Piscines intelligentes	r
ISI_PRIV_SMB	PME	r
STATISTIQUES_PRIV_ISI	Statistiques	r
ISI_PRIV_SWIFT	Rapide	r
MOTEUR DE TRAVAIL ISI_PRIV	Moteur d'emploi	r

Configuration

Champ	Description
Adresse IP d'Isilon	L'adresse IP ou le nom de domaine complet du stockage Isilon
Nom d'utilisateur	Nom d'utilisateur pour Isilon
Mot de passe	Mot de passe utilisé pour l'Isilon

Configuration avancée

Champ	Description
Port HTTPS	La valeur par défaut est 8080.
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 20.

Champ	Description
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est 300.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Informations de connexion non valides » avec le message d'erreur « Les commandes non activées pour l'administration basée sur les rôles nécessitent un accès utilisateur root »	* Vérifiez que l'utilisateur dispose des autorisations nécessaires pour exécuter les commandes suivantes sur le périphérique : > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Vérifiez que les informations d'identification utilisées dans l'assistant correspondent aux informations d'identification du périphérique
« Erreur interne » avec les messages d'erreur « L'exécution de la commande <Votre commande> a échoué avec l'autorisation : <Votre autorisation actuelle>. Problème d'autorisation d'exécution de la commande Sudo »	Vérifiez que l'utilisateur dispose des autorisations sudo pour exécuter la commande suivante sur l'appareil

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Dell EMC PowerStore

Le collecteur de données EMC PowerStore collecte les informations d'inventaire à partir du stockage EMC PowerStore. Pour la configuration, le collecteur de données nécessite l'adresse IP des processeurs de stockage ainsi qu'un nom d'utilisateur et un mot de passe en lecture seule.

Le collecteur de données EMC PowerStore rassemble les relations de réplication de volume à volume que PowerStore coordonne sur d'autres baies de stockage. Data Infrastructure Insights affiche une baie de stockage pour chaque cluster PowerStore et collecte des données d'inventaire pour les nœuds et les ports de stockage sur ce cluster. Aucune donnée de pool de stockage ou de volume n'est collectée.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
hôte	hôte
mappage_volume_hôte	mappage_volume_hôte

Terme du fournisseur/modèle	Data Infrastructure Insights
matériel (il a des lecteurs sous l'objet « extra_details ») : lecteurs	Disque
Appareil	Pool de stockage
Cluster	Baie de stockage
Nœud	Nœud de stockage
fc_port	Port
volume	Volume
Volume interne	système de fichiers

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les informations suivantes sont requises pour configurer ce collecteur de données :

- Adresse IP ou nom de domaine complet du processeur de stockage
- Nom d'utilisateur et mot de passe en lecture seule

Configuration

Champ	Description
Passerelle(s) PowerStore	Adresses IP ou noms de domaine complets du stockage PowerStore
Nom d'utilisateur	Nom d'utilisateur pour PowerStore
Mot de passe	Mot de passe utilisé pour PowerStore

Configuration avancée

Champ	Description
Port HTTPS	La valeur par défaut est 443
Intervalle d'interrogation d'inventaire (minutes)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.

La collecte des performances PowerStore de Cloud Insight utilise les données sources de granularité de 5 minutes de PowerStore. En tant que tel, Data Infrastructure Insights interroge ces données toutes les cinq minutes, et cela n'est pas configurable.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Dell EMC RecoverPoint

Le principal cas d'utilisation du collecteur de données EMC RecoverPoint est de découvrir les relations de réplication de volume à volume que l'appliance de stockage RecoverPoint facilite. Ce collecteur découvrira également l'appliance Recoverpoint elle-même. Veuillez noter que Dell/EMC vend une solution de sauvegarde VMware pour les machines virtuelles - « RecoverPoint pour machines virtuelles » - qui n'est pas prise en charge par ce collecteur.

Pour la configuration, le collecteur de données nécessite l'adresse IP des processeurs de stockage ainsi qu'un nom d'utilisateur et un mot de passe en lecture seule.

Le collecteur de données EMC RecoverPoint rassemble les relations de réplication de volume à volume que RecoverPoint coordonne sur d'autres baies de stockage. Data Infrastructure Insights affiche une baie de stockage pour chaque cluster RecoverPoint et collecte des données d'inventaire pour les nœuds et les ports de stockage sur ce cluster. Aucune donnée de pool de stockage ou de volume n'est collectée.

Exigences

Les informations suivantes sont requises pour configurer ce collecteur de données :

- Adresse IP ou nom de domaine complet du processeur de stockage
- Nom d'utilisateur et mot de passe en lecture seule
- Accès à l'API REST via le port 443

Configuration

Champ	Description
Adresse de RecoverPoint	Adresse IP ou nom de domaine complet du cluster RecoverPoint
Nom d'utilisateur	Nom d'utilisateur pour le cluster RecoverPoint
Mot de passe	Mot de passe utilisé pour le cluster RecoverPoint

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter au cluster Recoverpoint
Intervalle d'interrogation d'inventaire (minutes)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 20 minutes.
Clusters exclus	Liste séparée par des virgules d'ID ou de noms de cluster à exclure lors de l'interrogation.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données DELL EMC ScaleIO / PowerFlex

Le collecteur de données ScaleIO/PowerFlex collecte les informations d'inventaire à partir du stockage ScaleIO et PowerFlex. Pour la configuration, ce collecteur de données nécessite l'adresse de la passerelle ScaleIO/PowerFlex ainsi qu'un nom d'utilisateur et un mot de passe administrateur.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données ScaleIO/PowerFlex. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Cluster MDM (gestionnaire de métadonnées)	Stockage
SDS (serveur de données ScaleIO/PowerFlex)	Nœud de stockage
Piscine de stockage	Piscine de stockage
Volume	Volume
Appareil	Disque

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Accès en lecture seule au compte utilisateur Admin
- Exigence de port : port HTTPS 443

Configuration

Champ	Description
Passerelle(s) ScaleIO/PowerFlex	Adresses IP ou FQDN des passerelles ScaleIO/PowerFlex, séparées par une virgule (,) ou un point-virgule (;)
Nom d'utilisateur	Nom d'utilisateur administrateur utilisé pour se connecter au périphérique ScaleIO/PowerFlex
Mot de passe	Mot de passe utilisé pour se connecter à l'appareil ScaleIO/PowerFlex

Configuration avancée

Cliquez sur la case à cocher Inventaire pour activer la collecte d'inventaire.

Champ	Description
Port HTTPS	443

Champ	Description
Intervalle d'interrogation de l'inventaire (min)	La valeur par défaut est 60.
Délai d'expiration de la connexion (sec)	La valeur par défaut est 60.

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données EMC Unity

Le collecteur de données DELL EMC Unity (anciennement VNXe) fournit une prise en charge d'inventaire pour les baies de stockage unifiées VNXe. Data Infrastructure Insights prend actuellement en charge les protocoles iSCSI et NAS.

Exigences

- Le collecteur de données Unity est basé sur CLI ; vous devez installer Unisphere pour Unity CLI (uemcli.exe) sur l'unité d'acquisition où réside votre collecteur de données VNXe.
- uemcli.exe utilise HTTPS comme protocole de transport, l'unité d'acquisition devra donc pouvoir initier des connexions HTTPS vers Unity.
- Adresse IP ou nom de domaine complet de l'appareil Unity
- Vous devez disposer d'au moins un utilisateur en lecture seule pour pouvoir utiliser le collecteur de données.
- HTTPS sur le port 443 est requis
- Le collecteur de données EMC Unity fournit une prise en charge NAS et iSCSI pour l'inventaire ; les volumes Fibre Channel seront découverts, mais Data Infrastructure Insights ne génère pas de rapport sur le mappage FC, le masquage ou les ports de stockage.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Unity. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Baie de stockage	Stockage
Processeur	Nœud de stockage
Piscine de stockage	Piscine de stockage
Informations générales sur les blocs iSCSI, VMware VMFS	Partager
Système de réplication à distance	Synchronisation
Nœud iSCSI	Nœud cible iSCSI

Terme du fournisseur/modèle	Data Infrastructure Insights
Initiateur iSCSI	Initiateur cible iSCSI

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour cette source de données.

Configuration

Champ	Description
Stockage Unity	Adresse IP ou nom de domaine complet de l'appareil Unity
Nom d'utilisateur	Nom d'utilisateur pour l'appareil Unity
Mot de passe	Mot de passe pour l'appareil Unity
Chemin complet vers l'exécutable UEMCLI	Chemin complet vers le dossier contenant l'exécutable *uemcli.exe*

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 40 minutes
Port CLI Unity	Port utilisé pour l'interface de ligne de commande Unity
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Échec de l'exécution de l'utilitaire externe » avec le message d'erreur « Impossible de trouver l'exécutable Unisphere uemcli »	* Vérifiez l'adresse IP, le nom d'utilisateur et le mot de passe corrects. * Confirmez que Unisphere CLI est installé sur l'unité d'acquisition Data Infrastructure Insights. * Confirmez que le répertoire d'installation d'Unisphere CLI est correct dans la configuration de la source de données. * Confirmez que l'adresse IP du VNXe est correcte dans la configuration de la source de données. À partir de l'unité d'acquisition Data Infrastructure Insights , ouvrez un CMD et accédez au répertoire d'installation configuré : ${INSTALLDIR. Essayez d'établir une connexion avec le périphérique VNXe en tapant : uemcli -d <Votre IP> -u <Votre ID> /sys/general show

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de

support du collecteur de données" .

Collecteur de données de la famille d'appareils Dell EMC VMAX et PowerMax

Data Infrastructure Insights découvre les baies de stockage EMC VMAX et PowerMax à l'aide des commandes symcli Solutions Enabler en conjonction avec un serveur Solutions Enabler existant dans votre environnement. Le serveur Solutions Enabler existant dispose d'une connectivité à la baie de stockage VMAX/PowerMax via l'accès aux volumes de contrôle d'accès.

Exigences

Avant de configurer ce collecteur de données, vous devez vous assurer que Data Infrastructure Insights dispose d'une connectivité TCP au port 2707 sur le serveur Solutions Enabler existant. Data Infrastructure Insights découvre tous les tableaux Symmetrix qui sont « locaux » sur ce serveur, comme indiqué dans la sortie « symcfg list » de ce serveur.

- L'application EMC Solutions Enabler (CLI) avec fournisseur SMI-S doit être installée sur le serveur de l'unité d'acquisition et la version doit correspondre ou être antérieure à la version exécutée sur le serveur Solutions Enabler.
- Un fichier {installdir}\EMC\SYMAPI\config\netcnfg correctement configuré est requis. Ce fichier définit les noms de service pour les serveurs Solutions Enabler, ainsi que la méthode d'accès (SECURE / NOSECURE / ANY).
- Si vous avez besoin d'une latence de lecture/écriture au niveau du nœud de stockage, le fournisseur SMI-S doit communiquer avec une instance en cours d'exécution de l'application UNISPHERE pour VMAX.
- Adresse IP du serveur de gestion Solutions Enabler
- Autorisations d'administrateur sur le serveur Solutions Enabler (SE)
- Nom d'utilisateur et mot de passe en lecture seule pour le logiciel SE
- L'application UNISPHERE pour VMAX doit être en cours d'exécution et collecter des statistiques pour les baies de stockage EMC VMAX et PowerMax gérées par l'installation du fournisseur SMI-S
- Validation d'accès pour les performances : Dans un navigateur Web sur votre unité d'acquisition, accédez à *https://<Nom d'hôte ou IP SMI-S>:5989/ecomconfig* où « Nom d'hôte ou IP SMI-S » est l'adresse IP ou le nom d'hôte de votre serveur SMI-S. Cette URL est destinée à un portail administratif pour le service EMC SMI-S (alias « ECOM ») - vous recevrez une fenêtre contextuelle de connexion.
- Les autorisations doivent être déclarées dans le fichier de configuration du démon du serveur Solutions Enabler, généralement trouvé ici : */var/symapi/config/daemon_users*

  Voici un exemple de fichier avec les autorisations cisys appropriées.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
##############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de la source de données EMC VMAX/PowerMax. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de disques	Groupe de disques
Stockage	Stockage en réseau
Directeur	Nœud de stockage
Pool de périphériques, pool de ressources de stockage (SRP)	Piscine de stockage
Appareil TDev	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Configuration

Remarque : si l'authentification utilisateur SMI-S n'est pas activée, les valeurs par défaut du collecteur de données Data Infrastructure Insights sont ignorées.

Champ	Description
Nom du service	Nom du service tel que spécifié dans le fichier *netcnfg*
Chemin d'accès complet vers la CLI	Chemin d'accès complet au dossier contenant la CLI Symmetrix
Adresse IP de l'hôte SMI-S	Adresse IP de l'hôte SMI-S

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 40 minutes.
Choisissez « Exclure » ou « Inclure » pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste de tableaux ci-dessous lors de la collecte de données.
Liste des périphériques de filtrage d'inventaire	Liste séparée par des virgules des identifiants d'appareils à inclure ou à exclure
Mise en cache des connexions	Choisissez la méthode de mise en cache de connexion : * LOCAL signifie que le service Cloud Insights Acquisition s'exécute sur le serveur Solutions Enabler, qui dispose d'une connectivité Fibre Channel aux baies Symmetrix que vous cherchez à découvrir et a accès aux volumes du contrôleur d'accès. Cela peut être observé dans certaines configurations d'unité d'acquisition à distance (RAU). * REMOTE_CACHED est la valeur par défaut et doit être utilisé dans la plupart des cas. Cela utilise les paramètres du fichier NETCNFG pour se connecter via IP au serveur Solutions Enabler, qui doit disposer d'une connectivité Fibre Channel aux baies Symmetrix que vous cherchez à découvrir et a accès aux volumes Gatekeeper. * Dans le cas où les options REMOTE_CACHED font échouer les commandes CLI, utilisez l'option REMOTE. Gardez à l'esprit que cela ralentira le processus d'acquisition (éventuellement jusqu'à des heures, voire des jours, dans les cas extrêmes). Les paramètres du fichier NETCNFG sont toujours utilisés pour une connexion IP au serveur Solutions Enabler qui dispose d'une connectivité Fibre Channel aux baies Symmetrix en cours de découverte. **Remarque :** ce paramètre ne modifie pas le comportement de Data Infrastructure Insights par rapport aux tableaux répertoriés comme À DISTANCE par la sortie « symcfg list ». Data Infrastructure Insights collecte les données uniquement sur les périphériques affichés comme LOCAUX par cette commande.
Protocole SMI-S	Protocole utilisé pour se connecter au fournisseur SMI-S. Affiche également le port par défaut utilisé.
Remplacer le port SMIS	Si vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Nom d'utilisateur SMI-S	Nom d'utilisateur pour l'hôte du fournisseur SMI-S
Mot de passe SMI-S	Nom d'utilisateur pour l'hôte du fournisseur SMI-S
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performances (par défaut 1 000 secondes)

Champ	Description
choisissez « Exclure » ou « Inclure » pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste de tableaux ci-dessous lors de la collecte des données de performances
Liste des périphériques de filtrage des performances	Liste séparée par des virgules des identifiants d'appareils à inclure ou à exclure

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème:	Essayez ceci:
Erreur : la fonctionnalité demandée n'est actuellement pas sous licence	Installez la licence du serveur SYMAPI.
Erreur : aucun appareil n'a été trouvé	Assurez-vous que les périphériques Symmetrix sont configurés pour être gérés par le serveur Solutions Enabler : - Exécutez symcfg list -v pour voir la liste des périphériques Symmetrix configurés.
Erreur : aucun service réseau demandé n'a été trouvé dans le fichier de service	Assurez-vous que le nom du service Solutions Enabler est défini dans le fichier netcnfg pour Solutions Enabler. Ce fichier se trouve généralement sous SYMAPI\config\ dans l'installation du client Solutions Enabler.
Erreur : la liaison client/serveur distant a échoué	Vérifiez les fichiers storsrvd.log* les plus récents sur l'hôte Solutions Enabler que nous essayons de découvrir.
Erreur : le nom commun dans le certificat client n'est pas valide	Modifiez le fichier *hosts* sur le serveur Solutions Enabler afin que le nom d'hôte de l'unité d'acquisition corresponde à l'adresse IP telle qu'indiquée dans le fichier storsrvd.log sur le serveur Solutions Enabler.
Erreur : la fonction n'a pas pu obtenir de mémoire	Assurez-vous qu'il y a suffisamment de mémoire libre disponible dans le système pour exécuter Solutions Enabler
Erreur : Solutions Enabler n'a pas pu fournir toutes les données requises.	Enquêter sur l'état de santé et le profil de charge de Solutions Enabler
Erreur : • La commande CLI « symcfg list -tdev » peut renvoyer des données incorrectes lorsqu'elle est collectée avec Solutions Enabler 7.x à partir d'un serveur Solutions Enabler 8.x. • La commande CLI « symcfg list -srp » peut renvoyer des données incorrectes lorsqu'elle est collectée avec Solutions Enabler 8.1.0 ou une version antérieure à partir d'un serveur Solutions Enabler 8.3 ou une version ultérieure.	Assurez-vous d'utiliser la même version majeure de Solutions Enabler

Problème:	Essayez ceci:
Je vois des erreurs de collecte de données avec le message : « code inconnu »	Vous pouvez voir ce message si les autorisations ne sont pas déclarées dans le fichier de configuration du démon du serveur Solutions Enabler (voir leExigences au-dessus de.) Cela suppose que la version de votre client SE correspond à la version de votre serveur SE. Cette erreur peut également se produire si l'utilisateur *cisys* (qui exécute les commandes Solutions Enabler) n'a pas été configuré avec les autorisations de démon nécessaires dans le fichier de configuration /var/symapi/config/daemon_users. Pour résoudre ce problème, modifiez le fichier /var/symapi/config/daemon_users et assurez-vous que l'utilisateur cisys dispose de l'autorisation <all> spécifiée pour le démon storapid. Exemple : 14:11:25 # tail /var/symapi/config/daemon_users … cisys storapid <all>

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Dell EMC VNX Block Storage (NaviCLI)

Data Infrastructure Insights utilise le collecteur de données Dell EMC VNX Block Storage (NaviSec) (anciennement CLARiiON) pour acquérir des données d'inventaire et de performances.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données EMC VNX Block Storage. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Stockage	Stockage
Processeur de stockage	Nœud de stockage
Ce pool, groupe RAID	Piscine de stockage
LUN	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour cette source de données.

Exigences

Les exigences suivantes doivent être respectées pour pouvoir collecter des données :

- Une adresse IP de chaque processeur de stockage en bloc VNX

- Nom d’utilisateur et mot de passe Navisphere en lecture seule pour les baies de stockage en blocs VNX
- NaviSecCli doit être installé sur l’AU Data Infrastructure Insights
- Validation d’accès : exécutez NaviSecCLI à partir de l’AU Data Infrastructure Insights sur chaque tableau à l’aide du nom d’utilisateur et du mot de passe.
- Exigences portuaires : 80, 443
- La version de NaviSecCLI doit correspondre au code FLARE le plus récent sur votre baie
- Pour des performances optimales, la journalisation des statistiques doit être activée.

Syntaxe de l’interface de ligne de commande NaviSphere

naviseccli.exe -h <adresse IP> -user <utilisateur> -password <mot de passe> -scope <portée, utiliser 0 pour la portée globale> -port <utiliser 443 par défaut> commande

Configuration

Champ	Description
Adresse IP du stockage en bloc VNX	Adresse IP ou nom de domaine complet du stockage en blocs VNX
Nom d’utilisateur	Nom utilisé pour se connecter au périphérique de stockage en blocs VNX.
Mot de passe	Mot de passe utilisé pour se connecter au périphérique de stockage en blocs VNX.
Chemin CLI vers naviseccli.exe	Chemin complet vers le dossier contenant l’exécutable *naviseccli.exe*

Configuration avancée

Champ	Description
Intervalle d’interrogation d’inventaire (min)	Intervalle entre les sondages d’inventaire. La valeur par défaut est 40 minutes.
Portée	La portée du client sécurisé. La valeur par défaut est Global.
Intervalle d’interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur: • L'agent ne fonctionne pas • Impossible de trouver naviseccli • Impossible d'exécuter une commande	• Confirmez que NaviSphere CLI est installé sur l'unité d'acquisition Cloud Insight • Vous n'avez pas sélectionné l'option « Utiliser un client sécurisé » dans l'assistant de configuration du collecteur de données et vous n'avez pas installé de version non sécurisée de Naviphere CLI. • Confirmez que le répertoire d'installation de NaviSphere CLI est correct dans la configuration du collecteur de données • Confirmez que l'adresse IP du stockage en bloc VNX est correcte dans la configuration du collecteur de données : • De l'unité d'acquisition Data Infrastructure Insights : ◦ Ouvrir un CMD. ◦ Changez le répertoire vers le répertoire d'installation configuré ◦ Essayez d'établir une connexion avec le périphérique de stockage en bloc VNX en tapant « navicli -h {ip} getagent » (remplacez {ip} par l'IP réelle)
Erreur : 4.29 emc235848 emc241018 getall Échec de l'analyse des informations d'alias d'hôte	Cela est probablement dû à un problème de corruption FLARE 29 de la base de données de l'initiateur hôte sur la baie elle-même. Voir les articles de la base de connaissances EMC : emc235848, emc241018. Vous pouvez également vérifier https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Erreur : impossible de récupérer les méta LUN. Erreur lors de l'exécution de java -jar navicli.jar	• Modifier la configuration du collecteur de données pour utiliser le client sécurisé (recommandé) • Installez navicli.jar dans le chemin CLI vers navicli.exe OU naviseccli.exe • Remarque : navicli.jar est obsolète à partir de la version 6.26 d'EMC Navisphere • Le fichier navicli.jar peut être disponible sur \ http://powerlink.emc.com
Erreur : les pools de stockage ne signalent pas les disques sur le processeur de service à l'adresse IP configurée	Configurer le collecteur de données avec les deux adresses IP du processeur de service, séparées par une virgule

Problème:	Essayez ceci:
Erreur : erreur de non-concordance de révision	• Cela est généralement dû à la mise à jour du micrologiciel sur le périphérique de stockage en blocs VNX, mais pas à la mise à jour de l'installation de NaviCLI.exe. Cela peut également être dû au fait d'avoir différents appareils avec des firmwares différents, mais une seule CLI installée (avec une version de firmware différente). • Vérifiez que l'appareil et l'hôte exécutent tous deux des versions identiques du logiciel : ◦ À partir de l'unité d'acquisition Data Infrastructure Insights , ouvrez une fenêtre de ligne de commande ◦ Changez le répertoire vers le répertoire d'installation configuré ◦ Établissez une connexion avec l'appareil CLARiiON en tapant « navicli -h <ip> getagent » ◦ Recherchez le numéro de version sur les premières lignes. Exemple : « Agent Rev : 6.16.2 (0.1) » ◦ Recherchez et comparez la version sur la première ligne. Exemple : « Navisphere CLI Révision 6.07.00.04.07 »
Erreur : Configuration non prise en charge – Aucun port Fibre Channel	L'appareil n'est configuré avec aucun port Fibre Channel. Actuellement, seules les configurations FC sont prises en charge. Vérifiez que cette version/ce micrologiciel est pris en charge.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données DELL EMC VNX File (anciennement Celerra Unified Storage System)

Ce collecteur de données acquiert des informations d'inventaire à partir du système de stockage de fichiers VNX. Pour la configuration, ce collecteur de données nécessite l'adresse IP des processeurs de stockage ainsi qu'un nom d'utilisateur et un mot de passe en lecture seule.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données de fichiers VNX. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Serveur réseau Celerra/Pool de stockage Celerra	Piscine de stockage
Système de fichiers	Volume interne
Déplaceur de données	Contrôleur
Système de fichiers monté sur un dispositif de transfert de données	Partage de fichiers
Exportations CIFS et NFS	Partager
Volume du disque	LUN principal

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous avez besoin des éléments suivants pour configurer ce collecteur de données :

- L'adresse IP du processeur de stockage
- Nom d'utilisateur et mot de passe en lecture seule
- Port SSH 22

Configuration

Champ	Description
Adresse IP du fichier VNX	Adresse IP ou nom de domaine complet du périphérique de fichier VNX
Nom d'utilisateur	Nom utilisé pour se connecter au périphérique de fichier VNX
Mot de passe	Mot de passe utilisé pour se connecter au périphérique de fichier VNX

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (minutes)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 20 minutes.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : Impossible de continuer pendant la mise à jour de DART	Solution possible : mettez en pause le collecteur de données et attendez que la mise à niveau de DART soit terminée avant de tenter une autre demande d'acquisition.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données unifié Dell EMC VNX

Pour la configuration, le collecteur de données Dell EMC VNX Unified (SSH) nécessite l'adresse IP de la station de contrôle ainsi qu'un nom d'utilisateur et un mot de passe en lecture seule.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Dossier de disque	Groupe de disques
Système de fichiers	Volume interne
Stockage	Stockage
Processeur de stockage	Nœud de stockage
Pool de stockage, groupe RAID	Piscine de stockage
LUN	Volume
Déplaceur de données	Contrôleur
Système de fichiers monté sur un dispositif de transfert de données	Partage de fichiers
Exportations CIFS et NFS	Partager
Volume du disque	LUN principal

Exigences

Vous avez besoin des éléments suivants pour configurer le collecteur de données VNX (SSH) :

- Adresse IP VNX et informations d'identification pour la station de contrôle Celerra.
- Nom d'utilisateur et mot de passe en lecture seule.
- Le collecteur de données est capable d'exécuter des commandes NaviCLI/NaviSecCLI sur le tableau principal en utilisant les têtes NAS DART OS

Configuration

Champ	Description
Adresse IP VNX	Adresse IP ou nom de domaine complet de la station de contrôle VNX
Nom d'utilisateur	Nom d'utilisateur pour la station de contrôle VNX
Mot de passe	Mot de passe pour la station de contrôle VNX

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 40 minutes.
Intervalle d'interrogation des performances (sec).	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données EMC VPLEX

Ce collecteur de données acquiert les données d'inventaire et de performances des systèmes de stockage EMC VPLEX. Pour la configuration, le collecteur de données nécessite une adresse IP du serveur VPLEX et un compte de domaine de niveau administratif.

La collecte des performances de Data Infrastructure Insights à partir des clusters Vplex nécessite que le service d'archivage des performances soit opérationnel, afin de renseigner les fichiers .CSV et les journaux que Data Infrastructure Insights récupère via des copies de fichiers basées sur SCP. NetApp a observé que de nombreuses mises à jour de la station de gestion/mise à niveau du micrologiciel Vplex rendront cette fonctionnalité non opérationnelle. Les clients qui prévoient de telles mises à niveau peuvent souhaiter demander de manière proactive à Dell/EMC si leur mise à niveau prévue laissera cette fonctionnalité inutilisable et, si oui, comment peuvent-ils la réactiver pour minimiser les écarts de visibilité des performances ? Le code de performance Vplex de Cloud Insight évaluera à chaque interrogation si tous les fichiers attendus existent et s'ils sont correctement mis à jour ; s'ils sont manquants ou obsolètes, Data Infrastructure Insights enregistrera les échecs de collecte des performances.

Terminologie

Data Infrastructure Insightst acquiert les informations d'inventaire suivantes auprès du collecteur de données VPLEX. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Cluster	Stockage

Terme du fournisseur/modèle	Data Infrastructure Insights
Moteur	Nœud de stockage
Appareil, étendue du système	Pool de stockage principal
Volume virtuel	Volume
Port frontal, port dorsal	Port
Dispositif distribué	Synchronisation du stockage
Vue de stockage	Carte de volume, masque de volume
Volume de stockage	LUN principal
ITL	Chemin d'accès au backend

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Une adresse IP de la console de gestion VPLEX
- Compte de domaine de niveau administratif pour le serveur VPLEX
- Port 443 (HTTPS). Nécessite une connectivité sortante au port TCP 443 sur la station de gestion VPLEX.
- Pour des performances optimales, nom d'utilisateur et mot de passe en lecture seule pour l'accès ssh/scp.
- Pour les performances, le port 22 est requis.

Configuration

Champ	Description
Adresse IP de la console de gestion VPLEX	Adresse IP ou nom de domaine complet de la console de gestion VPLEX
Nom d'utilisateur	Nom d'utilisateur pour VPLEX CLI
Mot de passe	Mot de passe utilisé pour VPLEX CLI
Adresse IP distante de performance	Adresse IP distante des performances de la console de gestion VPLEX
Nom d'utilisateur à distance des performances	Nom d'utilisateur distant de la console de gestion VPLEX
Mot de passe à distance de performance	Mot de passe distant des performances de la console de gestion VPLEX

Configuration avancée

Champ	Description
Port de communication	Port utilisé pour VPLEX CLI. La valeur par défaut est 443.
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 20 minutes.

Champ	Description
Nombre de tentatives de connexion	La valeur par défaut est 3.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 600 secondes.
Nombre de tentatives	La valeur par défaut est 2.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : l'authentification de l'utilisateur a échoué.	Assurez-vous que vos informations d'identification pour cet appareil sont correctes.

Performances

Problème:	Essayez ceci:
Erreur : les performances VPLEX pour la version inférieure à 5.3 ne sont pas prises en charge.	Mettre à niveau VPLEX vers la version 5.3 ou supérieure
Erreur : les données collectées ne sont pas suffisantes.	• Vérifiez l'horodatage de la collecte dans le fichier journal et modifiez l'intervalle d'interrogation en conséquence • Attendez plus longtemps
Erreur : les fichiers journaux perpétuels ne sont pas mis à jour.	Veuillez contacter le support EMC pour activer la mise à jour des fichiers journaux perpétuels
Erreur : l'intervalle d'interrogation des performances est trop grand.	Vérifiez l'horodatage de la collecte dans le fichier journal ${logfile} et modifiez l'intervalle d'interrogation en conséquence
Erreur : l'adresse IP distante des performances de la console de gestion VPLEX n'est pas configurée.	Modifiez la source de données pour définir l'adresse IP distante des performances de la console de gestion VPLEX.
Erreur : aucune donnée de performance n'a été signalée par le directeur	• Vérifiez que les moniteurs de performances du système fonctionnent correctement. • Veuillez contacter le support EMC pour activer la mise à jour des fichiers journaux du moniteur de performances du système.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Dell EMC XtremeIO

Le collecteur de données EMC XtremIO acquiert les données d'inventaire et de performances du système de stockage EMC XtremIO.

Exigences

Pour configurer le collecteur de données EMC XtremIO (HTTP), vous devez disposer de :

- L'adresse de l'hôte du serveur de gestion XtremIO (XMS)
- Un compte avec des privilèges d'administrateur
- Accès au port 443 (HTTPS)

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données EMC XtremIO. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez cette source de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque (SSD)	Disque
Cluster	Stockage
Contrôleur	Nœud de stockage
Volume	Volume
Carte LUN	Carte des volumes
Initiateur FC cible	Masque de volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour cette source de données.

Exigences

- L'adresse IP de l'hôte du serveur de gestion XtremIO (XMS)
- Nom d'utilisateur et mot de passe administrateur pour XtremIO

Configuration

Champ	Description
Hôte XMS	Adresse IP ou nom de domaine complet du serveur de gestion XtremIO
Nom d'utilisateur	Nom d'utilisateur pour le serveur de gestion XtremIO
Mot de passe	Mot de passe pour le serveur de gestion XtremIO

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter au serveur de gestion XTremIO. La valeur par défaut est 443.
Intervalle d'interrogation de l'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.

Champ	Description
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Fujitsu Eternus

Le collecteur de données Fujitsu Eternus acquiert les données d'inventaire à l'aide d'un accès de niveau administrateur au système de stockage.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du stockage Fujitsu Eternus. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Stockage	Stockage
Pool mince, pool de niveaux flexible, groupe de raid	Piscine de stockage
Volume standard, volume de données Snap (SDV), volume de pool de données Snap (SDPV), volume de provisionnement léger (TPV), volume de niveau flexible (FTV), volume de répartition large (WSV)	Volume
Adaptateur de canal	Contrôleur

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les éléments suivants sont requis pour configurer ce collecteur de données :

- Une adresse IP du stockage Eternus, qui ne peut pas être délimitée par des virgules
- Nom d'utilisateur et mot de passe de niveau administration SSH
- Port 22
- Assurez-vous que le défilement de la page est désactivé (clienv-show-more-scroll disable)

Configuration

Champ	Description
Adresse IP du stockage Eternus	Adresse IP du stockage Eternus

Champ	Description
Nom d'utilisateur	Nom d'utilisateur pour le stockage Eternus
Mot de passe	Mot de passe pour le stockage Eternus

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 20 minutes.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Erreur lors de la récupération des données » avec les messages d'erreur « Erreur de recherche d'invite CLI » ou « Erreur de recherche d'invite à la fin des résultats du shell »	Probablement causé par : le système de stockage a activé le défilement des pages. Solution possible : * Essayez de désactiver le défilement des pages en exécutant la commande suivante : set clienv-show-more -scroll disable
« Erreur de connexion » avec les messages d'erreur « Échec de l'instanciation d'une connexion SSH au stockage » ou « Échec de l'instanciation d'une connexion à VirtualCenter »	Causes probables : * Informations d'identification incorrectes. * Adresse IP incorrecte. * Problème de réseau. * Le stockage peut être en panne ou ne pas répondre. Solutions possibles : * Vérifier les informations d'identification et l'adresse IP saisies. * Essayez de communiquer avec le stockage à l'aide du client SSH.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données NetApp Google Compute

Ce collecteur de données prend en charge la collecte d'inventaire et de performances à partir des configurations de la plate-forme cloud Google Compute. Ce collecteur cherchera à découvrir toutes les ressources de calcul au sein de tous les projets au sein d'une organisation Google. Si vous souhaitez découvrir plusieurs organisations Google avec Data Infrastructure Insights, vous devrez déployer un collecteur Data Infrastructure Insights par organisation.

Exigences relatives au compte de service

- Vous devez créer un compte de service en suivant les instructions de"Création/gestion des comptes de service" . Ce compte de service est identifié par un identifiant unique, appelé *clientId*, qui sera utilisé comme nom d'utilisateur.
- De plus, créez une clé de compte de service en suivant les instructions de"Création/gestion des clés de compte de service" . Cette clé peut être téléchargée sous forme de fichier json, dont le contenu sera utilisé

comme mot de passe.

- Le compte de service doit être limité à *compute.readonly*, *monitoring.read* et *cloud-platform*.

Configuration

Champ	Description
ID de l'organisation	L'ID de l'organisation que vous souhaitez découvrir avec ce collecteur. Ce champ est obligatoire si votre compte de service peut voir plusieurs organisations
Choisissez « Exclure » ou « Inclure » pour filtrer les projets GCP par identifiants	Si vous souhaitez limiter les ressources des projets importées dans Data Infrastructure Insights.
ID de projet	La liste des ID de projet que vous souhaitez filtrer ou exclure de la découverte, en fonction de la valeur « Choisir « Exclure »…. ». La liste par défaut est vide
ID client	ID client pour la configuration de Google Cloud Platform
Copiez et collez le contenu de votre fichier d'informations d'identification Google ici	Copiez vos identifiants Google pour le compte Cloud Platform dans ce champ

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 60 minutes
Choisissez « Exclure » ou « Inclure » pour appliquer le filtre aux machines virtuelles par étiquettes	Spécifiez s'il faut inclure ou exclure les machines virtuelles par étiquettes lors de la collecte de données. Si « Inclure » est sélectionné, le champ Clé d'étiquette ne peut pas être vide.
Clés et valeurs d'étiquettes sur lesquelles filtrer les machines virtuelles	Cliquez sur **+ Filtrer l'étiquette** pour choisir les machines virtuelles (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs qui correspondent aux clés et aux valeurs des étiquettes sur la machine virtuelle. La clé d'étiquette est obligatoire, la valeur d'étiquette est facultative. Lorsque la valeur de l'étiquette est vide, la machine virtuelle est filtrée tant qu'elle correspond à la clé de l'étiquette.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 1800 secondes

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Google Cloud NetApp Volumes

Ce collecteur de données prend en charge la collecte d'inventaire et de performances à partir des configurations Google Cloud NetApp Volumes . Le collecteur découvre les

volumes NetApp et les ressources de stockage dans tous les projets au sein d'une organisation Google. Si vous disposez de plusieurs organisations Google que vous souhaitez surveiller avec Data Infrastructure Insights, déployez un collecteur par organisation.

Exigences relatives au compte de service

- Vous devez créer un compte de service en suivant les instructions de"Création/gestion des comptes de service" . Ce compte de service est identifié par un identifiant unique, appelé *clientId*, qui sera utilisé comme nom d'utilisateur.
- De plus, créez une clé de compte de service en suivant les instructions de"Création/gestion des clés de compte de service" . Cette clé peut être téléchargée sous forme de fichier json, dont le contenu sera utilisé comme mot de passe.
- Le compte de service doit être limité à *compute.readonly*, *monitoring.read* et *cloud-platform*.

Configuration

Champ	Description
ID de l'organisation	L'ID de l'organisation que vous souhaitez découvrir avec ce collecteur. Ce champ est obligatoire si votre compte de service peut voir plusieurs organisations
Choisissez « Exclure » ou « Inclure » pour filtrer les actifs GCNV par emplacement	La valeur par défaut est Exclure, car ce collecteur a par défaut l'intention de découvrir tous les volumes GCNV dans le monde entier au sein de votre organisation.
Emplacements d'exclusion/d'inclusion GCNV	Cette valeur est vide par défaut et est utilisée en conjonction avec l'option « Choisir « Exclure » ou « Inclure ». Si vous souhaitez découvrir des actifs uniquement dans certaines régions, utilisez ces deux options pour limiter la portée de ce collecteur.
ID de projet	La liste des ID de projet que vous souhaitez filtrer ou exclure de la découverte, en fonction de la valeur « Choisir « Exclure »…. ». La liste par défaut est vide
ID client	ID client pour la configuration de Google Cloud Platform
Copiez et collez le contenu de votre fichier d'informations d'identification Google ici	Copiez vos identifiants Google pour le compte Cloud Platform dans ce champ

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 60 minutes

Champ	Description
Utiliser AU Proxy pour les appels d'API REST	Sélectionnez cette option pour que le collecteur utilise le même proxy que l'unité d'acquisition sur laquelle réside le collecteur. Par défaut, cette option est désactivée, ce qui signifie que le collecteur tente d'envoyer des appels API HTTPS directement à Google.
Clés et valeurs d'étiquettes sur lesquelles filtrer les machines virtuelles	Cliquez sur **+ Filtrer l'étiquette** pour choisir les machines virtuelles (et les disques associés) à inclure/exclure en filtrant les clés et les valeurs qui correspondent aux clés et aux valeurs des étiquettes sur la machine virtuelle. La clé d'étiquette est obligatoire, la valeur d'étiquette est facultative. Lorsque la valeur de l'étiquette est vide, la machine virtuelle est filtrée tant qu'elle correspond à la clé de l'étiquette.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 300 secondes

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

HP Entreprise

Collecteur de données HP Enterprise Alletra 9000 / Primera Storage

Data Infrastructure Insights utilise le collecteur de données HP Enterprise Alletra 9000 / HP Enterprise Primera (anciennement 3PAR) pour découvrir l'inventaire et les performances.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Champ	Description
Disque physique	Disque
Système de stockage	Stockage
Nœud contrôleur	Nœud de stockage
Groupe de provisionnement commun	Piscine de stockage
Volume virtuel	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les éléments suivants sont requis pour configurer ce collecteur de données :

- Adresse IP ou FQDN du cluster InServ
- Pour l'inventaire, nom d'utilisateur et mot de passe en lecture seule pour le serveur StoreServ
- Pour des performances optimales, lisez et écrivez le nom d'utilisateur et le mot de passe sur le serveur StoreServ.
- Configuration requise pour les ports : 22 (collecte d'inventaire), 5988 ou 5989 (collecte de performances) [Remarque : les performances sont prises en charge pour StoreServ OS 3.x+]
- Pour la collecte des performances, confirmez que SMI-S est activé en vous connectant à la baie via SSH.

Configuration

Champ	Description
Adresse IP de stockage	Adresse IP de stockage ou nom de domaine complet du cluster StoreServ
Nom d'utilisateur	Nom d'utilisateur pour le serveur StoreServ
Mot de passe	Mot de passe utilisé pour le serveur StoreServ
Nom d'utilisateur SMI-S	Nom d'utilisateur pour l'hôte du fournisseur SMI-S
Mot de passe SMI-S	Mot de passe utilisé pour l'hôte du fournisseur SMI-S

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 40 minutes.
Connectivité SMI-S	Protocole utilisé pour se connecter au fournisseur SMI-S
Remplacer le port par défaut SMI-S	Si vide, utilisez le port par défaut de SMI-S Connectivity, sinon entrez le port de connexion à utiliser
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
La commande « showsys » ne renvoie aucun résultat.	Exécutez « showsys » et « showversion -a » à partir de la ligne de commande et vérifiez si la version est prise en charge par la baie.

Performances

Problème:	Essayez ceci:
Échec de la connexion ou de l'ouverture de session. L'initialisation du fournisseur a échoué.	Un nom de tableau entièrement numérique peut entraîner des problèmes avec le serveur SMI-S. Essayez de changer le nom du tableau.
L'utilisateur SMI-S configuré n'a aucun domaine	Accorder les privilèges de domaine appropriés à l'utilisateur SMI-S configuré
Data Infrastructure Insights indique qu'il ne peut pas se connecter/se connecter au service SMI-S.	Confirmez qu'il n'y a pas de pare-feu entre le CI AU et la baie qui empêcherait le CI AU d'établir des connexions TCP vers 5988 ou 5989. Une fois cela fait, et si vous avez confirmé qu'il n'y a pas de pare-feu, vous devez vous connecter en SSH à la baie et utiliser la commande « showcim » pour confirmer. Vérifiez que : * Le service est activé * HTTPS est activé * Le port HTTPS doit être 5989 Si tout cela est le cas, vous pouvez essayer de faire « stopcim » puis « startcim » pour redémarrer le CIM (c'est-à-dire le service SMI-S).

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données HP Enterprise Command View

Le collecteur de données HP Enterprise Command View Advanced Edition prend en charge la découverte des baies XP et P9500 via le serveur Command View Advanced Edition (CVAE). Data Infrastructure Insights communique avec CVAE à l'aide de l'API Command View standard pour collecter des données d'inventaire et de performances.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données HP Enterprise Command View. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
PDEV	Disque
Journal Pool	Groupe de disques
Baie de stockage	Stockage
Contrôleur de port	Nœud de stockage
Groupe de tableaux, pool DP	Piscine de stockage
Unité logique, LDEV	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences en matière d'inventaire

Vous devez disposer des éléments suivants pour collecter des données d'inventaire :

- Adresse IP du serveur CVAE
- Nom d'utilisateur et mot de passe en lecture seule pour le logiciel CVAE et privilèges homologues
- Exigence portuaire : 2001

Exigences de performance

Les exigences suivantes doivent être respectées pour collecter des données de performance :

- Performances HDS USP, USP V et VSP
  - Performance Monitor doit être sous licence.
  - Le commutateur de surveillance doit être activé.
  - L'outil d'exportation (Export.exe) doit être copié dans l'AU Data Infrastructure Insights et extrait vers un emplacement. Sur les AU Linux CI, assurez-vous que « cisys » dispose des autorisations de lecture et d'exécution.
  - La version de l'outil d'exportation doit correspondre à la version du microcode du tableau cible.
- Performances AMS :
  - Performance Monitor doit être sous licence.
  - L'utilitaire CLI Storage Navigator Modular 2 (SNM2) doit être installé sur Data Infrastructure Insights AU.
- Exigences réseau
  - Les outils d'exportation sont basés sur Java et utilisent RMI pour communiquer avec le tableau. Ces outils peuvent ne pas être compatibles avec le pare-feu car ils peuvent négocier dynamiquement les ports TCP source et de destination à chaque appel. De plus, les outils d'exportation de différents modèles de matrice peuvent se comporter différemment sur le réseau ; consultez HPE pour connaître les exigences de votre modèle.

Configuration

Champ	Description
Serveur Command View	Adresse IP ou nom de domaine complet du serveur Command View
Nom d'utilisateur	Nom d'utilisateur pour le serveur Command View.
Mot de passe	Mot de passe utilisé pour le serveur Command View.
Appareils - Stockages VSP G1000 (R800), VSP (R700), HUS VM (HM700) et USP	Liste des périphériques pour les stockages VSP G1000 (R800), VSP (R700), HUS VM (HM700) et USP. Chaque stockage nécessite : * IP de la baie : adresse IP du stockage * Nom d'utilisateur : nom d'utilisateur pour le stockage * Mot de passe : mot de passe pour le stockage * Dossier contenant les fichiers JAR de l'utilitaire d'exportation

Champ	Description
SNM2Devices - Stockages WMS/SMS/AMS	Liste des périphériques pour les stockages WMS/SMS/AMS. Chaque stockage nécessite : * IP de la baie : adresse IP du stockage * Chemin d'accès CLI du navigateur de stockage : chemin d'accès CLI SNM2 * Authentification de compte valide : sélectionnez cette option pour choisir une authentification de compte valide * Nom d'utilisateur : nom d'utilisateur pour le stockage * Mot de passe : mot de passe pour le stockage
Choisissez Tuning Manager pour les performances	Remplacer les autres options de performances
Gestionnaire de réglage hôte	Adresse IP ou nom de domaine complet du gestionnaire de réglage
Port du gestionnaire de réglage	Port utilisé pour Tuning Manager
Nom d'utilisateur du gestionnaire de réglages	Nom d'utilisateur pour Tuning Manager
Mot de passe du gestionnaire de réglages	Mot de passe pour Tuning Manager

Remarque : dans HDS USP, USP V et VSP, n'importe quel disque peut appartenir à plusieurs groupes de baies.

Configuration avancée

Champ	Description
Port du serveur Command View	Port utilisé pour le serveur Command View
HTTPs activé	Sélectionnez pour activer HTTPS
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40.
Choisissez « Exclure » ou « Inclure » pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste de tableaux ci-dessous lors de la collecte de données.
Exclure ou inclure des appareils	Liste séparée par des virgules d'ID de périphérique ou de noms de tableau à inclure ou à exclure
Gestionnaire d'hôtes de requêtes	Sélectionnez pour interroger le gestionnaire d'hôte
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est 300.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : l'utilisateur ne dispose pas de suffisamment d'autorisations	Utilisez un autre compte d'utilisateur disposant de plus de privilèges ou augmentez les privilèges du compte d'utilisateur configuré dans le collecteur de données
Erreur : la liste des stockages est vide. Soit les appareils ne sont pas configurés, soit l'utilisateur ne dispose pas des autorisations suffisantes	* Utilisez DeviceManager pour vérifier si les périphériques sont configurés. * Utilisez un autre compte utilisateur disposant de plus de privilèges ou augmentez les privilèges du compte utilisateur
Erreur : la matrice de stockage HDS n'a pas été actualisée pendant quelques jours	Recherchez pourquoi ce tableau n'est pas actualisé dans HP CommandView AE.

Performances

Problème:	Essayez ceci:
Erreur : * Erreur lors de l'exécution de l'utilitaire d'exportation * Erreur lors de l'exécution de la commande externe	* Confirmez que l'utilitaire d'exportation est installé sur l'unité d'acquisition Data Infrastructure Insights * Confirmez que l'emplacement de l'utilitaire d'exportation est correct dans la configuration du collecteur de données * Confirmez que l'adresse IP de la baie USP/R600 est correcte dans la configuration du collecteur de données * Confirmez que le nom d'utilisateur et le mot de passe sont corrects dans la configuration du collecteur de données * Confirmez que la version de l'utilitaire d'exportation est compatible avec la version du microcode de la baie de stockage * À partir de l'unité d'acquisition Data Infrastructure Insights , ouvrez une invite de commande et procédez comme suit : - Modifiez le répertoire vers le répertoire d'installation configuré - Essayez d'établir une connexion avec la baie de stockage configurée en exécutant le fichier de commandes runWin.bat
Erreur : la connexion à l'outil d'exportation a échoué pour l'adresse IP cible	* Confirmer que le nom d'utilisateur/mot de passe est correct * Créer un identifiant utilisateur principalement pour ce collecteur de données HDS * Confirmer qu'aucun autre collecteur de données n'est configuré pour acquérir ce tableau
Erreur : les outils d'exportation ont enregistré « Impossible d'obtenir la plage horaire pour la surveillance ».	* Confirmez que la surveillance des performances est activée sur la baie. * Essayez d'appeler les outils d'exportation en dehors de Data Infrastructure Insights pour confirmer que le problème se situe en dehors de Data Infrastructure Insights.
Erreur : * Erreur de configuration : la baie de stockage n'est pas prise en charge par l'utilitaire d'exportation * Erreur de configuration : la baie de stockage n'est pas prise en charge par l'interface de ligne de commande modulaire Storage Navigator	* Configurez uniquement les baies de stockage prises en charge. * Utilisez « Filtrer la liste des périphériques » pour exclure les baies de stockage non prises en charge.

Problème:	Essayez ceci:
Erreur : * Erreur lors de l'exécution de la commande externe * Erreur de configuration : la baie de stockage n'est pas signalée par l'inventaire * Erreur de configuration : le dossier d'exportation ne contient pas de fichiers JAR	* Vérifiez l'emplacement de l'utilitaire d'exportation. * Vérifiez si la baie de stockage en question est configurée dans le serveur Command View. * Définissez l'intervalle d'interrogation des performances comme un multiple de 60 secondes.
Erreur : * Erreur du navigateur de stockage CLI * Erreur lors de l'exécution de la commande auperform * Erreur lors de l'exécution de la commande externe	* Confirmez que l'interface de ligne de commande modulaire Storage Navigator est installée sur l'unité d'acquisition Data Infrastructure Insights. * Confirmez que l'emplacement de l'interface de ligne de commande modulaire Storage Navigator est correct dans la configuration du collecteur de données. * Confirmez que l'adresse IP de la baie WMS/SMS/SMS est correcte dans la configuration du collecteur de données. * Confirmez que la version de l'interface de ligne de commande modulaire Storage Navigator est compatible avec la version du microcode de la baie de stockage configurée dans le collecteur de données. * Depuis l'unité d'acquisition Data Infrastructure Insights , ouvrez une invite de commande et procédez comme suit : - Modifiez le répertoire vers le répertoire d'installation configuré. - Essayez d'établir une connexion avec la baie de stockage configurée en exécutant la commande suivante : « auunitref.exe ».
Erreur : Erreur de configuration : la baie de stockage n'est pas signalée par l'inventaire	Vérifiez si la baie de stockage en question est configurée dans le serveur Command View
Erreur : * Aucune baie n'est enregistrée avec l'interface de ligne de commande Storage Navigator Modular 2 * La baie n'est pas enregistrée avec l'interface de ligne de commande Storage Navigator Modular 2 * Erreur de configuration : Baie de stockage non enregistrée avec l'interface de ligne de commande StorageNavigator Modular	* Ouvrez l'invite de commande et changez de répertoire pour le chemin configuré * Exécutez la commande « set=STONAVM_HOME=. » * Exécutez la commande « auunitref » * Confirmez que la sortie de la commande contient les détails de la baie avec l'IP * Si la sortie ne contient pas les détails de la baie, enregistrez la baie avec Storage Navigator CLI : - Ouvrez l'invite de commande et changez de répertoire pour le chemin configuré - Exécutez la commande « set=STONAVM_HOME=. » - Exécutez la commande « auunitaddauto -ip ${ip} ». Remplacez ${ip} par une adresse IP réelle

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données HPE Alletra 6000

Le collecteur de données HP Enterprise Alletra 6000 (anciennement Nimble) prend en charge les données d'inventaire et de performances des baies de stockage Alletra 6000.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur. Pour

chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Tableau	Stockage
Disque	Disque
Volume	Volume
Piscine	Piscine de stockage
Initiateur	Alias de l'hôte de stockage
Contrôleur	Nœud de stockage
Interface Fibre Channel	Contrôleur

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous devez disposer des éléments suivants pour collecter les données d'inventaire et de configuration de la baie de stockage :

- La baie doit être installée et configurée, et accessible depuis le client via son nom de domaine complet (FQDN) ou son adresse IP de gestion de baie.
- Le tableau doit exécuter NimbleOS 2.3.x ou une version ultérieure.
- Vous devez disposer d'un nom d'utilisateur et d'un mot de passe valides pour la baie avec au moins le rôle de niveau « Opérateur ». Le rôle « Invité » ne dispose pas d'un accès suffisant pour comprendre les configurations de l'initiateur.
- Le port 5392 doit être ouvert sur la baie.

Vous devez disposer des éléments suivants pour collecter les données de performances de la baie de stockage :

- Le tableau doit exécuter NimbleOS 4.0.0 ou une version ultérieure
- La baie doit avoir des volumes configurés. La seule API de performance dont dispose NimbleOS concerne les volumes, et tous les rapports statistiques de Data Infrastructure Insights sont dérivés des statistiques sur les volumes.

Configuration

Champ	Description
Adresse IP de gestion de la baie	Nom de domaine entièrement qualifié (FQDN) ou adresse IP de gestion de tableau.
Nom d'utilisateur	Nom d'utilisateur pour le tableau
Mot de passe	Mot de passe pour le tableau

Configuration avancée

Champ	Description
Port	Port utilisé par l'API REST Nimble. La valeur par défaut est 5392.
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.

Remarque : l'intervalle d'interrogation des performances par défaut est de 300 secondes et ne peut pas être modifié. Il s'agit du seul intervalle pris en charge par HPE Alletra 6000.

Systèmes de données Hitachi

Collecteur de données Hitachi Vantara Command Suite

Le collecteur de données Hitachi Vantara Command Suite prend en charge le serveur HiCommand Device Manager. Data Infrastructure Insights communique avec le serveur HiCommand Device Manager à l'aide de l'API HiCommand standard.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données Hitachi Vantara Command Suite. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
PDEV	Disque
Journal Pool	Groupe de disques
Baie de stockage	Stockage
Contrôleur de port	Nœud de stockage
Groupe de matrices, pool HDS	Piscine de stockage
Unité logique, LDEV	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Stockage

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources de stockage HDS. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

- Nom – provient directement de l'attribut « nom » du gestionnaire de périphériques HDS HiCommand via l'appel d'API XML GetStorageArray
- Modèle - provient directement de l'attribut « arrayType » du gestionnaire de périphériques HDS HiCommand via l'appel d'API XML GetStorageArray

- Fournisseur – HDS
- Famille - provient directement de l'attribut « arrayFamily » du gestionnaire de périphériques HDS HiCommand via l'appel d'API XML GetStorageArray
- IP – il s'agit de l'adresse IP de gestion de la baie, et non d'une liste exhaustive de toutes les adresses IP de la baie
- Capacité brute – une valeur de base 2 représentant la somme de la capacité totale de tous les disques de ce système, quel que soit le rôle du disque.

Piscine de stockage

Les termes suivants s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources du pool de stockage HDS. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

- Type : La valeur ici sera l'une des suivantes :
  - RÉSERVÉ – si ce pool est dédié à des fins autres que les volumes de données, c'est-à-dire la journalisation, les instantanés
  - Provisionnement léger – s'il s'agit d'un pool HDP
  - Groupe de raid – vous ne les verrez probablement pas pour plusieurs raisons :

    Data Infrastructure Insights adopte une position ferme pour éviter à tout prix le double comptage des capacités. Sur HDS, il faut généralement créer des groupes Raid à partir de disques, créer des volumes de pool sur ces groupes Raid et construire des pools (souvent HDP, mais qui peuvent être à usage spécial) à partir de ces volumes de pool. Si Data Infrastructure Insights signalait à la fois les groupes Raid sous-jacents tels quels, ainsi que les pools, la somme de leur capacité brute dépasserait largement la somme des disques.

  Au lieu de cela, le collecteur de données HDS Command Suite de Data Infrastructure Insights réduit arbitrairement la taille des groupes Raid en fonction de la capacité des volumes de pool. Cela peut entraîner le fait que Data Infrastructure Insights ne signale pas du tout le groupe Raid. De plus, tous les groupes de raid résultants sont signalés de manière à ne pas être visibles dans l'interface Web de Data Infrastructure Insights , mais ils sont transférés dans l'entrepôt de données de Data Infrastructure Insights (DWH). Le but de ces décisions est d'éviter l'encombrement de l'interface utilisateur pour des éléments qui ne s'intéressent pas à la plupart des utilisateurs. Si votre baie HDS dispose de groupes Raid avec 50 Mo d'espace libre, vous ne pouvez probablement pas utiliser cet espace libre pour obtenir un résultat significatif.

- Nœud - N/A, car les pools HDS ne sont liés à aucun nœud spécifique
- Redondance - le niveau RAID du pool. Plusieurs valeurs possibles pour un pool HDP composé de plusieurs types RAID
- Capacité % - le pourcentage utilisé du pool pour l'utilisation des données, avec les Go utilisés et la taille totale en Go logiques du pool
- Capacité surengagée - une valeur dérivée, indiquant que « la capacité logique de ce pool est sursouscrite de ce pourcentage en raison de la somme des volumes logiques dépassant la capacité logique du pool de ce pourcentage »
- Instantané - affiche la capacité réservée à l'utilisation des instantanés sur ce pool

Nœud de stockage

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources des nœuds de stockage HDS. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

- Nom – Le nom du directeur frontal (FED) ou de l'adaptateur de canal sur les baies monolithiques, ou le nom du contrôleur sur une baie modulaire. Une baie HDS donnée aura 2 nœuds de stockage ou plus
- Volumes – Le tableau des volumes affichera tout volume mappé à n'importe quel port appartenant à ce nœud de stockage

Exigences en matière d'inventaire

Vous devez disposer des éléments suivants pour collecter des données d'inventaire :

- Adresse IP du serveur HiCommand Device Manager
- Nom d'utilisateur et mot de passe en lecture seule pour le logiciel HiCommand Device Manager et privilèges homologues
- Exigences de port : 2001 (http) ou 2443 (https)
- Connectez-vous au logiciel HiCommand Device Manager à l'aide du nom d'utilisateur et du mot de passe
- Vérifier l'accès à HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Exigences de performance

Les exigences suivantes doivent être respectées pour collecter des données de performance :

- Performances HDS USP, USP V et VSP
  - Performance Monitor doit être sous licence.
  - Le commutateur de surveillance doit être activé.
  - L'outil d'exportation (Export.exe) doit être copié dans l'AU Data Infrastructure Insights .
  - La version de l'outil d'exportation doit correspondre à la version du microcode du tableau cible.
- Performances AMS :
  - NetApp recommande fortement de créer un compte de service dédié sur les baies AMS pour que Data Infrastructure Insights puisse l'utiliser pour récupérer les données de performances. Storage Navigator n'autorise qu'une seule connexion simultanée à un compte utilisateur sur la baie. Le fait que Data Infrastructure Insights utilise le même compte utilisateur que les scripts de gestion ou HiCommand peut empêcher Data Infrastructure Insights, les scripts de gestion ou HiCommand de communiquer avec la baie en raison de la limite de connexion d'un seul compte utilisateur simultané.
  - Performance Monitor doit être sous licence.
  - L'utilitaire CLI Storage Navigator Modular 2 (SNM2) doit être installé sur l'AU Data Infrastructure Insights .

Configuration

Champ	Description
Serveur HiCommand	Adresse IP ou nom de domaine complet du serveur HiCommand Device Manager

Champ	Description
Nom d’utilisateur	Nom d’utilisateur pour le serveur HiCommand Device Manager.
Mot de passe	Mot de passe utilisé pour le serveur HiCommand Device Manager.
Appareils - Stockages VSP G1000 (R800), VSP (R700), HUS VM (HM700) et USP	Liste des périphériques pour les stockages VSP G1000 (R800), VSP (R700), HUS VM (HM700) et USP. Chaque stockage nécessite : * IP de la baie : adresse IP du stockage * Nom d’utilisateur : nom d’utilisateur pour le stockage * Mot de passe : mot de passe pour le stockage * Dossier contenant les fichiers JAR de l’utilitaire d’exportation
SNM2Devices - Stockages WMS/SMS/AMS	Liste des périphériques pour les stockages WMS/SMS/AMS. Chaque stockage nécessite : * IP de la baie : adresse IP du stockage * Chemin d’accès CLI du navigateur de stockage : chemin d’accès CLI SNM2 * Authentification de compte valide : sélectionnez cette option pour choisir une authentification de compte valide * Nom d’utilisateur : nom d’utilisateur pour le stockage * Mot de passe : mot de passe pour le stockage
Choisissez Tuning Manager pour les performances	Remplacer les autres options de performances
Gestionnaire de réglage hôte	Adresse IP ou nom de domaine complet du gestionnaire de réglage
Remplacer le port du gestionnaire de réglage	Si vide, utilisez le port par défaut dans le champ Choisir le gestionnaire de réglage pour les performances, sinon entrez le port à utiliser
Nom d’utilisateur du gestionnaire de réglages	Nom d’utilisateur pour Tuning Manager
Mot de passe du gestionnaire de réglages	Mot de passe pour Tuning Manager

Remarque : dans HDS USP, USP V et VSP, n’importe quel disque peut appartenir à plusieurs groupes de baies.

Configuration avancée

Champ	Description
Type de connexion	HTTPS ou HTTP, affiche également le port par défaut
Port du serveur HiCommand	Port utilisé pour le gestionnaire de périphériques HiCommand
Intervalle d’interrogation d’inventaire (min)	Intervalle entre les sondages d’inventaire. La valeur par défaut est 40.
Choisissez « Exclure » ou « Inclure » pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste de tableaux ci-dessous lors de la collecte de données.
Liste des appareils de filtrage	Liste séparée par des virgules des numéros de série des appareils à inclure ou à exclure

Intervalle d’interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est 300.
Délai d’expiration de l’exportation en secondes	Délai d’expiration de l’utilitaire d’exportation. La valeur par défaut est 300.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : l’utilisateur ne dispose pas de suffisamment d’autorisations	Utilisez un autre compte d’utilisateur disposant de plus de privilèges ou augmentez les privilèges du compte d’utilisateur configuré dans le collecteur de données
Erreur : la liste des stockages est vide. Soit les appareils ne sont pas configurés, soit l’utilisateur ne dispose pas des autorisations suffisantes	* Utilisez DeviceManager pour vérifier si les périphériques sont configurés. * Utilisez un autre compte utilisateur disposant de plus de privilèges ou augmentez les privilèges du compte utilisateur
Erreur : la matrice de stockage HDS n’a pas été actualisée pendant quelques jours	Recherchez pourquoi ce tableau n’est pas actualisé dans HDS HiCommand.

Performances

Problème:	Essayez ceci:
Erreur : * Erreur lors de l’exécution de l’utilitaire d’exportation * Erreur lors de l’exécution de la commande externe	* Confirmez que l’utilitaire d’exportation est installé sur l’unité d’acquisition Data Infrastructure Insights * Confirmez que l’emplacement de l’utilitaire d’exportation est correct dans la configuration du collecteur de données * Confirmez que l’adresse IP de la baie USP/R600 est correcte dans la configuration du collecteur de données * Confirmez que le nom d’utilisateur et le mot de passe sont corrects dans la configuration du collecteur de données * Confirmez que la version de l’utilitaire d’exportation est compatible avec la version du microcode de la baie de stockage * À partir de l’unité d’acquisition Data Infrastructure Insights , ouvrez une invite de commande et procédez comme suit : - Modifiez le répertoire vers le répertoire d’installation configuré - Essayez d’établir une connexion avec la baie de stockage configurée en exécutant le fichier de commandes runWin.bat
Erreur : la connexion à l’outil d’exportation a échoué pour l’adresse IP cible	* Confirmer que le nom d’utilisateur/mot de passe est correct * Créer un identifiant utilisateur principalement pour ce collecteur de données HDS * Confirmer qu’aucun autre collecteur de données n’est configuré pour acquérir ce tableau

Problème:	Essayez ceci:
Erreur : les outils d'exportation ont enregistré « Impossible d'obtenir la plage horaire pour la surveillance ».	* Confirmez que la surveillance des performances est activée sur la baie. * Essayez d'appeler les outils d'exportation en dehors de Data Infrastructure Insights pour confirmer que le problème se situe en dehors de Data Infrastructure Insights.
Erreur : * Erreur de configuration : la baie de stockage n'est pas prise en charge par l'utilitaire d'exportation * Erreur de configuration : la baie de stockage n'est pas prise en charge par l'interface de ligne de commande modulaire Storage Navigator	* Configurez uniquement les baies de stockage prises en charge. * Utilisez « Filtrer la liste des périphériques » pour exclure les baies de stockage non prises en charge.
Erreur : * Erreur lors de l'exécution de la commande externe * Erreur de configuration : la baie de stockage n'est pas signalée par l'inventaire * Erreur de configuration : le dossier d'exportation ne contient pas de fichiers JAR	* Vérifiez l'emplacement de l'utilitaire d'exportation. * Vérifiez si la baie de stockage en question est configurée sur le serveur HiCommand. * Définissez l'intervalle d'interrogation des performances comme un multiple de 60 secondes.
Erreur : * Erreur du navigateur de stockage CLI * Erreur lors de l'exécution de la commande auperform * Erreur lors de l'exécution de la commande externe	* Confirmez que l'interface de ligne de commande modulaire Storage Navigator est installée sur l'unité d'acquisition Data Infrastructure Insights. * Confirmez que l'emplacement de l'interface de ligne de commande modulaire Storage Navigator est correct dans la configuration du collecteur de données. * Confirmez que l'adresse IP de la baie WMS/SMS/SMS est correcte dans la configuration du collecteur de données. * Confirmez que la version de l'interface de ligne de commande modulaire Storage Navigator est compatible avec la version du microcode de la baie de stockage configurée dans le collecteur de données. * Depuis l'unité d'acquisition Data Infrastructure Insights , ouvrez une invite de commande et procédez comme suit : - Modifiez le répertoire vers le répertoire d'installation configuré. - Essayez d'établir une connexion avec la baie de stockage configurée en exécutant la commande suivante : « auunitref.exe ».
Erreur : Erreur de configuration : la baie de stockage n'est pas signalée par l'inventaire	Vérifiez si la baie de stockage en question est configurée sur le serveur HiCommand
Erreur : * Aucune baie n'est enregistrée avec l'interface de ligne de commande Storage Navigator Modular 2 * La baie n'est pas enregistrée avec l'interface de ligne de commande Storage Navigator Modular 2 * Erreur de configuration : Baie de stockage non enregistrée avec l'interface de ligne de commande StorageNavigator Modular	* Ouvrez l'invite de commande et changez de répertoire pour le chemin configuré * Exécutez la commande « set=STONAVM_HOME=. » * Exécutez la commande « auunitref » * Confirmez que la sortie de la commande contient les détails de la baie avec l'IP * Si la sortie ne contient pas les détails de la baie, enregistrez la baie avec Storage Navigator CLI : - Ouvrez l'invite de commande et changez de répertoire pour le chemin configuré - Exécutez la commande « set=STONAVM_HOME=. » - Exécutez la commande « auunitaddauto -ip <ip> ». Remplacez <ip> par l'IP correcte.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données Hitachi Vantara NAS

Le collecteur de données Hitachi Vantara NAS est un collecteur de données d'inventaire et de configuration qui prend en charge la découverte de clusters NAS HDS. Data Infrastructure Insights prend en charge la découverte des partages NFS et CIFS, des systèmes de fichiers (volumes internes) et des étendues (pools de stockage).

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données HNAS. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Étage	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
Portée	Piscine de stockage
Lecteur système	Lun arrière-plan
Système de fichiers	Volume interne

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Adresse IP de l'appareil
- Port 22, protocole SSH
- Nom d'utilisateur et mot de passe - niveau de privilège : Superviseur
- Remarque : ce collecteur de données est basé sur SSH. L'AU qui l'héberge doit donc pouvoir lancer des sessions SSH sur TCP 22 sur le HNAS lui-même ou sur l'unité de gestion des systèmes (SMU) à laquelle le cluster est connecté.

Configuration

Champ	Description
Hôte HNAS	Adresse IP ou nom de domaine complet de l'hôte de gestion HNAS
Nom d'utilisateur	Nom d'utilisateur pour HNAS CLI
Mot de passe	Mot de passe utilisé pour HNAS CLI

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 30 minutes.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Erreur de connexion » avec les messages d'erreur « Erreur de configuration du canal shell » ou « Erreur d'ouverture du canal shell »	Probablement causé par des problèmes de connectivité réseau ou par une mauvaise configuration de SSH. Confirmer la connexion avec un autre client SSH
« Délai d'expiration » ou « Erreur lors de la récupération des données » avec les messages d'erreur « Commande : XXX a expiré. »	* Essayez la commande avec un autre client SSH * Augmentez le délai d'expiration
« Erreur de connexion » ou « Informations de connexion non valides » avec les messages d'erreur « Impossible de communiquer avec l'appareil : »	* Vérifier l'adresse IP * Vérifier le nom d'utilisateur et le mot de passe * Confirmer la connexion avec un autre client SSH

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Hitachi Ops Center

Ce collecteur de données utilise la suite d'applications intégrée de Hitachi Ops Center pour accéder aux données d'inventaire et de performances de plusieurs périphériques de stockage. Pour la découverte de l'inventaire et de la capacité, votre installation Ops Center doit inclure les composants « Services communs » et « Administrateur ». Pour la collecte des performances, vous devez également avoir « Analyzer » déployé.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Systèmes de stockage	Stockage
Volume	Volume
Groupes de parité	Pool de stockage (RAID), groupes de disques
Disque	Disque

Terme du fournisseur/modèle	Data Infrastructure Insights
Piscine de stockage	Pool de stockage (mince, SNAP)
Groupes de parité externes	Pool de stockage (backend), groupes de disques
Port	Nœud de stockage → Nœud de contrôleur → Port
Groupes d'accueil	Cartographie et masquage des volumes
Paires de volumes	Synchronisation du stockage

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences en matière d'inventaire

Vous devez disposer des éléments suivants pour collecter des données d'inventaire :

- Adresse IP ou nom d'hôte du serveur Ops Center hébergeant le composant « Services communs »
- Compte utilisateur root/sysadmin et mot de passe qui existent sur tous les serveurs hébergeant les composants Ops Center. HDS n'a pas implémenté la prise en charge de l'API REST pour l'utilisation par les utilisateurs LDAP/SSO avant Ops Center 10.8+

Exigences de performance

Les exigences suivantes doivent être respectées pour collecter des données de performance :

Le module « Analyzer » du HDS Ops Center doit être installé. Les baies de stockage doivent alimenter le module « Analyzer » du Ops Center.

Configuration

Champ	Description
Adresse IP du centre d'opérations Hitachi	Adresse IP ou nom de domaine complet du serveur Ops Center hébergeant le composant « Services communs »
Nom d'utilisateur	Nom d'utilisateur pour le serveur Ops Center.
Mot de passe	Mot de passe utilisé pour le serveur Ops Center.

Configuration avancée

Champ	Description
Type de connexion	HTTPS (port 443) est la valeur par défaut
Remplacer le port TCP	Spécifiez le port à utiliser s'il n'est pas celui par défaut
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est 40.
Choisissez « Exclure » ou « Inclure » pour spécifier une liste	Indiquez si vous souhaitez inclure ou exclure la liste de tableaux ci-dessous lors de la collecte de données.

Liste des appareils de filtrage	Liste séparée par des virgules des numéros de série des appareils à inclure ou à exclure
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est 300.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Infinidat InfiniBox

Le collecteur de données Infinidat InfiniBox (HTTP) est utilisé pour collecter des informations d'inventaire à partir du système de stockage Infinidat InfiniBox.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Infinidat InfiniBox. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Piscine de stockage	Piscine de stockage
Nœud	Contrôleur
Système de fichiers	Volume interne
Système de fichiers	Partage de fichiers
Exportations du système de fichiers	Partager

Exigences

Les exigences suivantes doivent être respectées lors de la configuration de ce collecteur de données.

- Adresse IP ou FQDN du nœud de gestion InfiniBox
- Identifiant et mot de passe de l'administrateur
- Port 443 via l'API REST

Configuration

Champ	Description
Hôte InfiniBox	Adresse IP ou nom de domaine complet du nœud de gestion InfiniBox
Nom d'utilisateur	Nom d'utilisateur pour le nœud de gestion InfiniBox
Mot de passe	Mot de passe pour le nœud de gestion InfiniBox

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter au serveur InfiniBox. La valeur par défaut est 443.
Intervalle d'interrogation de l'inventaire	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Huawei OceanStor

Data Infrastructure Insights utilise le collecteur de données Huawei OceanStor (REST/HTTPS) pour découvrir l'inventaire et les performances du stockage Huawei OceanStor et OceanStor Dorado.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire et de performances suivantes auprès de Huawei OceanStor. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Piscine de stockage	Piscine de stockage
Système de fichiers	Volume interne
Contrôleur	Nœud de stockage
Port FC (cartographié)	Carte des volumes
Initiateur FC hôte (mappé)	Masque de volume
Partage NFS/CIFS	Partager
Cible de liaison iSCSI	Nœud cible iSCSI
Initiateur de lien iSCSI	Nœud initiateur iSCSI
Disque	Disque
LUN	Volume

Exigences

Les exigences suivantes sont requises pour configurer ce collecteur de données :

- Adresse IP de l'appareil
- Informations d'identification pour accéder au gestionnaire de périphériques OceanStor

- Le port 8088 doit être disponible

Configuration

Champ	Description
Adresse IP de l'hôte OceanStor	Adresse IP ou nom de domaine complet du gestionnaire de périphériques OceanStor
Nom d'utilisateur	Nom utilisé pour se connecter au gestionnaire de périphériques OceanStor
Mot de passe	Mot de passe utilisé pour se connecter au gestionnaire de périphériques OceanStor

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter à OceanStor Device Manager. La valeur par défaut est 8088.
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.
Intervalle d'interrogation des performances (sec).	La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

IBM

Collecteur de données IBM Cleversafe

Data Infrastructure Insights utilise ce collecteur de données pour découvrir les données d'inventaire et de performances des systèmes de stockage IBM Cleversafe.

IBM Cleversafe est mesuré à un taux différent entre les To bruts et les unités gérées. Chaque 40 To de capacité IBM Cleversafe non formatée est facturé 1"Unité gérée (UG)" .

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données IBM Cleversafe. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Piscine de stockage	Piscine de stockage
Récipient	Volume interne

Terme du fournisseur/modèle	Data Infrastructure Insights
Récipient	Partage de fichiers
Partage NFS	Partager

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- L'adresse IP des services de données externes pour le cluster
- Nom d'utilisateur et mot de passe de l'administrateur
- Port 9440

Configuration

Champ	Description
IP du gestionnaire ou nom d'hôte	Adresse IP ou nom d'hôte du nœud de gestion
Nom d'utilisateur	Nom d'utilisateur pour le compte utilisateur avec le rôle de superutilisateur ou d'administrateur système
Mot de passe	Mot de passe pour le compte utilisateur avec le rôle de super utilisateur ou d'administrateur système

Configuration avancée

Champ	Description
Intervalle d'interrogation de l'inventaire (min)	Intervalle entre les sondages d'inventaire.
Délai d'expiration de la connexion HTTP (sec)	Délai d'expiration HTTP en secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données IBM CS

Data Infrastructure Insights utilise ce collecteur de données pour découvrir les données d'inventaire et de performances des systèmes de stockage IBM CS.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données IBM CS. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Piscine de stockage	Piscine de stockage

Terme du fournisseur/modèle	Data Infrastructure Insights
Récipient	Volume interne
Récipient	Partage de fichiers
Partage NFS	Partager

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- L'adresse IP des services de données externes pour le cluster
- Nom d'utilisateur et mot de passe de l'administrateur
- Port 9440

Configuration

Champ	Description
Adresse IP externe de Prism	L'adresse IP des services de données externes pour le cluster
Nom d'utilisateur	Nom d'utilisateur pour le compte administrateur
Mot de passe	Mot de passe pour le compte administrateur

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter au tableau IBM CS. La valeur par défaut est 9440.
Intervalle d'interrogation de l'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données IBM System Storage DS8000 Series

Le collecteur de données IBM DS (CLI) prend en charge l'acquisition de données d'inventaire et de performances pour les périphériques DS6xxx et DS8xxx.

Les périphériques DS3xxx, DS4xxx et DS5xxx sont pris en charge par le"Collecteur de données NetApp E-Series" . Vous devez vous référer à la matrice de support de Data Infrastructure Insights pour connaître les modèles et les versions de micrologiciels pris en charge.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données IBM DS. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Module de lecteur de disque	Disque
Image de stockage	Stockage
Piscine étendue	Nœud de stockage
Volume de bloc fixe	Volume
Initiateur FC hôte (mappé)	Masque de volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous avez besoin des éléments suivants pour configurer ce collecteur de données :

- Adresse IP de chaque baie DS
- Nom d'utilisateur et mot de passe en lecture seule sur chaque baie DS
- Logiciel tiers installé sur l'AU Data Infrastructure Insights : IBM *dscli*
- Validation d'accès : exécutez les commandes *dscli* en utilisant le nom d'utilisateur et le mot de passe
- Exigences portuaires : 80, 443 et 1 750

Configuration

Champ	Description
Stockage DS	Adresse IP ou nom de domaine complet de l'appareil DS
Nom d'utilisateur	Nom d'utilisateur pour la DS CLI
Mot de passe	Mot de passe pour la DS CLI
chemin exécutable *dscli*	Chemin complet vers l'exécutable *dscli*

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire (min). La valeur par défaut est 40.
Nom d'affichage du stockage	Nom de la baie de stockage IBM DS
Appareils exclus de l'inventaire	Liste séparée par des virgules des numéros de série des appareils à exclure de la collecte d'inventaire

Champ	Description
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300.
Type de filtre de performance	Inclure : données collectées uniquement à partir des appareils de la liste. Exclure : aucune donnée de ces appareils n'est collectée
Liste des périphériques de filtrage des performances	Liste séparée par des virgules des identifiants d'appareils à inclure ou à exclure de la collecte des performances

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur contenant : CMUC00192E, CMUC00191E ou CMUC00190E	* Vérifiez les informations d'identification et l'adresse IP saisie. * Essayez de communiquer avec la baie via la console de gestion Web https://<ip>:8452/DS8000/Console. Remplacez <ip> par l'adresse IP configurée du collecteur de données.
Erreur : * Impossible d'exécuter le programme * Erreur lors de l'exécution de la commande	* Depuis l'unité d'acquisition Data Infrastructure Insights, ouvrez un CMD * Ouvrez le fichier CLI.CFG dans le répertoire/lib de base de la CLI et vérifiez la propriété JAVA_INSTALL, modifiez la valeur pour qu'elle corresponde à votre environnement * Affichez la version Java installée sur cette machine en tapant : « java -version » * Envoyez une requête ping à l'adresse IP du périphérique de stockage IBM spécifié dans la commande CLI émise. * Si tout ce qui précède a fonctionné correctement, exécutez manuellement une commande CLI

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données IBM SAN Volume Controller

Le collecteur de données IBM SAN Volume Controller (SVC) collecte les données d'inventaire et de performances à l'aide de SSH, prenant en charge une variété de périphériques exécutant le système d'exploitation SVC.

La liste des appareils pris en charge comprend des modèles tels que le SVC, le v7000, le v5000 et le v3700. Consultez la matrice de support de Data Infrastructure Insights pour connaître les modèles et les versions de micrologiciels pris en charge.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données IBM SVC. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante

utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Conduire	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Groupe Mdisk	Piscine de stockage
Disque virtuel	Volume
Disque M	LUN et chemins d'accès backend

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences en matière d'inventaire

- Adresse IP de chaque cluster SVC
- Port 22 disponible
- Nom d'utilisateur et mot de passe en lecture seule

Exigences de performance

- Console SVC, obligatoire pour tout cluster SVC et requise pour le package de base de découverte SVC.
- Les informations d'identification nécessiteront un niveau d'accès administratif uniquement pour copier les fichiers de performances des nœuds de cluster vers le nœud de configuration.
- Activez la collecte de données en vous connectant au cluster SVC via SSH et en exécutant : *svctask startstats -interval 1*

  Remarque : vous pouvez également activer la collecte de données à l'aide de l'interface utilisateur de gestion SVC.

Configuration

Champ	Description
Adresses IP de cluster	Adresses IP ou noms de domaine complets du stockage SVC
Nom d'utilisateur d'inventaire	Nom d'utilisateur pour l'interface de ligne de commande SVC
Mot de passe d'inventaire	Mot de passe pour l'interface de ligne de commande SVC

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 40 minutes.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.
Pour nettoyer les fichiers de statistiques vidés	Cochez cette case pour nettoyer les fichiers de statistiques vidés

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème:	Essayez ceci:
Erreur : « La commande ne peut pas être lancée car elle n'a pas été exécutée sur le nœud de configuration. »	La commande doit être exécutée sur le nœud de configuration.

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème:	Essayez ceci:
Erreur : « La commande ne peut pas être lancée car elle n'a pas été exécutée sur le nœud de configuration. »	La commande doit être exécutée sur le nœud de configuration.

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données IBM XIV/A9000

Le collecteur de données IBM XIV et A9000 (CLI) utilise l'interface de ligne de commande XIV pour collecter les données d'inventaire tandis que la collecte des performances est réalisée en effectuant des appels SMI-S vers la matrice XIV/A9000, qui exécute un fournisseur SMI-S sur le port 7778.

Terminologie

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Système de stockage	Stockage
Piscine de stockage	Piscine de stockage
Volume	Volume

Exigences

Les exigences suivantes doivent être remplies pour configurer et utiliser ce collecteur de données :

- Exigence de port : port TCP 7778
- Nom d'utilisateur et mot de passe en lecture seule
- La CLI XIV doit être installée sur l'AU

Exigences de performance

Les exigences suivantes sont requises pour la collecte des performances :

- Agent SMI-S 1.4 ou supérieur
- Service CIM compatible SMI-S exécuté sur une baie. La plupart des baies XIV ont un CIMServer installé par défaut.
- La connexion utilisateur doit être fournie pour le CIMServer. La connexion doit avoir un accès en lecture complète à la configuration et aux propriétés du tableau.
- Espace de noms SMI-S. La valeur par défaut est root/ibm. Ceci est configurable dans le CIMServer.
- Exigences de port : 5988 pour HTTP, 5989 pour HTTPS.
- Consultez le lien suivant pour savoir comment créer un compte pour la collecte des performances SMI-S : https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Configuration

Champ	Description
XIV Adresse IP	Adresse IP ou nom de domaine complet du stockage XIV
Nom d'utilisateur	Nom d'utilisateur pour le stockage XIV
Mot de passe	Mot de passe pour le stockage XIV
Chemin d'accès complet au répertoire XIV CLI	Chemin complet vers le dossier contenant la CLI XIV
Adresse IP de l'hôte SMI-S	Adresse IP de l'hôte SMI-S

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 40 minutes.
Protocole SMI-S	Protocole utilisé pour se connecter au fournisseur SMI-S. Affiche également le port par défaut.
Remplacer le port SMI-S	Si vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Nom d'utilisateur	Nom d'utilisateur pour l'hôte du fournisseur SMI-S
Mot de passe	Mot de passe pour l'hôte du fournisseur SMI-S
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Lenovo

Data Infrastructure Insights utilise le collecteur de données Lenovo pour découvrir les données d'inventaire et de performances des systèmes de stockage Lenovo HX.

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Adresse IP externe de Prism
- Nom d'utilisateur et mot de passe de l'administrateur
- Exigence de port TCP : 9440

Configuration

Champ	Description
Adresse IP externe de Prism	L'adresse IP des services de données externes pour le cluster
Nom d'utilisateur	Nom d'utilisateur pour le compte administrateur
Mot de passe	Mot de passe pour le compte administrateur

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter au tableau. La valeur par défaut est 9440.
Intervalle d'interrogation de l'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Microsoft

Configuration du collecteur de données Azure NetApp Files

Data Infrastructure Insights utilise le collecteur de données Azure NetApp Files pour acquérir des données d'inventaire et de performances.

Exigences

Vous avez besoin des informations suivantes pour configurer ce collecteur de données.

- Exigence de port : 443 HTTPS
- IP REST de gestion Azure (management.azure.com)
- ID client du principal du service Azure (compte d'utilisateur)
- Clé d'authentification du principal du service Azure (mot de passe utilisateur)
- Vous devez configurer un compte Azure pour la découverte de Data Infrastructure Insights .

  Une fois le compte correctement configuré et l'application enregistrée dans Azure, vous disposerez des informations d'identification requises pour découvrir l'instance Azure avec Data Infrastructure Insights. Le lien suivant décrit comment configurer le compte pour la découverte :

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configuration

Saisissez les données dans les champs du collecteur de données conformément au tableau ci-dessous :

Champ	Description
ID client du principal du service Azure	ID de connexion à Azure
ID de locataire Azure	ID de locataire Azure
Clé d'authentification du principal du service Azure	Clé d'authentification de connexion
Je comprends que Microsoft me facture les demandes d'API	Cochez cette case pour vérifier que vous avez bien compris que Microsoft vous facture les demandes d'API effectuées par le sondage Insight.

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60

Dépannage

- Les informations d'identification utilisées par votre collecteur de données ANF doivent avoir accès à tous les abonnements Azure contenant des volumes ANF.
- Si l'accès du lecteur entraîne l'échec de la collecte des performances, essayez d'accorder l'accès du contributeur au niveau du groupe de ressources.

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Microsoft Hyper-V

Le collecteur de données Microsoft Hyper-V acquiert les données d'inventaire et de performances de l'environnement informatique du serveur virtualisé. Ce collecteur de données peut découvrir un hôte Hyper-V autonome ou un cluster entier : créez un

collecteur par hôte ou cluster autonome.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir de Microsoft Hyper-V (WMI). Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque dur virtuel	Disque virtuel
Hôte	Hôte
Machine virtuelle	Machine virtuelle
Volumes partagés en cluster (CSV), volume de partition	Magasin de données
Périphérique SCSI Internet, LUN SCSI multi-chemins	LUN
Port Fibre Channel	Port

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les éléments suivants sont requis pour configurer ce collecteur de données :

- Hyper-V nécessite que le port 5985 soit ouvert pour la collecte de données et l'accès/la gestion à distance.
- Adresse IP ou FQDN du cluster ou de l'hyperviseur autonome. L'utilisation du nom d'hôte ou de l'adresse IP du cluster flottant est probablement l'approche la plus fiable par rapport au fait de pointer le collecteur vers un seul nœud spécifique d'un cluster.
- Compte utilisateur de niveau administratif qui fonctionne sur tous les hyperviseurs du cluster.
- WinRM doit être activé et à l'écoute sur tous les hyperviseurs
- Configuration requise pour le port : port 135 via WMI et ports TCP dynamiques attribués 1024-65535 pour Windows 2003 et versions antérieures et 49152-65535 pour Windows 2008.
- La résolution DNS doit réussir, même si le collecteur de données est dirigé uniquement vers une adresse IP
- Chaque hyperviseur Hyper-V doit avoir la « Mesure des ressources » activée pour chaque machine virtuelle, sur chaque hôte. Cela permet à chaque hyperviseur de disposer de plus de données disponibles pour Data Infrastructure Insights sur chaque invité. Si cette option n'est pas définie, moins de mesures de performances sont acquises pour chaque invité. Vous trouverez plus d'informations sur la mesure des ressources dans la documentation Microsoft :

  "Présentation de la mesure des ressources Hyper-V"

  "Activer-VMResourceMetering"

Le collecteur de données Hyper-V nécessite une unité d'acquisition Windows.

Configuration

Champ	Description
Adresse IP du cluster ou nom de domaine complet du cluster flottant	L'adresse IP ou le nom de domaine complet du cluster, ou d'un hyperviseur autonome non clusterisé
Nom d'utilisateur	Nom d'utilisateur administrateur de l'hyperviseur
Mot de passe	Mot de passe pour l'hyperviseur
Suffixe de domaine DNS	Le suffixe du nom d'hôte qui se combine avec le nom d'hôte simple pour restituer le FQDN d'un hyperviseur

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 20 minutes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

NetApp

Collecteur de données NetApp Cloud Volumes ONTAP

Ce collecteur de données prend en charge la collecte d'inventaire à partir des configurations Cloud Volumes ONTAP .

Configuration

Champ	Description
Adresse IP de gestion NetApp	Adresse IP pour Cloud Volumens ONTAP
Nom d'utilisateur	Nom d'utilisateur pour Cloud Volumes ONTAP
Mot de passe	Mot de passe pour l'utilisateur ci-dessus

Configuration avancée

Champ	Description
Type de connexion	HTTPS recommandé. Affiche également le port par défaut.
Remplacer le port de communication	Port à utiliser s'il n'est pas par défaut.
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60 minutes.
Nombre de threads simultanés d'inventaire	Nombre de threads simultanés.
Forcer TLS pour HTTPS	Forcer TLS sur HTTPS
Rechercher automatiquement les groupes réseau	Rechercher automatiquement les groupes réseau

Champ	Description
Extension du groupe Netgroup	Sélectionnez Shell ou Fichier
Délai d'expiration de lecture HTTP secondes	La valeur par défaut est de 30 secondes
Réponses de force en UTF-8	Réponses de force en UTF-8
Intervalle de sondage des performances (min)	La valeur par défaut est 900 secondes.
Nombre de threads simultanés de performances	Nombre de threads simultanés.
Collecte avancée de données de compteur	Cochez cette case pour que Data Infrastructure Insights collecte les mesures avancées de la liste ci-dessous.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données NetApp ONTAP AFX

Ce collecteur de données acquiert l'inventaire, les journaux EMS et les données de performances des systèmes de stockage exécutant ONTAP 9.16.0 et versions ultérieures à l'aide d'appels d'API REST.

Exigences

Les exigences suivantes sont requises pour configurer et utiliser ce collecteur de données :

- Vous devez avoir accès à un compte utilisateur avec le niveau d'accès requis. Notez que les autorisations d'administrateur sont requises lors de la création d'un nouvel utilisateur/rôle REST.
  - Sur le plan fonctionnel, Data Infrastructure Insights effectue principalement des demandes de lecture, mais certaines autorisations d'écriture sont requises pour que Data Infrastructure Insights s'enregistre auprès du tableau ONTAP . Voir la *Remarque sur les autorisations* immédiatement ci-dessous.
- ONTAP version 9.16.0 ou supérieure.
- Exigences du port : 443

Remarque sur les autorisations

Étant donné qu'un certain nombre de tableaux de bord ONTAP de Data Infrastructure Insights s'appuient sur des compteurs ONTAP avancés, vous devez conserver l'option **Activer la collecte de données de compteur avancé** activée dans la section Configuration avancée du collecteur de données.

Pour créer un compte local pour Data Infrastructure Insights au niveau du cluster, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP :

1. Avant de commencer, vous devez être connecté à ONTAP avec un compte *Administrateur* et les *commandes de niveau diagnostic* doivent être activées.
2. Récupérer le nom du vserver qui est de type *admin*. Vous utiliserez ce nom dans les commandes suivantes.

```
 vserver show -type admin
. Créez un rôle à l'aide des commandes suivantes :
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Créez l'utilisateur en lecture seule à l'aide de la commande suivante. Une fois la commande de création exécutée, vous serez invité à saisir un mot de passe pour cet utilisateur.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Si un compte AD/LDAP est utilisé, la commande doit être

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Le rôle et la connexion utilisateur résultants ressembleront à ce qui
suit.  Votre sortie réelle peut varier :
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migration

Pour migrer d'un ancien collecteur de données ONTAP (ontapi) vers le nouveau collecteur ONTAP REST, procédez comme suit :

1. Ajoutez le collecteur REST. Il est recommandé de saisir les informations d'un utilisateur différent de celui configuré pour le collecteur précédent. Par exemple, utilisez l'utilisateur indiqué dans la section Autorisations ci-dessus.
2. Mettez en pause le collecteur précédent afin qu'il ne continue pas à collecter des données.
3. Laissez le nouveau collecteur REST acquérir des données pendant au moins 30 minutes. Ignorez toutes les données pendant cette période qui ne semblent pas « normales ».
4. Après la période de repos, vous devriez voir vos données se stabiliser à mesure que le collecteur REST continue d'acquérir.

Vous pouvez utiliser ce même processus pour revenir au collecteur précédent, si vous le souhaitez.

Configuration

Champ	Description
Adresse IP de gestion ONTAP	Adresse IP ou nom de domaine complet du cluster NetApp . Doit être l'adresse IP/FQDN de gestion de cluster.
Nom d'utilisateur ONTAP REST	Nom d'utilisateur pour le cluster NetApp
Mot de passe ONTAP REST	Mot de passe pour le cluster NetApp

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 60 secondes.
Collecte avancée de données de compteur	Sélectionnez cette option pour inclure les données du compteur avancé ONTAP dans les sondages. Activé par défaut.
Activer la collecte d'événements EMS	Sélectionnez cette option pour inclure les données d'événements du journal ONTAP EMS. Activé par défaut.
Intervalle d'interrogation EMS (sec)	La valeur par défaut est de 60 secondes.

Terminologie

Data Infrastructure Insights acquiert les données d'inventaire, de journaux et de performances du collecteur de données ONTAP . Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Cluster	Stockage
Nœud	Nœud de stockage
Volume/ FlexVol/ FlexGroup	Volume interne
Qtree/FlexTree	Qtree (type : Explixit/Par défaut)
Godet S3	Qtree (type : Bucket)
StoragePod/StorageAvailabilityZone	Pool de stockage
Partager	Partager
Quota	Quota
SVM (machine virtuelle de stockage)	Machine virtuelle de stockage

Terminologie de la gestion des données ONTAP

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources de stockage ONTAP Data Management. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – Une liste délimitée par des virgules des noms de modèles de nœuds uniques et discrets au sein de ce cluster. Si tous les nœuds des clusters sont du même type de modèle, un seul nom de modèle apparaîtra.
- Fournisseur – même nom de fournisseur que vous verriez si vous configuriez une nouvelle source de données.

- Numéro de série – L'UUID du tableau
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données.
- Version du microcode – firmware.
- Capacité brute – somme de base 2 de tous les disques physiques du système, quel que soit leur rôle.
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes internes individuels.
- Débit – agrégé à partir de volumes internes. Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire.

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire.
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Agrégat » ou de « Groupe RAID ».
- Nœud – si l'architecture de cette baie de stockage est telle que les pools appartiennent à un nœud de stockage spécifique, son nom sera vu ici comme un lien hypertexte vers sa propre page de destination.
- Utilise Flash Pool – Valeur Oui/Non – ce pool basé sur SATA/SAS dispose-t-il de SSD utilisés pour l'accélération de la mise en cache ?
- Redondance – Niveau RAID ou schéma de protection. RAID_DP est à double parité, RAID_TP est à triple parité.
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs.
- Capacité surengagée – Si, en utilisant des technologies d'efficacité, vous avez alloué une somme totale de capacités de volume ou de volume interne supérieure à la capacité logique du pool de stockage, la valeur de pourcentage ici sera supérieure à 0 %.
- Instantané – capacités d'instantané utilisées et totales, si votre architecture de pool de stockage consacre une partie de sa capacité aux zones de segments exclusivement pour les instantanés. Les configurations ONTAP dans MetroCluster sont susceptibles de présenter ce problème, tandis que d'autres configurations ONTAP le sont moins.
- Utilisation – une valeur en pourcentage indiquant le pourcentage d'occupation de disque le plus élevé de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'a pas nécessairement une forte corrélation avec les performances de la baie : l'utilisation peut être élevée en raison des reconstructions de disque, des activités de déduplication, etc. en l'absence de charges de travail pilotées par l'hôte. De plus, de nombreuses implémentations de réplication de baies peuvent entraîner une utilisation du disque sans apparaître comme volume interne ou charge de travail de volume.
- IOPS – la somme des IOPS de tous les disques contribuant à la capacité de ce pool de stockage. Débit – le débit total de tous les disques contribuant à la capacité de ce pool de stockage.

Nœud de stockage

- Stockage – à quelle baie de stockage ce nœud fait partie. Obligatoire.
- Partenaire HA – sur les plateformes où un nœud bascule vers un et un seul autre nœud, il sera généralement visible ici.
- État – santé du nœud. Disponible uniquement lorsque le tableau est suffisamment sain pour être inventorié

par une source de données.

- Modèle – nom du modèle du nœud.
- Version – nom de la version de l'appareil.
- Numéro de série – Le numéro de série du nœud.
- Mémoire – mémoire de base 2 si disponible.
- Utilisation – Sur ONTAP, il s'agit d'un indice de stress du contrôleur issu d'un algorithme propriétaire. À chaque sondage de performances, un nombre compris entre 0 et 100 % sera signalé, correspondant au plus élevé des deux facteurs suivants : la contention du disque WAFL ou l'utilisation moyenne du processeur. Si vous observez des valeurs soutenues > 50 %, cela indique un sous-dimensionnement : potentiellement un contrôleur/nœud pas assez grand ou pas assez de disques rotatifs pour absorber la charge de travail d'écriture.
- IOPS – Dérivé directement des appels ONTAP REST sur l'objet nœud.
- Latence – Dérivée directement des appels ONTAP REST sur l'objet nœud.
- Débit – Dérivé directement des appels ONTAP REST sur l'objet nœud.
- Processeurs – Nombre de CPU.

Mesures de puissance ONTAP

Plusieurs modèles ONTAP fournissent des mesures de puissance pour Data Infrastructure Insights qui peuvent être utilisées pour la surveillance ou l'alerte. Les listes de modèles pris en charge et non pris en charge ci-dessous ne sont pas exhaustives mais devraient fournir quelques indications ; en général, si un modèle appartient à la même famille qu'un modèle de la liste, la prise en charge doit être la même.

Modèles pris en charge :

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modèles non pris en charge :

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème:	Essayez ceci:
Lors de la tentative de création d'un collecteur de données ONTAP REST, une erreur semblable à la suivante s'affiche : Configuration : 10.193.70.14 : l'API REST ONTAP à 10.193.70.14 n'est pas disponible : 10.193.70.14 n'a pas pu obtenir /api/cluster : 400 Mauvaise requête	Cela est probablement dû à un ancien tableau ONTAP) par exemple, ONTAP 9.6) qui n'a pas de capacités d'API REST. ONTAP 9.14.1 est la version ONTAP minimale prise en charge par le collecteur ONTAP REST. Les réponses « 400 Bad Request » doivent être attendues sur les versions antérieures à REST ONTAP . Pour les versions ONTAP qui prennent en charge REST mais qui ne sont pas 9.14.1 ou ultérieures, vous pouvez voir le message similaire suivant : Configuration : 10.193.98.84 : l'API REST ONTAP à 10.193.98.84 n'est pas disponible : 10.193.98.84 : l'API REST ONTAP à 10.193.98.84 est disponible : cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 mais n'est pas de version minimale 9.14.1.
Je vois des métriques vides ou « 0 » là où le collecteur ONTAP ontapi affiche des données.	ONTAP REST ne signale pas les métriques utilisées en interne sur le système ONTAP uniquement. Par exemple, les agrégats système ne seront pas collectés par ONTAP REST, seuls les SVM de type « données » seront collectés. Autres exemples de mesures ONTAP REST qui peuvent signaler des données nulles ou vides : InternalVolumes : REST ne signale plus vol0. Agrégats : REST ne signale plus aggr0. Stockage : la plupart des mesures sont une combinaison des mesures de volume interne et seront affectées par ce qui précède. Machines virtuelles de stockage : REST ne signale plus les SVM de type autre que « données » (par exemple, « cluster », « mgmt », « nœud »). Vous remarquerez peut-être également un changement dans l'apparence des graphiques contenant des données, en raison du changement de la période d'interrogation des performances par défaut de 15 minutes à 5 minutes. Des sondages plus fréquents signifient plus de points de données à tracer.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données NetApp ONTAP ASA r2 (All-SAN Array)

Ce collecteur de données acquiert l'inventaire, les journaux EMS et les données de performances des systèmes de stockage exécutant ONTAP 9.16.0 et versions ultérieures à l'aide d'appels d'API REST.

Exigences

Les exigences suivantes sont requises pour configurer et utiliser ce collecteur de données :

- Vous devez avoir accès à un compte utilisateur avec le niveau d'accès requis. Notez que les autorisations d'administrateur sont requises lors de la création d'un nouvel utilisateur/rôle REST.

    - Sur le plan fonctionnel, Data Infrastructure Insights effectue principalement des demandes de lecture, mais certaines autorisations d'écriture sont requises pour que Data Infrastructure Insights s'enregistre auprès du tableau ONTAP . Voir la *Remarque sur les autorisations* immédiatement ci-dessous.
- ONTAP version 9.16.0 ou supérieure.
- Exigences du port : 443

ASA R2 désigne les modèles de dernière génération de la plate-forme de stockage ONTAP ASA . Cela inclut les modèles de matrice ASA A1K, A90, A70, A50, A30 et A20.

Pour tous les systèmes ASA de génération précédente, veuillez utiliser le"RESTE ONTAP" collectionneur.

Remarque sur les autorisations

Étant donné qu'un certain nombre de tableaux de bord ONTAP de Data Infrastructure Insights s'appuient sur des compteurs ONTAP avancés, vous devez conserver l'option **Activer la collecte de données de compteur avancé** activée dans la section Configuration avancée du collecteur de données.

Pour créer un compte local pour Data Infrastructure Insights au niveau du cluster, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP :

1. Avant de commencer, vous devez être connecté à ONTAP avec un compte *Administrateur* et les *commandes de niveau diagnostic* doivent être activées.
2. Récupérer le nom du vserver qui est de type *admin*. Vous utiliserez ce nom dans les commandes suivantes.

```
 vserver show -type admin
. Créez un rôle à l'aide des commandes suivantes :
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Créez l'utilisateur en lecture seule à l'aide de la commande suivante. Une fois la commande de création exécutée, vous serez invité à saisir un mot de passe pour cet utilisateur.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Si un compte AD/LDAP est utilisé, la commande doit être

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Le rôle et la connexion utilisateur résultants ressembleront à ce qui
suit.  Votre sortie réelle peut varier :
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migration

Pour migrer d'un ancien collecteur de données ONTAP (ontapi) vers le nouveau collecteur ONTAP REST, procédez comme suit :

1. Ajoutez le collecteur REST. Il est recommandé de saisir les informations d'un utilisateur différent de celui configuré pour le collecteur précédent. Par exemple, utilisez l'utilisateur indiqué dans la section Autorisations ci-dessus.
2. Mettez en pause le collecteur précédent afin qu'il ne continue pas à collecter des données.
3. Laissez le nouveau collecteur REST acquérir des données pendant au moins 30 minutes. Ignorez toutes les données pendant cette période qui ne semblent pas « normales ».
4. Après la période de repos, vous devriez voir vos données se stabiliser à mesure que le collecteur REST continue d'acquérir.

Vous pouvez utiliser ce même processus pour revenir au collecteur précédent, si vous le souhaitez.

Configuration

Champ	Description
Adresse IP de gestion ONTAP	Adresse IP ou nom de domaine complet du cluster NetApp . Doit être l'adresse IP/FQDN de gestion de cluster.
Nom d'utilisateur ONTAP REST	Nom d'utilisateur pour le cluster NetApp
Mot de passe ONTAP REST	Mot de passe pour le cluster NetApp

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 60 secondes.
Collecte avancée de données de compteur	Sélectionnez cette option pour inclure les données du compteur avancé ONTAP dans les sondages. Activé par défaut.
Activer la collecte d'événements EMS	Sélectionnez cette option pour inclure les données d'événements du journal ONTAP EMS. Activé par défaut.
Intervalle d'interrogation EMS (sec)	La valeur par défaut est de 60 secondes.

Terminologie

Data Infrastructure Insights acquiert les données d'inventaire, de journaux et de performances du collecteur de données ONTAP . Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de raid	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
Agrégat	Piscine de stockage
LUN	Volume
Volume	Volume interne
Machine virtuelle de stockage/serveur virtuel	Machine virtuelle de stockage

Terminologie de la gestion des données ONTAP

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources de stockage ONTAP Data Management. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – Une liste délimitée par des virgules des noms de modèles de nœuds uniques et discrets au sein de ce cluster. Si tous les nœuds des clusters sont du même type de modèle, un seul nom de modèle apparaîtra.
- Fournisseur – même nom de fournisseur que vous verriez si vous configuriez une nouvelle source de données.
- Numéro de série – L'UUID du tableau
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données.
- Version du microcode – firmware.
- Capacité brute – somme de base 2 de tous les disques physiques du système, quel que soit leur rôle.
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes internes individuels.
- Débit – agrégé à partir de volumes internes. Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire.

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire.
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Agrégat » ou de « Groupe RAID ».
- Nœud – si l'architecture de cette baie de stockage est telle que les pools appartiennent à un nœud de stockage spécifique, son nom sera vu ici comme un lien hypertexte vers sa propre page de destination.
- Utilise Flash Pool – Valeur Oui/Non – ce pool basé sur SATA/SAS dispose-t-il de SSD utilisés pour l'accélération de la mise en cache ?
- Redondance – Niveau RAID ou schéma de protection. RAID_DP est à double parité, RAID_TP est à triple parité.
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs.
- Capacité surengagée – Si, en utilisant des technologies d'efficacité, vous avez alloué une somme totale de capacités de volume ou de volume interne supérieure à la capacité logique du pool de stockage, la valeur de pourcentage ici sera supérieure à 0 %.
- Instantané – capacités d'instantané utilisées et totales, si votre architecture de pool de stockage consacre une partie de sa capacité aux zones de segments exclusivement pour les instantanés. Les configurations ONTAP dans MetroCluster sont susceptibles de présenter ce problème, tandis que d'autres configurations ONTAP le sont moins.
- Utilisation – une valeur en pourcentage indiquant le pourcentage d'occupation de disque le plus élevé de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'a pas nécessairement une forte corrélation avec les performances de la baie : l'utilisation peut être élevée en raison des reconstructions de disque, des activités de déduplication, etc. en l'absence de charges de travail pilotées par l'hôte. De plus, de nombreuses implémentations de réplication de baies peuvent entraîner une utilisation du disque sans apparaître comme volume interne ou charge de travail de volume.
- IOPS – la somme des IOPS de tous les disques contribuant à la capacité de ce pool de stockage. Débit – le débit total de tous les disques contribuant à la capacité de ce pool de stockage.

Nœud de stockage

- Stockage – à quelle baie de stockage ce nœud fait partie. Obligatoire.
- Partenaire HA – sur les plateformes où un nœud bascule vers un et un seul autre nœud, il sera généralement visible ici.
- État – santé du nœud. Disponible uniquement lorsque le tableau est suffisamment sain pour être inventorié par une source de données.
- Modèle – nom du modèle du nœud.
- Version – nom de la version de l'appareil.
- Numéro de série – Le numéro de série du nœud.
- Mémoire – mémoire de base 2 si disponible.
- Utilisation – Sur ONTAP, il s'agit d'un indice de stress du contrôleur issu d'un algorithme propriétaire. À chaque sondage de performances, un nombre compris entre 0 et 100 % sera signalé, correspondant au plus élevé des deux facteurs suivants : la contention du disque WAFL ou l'utilisation moyenne du processeur. Si vous observez des valeurs soutenues > 50 %, cela indique un sous-dimensionnement : potentiellement un contrôleur/nœud pas assez grand ou pas assez de disques rotatifs pour absorber la charge de travail d'écriture.
- IOPS – Dérivé directement des appels ONTAP REST sur l'objet nœud.
- Latence – Dérivée directement des appels ONTAP REST sur l'objet nœud.
- Débit – Dérivé directement des appels ONTAP REST sur l'objet nœud.
- Processeurs – Nombre de CPU.

Mesures de puissance ONTAP

Plusieurs modèles ONTAP fournissent des mesures de puissance pour Data Infrastructure Insights qui peuvent être utilisées pour la surveillance ou l'alerte. Les listes de modèles pris en charge et non pris en charge ci-dessous ne sont pas exhaustives mais devraient fournir quelques indications ; en général, si un modèle appartient à la même famille qu'un modèle de la liste, la prise en charge doit être la même.

Modèles pris en charge :

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modèles non pris en charge :

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème:	Essayez ceci:
Lors de la tentative de création d'un collecteur de données ONTAP REST, une erreur semblable à la suivante s'affiche : Configuration : 10.193.70.14 : l'API REST ONTAP à 10.193.70.14 n'est pas disponible : 10.193.70.14 n'a pas pu obtenir /api/cluster : 400 Mauvaise requête	Cela est probablement dû à un ancien tableau ONTAP) par exemple, ONTAP 9.6) qui n'a pas de capacités d'API REST. ONTAP 9.14.1 est la version ONTAP minimale prise en charge par le collecteur ONTAP REST. Les réponses « 400 Bad Request » doivent être attendues sur les versions antérieures à REST ONTAP . Pour les versions ONTAP qui prennent en charge REST mais qui ne sont pas 9.14.1 ou ultérieures, vous pouvez voir le message similaire suivant : Configuration : 10.193.98.84 : l'API REST ONTAP à 10.193.98.84 n'est pas disponible : 10.193.98.84 : l'API REST ONTAP à 10.193.98.84 est disponible : cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 mais n'est pas de version minimale 9.14.1.
Je vois des métriques vides ou « 0 » là où le collecteur ONTAP ontapi affiche des données.	ONTAP REST ne signale pas les métriques utilisées en interne sur le système ONTAP uniquement. Par exemple, les agrégats système ne seront pas collectés par ONTAP REST, seuls les SVM de type « données » seront collectés. Autres exemples de mesures ONTAP REST qui peuvent signaler des données nulles ou vides : InternalVolumes : REST ne signale plus vol0. Agrégats : REST ne signale plus aggr0. Stockage : la plupart des mesures sont une combinaison des mesures de volume interne et seront affectées par ce qui précède. Machines virtuelles de stockage : REST ne signale plus les SVM de type autre que « données » (par exemple, « cluster », « mgmt », « nœud »). Vous remarquerez peut-être également un changement dans l'apparence des graphiques contenant des données, en raison du changement de la période d'interrogation des performances par défaut de 15 minutes à 5 minutes. Des sondages plus fréquents signifient plus de points de données à tracer.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données du logiciel de gestion des données NetApp ONTAP

Ce collecteur de données acquiert des données d'inventaire et de performances à partir de systèmes de stockage exécutant ONTAP à l'aide d'appels API en lecture seule à partir d'un compte ONTAP . Ce collecteur de données crée également un enregistrement dans le registre des applications du cluster pour accélérer le support.

Terminologie

Data Infrastructure Insights acquiert les données d'inventaire et de performances du collecteur de données ONTAP . Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de raid	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
Agrégat	Piscine de stockage
LUN	Volume
Volume	Volume interne

Terminologie de la gestion des données ONTAP

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources de stockage ONTAP Data Management. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – Une liste délimitée par des virgules des noms de modèles de nœuds uniques et discrets au sein de ce cluster. Si tous les nœuds des clusters sont du même type de modèle, un seul nom de modèle apparaîtra.
- Fournisseur – même nom de fournisseur que vous verriez si vous configuriez une nouvelle source de données.
- Numéro de série – Le numéro de série de la matrice. Sur les systèmes de stockage d'architecture en cluster comme ONTAP Data Management, ce numéro de série peut être moins utile que les numéros de série individuels des « nœuds de stockage ».
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données.
- Version du microcode – firmware.
- Capacité brute – somme de base 2 de tous les disques physiques du système, quel que soit leur rôle.
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes internes individuels.
- Débit – agrégé à partir de volumes internes. Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire.

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire.
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Agrégat » ou de « Groupe RAID ».
- Nœud – si l'architecture de cette baie de stockage est telle que les pools appartiennent à un nœud de stockage spécifique, son nom sera vu ici comme un lien hypertexte vers sa propre page de destination.
- Utilise Flash Pool – Valeur Oui/Non – ce pool basé sur SATA/SAS dispose-t-il de SSD utilisés pour l'accélération de la mise en cache ?

- Redondance – Niveau RAID ou schéma de protection. RAID_DP est à double parité, RAID_TP est à triple parité.
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs.
- Capacité surengagée – Si, en utilisant des technologies d'efficacité, vous avez alloué une somme totale de capacités de volume ou de volume interne supérieure à la capacité logique du pool de stockage, la valeur de pourcentage ici sera supérieure à 0 %.
- Instantané – capacités d'instantané utilisées et totales, si votre architecture de pool de stockage consacre une partie de sa capacité aux zones de segments exclusivement pour les instantanés. Les configurations ONTAP dans MetroCluster sont susceptibles de présenter ce problème, tandis que d'autres configurations ONTAP le sont moins.
- Utilisation – une valeur en pourcentage indiquant le pourcentage d'occupation de disque le plus élevé de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'a pas nécessairement une forte corrélation avec les performances de la baie : l'utilisation peut être élevée en raison des reconstructions de disque, des activités de déduplication, etc. en l'absence de charges de travail pilotées par l'hôte. De plus, de nombreuses implémentations de réplication de baies peuvent entraîner une utilisation du disque sans apparaître comme volume interne ou charge de travail de volume.
- IOPS – la somme des IOPS de tous les disques contribuant à la capacité de ce pool de stockage. Débit – le débit total de tous les disques contribuant à la capacité de ce pool de stockage.

Nœud de stockage

- Stockage – à quelle baie de stockage ce nœud fait partie. Obligatoire.
- Partenaire HA – sur les plateformes où un nœud bascule vers un et un seul autre nœud, il sera généralement visible ici.
- État – santé du nœud. Disponible uniquement lorsque le tableau est suffisamment sain pour être inventorié par une source de données.
- Modèle – nom du modèle du nœud.
- Version – nom de la version de l'appareil.
- Numéro de série – Le numéro de série du nœud.
- Mémoire – mémoire de base 2 si disponible.
- Utilisation – Sur ONTAP, il s'agit d'un indice de stress du contrôleur issu d'un algorithme propriétaire. À chaque sondage de performances, un nombre compris entre 0 et 100 % sera signalé, correspondant au plus élevé des deux facteurs suivants : la contention du disque WAFL ou l'utilisation moyenne du processeur. Si vous observez des valeurs soutenues > 50 %, cela indique un sous-dimensionnement : potentiellement un contrôleur/nœud pas assez grand ou pas assez de disques rotatifs pour absorber la charge de travail d'écriture.
- IOPS – Dérivé directement des appels ONTAP ZAPI sur l'objet nœud.
- Latence – Dérivée directement des appels ONTAP ZAPI sur l'objet nœud.
- Débit – Dérivé directement des appels ONTAP ZAPI sur l'objet nœud.
- Processeurs – Nombre de CPU.

Exigences

Les exigences suivantes sont requises pour configurer et utiliser ce collecteur de données :

- Vous devez avoir accès à un compte administrateur configuré pour les appels API en lecture seule.

- Les détails du compte incluent le nom d'utilisateur et le mot de passe.
- Exigences de port : 80 ou 443
- Autorisations du compte :
  - Nom de rôle en lecture seule pour l'application ontapi sur le Vserver par défaut
  - Vous pourriez avoir besoin d'autorisations d'écriture facultatives supplémentaires. Voir la note sur les autorisations ci-dessous.
- Conditions requises pour la licence ONTAP :
  - Licence FCP et volumes mappés/masqués requis pour la découverte Fibre Channel

Exigences d'autorisation pour la collecte des métriques de commutation ONTAP

Data Infrastructure Insights a la capacité de collecter des données de commutation de cluster ONTAP en tant qu'option dans le collecteurConfiguration avancée paramètres. En plus d'activer cette fonctionnalité sur le collecteur Data Infrastructure Insights , vous devez également *configurer le système ONTAP * lui-même pour fournir"informations sur le commutateur" , et assurer le bonautorisations sont définis afin de permettre l'envoi des données du commutateur à Data Infrastructure Insights.

Configuration

Champ	Description
IP de gestion NetApp	Adresse IP ou nom de domaine complet du cluster NetApp
Nom d'utilisateur	Nom d'utilisateur pour le cluster NetApp
Mot de passe	Mot de passe pour le cluster NetApp

Configuration avancée

Champ	Description
Type de connexion	Choisissez HTTP (port par défaut 80) ou HTTPS (port par défaut 443). La valeur par défaut est HTTPS
Remplacer le port de communication	Spécifiez un port différent si vous ne souhaitez pas utiliser le port par défaut
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60 minutes.
Pour TLS pour HTTPS	Autoriser TLS comme protocole uniquement lors de l'utilisation de HTTPS
Rechercher automatiquement les groupes réseau	Activer les recherches automatiques de groupes réseau pour les règles de politique d'exportation
Extension du groupe Netgroup	Stratégie d'expansion de Netgroup. Choisissez *fichier* ou *shell*. La valeur par défaut est *shell*.
Délai d'expiration de lecture HTTP secondes	La valeur par défaut est 30
Réponses de force en UTF-8	Force le code du collecteur de données à interpréter les réponses de la CLI comme étant en UTF-8
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 900 secondes.

Champ	Description
Collecte avancée de données de compteur	Activer l'intégration ONTAP . Sélectionnez cette option pour inclure les données du compteur avancé ONTAP dans les sondages. Choisissez les compteurs souhaités dans la liste.
Mesures de commutation de cluster	Autoriser Data Infrastructure Insights à collecter les données de commutation de cluster. Notez qu'en plus d'activer cette fonctionnalité du côté de Data Infrastructure Insights , vous devez également configurer le système ONTAP pour fournir"informations sur le commutateur" , et assurer le bonautorisations sont définis afin de permettre l'envoi des données du commutateur à Data Infrastructure Insights. Voir « Remarque sur les autorisations » ci-dessous.

Mesures de puissance ONTAP

Plusieurs modèles ONTAP fournissent des mesures de puissance pour Data Infrastructure Insights qui peuvent être utilisées pour la surveillance ou l'alerte.

Ces listes ne sont pas exhaustives et sont susceptibles d'être modifiées. En général, si un modèle appartient à la même famille qu'un modèle de la liste, le support devrait être le même, mais cela n'est pas garanti. Si vous n'êtes pas sûr que votre modèle prend en charge les mesures de puissance, contactez le support ONTAP .

Modèles pris en charge :

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modèles non pris en charge :

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Remarque sur les autorisations

Étant donné qu'un certain nombre de tableaux de bord ONTAP de Data Infrastructure Insights s'appuient sur des compteurs ONTAP avancés, vous devez activer la **Collecte de données de compteur avancée** dans la section Configuration avancée du collecteur de données.

Vous devez également vous assurer que l'autorisation d'écriture sur l'API ONTAP est activée. Cela nécessite généralement un compte au niveau du cluster avec les autorisations nécessaires.

Pour créer un compte local pour Data Infrastructure Insights au niveau du cluster, connectez-vous à ONTAP avec le nom d'utilisateur/mot de passe de l'administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP :

1. Avant de commencer, vous devez être connecté à ONTAP avec un compte *Administrateur* et les *commandes de niveau diagnostic* doivent être activées.
2. Créez un rôle en lecture seule à l'aide des commandes suivantes.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Créez l'utilisateur en lecture seule à l'aide de la commande suivante. Une fois la commande de création exécutée, vous serez invité à saisir un mot de passe pour cet utilisateur.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Si un compte AD/LDAP est utilisé, la commande doit être

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Si vous collectez des données de commutation de cluster :
```

```
security login rest-role create -role ci_readonly_rest -api
/api/network/ethernet -access readonly
security login create -user-or-group-name ci_user -application http
-authmethod password -role ci_readonly_rest
```

Le rôle et la connexion utilisateur résultants ressembleront à ce qui suit. Votre sortie réelle peut varier :

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------ --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1:security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Si le contrôle d'accès ONTAP n'est pas correctement défini, les appels REST de Data Infrastructure Insights peuvent échouer, ce qui entraîne des lacunes dans les données du périphérique. Par exemple, si vous l'avez activé sur le collecteur Data Infrastructure Insights mais que vous n'avez pas configuré les autorisations sur ONTAP, l'acquisition échouera. De plus, si le rôle est précédemment défini sur ONTAP et que vous ajoutez les capacités de l'API Rest, assurez-vous que *http* est ajouté au rôle.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Recevez une réponse HTTP 401 ou un code d'erreur ZAPI 13003 et ZAPI renvoie « Privilèges insuffisants » ou « non autorisé pour cette commande »	Vérifiez le nom d'utilisateur et le mot de passe, ainsi que les privilèges/autorisations de l'utilisateur.
La version du cluster est < 8.1	La version minimale prise en charge du cluster est 8.1. Effectuez une mise à niveau vers la version minimale prise en charge.
ZAPI renvoie « le rôle du cluster n'est pas cluster_mgmt LIF »	AU doit communiquer avec l'IP de gestion du cluster. Vérifiez l'IP et changez-la si nécessaire
Erreur : « Les filtres en mode 7 ne sont pas pris en charge »	Cela peut se produire si vous utilisez ce collecteur de données pour découvrir le filtre en mode 7. Modifiez l'IP pour qu'elle pointe vers le cluster cdot à la place.
La commande ZAPI échoue après une nouvelle tentative	AU a un problème de communication avec le cluster. Vérifiez le réseau, le numéro de port et l'adresse IP. L'utilisateur doit également essayer d'exécuter une commande à partir de la ligne de commande à partir de la machine AU.
AU n'a pas réussi à se connecter à ZAPI via HTTP	Vérifiez si le port ZAPI accepte le texte en clair. Si AU tente d'envoyer du texte en clair à un socket SSL, la communication échoue.
La communication échoue avec SSLException	AU tente d'envoyer SSL à un port en texte clair sur un fichier. Vérifiez si le port ZAPI accepte SSL ou utilisez un autre port.
Erreurs de connexion supplémentaires : la réponse ZAPI contient le code d'erreur 13001, « la base de données n'est pas ouverte ». Le code d'erreur ZAPI est 60 et la réponse contient « l'API ne s'est pas terminée à temps ». La réponse ZAPI contient « initialize_session() a renvoyé un environnement NULL ». Le code d'erreur ZAPI est 14007 et la réponse contient « le nœud n'est pas sain ».	Vérifiez le réseau, le numéro de port et l'adresse IP. L'utilisateur doit également essayer d'exécuter une commande à partir de la ligne de commande à partir de la machine AU.

Performances

Problème:	Essayez ceci:
Erreur « Échec de la collecte des performances à partir de ZAPI »	Cela est généralement dû au fait que les statistiques de performances ne fonctionnent pas. Essayez la commande suivante sur chaque nœud : > *system node systemshell -node * -command “spmctl -h cmd –stop; spmctl -h cmd –exec”*

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données NetApp ONTAP REST

Ce collecteur de données acquiert l’inventaire, les journaux EMS et les données de performances des systèmes de stockage exécutant ONTAP 9.14.1 et versions ultérieures à l’aide d’appels d’API REST. Pour les systèmes ONTAP sur les versions antérieures, utilisez le type de collecteur « NetApp ONTAP Data Management Software » basé sur ZAPI.

> Le collecteur ONTAP REST peut être utilisé en remplacement du collecteur précédent basé sur ONTAPI. Il peut donc y avoir des différences dans les mesures collectées ou rapportées. Pour plus d’informations sur les différences entre ONTAPI et REST, consultez le"Mappage ONTAP 9.14.1 ONTAPI vers REST" documentation.

Exigences

Les exigences suivantes sont requises pour configurer et utiliser ce collecteur de données :

- Vous devez avoir accès à un compte utilisateur avec le niveau d’accès requis. Notez que les autorisations d’administrateur sont requises lors de la création d’un nouvel utilisateur/rôle REST.
  - Sur le plan fonctionnel, Data Infrastructure Insights effectue principalement des demandes de lecture, mais certaines autorisations d’écriture sont requises pour que Data Infrastructure Insights s’enregistre auprès du tableau ONTAP . Voir la *Remarque sur les autorisations* immédiatement ci-dessous.
- ONTAP version 9.14.1 ou supérieure.
- Exigences du port : 443
- Notez que les métriques Fpolicy ne sont pas prises en charge dans le collecteur ONTAP REST (les collecteurs de données Workload Security utilisent les serveurs FPolicy et les métriques FPolicy vous permettent de surveiller l’activité de collecte de données Workload Security). Pour prendre en charge les mesures Fpolicy, utilisez le "Gestion des données ONTAP" collectionneur.

Remarque sur les autorisations

Étant donné qu’un certain nombre de tableaux de bord ONTAP de Data Infrastructure Insights s’appuient sur des compteurs ONTAP avancés, vous devez conserver l’option **Activer la collecte de données de compteur avancé** activée dans la section Configuration avancée du collecteur de données.

Pour créer un compte local pour Data Infrastructure Insights au niveau du cluster, connectez-vous à ONTAP avec le nom d’utilisateur/mot de passe de l’administrateur de gestion de cluster et exécutez les commandes suivantes sur le serveur ONTAP :

1. Avant de commencer, vous devez être connecté à ONTAP avec un compte *Administrateur* et les

commandes de niveau diagnostic doivent être activées.

2. Récupérer le nom du vserver qui est de type *admin*. Vous utiliserez ce nom dans les commandes suivantes.

```
 vserver show -type admin
. Créez un rôle à l'aide des commandes suivantes :
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
```

3. Créez l'utilisateur en lecture seule à l'aide de la commande suivante. Une fois la commande de création exécutée, vous serez invité à saisir un mot de passe pour cet utilisateur. Notez que dans la commande suivante, nous affichons le rôle défini sur *ci_readonly*. Si vous créez un rôle avec un nom différent à l'étape 3 ci-dessus, utilisez plutôt ce nom de rôle personnalisé.

```
 security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
Si un compte AD/LDAP est utilisé, la commande doit être
```

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Le rôle et la connexion utilisateur résultants ressembleront à ce qui
suit.  Votre sortie réelle peut varier :
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   -------------------     ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Vous pouvez vérifier l'accès spi si nécessaire :

```
**Vserver:> vserver services web access show -name spi
 Vserver                      Type     Service Name     Role
-------------- -------- ---------------- ----------------
<vserver name >     admin             spi           admin
<vserver name >     admin             spi           csrestrole

2 entries were displayed.**
```

Migration

Pour migrer d'un ancien collecteur de données ONTAP (ontapi) vers le nouveau collecteur ONTAP REST, procédez comme suit :

1. Ajoutez le collecteur REST. Il est recommandé de saisir les informations d'un utilisateur différent de celui configuré pour le collecteur précédent. Par exemple, utilisez l'utilisateur indiqué dans la section Autorisations ci-dessus.
2. Mettez en pause le collecteur précédent afin qu'il ne continue pas à collecter des données.
3. Laissez le nouveau collecteur REST acquérir des données pendant au moins 30 minutes. Ignorez toutes les données pendant cette période qui ne semblent pas « normales ».
4. Après la période de repos, vous devriez voir vos données se stabiliser à mesure que le collecteur REST continue d'acquérir.

Vous pouvez utiliser ce même processus pour revenir au collecteur précédent, si vous le souhaitez.

Configuration

Champ	Description
Adresse IP de gestion ONTAP	Adresse IP ou nom de domaine complet du cluster NetApp . Doit être l'adresse IP/FQDN de gestion de cluster.
Nom d'utilisateur ONTAP REST	Nom d'utilisateur pour le cluster NetApp
Mot de passe ONTAP REST	Mot de passe pour le cluster NetApp

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est 60 minutes.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 60 secondes.
Collecte avancée de données de compteur	Sélectionnez cette option pour inclure les données du compteur avancé ONTAP dans les sondages. Activé par défaut.
Activer la collecte d'événements EMS	Sélectionnez cette option pour inclure les données d'événements du journal ONTAP EMS. Activé par défaut.
Intervalle d'interrogation EMS (sec)	La valeur par défaut est de 60 secondes.

Terminologie

Data Infrastructure Insights acquiert les données d'inventaire, de journaux et de performances du collecteur de données ONTAP . Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de raid	Groupe de disques
Cluster	Stockage
Nœud	Nœud de stockage
Agrégat	Piscine de stockage
LUN	Volume
Volume	Volume interne
Machine virtuelle de stockage/serveur virtuel	Machine virtuelle de stockage

Terminologie de la gestion des données ONTAP

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources de stockage ONTAP Data Management. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – Une liste délimitée par des virgules des noms de modèles de nœuds uniques et discrets au sein de ce cluster. Si tous les nœuds des clusters sont du même type de modèle, un seul nom de modèle apparaîtra.
- Fournisseur – même nom de fournisseur que vous verriez si vous configuriez une nouvelle source de données.
- Numéro de série – L'UUID du tableau
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données.
- Version du microcode – firmware.
- Capacité brute – somme de base 2 de tous les disques physiques du système, quel que soit leur rôle.
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes internes individuels.
- Débit – agrégé à partir de volumes internes. Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire.

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire.
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Agrégat » ou de « Groupe RAID ».
- Nœud – si l'architecture de cette baie de stockage est telle que les pools appartiennent à un nœud de stockage spécifique, son nom sera vu ici comme un lien hypertexte vers sa propre page de destination.
- Utilise Flash Pool – Valeur Oui/Non – ce pool basé sur SATA/SAS dispose-t-il de SSD utilisés pour l'accélération de la mise en cache ?
- Redondance – Niveau RAID ou schéma de protection. RAID_DP est à double parité, RAID_TP est à triple parité.
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs.
- Capacité surengagée – Si, en utilisant des technologies d'efficacité, vous avez alloué une somme totale de capacités de volume ou de volume interne supérieure à la capacité logique du pool de stockage, la valeur de pourcentage ici sera supérieure à 0 %.
- Instantané – capacités d'instantané utilisées et totales, si votre architecture de pool de stockage consacre une partie de sa capacité aux zones de segments exclusivement pour les instantanés. Les configurations ONTAP dans MetroCluster sont susceptibles de présenter ce problème, tandis que d'autres configurations ONTAP le sont moins.
- Utilisation – une valeur en pourcentage indiquant le pourcentage d'occupation de disque le plus élevé de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'a pas nécessairement une forte corrélation avec les performances de la baie : l'utilisation peut être élevée en raison des reconstructions de disque, des activités de déduplication, etc. en l'absence de charges de travail pilotées par l'hôte. De plus, de nombreuses implémentations de réplication de baies peuvent entraîner une utilisation du disque sans apparaître comme volume interne ou charge de travail de volume.
- IOPS – la somme des IOPS de tous les disques contribuant à la capacité de ce pool de stockage. Débit – le débit total de tous les disques contribuant à la capacité de ce pool de stockage.

Nœud de stockage

- Stockage – à quelle baie de stockage ce nœud fait partie. Obligatoire.
- Partenaire HA – sur les plateformes où un nœud bascule vers un et un seul autre nœud, il sera généralement visible ici.
- État – santé du nœud. Disponible uniquement lorsque le tableau est suffisamment sain pour être inventorié par une source de données.
- Modèle – nom du modèle du nœud.
- Version – nom de la version de l'appareil.
- Numéro de série – Le numéro de série du nœud.
- Mémoire – mémoire de base 2 si disponible.
- Utilisation – Sur ONTAP, il s'agit d'un indice de stress du contrôleur issu d'un algorithme propriétaire. À chaque sondage de performances, un nombre compris entre 0 et 100 % sera signalé, correspondant au plus élevé des deux facteurs suivants : la contention du disque WAFL ou l'utilisation moyenne du processeur. Si vous observez des valeurs soutenues > 50 %, cela indique un sous-dimensionnement : potentiellement un contrôleur/nœud pas assez grand ou pas assez de disques rotatifs pour absorber la charge de travail d'écriture.
- IOPS – Dérivé directement des appels ONTAP REST sur l'objet nœud.
- Latence – Dérivée directement des appels ONTAP REST sur l'objet nœud.
- Débit – Dérivé directement des appels ONTAP REST sur l'objet nœud.
- Processeurs – Nombre de CPU.

Mesures de puissance ONTAP

Plusieurs modèles ONTAP fournissent des mesures de puissance pour Data Infrastructure Insights qui peuvent être utilisées pour la surveillance ou l'alerte. Les listes de modèles pris en charge et non pris en charge ci-dessous ne sont pas exhaustives mais devraient fournir quelques indications ; en général, si un modèle appartient à la même famille qu'un modèle de la liste, la prise en charge doit être la même.

Modèles pris en charge :

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modèles non pris en charge :

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Problème:	Essayez ceci:
Lors de la tentative de création d'un collecteur de données ONTAP REST, une erreur semblable à la suivante s'affiche : Configuration : 10.193.70.14 : l'API REST ONTAP à 10.193.70.14 n'est pas disponible : 10.193.70.14 n'a pas pu obtenir /api/cluster : 400 Mauvaise requête	Cela est probablement dû à un ancien tableau ONTAP) par exemple, ONTAP 9.6) qui n'a pas de capacités d'API REST. ONTAP 9.14.1 est la version ONTAP minimale prise en charge par le collecteur ONTAP REST. Les réponses « 400 Bad Request » doivent être attendues sur les versions antérieures à REST ONTAP . Pour les versions ONTAP qui prennent en charge REST mais qui ne sont pas 9.14.1 ou ultérieures, vous pouvez voir le message similaire suivant : Configuration : 10.193.98.84 : l'API REST ONTAP à 10.193.98.84 n'est pas disponible : 10.193.98.84 : l'API REST ONTAP à 10.193.98.84 est disponible : cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 mais n'est pas de version minimale 9.14.1.
Je vois des métriques vides ou « 0 » là où le collecteur ONTAP ontapi affiche des données.	ONTAP REST ne signale pas les métriques utilisées en interne sur le système ONTAP uniquement. Par exemple, les agrégats système ne seront pas collectés par ONTAP REST, seuls les SVM de type « données » seront collectés. Autres exemples de mesures ONTAP REST qui peuvent signaler des données nulles ou vides : InternalVolumes : REST ne signale plus vol0. Agrégats : REST ne signale plus aggr0. Stockage : la plupart des mesures sont une combinaison des mesures de volume interne et seront affectées par ce qui précède. Machines virtuelles de stockage : REST ne signale plus les SVM de type autre que « données » (par exemple, « cluster », « mgmt », « nœud »). Vous remarquerez peut-être également un changement dans l'apparence des graphiques contenant des données, en raison du changement de la période d'interrogation des performances par défaut de 15 minutes à 5 minutes. Des sondages plus fréquents signifient plus de points de données à tracer.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

NetApp Data ONTAP fonctionnant dans un collecteur de données en mode 7

Pour les systèmes de stockage utilisant le logiciel Data ONTAP fonctionnant en mode 7, vous utilisez le collecteur de données en mode 7, qui utilise l'interface de ligne de commande pour obtenir des données de capacité et de performances.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données NetApp en mode 7. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Ce collecteur de données est"obsolète" .

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de raid	Groupe de disques
Déposant	Stockage
Déposant	Nœud de stockage
Agrégat	Piscine de stockage
LUN	Volume
Volume	Volume interne

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Vous avez besoin des éléments suivants pour configurer et utiliser ce collecteur de données :

- Adresses IP du contrôleur de stockage FAS et du partenaire.
- Port 443
- Un nom d'utilisateur et un mot de passe de niveau administrateur personnalisés pour le contrôleur et le contrôleur partenaire avec les capacités de rôle suivantes pour 7-Mode :
  - "api-*" : utilisez ceci pour permettre à OnCommand Insight d'exécuter toutes les commandes API de stockage NetApp .
  - "login-http-admin" : utilisez ceci pour permettre à OnCommand Insight de se connecter au stockage NetApp via HTTP.
  - "security-api-vfiler" : utilisez ceci pour permettre à OnCommand Insight d'exécuter des commandes d'API de stockage NetApp pour récupérer les informations de l'unité vFiler.
  - « cli-options » : utilisez ceci pour lire les options du système de stockage.
  - « cli-lun » : accédez à ces commandes pour gérer les LUN. Affiche l'état (chemin LUN, taille, état en ligne/hors ligne et état partagé) du LUN ou de la classe de LUN donné.
  - "cli-df" : utilisez ceci pour afficher l'espace disque libre.
  - "cli-ifconfig" : utilisez ceci pour afficher les interfaces et les adresses IP.

Configuration

Champ	Description
Adresse du système de stockage	Adresse IP ou nom de domaine complet pour le système de stockage NetApp
Nom d'utilisateur	Nom d'utilisateur pour le système de stockage NetApp
Mot de passe	Mot de passe pour le système de stockage NetApp

Champ	Description
Adresse du partenaire HA du cluster	Adresse IP ou nom de domaine complet pour le partenaire HA
Nom d'utilisateur du partenaire HA dans le cluster	Nom d'utilisateur du partenaire HA
Mot de passe du fichier partenaire HA dans le cluster	Mot de passe pour le partenaire HA

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 20 minutes.
Type de connexion	HTTPS ou HTTP, affiche également le port par défaut
Remplacer le port de connexion	Si vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Connexion des systèmes de stockage

Au lieu d'utiliser l'utilisateur administratif par défaut pour ce collecteur de données, vous pouvez configurer un utilisateur avec des droits administratifs directement sur les systèmes de stockage NetApp afin que ce collecteur de données puisse acquérir des données à partir des systèmes de stockage NetApp .

La connexion aux systèmes de stockage NetApp nécessite que l'utilisateur, spécifié lors de l'acquisition du pfiler principal (sur lequel existe le système de stockage), remplisse les conditions suivantes :

- L'utilisateur doit être sur vfiler0 (root filer/pfiler).

  Les systèmes de stockage sont acquis lors de l'acquisition du pfiler principal.

- Les commandes suivantes définissent les capacités du rôle utilisateur :
  - "api-*" : utilisez ceci pour permettre à Data Infrastructure Insights d'exécuter toutes les commandes API de stockage NetApp .

    Cette commande est nécessaire pour utiliser le ZAPI.

  - "login-http-admin" : utilisez ceci pour permettre à Data Infrastructure Insights de se connecter au stockage NetApp via HTTP. Cette commande est nécessaire pour utiliser le ZAPI.
  - "security-api-vfiler" : utilisez ceci pour permettre à Data Infrastructure Insights d'exécuter des commandes d'API de stockage NetApp pour récupérer les informations de l'unité vFiler.
  - "cli-options" : pour la commande « options » et utilisé pour l'IP du partenaire et les licences activées.
  - « cli-lun » : accédez à cette commande pour gérer les LUN. Affiche l'état (chemin LUN, taille, état en ligne/hors ligne et état partagé) du LUN ou de la classe de LUN donné.
  - "cli-df" : pour les commandes "df -s", "df -r", "df -A -r" et utilisé pour afficher l'espace libre.
  - "cli-ifconfig" : pour la commande « ifconfig -a » et utilisé pour obtenir l'adresse IP du fichier.

- "cli-rdfile" : pour la commande "rdfile /etc/netgroup" et utilisé pour obtenir des groupes réseau.
- "cli-date" : pour la commande « date » et utilisé pour obtenir la date complète pour obtenir des copies instantanées.
- "cli-snap" : pour la commande « snap list » et utilisé pour obtenir des copies de snapshots.

Si les autorisations cli-date ou cli-snap ne sont pas fournies, l'acquisition peut se terminer, mais les copies Snapshot ne sont pas signalées.

Pour acquérir une source de données 7-Mode avec succès et ne générer aucun avertissement sur le système de stockage, vous devez utiliser l'une des chaînes de commande suivantes pour définir vos rôles d'utilisateur. La deuxième chaîne répertoriée ici est une version simplifiée de la première :

- login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-df,cli-lun,cli-ifconfig,cli-date,cli-snap,_
- login-http-admin,api-* ,sécurité-api-vfile,cli-

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Recevez une réponse HTTP 401 ou un code d'erreur ZAPI 13003 et ZAPI renvoie « Privilèges insuffisants » ou « non autorisé pour cette commande »	Vérifiez le nom d'utilisateur et le mot de passe, ainsi que les privilèges/autorisations de l'utilisateur.
Erreur « Échec de l'exécution de la commande »	Vérifiez si l'utilisateur dispose de l'autorisation suivante sur l'appareil : • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler Vérifiez également si la version ONTAP est prise en charge par Data Infrastructure Insights et vérifiez si les informations d'identification utilisées correspondent aux informations d'identification de l'appareil.
La version du cluster est < 8.1	La version minimale prise en charge du cluster est 8.1. Effectuez une mise à niveau vers la version minimale prise en charge.
ZAPI renvoie « le rôle du cluster n'est pas cluster_mgmt LIF »	AU doit communiquer avec l'IP de gestion du cluster. Vérifiez l'IP et changez-la si nécessaire
Erreur : « Les filtres en mode 7 ne sont pas pris en charge »	Cela peut se produire si vous utilisez ce collecteur de données pour découvrir le filtre en mode 7. Modifiez l'IP pour qu'elle pointe vers le fichier cdot à la place.
La commande ZAPI échoue après une nouvelle tentative	AU a un problème de communication avec le cluster. Vérifiez le réseau, le numéro de port et l'adresse IP. L'utilisateur doit également essayer d'exécuter une commande à partir de la ligne de commande à partir de la machine AU.
AU n'a pas réussi à se connecter à ZAPI	Vérifiez la connectivité IP/port et affirmez la configuration ZAPI.

Problème:	Essayez ceci:
AU n'a pas réussi à se connecter à ZAPI via HTTP	Vérifiez si le port ZAPI accepte le texte en clair. Si AU tente d'envoyer du texte en clair à un socket SSL, la communication échoue.
La communication échoue avec SSLException	AU tente d'envoyer SSL à un port en texte clair sur un fichier. Vérifiez si le port ZAPI accepte SSL ou utilisez un autre port.
Erreurs de connexion supplémentaires : la réponse ZAPI contient le code d'erreur 13001, « la base de données n'est pas ouverte ». Le code d'erreur ZAPI est 60 et la réponse contient « l'API ne s'est pas terminée à temps ». La réponse ZAPI contient « initialize_session() a renvoyé un environnement NULL ». Le code d'erreur ZAPI est 14007 et la réponse contient « le nœud n'est pas sain ».	Vérifiez le réseau, le numéro de port et l'adresse IP. L'utilisateur doit également essayer d'exécuter une commande à partir de la ligne de commande à partir de la machine AU.
Erreur de délai d'attente du socket avec ZAPI	Vérifiez la connectivité du fichier et/ou augmentez le délai d'expiration.
Erreur « Les clusters en mode C ne sont pas pris en charge par la source de données en mode 7 »	Vérifiez l'IP et changez l'IP en un cluster en mode 7.
Erreur « Échec de la connexion à vFiler »	Vérifiez que les capacités d'acquisition d'utilisateur incluent au minimum les éléments suivants : api-* security-api-vfiler login-http-admin Confirmez que le filer exécute au minimum la version ONTAPI 1.7.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données API Santricity hérité de NetApp E-Series

Le collecteur de données de l'API NetApp E-Series Legacy Santricity collecte les données d'inventaire et de performances. Le collecteur prend en charge le firmware 7.x+ en utilisant les mêmes configurations et en signalant les mêmes données.

Terminologie

Cloud Insight acquiert les informations d'inventaire suivantes à partir du collecteur de données NetApp E-Series. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de volumes	Groupe de disques
Baie de stockage	Stockage
Contrôleur	Nœud de stockage
Groupe de volumes	Piscine de stockage
Volume	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Terminologie de la série E (page de destination)

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources NetApp E-Series. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – nom du modèle de l'appareil.
- Fournisseur – même nom de fournisseur que vous verriez si vous configuriez une nouvelle source de données
- Numéro de série – Le numéro de série de la matrice. Sur les systèmes de stockage à architecture cluster comme NetApp Clustered Data Ontap, ce numéro de série peut être moins utile que les numéros de série individuels des « nœuds de stockage ».
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données
- Version du microcode – firmware
- Capacité brute – somme de base 2 de tous les disques physiques du système, quel que soit leur rôle
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes individuels.
- Débit – débit total de la baie orienté hôte. Idéalement, provenant directement de la baie, si elle n'est pas disponible, Data Infrastructure Insights additionne le débit des volumes pour dériver cette valeur
- Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Thin Provisioning » ou de « RAID Group »
- Nœud – si l'architecture de cette baie de stockage est telle que les pools appartiennent à un nœud de stockage spécifique, son nom sera vu ici comme un lien hypertexte vers sa propre page de destination
- Utilise Flash Pool – Valeur Oui/Non
- Redondance – Niveau RAID ou schéma de protection. La série E signale « RAID 7 » pour les pools DDP
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs. Ces valeurs incluent toutes deux la capacité de « conservation » de la série E, ce qui donne des chiffres et un pourcentage supérieurs à ce que l'interface utilisateur de la série E peut afficher.
- Capacité surengagée – Si, grâce à des technologies d'efficacité, vous avez alloué une somme totale de capacités de volume ou de volume interne supérieure à la capacité logique du pool de stockage, la valeur de pourcentage ici sera supérieure à 0 %.
- Instantané – capacités d'instantané utilisées et totales, si votre architecture de pool de stockage consacre

une partie de sa capacité aux zones de segments exclusivement pour les instantanés

- Utilisation – une valeur en pourcentage indiquant le pourcentage d'occupation de disque le plus élevé de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'a pas nécessairement une forte corrélation avec les performances de la baie : l'utilisation peut être élevée en raison des reconstructions de disque, des activités de déduplication, etc. en l'absence de charges de travail pilotées par l'hôte. De plus, de nombreuses implémentations de réplication de baies peuvent entraîner une utilisation accrue du disque sans apparaître comme une charge de travail de volume.
- IOPS – la somme des IOPS de tous les disques contribuant à la capacité de ce pool de stockage. Si les E/S par seconde (IOPS) du disque ne sont pas disponibles sur une plate-forme donnée, cette valeur sera extraite de la somme des E/S par seconde (IOPS) du volume pour tous les volumes situés sur ce pool de stockage.
- Débit – le débit total de tous les disques contribuant à la capacité de ce pool de stockage. Si le débit du disque n'est pas disponible sur une plate-forme donnée, cette valeur sera extraite de la somme du volume pour tous les volumes situés sur ce pool de stockage.

Nœud de stockage

- Stockage – à quelle baie de stockage ce nœud fait partie. Obligatoire
- Partenaire HA – sur les plateformes où un nœud bascule vers un et un seul autre nœud, il sera généralement vu ici
- État – santé du nœud. Disponible uniquement lorsque le tableau est suffisamment sain pour être inventorié par une source de données
- Modèle – nom du modèle du nœud
- Version – nom de la version de l'appareil.
- Numéro de série – Le numéro de série du nœud
- Mémoire – mémoire de base 2 si disponible
- Utilisation – Généralement un numéro d'utilisation du processeur ou, dans le cas de NetApp Ontap, un indice de stress du contrôleur. L'utilisation n'est actuellement pas disponible pour NetApp E-Series
- IOPS – un nombre représentant les IOPS pilotées par l'hôte sur ce contrôleur. Idéalement, il provient directement de la baie. S'il n'est pas disponible, il sera calculé en additionnant tous les IOP pour les volumes appartenant exclusivement à ce nœud.
- Latence – un nombre représentant la latence ou le temps de réponse typique de l'hôte sur ce contrôleur. Idéalement, il provient directement du réseau. S'il n'est pas disponible, il sera calculé en effectuant un calcul pondéré des IOP à partir des volumes appartenant exclusivement à ce nœud.
- Débit – un nombre représentant le débit piloté par l'hôte sur ce contrôleur. Idéalement, il provient directement de la baie. S'il n'est pas disponible, il sera calculé en additionnant tout le débit des volumes appartenant exclusivement à ce nœud.
- Processeurs – Nombre de CPU

Exigences

- L'adresse IP de chaque contrôleur de la baie
- Exigence de port 2463

Configuration

Champ	Description
Liste séparée par des virgules des adresses IP des contrôleurs SANtricity de la baie	Adresses IP et/ou noms de domaine complets pour les contrôleurs de réseau

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 30 minutes
Intervalle d'interrogation des performances jusqu'à 3 600 secondes	La valeur par défaut est de 300 secondes

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données REST NetApp E-Series

Le collecteur de données REST NetApp E-Series collecte les données d'inventaire, de journaux et de performances. Le collecteur prend en charge le firmware 7.x+ en utilisant les mêmes configurations et en signalant les mêmes données. Le collecteur REST surveille l'état de chiffrement des pools de stockage, des disques et des volumes, l'utilisation du processeur du nœud de stockage ainsi que les fonctionnalités de journaux non fournies dans l'ancien collecteur SANtricity E-Series.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de NetApp E-Series, à l'aide de REST. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque
Groupe de volumes	Groupe de disques
Baie de stockage	Stockage
Contrôleur	Nœud de stockage
Groupe de volumes	Piscine de stockage
Volume	Volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- L'adresse IP de chaque contrôleur de la baie

- Ce collecteur prend uniquement en charge les tableaux de modèles de la série E avec des **capacités API REST natives**. L'organisation E-Series fournit une distribution d'API REST installable hors tableau pour les anciennes baies E-Series : ce collecteur ne prend pas en charge ce scénario. Les utilisateurs disposant d'anciennes baies doivent continuer à utiliser Data Infrastructure Insights."API SANtricity série E" collectionneur.
- Le champ « Adresses IP du contrôleur série E » prend en charge une chaîne délimitée par des virgules de 2 IP/noms d'hôte ; le collecteur essaiera intelligemment la deuxième IP/nom d'hôte si la première est inaccessible.
- Port HTTPS : la valeur par défaut est 8443.

Configuration

Champ	Description
Adresses IP des contrôleurs de la série E	adresses IP séparées par des virgules et/ou noms de domaine complets pour les contrôleurs de baie

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 30 minutes
Intervalle d'interrogation des performances jusqu'à 3 600 secondes	La valeur par défaut est de 300 secondes

Terminologie de la série E (page de destination)

Les conditions suivantes s'appliquent aux objets ou références que vous pourriez trouver sur les pages de destination des ressources NetApp E-Series. Bon nombre de ces termes s'appliquent également à d'autres collecteurs de données.

Stockage

- Modèle – nom du modèle de l'appareil.
- Fournisseur – même nom de fournisseur que vous verriez si vous configuriez une nouvelle source de données
- Numéro de série – Le numéro de série de la matrice. Sur les systèmes de stockage à architecture cluster comme NetApp Clustered Data Ontap, ce numéro de série peut être moins utile que les numéros de série individuels des « nœuds de stockage ».
- IP – il s'agira généralement de l'adresse IP ou du nom d'hôte tel que configuré dans la source de données
- Version du microcode – firmware
- Capacité brute – somme de base 2 de tous les disques physiques du système, quel que soit leur rôle
- Latence – une représentation de ce que subissent les charges de travail de l'hôte, à la fois en lecture et en écriture. Idéalement, Data Infrastructure Insights s'approvisionne directement en valeur, mais ce n'est souvent pas le cas. Au lieu que le tableau propose cela, Data Infrastructure Insights effectue généralement un calcul pondéré par les IOP dérivé des statistiques des volumes individuels.
- Débit – débit total de la baie orienté hôte. Idéalement, provenant directement de la baie, si elle n'est pas disponible, Data Infrastructure Insights additionne le débit des volumes pour dériver cette valeur
- Gestion – cela peut contenir un lien hypertexte vers l'interface de gestion de l'appareil. Créé par

programmation par la source de données Data Infrastructure Insights dans le cadre du rapport d'inventaire

Piscine de stockage

- Stockage – sur quelle baie de stockage ce pool réside. Obligatoire
- Type – une valeur descriptive issue d'une liste énumérée de possibilités. Le plus souvent, il s'agira de « Thin Provisioning » ou de « RAID Group »
- Nœud – si l'architecture de cette baie de stockage est telle que les pools appartiennent à un nœud de stockage spécifique, son nom sera vu ici comme un lien hypertexte vers sa propre page de destination
- Utilise Flash Pool – Valeur Oui/Non
- Redondance – Niveau RAID ou schéma de protection. La série E signale « RAID 7 » pour les pools DDP
- Capacité – les valeurs ici sont la capacité logique utilisée, la capacité utilisable et la capacité logique totale, ainsi que le pourcentage utilisé sur ces valeurs. Ces valeurs incluent toutes deux la capacité de « conservation » de la série E, ce qui donne des chiffres et un pourcentage supérieurs à ce que l'interface utilisateur de la série E peut afficher.
- Capacité surengagée – Si, grâce à des technologies d'efficacité, vous avez alloué une somme totale de capacités de volume ou de volume interne supérieure à la capacité logique du pool de stockage, la valeur de pourcentage ici sera supérieure à 0 %.
- Instantané – capacités d'instantané utilisées et totales, si votre architecture de pool de stockage consacre une partie de sa capacité aux zones de segments exclusivement pour les instantanés
- Utilisation – une valeur en pourcentage indiquant le pourcentage d'occupation de disque le plus élevé de tout disque contribuant à la capacité de ce pool de stockage. L'utilisation du disque n'a pas nécessairement une forte corrélation avec les performances de la baie : l'utilisation peut être élevée en raison des reconstructions de disque, des activités de déduplication, etc. en l'absence de charges de travail pilotées par l'hôte. De plus, de nombreuses implémentations de réplication de baies peuvent entraîner une utilisation accrue du disque sans apparaître comme une charge de travail de volume.
- IOPS – la somme des IOPS de tous les disques contribuant à la capacité de ce pool de stockage. Si les E/S par seconde (IOPS) du disque ne sont pas disponibles sur une plate-forme donnée, cette valeur sera extraite de la somme des E/S par seconde (IOPS) du volume pour tous les volumes situés sur ce pool de stockage.
- Débit – le débit total de tous les disques contribuant à la capacité de ce pool de stockage. Si le débit du disque n'est pas disponible sur une plate-forme donnée, cette valeur sera extraite de la somme du volume pour tous les volumes situés sur ce pool de stockage.

Nœud de stockage

- Stockage – à quelle baie de stockage ce nœud fait partie. Obligatoire
- Partenaire HA – sur les plateformes où un nœud bascule vers un et un seul autre nœud, il sera généralement vu ici
- État – santé du nœud. Disponible uniquement lorsque le tableau est suffisamment sain pour être inventorié par une source de données
- Modèle – nom du modèle du nœud
- Version – nom de la version de l'appareil.
- Numéro de série – Le numéro de série du nœud
- Mémoire – mémoire de base 2 si disponible

- Utilisation – Généralement un numéro d'utilisation du processeur ou, dans le cas de NetApp Ontap, un indice de stress du contrôleur. L'utilisation n'est actuellement pas disponible pour NetApp E-Series
- IOPS – un nombre représentant les IOPS pilotées par l'hôte sur ce contrôleur. Idéalement, il provient directement de la baie. S'il n'est pas disponible, il sera calculé en additionnant tous les IOP pour les volumes appartenant exclusivement à ce nœud.
- Latence – un nombre représentant la latence ou le temps de réponse typique de l'hôte sur ce contrôleur. Idéalement, il provient directement du réseau. S'il n'est pas disponible, il sera calculé en effectuant un calcul pondéré des IOP à partir des volumes appartenant exclusivement à ce nœud.
- Débit – un nombre représentant le débit piloté par l'hôte sur ce contrôleur. Idéalement, il provient directement de la baie. S'il n'est pas disponible, il sera calculé en additionnant tout le débit des volumes appartenant exclusivement à ce nœud.
- Processeurs – Nombre de CPU

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données du serveur de gestion NetApp HCI

Le collecteur de données du serveur de gestion NetApp HCI collecte les informations de l'hôte NetApp HCI et requiert des privilèges en lecture seule sur tous les objets du serveur de gestion.

Ce collecteur de données acquiert uniquement auprès du * serveur de gestion NetApp HCI *. Pour collecter des données à partir du système de stockage, vous devez également configurer le"NetApp SolidFire" collecteur de données.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès de ce collecteur de données. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque virtuel	Disque
Hôte	Hôte
Machine virtuelle	Machine virtuelle
Magasin de données	Magasin de données
LUN	Volume
Port Fibre Channel	Port

Il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les informations suivantes sont requises pour configurer ce collecteur de données :

- Adresse IP du serveur de gestion NetApp HCI
- Nom d'utilisateur et mot de passe en lecture seule pour le serveur de gestion NetApp HCI
- Privilèges en lecture seule sur tous les objets du serveur de gestion NetApp HCI .
- Accès au SDK sur le serveur de gestion NetApp HCI – normalement déjà configuré.
- Exigences de port : http-80 https-443
- Valider l'accès :
  - Connectez-vous au serveur de gestion NetApp HCI à l'aide du nom d'utilisateur et du mot de passe ci-dessus
  - Vérifier que le SDK est activé : telnet <vc_ip> 443

Installation et connexion

Champ	Description
Nom	Nom unique pour le collecteur de données
Unité d'acquisition	Nom de l'unité d'acquisition

Configuration

Champ	Description
Cluster de stockage NetApp HCI MVIP	Adresse IP virtuelle de gestion
Nœud de gestion SolidFire (mNode)	Adresse IP du nœud de gestion
Nom d'utilisateur	Nom d'utilisateur utilisé pour accéder au serveur de gestion NetApp HCI
Mot de passe	Mot de passe utilisé pour accéder au serveur de gestion NetApp HCI
Nom d'utilisateur VCenter	Nom d'utilisateur pour VCenter
Mot de passe VCenter	Mot de passe pour VCenter

Configuration avancée

Dans l'écran de configuration avancée, cochez la case **Performances VM** pour collecter les données de performances. La collecte d'inventaire est activée par défaut. Les champs suivants peuvent être configurés :

Champ	Description
Intervalle d'interrogation de l'inventaire (min)	Sourd a 20 ans
Filtrer les machines virtuelles par	Sélectionnez CLUSTER, DATACENTER ou ESX HOST
Choisissez « Exclure » ou « Inclure » pour spécifier une liste	Spécifier s'il faut inclure ou exclure les machines virtuelles
Filtrer la liste des appareils	Liste des machines virtuelles à filtrer (séparées par des virgules ou des points-virgules si une virgule est utilisée dans la valeur) pour le filtrage par ESX_HOST, CLUSTER et DATACENTER uniquement

Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : la liste d'inclusion pour filtrer les machines virtuelles ne peut pas être vide	Si l'option Inclure la liste est sélectionnée, veuillez répertorier les noms de centre de données, de cluster ou d'hôte valides pour filtrer les machines virtuelles.
Erreur : échec de l'instanciation d'une connexion à VirtualCenter à l'adresse IP	Solutions possibles : * Vérifier les informations d'identification et l'adresse IP saisies. * Essayez de communiquer avec Virtual Center à l'aide du client d'infrastructure. * Essayez de communiquer avec Virtual Center à l'aide du navigateur d'objets gérés (par exemple MOB).
Erreur : VirtualCenter sur IP possède un certificat non conforme requis par JVM	Solutions possibles : * Recommandé : régénérez le certificat pour Virtual Center en utilisant une clé RSA plus forte (par exemple 1 024 bits). * Non recommandé : modifiez la configuration java.security de la JVM pour exploiter la contrainte jdk.certpath.disabledAlgorithms afin d’autoriser la clé RSA 512 bits. Consultez les notes de publication de la mise à jour 40 du JDK 7 sur"http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données NetApp SolidFire All-Flash Array

Le collecteur de données NetApp SolidFire All-Flash Array prend en charge l'inventaire et la collecte des performances à partir des configurations SolidFire iSCSI et Fibre Channel.

Le collecteur de données SolidFire utilise l'API REST SolidFire . L'unité d'acquisition où réside le collecteur de données doit pouvoir initier des connexions HTTPS au port TCP 443 sur l'adresse IP de gestion du cluster SolidFire . Le collecteur de données a besoin d'informations d'identification capables d'effectuer des requêtes API REST sur le cluster SolidFire .

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes à partir du collecteur de données NetApp SolidFire All-Flash Array. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Conduire	Disque
Cluster	Stockage
Nœud	Nœud de stockage
Volume	Volume
Port Fibre Channel	Port
Groupe d'accès aux volumes, attribution de LUN	Carte des volumes
Session iSCSI	Masque de volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les exigences suivantes sont requises pour la configuration de ce collecteur de données :

- Adresse IP virtuelle de gestion
- Nom d'utilisateur et informations d'identification en lecture seule
- Port 443

Configuration

Champ	Description
Adresse IP virtuelle de gestion (MVIP)	Gestion de l'adresse IP virtuelle du cluster SolidFire
Nom d'utilisateur	Nom utilisé pour se connecter au cluster SolidFire
Mot de passe	Mot de passe utilisé pour se connecter au cluster SolidFire

Configuration avancée

Champ	Description
Type de connexion	Choisissez le type de connexion
Port de communication	Port utilisé pour l'API NetApp
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 20 minutes
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 300 secondes

Dépannage

Lorsque SolidFire signale une erreur, celle-ci s'affiche dans Data Infrastructure Insights comme suit :

Un message d'erreur a été reçu d'un périphérique SolidFire lors de la tentative de récupération de données. L'appel était <méthode> (<parameterString>). Le message d'erreur de l'appareil était (consultez le manuel de l'appareil) : <message>

Où:

- La <méthode> est une méthode HTTP, telle que GET ou PUT.
- Le <parameterString> est une liste séparée par des virgules de paramètres qui ont été inclus dans l'appel REST.
- Le <message> est le message d'erreur renvoyé par l'appareil.

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données NetApp StorageGRID

Le collecteur de données NetApp StorageGRID prend en charge la collecte d'inventaire et de performances à partir des configurations StorageGRID .

> Pour fournir une mesure cohérente des droits DII sur tous les systèmes StorageGRID , quelle que soit la topologie et la configuration matérielles sous-jacentes, Data Infrastructure Insights utilise la capacité totale disponible (storagegrid_storage_utilization_total_space_bytes), au lieu de la capacité RAW basée sur la disposition du disque physique.
>
> Pour les clients utilisant le modèle de licence basé sur la capacité, StorageGRID est mesuré comme un stockage « objet ».
>
> Pour les clients utilisant le modèle de licence hérité (MU), StorageGRID est mesuré comme stockage secondaire, à un taux de 40 Tio pour 1 MU.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur NetApp StorageGRID . Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
StorageGRID	Stockage
Nœud	Nœud
Locataire	Piscine de stockage
Seau	Volume interne

Exigences

Voici les exigences pour la configuration de cette source de données :

- Adresse IP de l'hôte StorageGRID
- Un nom d'utilisateur et un mot de passe pour un utilisateur auquel les rôles Requête de métrique et Accès au locataire ont été attribués
- Port 443 (ou 8443 si configuré)

Configuration

Champ	Description
Adresse IP de l'hôte StorageGRID	Adresse IP virtuelle de gestion de l'appliance StorageGRID
Nom d'utilisateur	Nom utilisé pour se connecter à l'appliance StorageGRID
Mot de passe	Mot de passe utilisé pour se connecter à l'appliance StorageGRID

Configuration avancée

Champ	Description
Intervalle d'interrogation d'inventaire (min)	La valeur par défaut est de 60 minutes
Intervalle d'interrogation des performances (sec)	La valeur par défaut est de 900 secondes

Authentification unique (SSO)

Le"StorageGRID" les versions du micrologiciel ont des versions d'API correspondantes ; l'API 3.0 et les versions plus récentes prennent en charge la connexion par authentification unique (SSO).

Version du micrologiciel	Version API	Prise en charge de l'authentification unique (SSO)
11,1	2	Non
11,2	3,0	Oui
11,5	3,3	Oui

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Nutanix NX

Data Infrastructure Insights utilise le collecteur de données Nutanix pour découvrir les données d'inventaire et de performances des systèmes de stockage Nutanix NX.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Nutanix. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Piscine de stockage	Piscine de stockage

Terme du fournisseur/modèle	Data Infrastructure Insights
Conteneur Nutanix	Volume interne
Conteneur Nutanix	Partage de fichiers
Partage NFS	Partager

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- L'adresse IP des services de données externes pour le cluster
- Nom d'utilisateur et mot de passe en lecture seule, sauf si des volumes_groups sont utilisés, auquel cas, le nom d'utilisateur et le mot de passe administrateur sont requis
- Exigence de port : HTTPS 443

Configuration

Champ	Description
Adresse IP externe de Prism	L'adresse IP des services de données externes pour le cluster
Nom d'utilisateur	Nom d'utilisateur pour le compte administrateur
Mot de passe	Mot de passe pour le compte administrateur

Configuration avancée

Champ	Description
Port TCP	Port TCP utilisé pour se connecter à la baie Nutanix. La valeur par défaut est 9440.
Intervalle d'interrogation de l'inventaire (min)	Intervalle entre les sondages d'inventaire. La valeur par défaut est de 60 minutes.
Intervalle d'interrogation des performances (sec)	Intervalle entre les sondages de performance. La valeur par défaut est de 300 secondes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Oracle ZFS Storage Appliance

Data Infrastructure Insights utilise le collecteur de données Oracle ZFS Storage Appliance pour collecter des données d'inventaire et de performances.

Terminologie

Data Infrastructure Insights acquiert des informations d'inventaire avec le collecteur de données Oracle ZFS. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque (SSD)	Disque
Cluster	Stockage
Contrôleur	Nœud de stockage
LUN	Volume
Carte LUN	Carte des volumes
Initiateur, cible	Masque de volume
Partager	Volume interne

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour cette source de données.

Exigences

- Noms d'hôte pour le contrôleur ZFS-1 et le contrôleur ZFS-2
- Nom d'utilisateur et mot de passe de l'administrateur
- Exigence de port : 215 HTTP/HTTPS

Mesures de performance requises

Les appliances Oracle ZFS offrent aux administrateurs de stockage une grande flexibilité pour capturer les statistiques de performances. Data Infrastructure Insights s'attend à ce que chaque contrôleur d'une paire à haute disponibilité soit configuré pour capturer les métriques suivantes :

- smb2.ops[partager]
- nfs3.ops[partager]
- nfs4.ops[partager]
- nfs4-1.ops[partager]

Si le contrôleur ne parvient pas à capturer tout ou partie de ces éléments, Data Infrastructure Insights risque de ne pas avoir, ou de sous-déclarer, la charge de travail sur les « volumes internes ».

Configuration

Champ	Description
Nom d'hôte du contrôleur ZFS-1	Nom d'hôte pour le contrôleur de stockage 1
Nom d'hôte du contrôleur ZFS-2	Nom d'hôte pour le contrôleur de stockage 2

Champ	Description
Nom d’utilisateur	Nom d’utilisateur pour le compte d’utilisateur administrateur du système de stockage
Mot de passe	Mot de passe pour le compte utilisateur administrateur

Configuration avancée

Champ	Description
Type de connexion	HTTPS ou HTTP, affiche également le port par défaut
Remplacer le port de connexion	Si vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Intervalle d’interrogation de l’inventaire	La valeur par défaut est de 60 secondes
Intervalle d’interrogation des performances (sec)	La valeur par défaut est 300.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Informations de connexion non valides »	valider le compte utilisateur et le mot de passe Zfs
« La requête a échoué avec le statut 404 https://…..:215/api/access/v1 »	Votre tableau ZFS est peut-être trop ancien pour bénéficier de la prise en charge de l’API REST. AK 2013.1.3.0 a été la première version du système d’exploitation ZFS compatible avec l’API REST, et tous les appareils ZFS ne peuvent pas être mis à niveau vers cette version.
« Erreur de configuration » avec le message d’erreur « Le service REST est désactivé »	Vérifiez que le service REST est activé sur cet appareil.

Problème:	Essayez ceci:
« Erreur de configuration » avec le message d'erreur « Utilisateur non autorisé pour la commande »	Cette erreur est probablement due au fait que certains rôles (par exemple, « advanced_analytics ») ne sont pas inclus pour l'utilisateur configuré. L'application de la portée Analytics pour l'utilisateur avec un rôle en lecture seule peut supprimer l'erreur. Suivez ces étapes : 1. Sur le système ZFs, depuis l'écran Configuration → Utilisateurs, déplacez votre souris sur le rôle et double-cliquez pour autoriser la modification 2. Sélectionnez « Analyse » dans le menu déroulant Portée. Une liste des propriétés possibles apparaît. 3. Cliquez sur la case à cocher la plus haute et elle sélectionnera les trois propriétés. 4. Cliquez sur le bouton Ajouter sur le côté droit. 5. Cliquez sur le bouton Appliquer en haut à droite de la fenêtre contextuelle. La fenêtre contextuelle se fermera.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Pure Storage FlashArray

Data Infrastructure Insights utilise le collecteur de données Pure Storage FlashArray pour collecter des données d'inventaire et de performances.

Terminologie

Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque (SSD)	Disque
Tableau	Stockage
Contrôleur	Nœud de stockage
Volume	Volume
Carte LUN	Carte des volumes
Initiateur, cible	Masque de volume

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Adresse IP du système de stockage
- Nom d'utilisateur et mot de passe pour le compte Administrateur du système de stockage Pure.
- Exigence de port : HTTP/HTTPS 80/443

Configuration

Champ	Description
Adresse IP de l'hôte FlashArray	Adresse IP du système de stockage
Nom d'utilisateur	Nom d'utilisateur avec privilèges d'administrateur
Mot de passe pour le compte privilégié administrateur	Mot de passe

Configuration avancée

Champ	Description
Type de connexion	Choisissez HTTP ou HTTPS. Affiche également le port par défaut.
Remplacer le port TCP	Si vide, utilisez le port par défaut dans le champ Type de connexion, sinon entrez le port de connexion à utiliser
Intervalle d'interrogation de l'inventaire (min)	La valeur par défaut est de 60 minutes
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
« Identifiants de connexion non valides » avec les messages d'erreur « La politique ne le permet pas » ou « Vous n'êtes pas autorisé »	Valider le compte utilisateur et le mot de passe Pure via l'interface http Pure

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données de virtualisation Red Hat

Data Infrastructure Insights utilise le collecteur de données Red Hat Virtualization pour collecter des données d'inventaire à partir de charges de travail Linux et Microsoft Windows virtualisées.

Terminologie

Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque	Disque virtuel
Hôte	Hôte
Machine virtuelle	Machine virtuelle
Domaine de stockage	Magasin de données
Unité logique	LUN

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

- Adresse IP du serveur RHEV sur le port 443 via l'API REST
- Nom d'utilisateur et mot de passe en lecture seule
- RHEV Version 3.0+

Configuration

Champ	Description
Adresse IP du serveur RHEV	Adresse IP du système de stockage
Nom d'utilisateur	Nom d'utilisateur avec privilèges d'administrateur
Mot de passe pour le compte privilégié administrateur	Mot de passe

Configuration avancée

Champ	Description
Port de communication HTTPS	Port utilisé pour la communication HTTPS vers RHEV
Intervalle d'interrogation de l'inventaire (min)	La valeur par défaut est de 20 minutes.

Dépannage

Des informations complémentaires sur ce collecteur de données peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Rubrik CDM

Data Infrastructure Insights utilise le collecteur de données Rubrik pour acquérir des données d'inventaire et de performances à partir des appliances de stockage Rubrik.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données Rubrik. Pour chaque type d'actif acquis par Data Infrastructure Insights, la terminologie la plus courante utilisée pour cet actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Cluster	Stockage, réserve de stockage
Nœud	Nœud de stockage
Disque	Disque

Remarque : il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour cette source de données.

Exigences

Les éléments suivants sont requis pour configurer ce collecteur de données :

- L'unité d'acquisition Data Infrastructure Insights initiera les connexions au port TCP 443 vers le cluster Rubrik. Un collecteur par cluster.
- Adresse IP du cluster Rubrik.
- Nom d'utilisateur et mot de passe du cluster.
- Adresse IP ou nom d'hôte du cluster Rubrik.
- Pour l'authentification de base, un nom d'utilisateur et un mot de passe pour le cluster. Si vous préférez utiliser l'authentification basée sur le compte de service, vous avez besoin d'un compte de service, d'un secret et d'un ID d'organisation
- Exigence de port : HTTPS 443

Configuration

Champ	Description
propriété intellectuelle	Adresse IP du cluster Rubrik
Nom d'utilisateur / Compte de service	Nom d'utilisateur pour le cluster
Mot de passe / Secret	Mot de passe pour le cluster
ID d'organisation pour le compte de service	Il doit s'agir de la chaîne complète comme « Organisation:::nnnnnn-nnnn….. ».

Configuration avancée

Intervalle d'interrogation de l'inventaire (min)	La valeur par défaut est 60
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
J'ai reçu un message indiquant que plusieurs stockages ont été créés.	Vérifiez que le cluster est correctement configuré et que le collecteur pointe vers un seul cluster.
Le sondage échoue avec 400 [Bad Request]… ManagedId non valide….	Vous avez renseigné le champ ID d'organisation avec une valeur, mais le cluster Rubrik ne considère PAS qu'il s'agit d'un ID d'organisation valide, malgré le message d'erreur de Rubrik le désignant comme un « ManagedId ».

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Configuration du collecteur de données VMware VSphere

Le collecteur de données pour VMware vSphere collecte les informations de performances et de configuration des invités VM et des hôtes ESXi et requiert des privilèges en lecture seule sur tous les objets de vSphere. Depuis août 2024, le collecteur vSphere récupère également des messages de journal provenant d'environnements vSphere et certaines mesures spécifiques à VMware. Veuillez noter que Data Infrastructure Insights ne peut récupérer les informations des journaux VMware qu'à partir d'environnements vSphere 8.0.1 ou supérieurs. De même, les mesures spécifiques au fournisseur ne sont prises en charge que pour les environnements vSphere 7+. Par conséquent, vous souhaiterez peut-être désactiver la case à cocher des journaux et/ou des mesures spécifiques au fournisseur sur un collecteur donné s'il pointe vers une instance vSphere plus ancienne.

Terminologie

Data Infrastructure Insights acquiert les informations d'inventaire suivantes auprès du collecteur de données VMware vSphere. Pour chaque type d'actif acquis, la terminologie la plus courante utilisée pour l'actif est indiquée. Lorsque vous consultez ou dépannez ce collecteur de données, gardez à l'esprit la terminologie suivante :

Terme du fournisseur/modèle	Data Infrastructure Insights
Disque virtuel	Disque
Hôte	Hôte
Machine virtuelle	Machine virtuelle
Magasin de données	Magasin de données
LUN	Volume
Port Fibre Channel	Port

Il s'agit uniquement de mappages de terminologie courants et ils peuvent ne pas représenter tous les cas pour ce collecteur de données.

Exigences

Les informations suivantes sont requises pour configurer ce collecteur de données :

- Adresse IP du serveur Virtual Center
- Nom d'utilisateur et mot de passe en lecture seule dans Virtual Center
- Nous exigeons des privilèges de lecture seule sur tous les objets dans Virtual Center.
- Accès au SDK sur le serveur Virtual Center – normalement déjà configuré.
- Exigences de port : http-80 https-443
- Valider l'accès :
  - Connectez-vous au client Virtual Center en utilisant le nom d'utilisateur et le mot de passe ci-dessus
  - Vérifier que le SDK est activé : telnet <vc_ip> 443

Installation et connexion

Champ	Description
Nom	Nom unique pour le collecteur de données
Unité d'acquisition	Nom de l'unité d'acquisition

Configuration

Champ	Description
Adresse IP du centre virtuel	Adresse IP du centre virtuel
Nom d'utilisateur	Nom d'utilisateur utilisé pour accéder au centre virtuel
Mot de passe	Mot de passe utilisé pour accéder au centre virtuel

Configuration avancée

Dans l'écran de configuration avancée, cochez la case **Performances VM** pour collecter les données de performances. La collecte d'inventaire est activée par défaut. Les champs suivants peuvent être configurés :

Champ	Description
Intervalle d'interrogation de l'inventaire (min)	La valeur par défaut est 20
Filtrer les machines virtuelles	Sélectionnez CLUSTER, DATACENTER ou ESX HOST
Choisissez « Exclure » ou « Inclure » pour spécifier une liste	Créer une liste de filtres (CLUSTER, DATACENTER et/ou ESX_HOST)
Nombre de tentatives	La valeur par défaut est 3
Port de communication	La valeur par défaut est 443

Filtrer la liste des appareils…	Cette liste doit être composée de correspondances de chaînes exactes. Si vous avez l'intention de filtrer par ESX_HOST, vous devez créer une liste délimitée par des virgules des « noms » exacts de vos hôtes ESX tels que rapportés dans Data Infrastructure Insights et vSphere. Ces « noms » peuvent être des adresses IP, des noms d'hôtes simples ou des noms de domaine complets (FQDN) ; cela est déterminé par la façon dont ces hôtes ont été nommés lors de leur ajout initial à vSphere. Lors du filtrage par CLUSTER, utilisez les noms de cluster de style Data Infrastructure Insights tels que rapportés par CI sur les hyperviseurs - Data Infrastructure Insights ajoute au nom du cluster vSphere le nom du centre de données vSphere et une barre oblique - « DC1/clusterA » est le nom du cluster que Data Infrastructure Insights signalerait sur un hyperviseur dans clusterA au sein du centre de données DC1.
Intervalle d'interrogation des performances (sec)	La valeur par défaut est 300

Mappage des balises VMware aux annotations Data Infrastructure Insights

Le collecteur de données VMware vous permet de renseigner les annotations Data Infrastructure Insights avec des balises configurées sur VMware. Le nom de l'annotation DII doit être identique au nom de la **catégorie** VMware ; la balise est ensuite appliquée comme valeur d'annotation d'une annotation DII du même nom que la catégorie. Data Infrastructure Insights renseignera toujours les annotations de type texte portant le même nom et fera de son mieux pour renseigner les annotations d'autres types (nombre, booléen, etc.). Si votre annotation est d'un type différent et que le collecteur de données ne parvient pas à la renseigner, il peut être nécessaire de supprimer l'annotation et de la recréer en tant que type de texte.

Notez que les balises VMware peuvent être sensibles à la casse, tandis que les balises Data Infrastructure Insights ne le sont pas. Ainsi, si vous créez une annotation nommée « OWNER » dans Data Infrastructure Insights et des balises nommées « OWNER », « Owner » et « owner » dans VMware, toutes ces variantes de « owner » seront mappées à l'annotation « OWNER » de Cloud Insight.

Gardez à l'esprit les points suivants :

- Data Infrastructure Insights publie actuellement automatiquement uniquement les informations de support pour les appareils NetApp .
- Étant donné que ces informations d'assistance sont conservées sous forme d'annotation, vous pouvez les interroger ou les utiliser dans des tableaux de bord.
- Si un utilisateur écrase ou vide la valeur d'annotation, la valeur est à nouveau remplie automatiquement lorsque Data Infrastructure Insights met à jour les annotations, ce qu'il fait une fois par jour.

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes avec ce collecteur de données :

Inventaire

Problème:	Essayez ceci:
Erreur : la liste d'inclusion pour filtrer les machines virtuelles ne peut pas être vide	Si l'option Inclure la liste est sélectionnée, veuillez répertorier les noms de centre de données, de cluster ou d'hôte valides pour filtrer les machines virtuelles.
Erreur : échec de l'instanciation d'une connexion à VirtualCenter à l'adresse IP	Solutions possibles : * Vérifier les informations d'identification et l'adresse IP saisies. * Essayez de communiquer avec Virtual Center à l'aide de VMware Infrastructure Client. * Essayez de communiquer avec Virtual Center à l'aide du navigateur d'objets gérés (par exemple MOB).
Erreur : VirtualCenter sur IP possède un certificat non conforme requis par JVM	Solutions possibles : * Recommandé : régénérez le certificat pour Virtual Center en utilisant une clé RSA plus forte (par exemple 1 024 bits). * Non recommandé : modifiez la configuration java.security de la JVM pour exploiter la contrainte jdk.certpath.disabledAlgorithms afin d'autoriser la clé RSA 512 bits. Voir "Notes de publication de la mise à jour 40 du JDK 7" .
Je vois le message : « Le package VMware Logs n'est pas pris en charge sur VMware avant la version 8.0.1 »	La collecte de journaux n'est pas prise en charge sur les versions de VMware antérieures à 8.0.1. Mettez à niveau votre infrastructure VI Center vers la version 8.0.1 ou une version ultérieure si vous souhaitez utiliser la fonctionnalité Collections de journaux dans Data Infrastructure Insights. Pour plus d'informations, voir ceci"Article de la base de connaissances" .

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Référence du collecteur de données - Services

Collecte de données de nœuds

Data Infrastructure Insights collecte les métriques du nœud sur lequel vous installez un agent.

Installation

1. Dans **Observabilité > Collecteurs**, choisissez un système d'exploitation/une plateforme. Notez que l'installation de n'importe quel collecteur de données d'intégration (Kubernetes, Docker, Apache, etc.) configurera également la collecte de données de nœud.
2. Suivez les instructions pour configurer l'agent. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés en tant que métriques de nœud :

Objet:	Identifiants :	Attributs:	Points de données :
Système de fichiers Node	Type de chemin d'accès du périphérique UUID du nœud	IP du nœud Nom du nœud Mode du système d'exploitation du nœud	Inodes libres Inodes libres Total des inodes utilisés Total utilisé Total utilisé
Disque de nœud	Disque UUID du nœud	IP du nœud Nom du nœud Système d'exploitation du nœud	Temps d'E/S Total des IOPS en cours Octets lus (par seconde) Temps de lecture Total des lectures (par seconde) Temps d'E/S pondéré Total des octets d'écriture (par seconde) Temps d'écriture Total des écritures (par seconde) Longueur actuelle de la file d'attente du disque Temps d'écriture Temps de lecture Temps d'E/S
Nœud CPU	UUID du nœud CPU	IP du nœud Nom du nœud Système d'exploitation du nœud	Utilisation du processeur système Utilisation du processeur utilisateur Utilisation du processeur inactif Utilisation du processeur du processeur Utilisation du processeur d'interruption Utilisation du processeur DPC

Objet:	Identifiants :	Attributs:	Points de données :
Nœud	Nœud UUID	IP du nœud Nom du nœud Système d'exploitation du nœud	Temps de démarrage du noyau Changements de contexte du noyau (par seconde) Entropie du noyau disponible Interruptions du noyau (par seconde) Processus du noyau forkés (par seconde) Mémoire Mémoire active disponible Mémoire totale disponible Mémoire tamponnée Mémoire en cache Limite de validation Mémoire validée en tant que mémoire Mémoire sale Mémoire libre élevée Mémoire libre élevée Mémoire totale énorme Taille de page Mémoire Grandes pages Mémoire libre Grandes pages Mémoire totale faible Mémoire libre faible Mémoire totale Mémoire mappée Tables de pages Mémoire Mémoire partagée Mémoire en bloc Swap Mémoire en cache Swap Mémoire libre Swap Mémoire totale Mémoire totale utilisée Mémoire totale utilisée Mémoire Vmalloc Bloc de mémoire Vmalloc Mémoire totale Vmalloc Mémoire utilisée Mémoire câblée Écriture différée Mémoire totale Écriture différée Mémoire temporaire Défauts de cache Demande de mémoire Défauts de page mémoire Pages mémoire Mémoire non paginée Mémoire paginée Cache Mémoire principale Cache de secours Mémoire normale Cache de secours Réserve de mémoire Défauts de transition Processus Processus bloqués Processus morts Processus inactifs Processus de pagination

Objet:	Identifiants :	Attributs:	Points de données :
Réseau de nœuds	UUID du nœud d'interface réseau	Nom du nœud IP du nœud Système d'exploitation du nœud	Octets reçus Octets envoyés Paquets sortants Paquets rejetés Erreurs sortantes Paquets reçus Paquets rejetés Erreurs reçues Paquets reçus Paquets envoyés

Installation

Les informations de configuration et de dépannage sont disponibles sur le"Configuration d'un agent" page.

Collecteur de données ActiveMQ

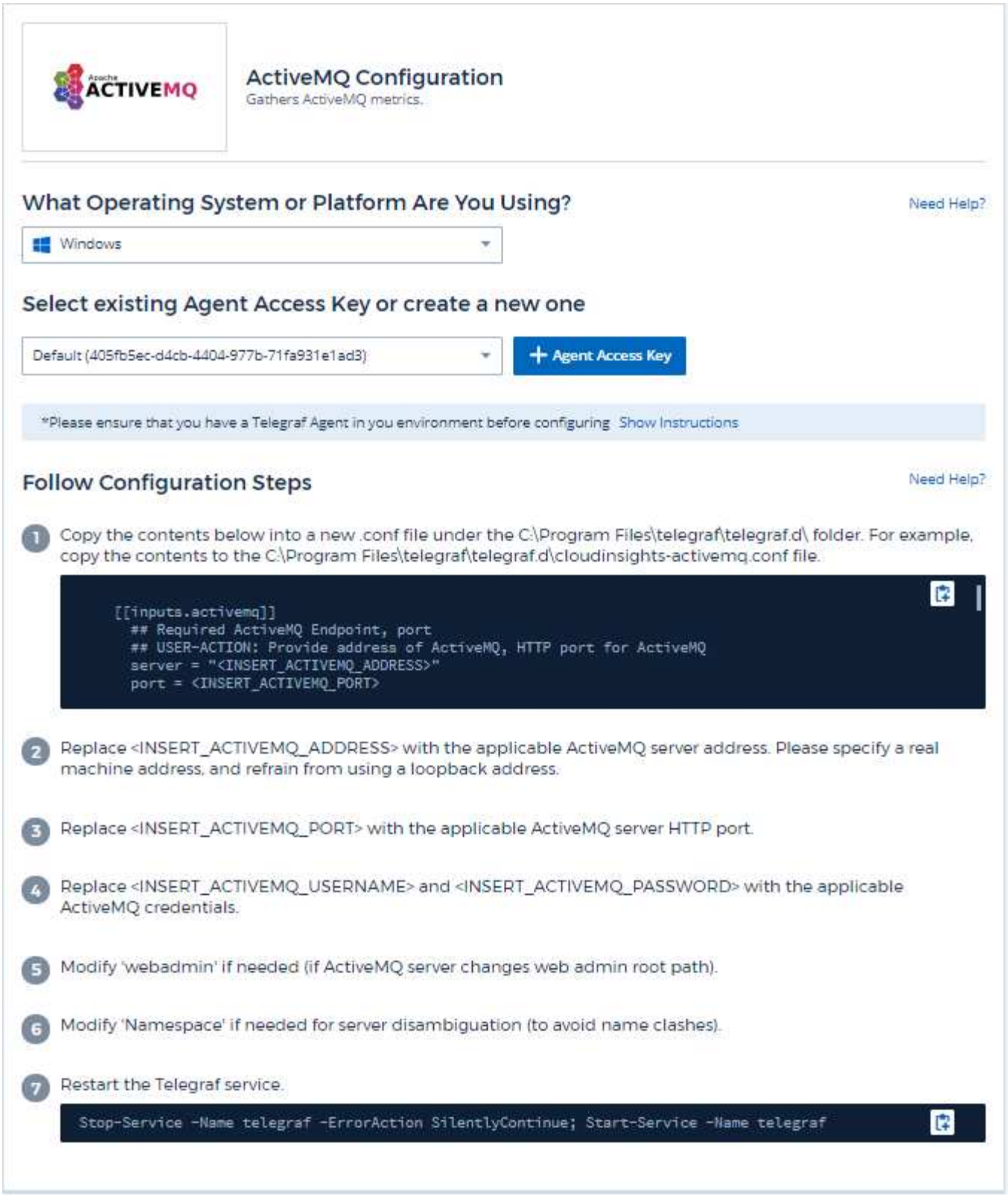
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir d'ActiveMQ.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez ActiveMQ.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le "Documentation d'ActiveMQ"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
File d'attente ActiveMQ	Serveur de port de file d'attente d'espace de noms	Nom du nœud IP du nœud UUID du nœud	Nombre de consommateurs Nombre de sorties de file d'attente Nombre de mises en file d'attente Taille de la file d'attente
Abonné ActiveMQ	ID client ID de connexion Port Espace de noms du serveur	Est actif Nom du nœud de destination IP du nœud UUID du nœud Sélecteur de système d'exploitation du nœud Abonnement	Nombre de sorties de file d'attente Nombre de sorties expédiées Taille de la file d'attente expédiée Nombre de sorties de file d'attente Taille de la file d'attente en attente
Sujet ActiveMQ	Espace de noms du serveur de port de sujet	Nom du nœud IP du nœud UUID du nœud Système d'exploitation du nœud	Nombre de consommateurs Nombre de sorties de file d'attente Nombre de mises en file d'attente Taille

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Apache

Ce collecteur de données permet la collecte de données à partir des serveurs Apache sur votre locataire.

Prérequis

- Votre serveur HTTP Apache doit être configuré et fonctionner correctement.
- Vous devez disposer des autorisations sudo ou administrateur sur votre hôte/VM d'agent
- En règle générale, le module Apache *mod_status* est configuré pour exposer une page à l'emplacement '/server-status?auto' du serveur Apache. L'option *ExtendedStatus* doit être activée pour collecter tous les champs disponibles. Pour plus d'informations sur la configuration de votre serveur, consultez la documentation du module Apache : https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

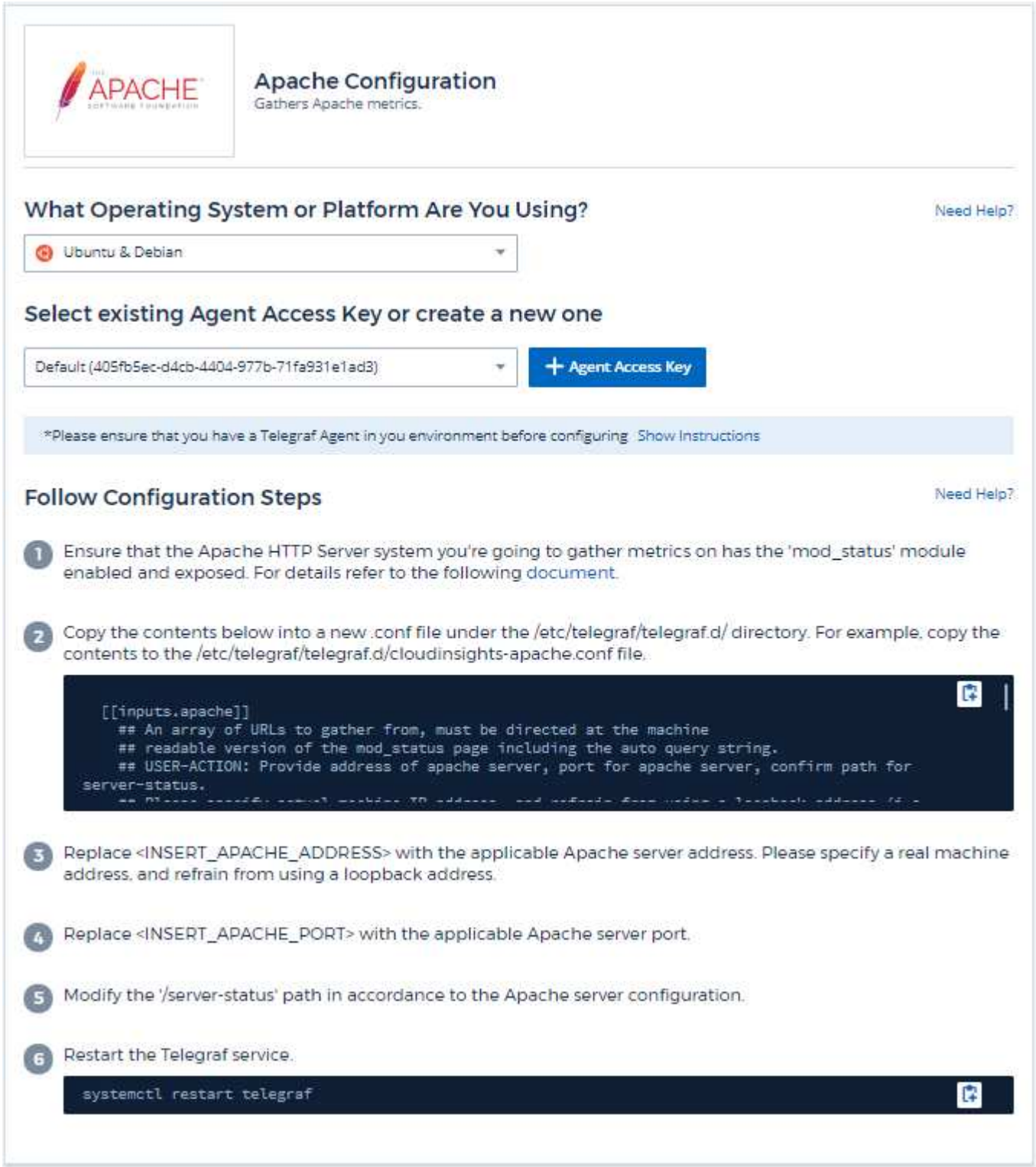
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Apache.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.

3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Le plugin de Telegraf pour le serveur HTTP d'Apache s'appuie sur le module « mod_status » pour être activé. Lorsque cette option est activée, le serveur HTTP d'Apache exposera un point de terminaison HTML qui peut être visualisé sur votre navigateur ou récupéré pour l'extraction de l'état de toute la configuration du serveur HTTP d'Apache.

Compatibilité:

La configuration a été développée sur la version 2.4.38 du serveur HTTP d'Apache.

Activation de mod_status :

L'activation et l'exposition des modules « mod_status » impliquent deux étapes :

- Module d'activation
- Exposer les statistiques du module

Module d'activation :

Le chargement des modules est contrôlé par le fichier de configuration sous '/usr/local/apache/conf/httpd.conf'. Modifiez le fichier de configuration et décommentez les lignes suivantes :

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Exposer les statistiques du module :

L'exposition de « mod_status » est contrôlée par le fichier de configuration sous « /usr/local/apache2/conf/extra/httpd-info.conf ». Assurez-vous d'avoir les éléments suivants dans ce fichier de configuration (au moins, d'autres directives seront présentes) :

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Pour des instructions détaillées sur le module « mod_status », consultez le"Documentation Apache"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Apache	Serveur d'espace de noms	Nœud IP Nom du nœud Port Génération de configuration du serveur parent Génération MPM du serveur parent La disponibilité du serveur s'arrête	Travailleurs occupés Octets par requête Octets par seconde CPU Enfants CPU système Enfants Charge CPU utilisateur CPU système CPU utilisateur Connexions asynchrones Fermeture des connexions asynchrones Maintien en activité des connexions asynchrones Écriture des connexions Durée totale par requête Travailleurs inactifs Charge moyenne (dernier 1 min) Charge moyenne (derniers 15 min) Charge moyenne (derniers 5 min) Processus Requêtes par seconde Accès totaux Durée totale Total Ko Tableau de bord Fermeture Tableau de bord Recherches DNS Tableau de bord Fin Tableau de bord Nettoyage d'inactivité Tableau de bord Maintien en activité Tableau de bord Journalisation Tableau de bord Ouverture Tableau de bord Lecture Tableau de bord Envoi Tableau de bord Démarrage Tableau de bord Attente

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données consulaires

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques auprès de Consul.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Consul.

   Si vous n'avez pas configuré d'agent pour la collecte, vous êtes invité à"installer un agent" sur votre locataire.

   Si vous avez déjà configuré un agent, sélectionnez le système d'exploitation ou la plateforme approprié et cliquez sur **Continuer**.

2. Suivez les instructions de l'écran de configuration du Consul pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.

Installation

Des informations peuvent être trouvées dans le"Documentation du consul" .

Objets et compteurs pour consul

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Consul	Nœud de service d'identification de vérification d'espace de noms	IP du nœud OS du nœud UUID du nœud Nom du nœud Nom du service Nom de vérification ID du service Statut	Avertissement de dépassement critique

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Couchbase

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Couchbase.

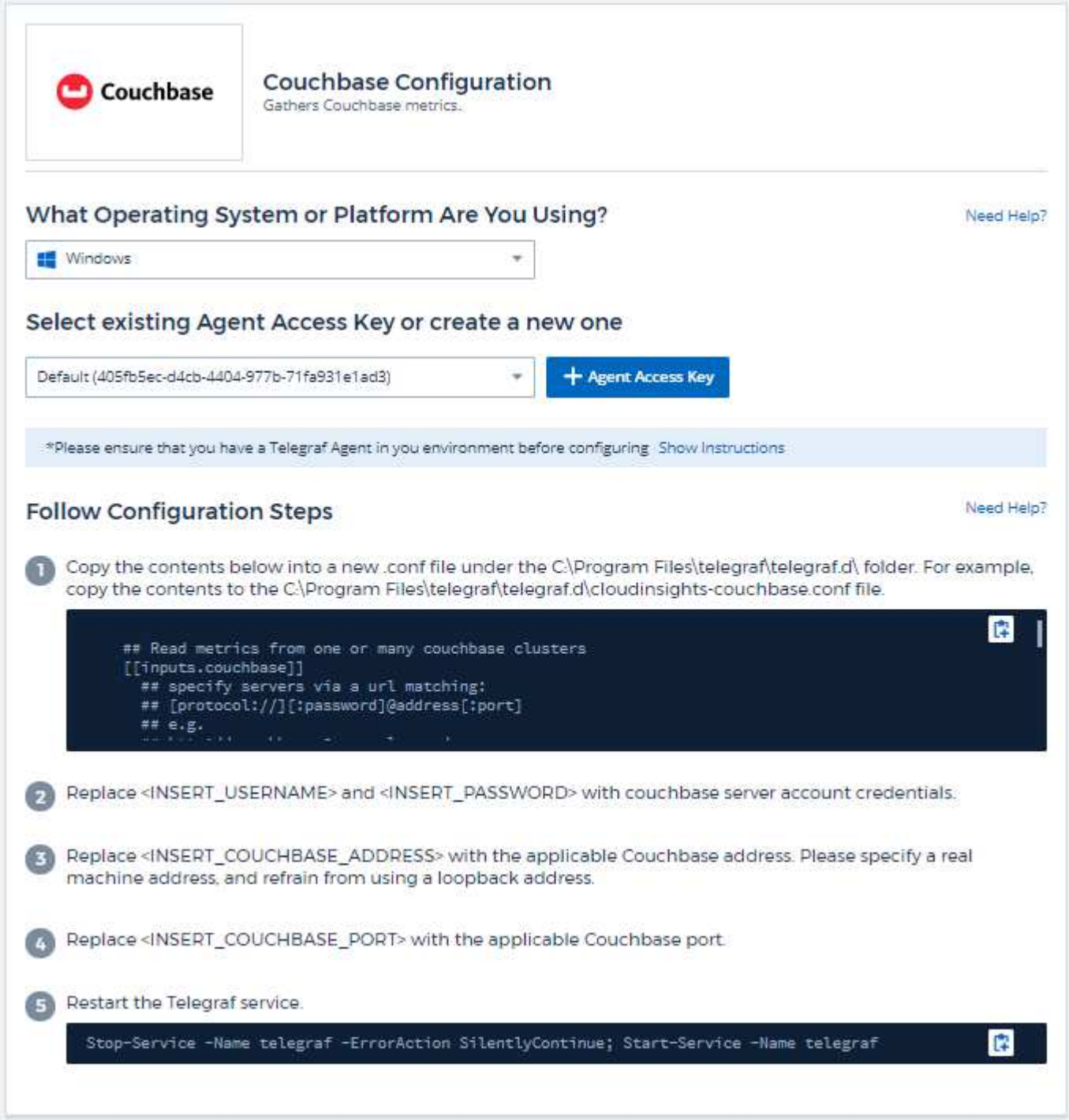
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Couchbase.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en

fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation de Couchbase" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Nœud Couchbase	Espace de noms Cluster Couchbase Node Nom d'hôte	Nom du nœud IP du nœud	Mémoire libre Mémoire totale
Seau Couchbase	Cluster de compartiments d'espace de noms	Nom du nœud IP du nœud	Données utilisées Récupérations de données Disque utilisé Nombre d'éléments Mémoire utilisée Opérations par seconde Quota utilisé

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données CouchDB

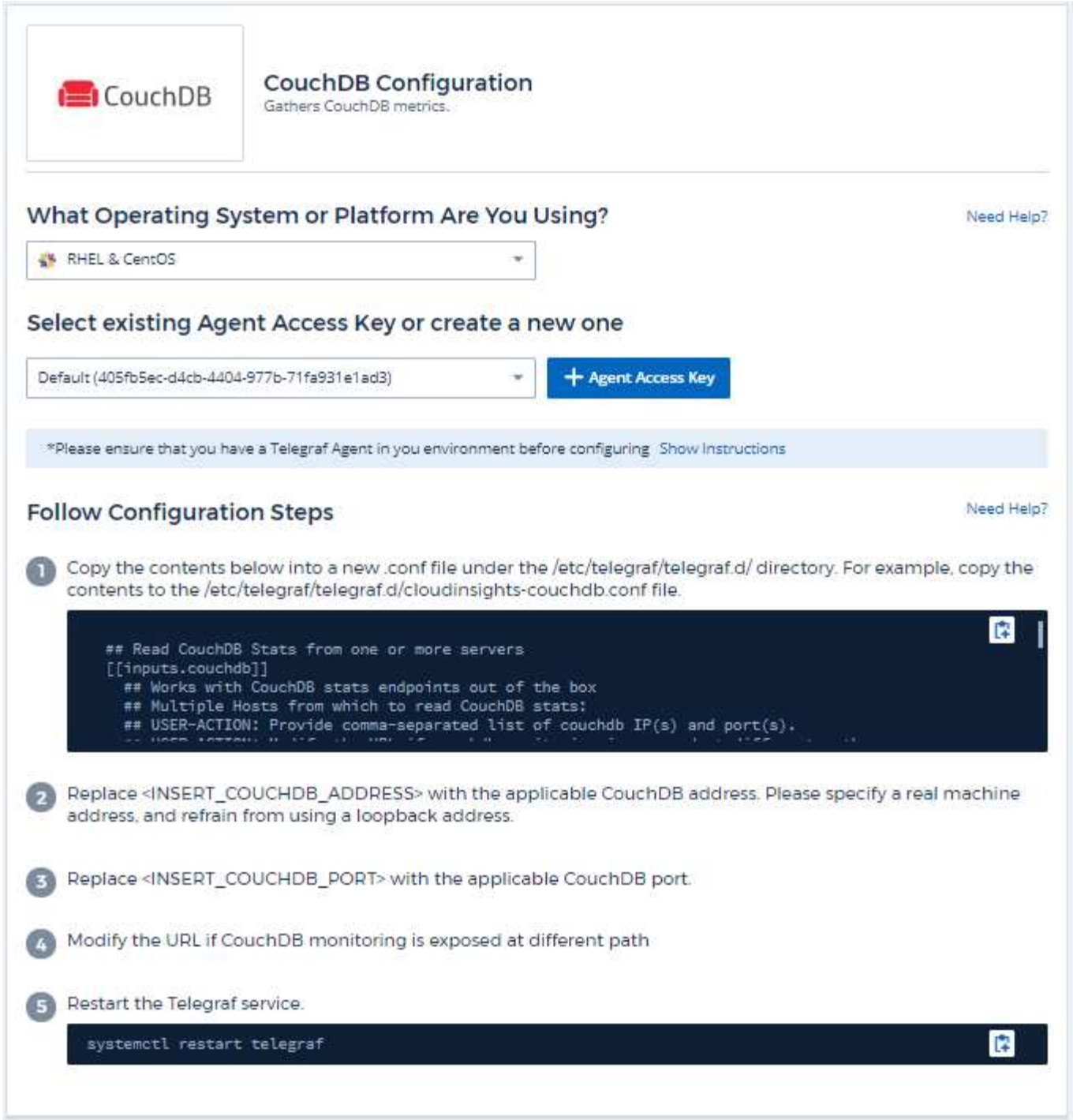
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de CouchDB.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez CouchDB.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation de CouchDB" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
CouchDB	Serveur d'espace de noms	Nom du nœud IP du nœud	Authentification Cache Hits Authentification Cache Miss Lectures de base de données Écritures de base de données Bases de données Ouvrir Ouvrir Fichiers OS Durée maximale de la requête Durée minimale de la requête Méthodes de requête HTTP Copier Méthodes de requête HTTP Supprimer Méthodes de requête HTTP Obtenir Méthodes de requête HTTP En-tête Méthodes de requête HTTP Publier Méthodes de requête HTTP Mettre Codes d'état 200 Codes d'état 201 Codes d'état 202 Codes d'état 301 Codes d'état 304 Codes d'état 400 Codes d'état 401 Codes d'état 403 Codes d'état 404 Codes d'état 405 Codes d'état 409 Codes d'état 412 Codes d'état 500

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Docker

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Docker.

Installation

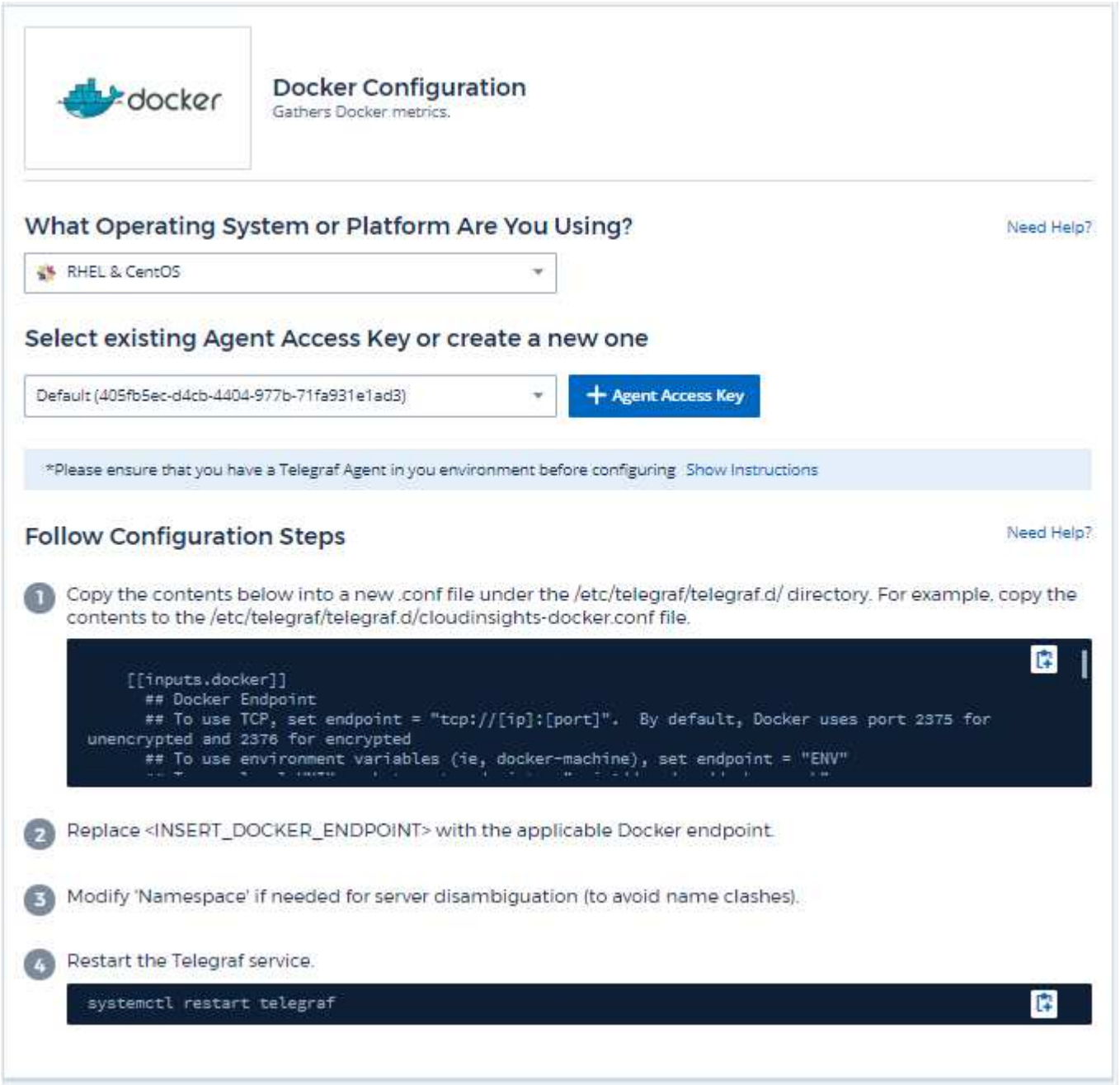
1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Docker.

   Si vous n'avez pas configuré d'agent pour la collecte, vous êtes invité à"installer un agent" sur votre locataire.

   Si vous avez déjà configuré un agent, sélectionnez le système d'exploitation ou la plateforme approprié et cliquez sur **Continuer**.

2. Suivez les instructions de l'écran de configuration Docker pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour

collecter des données.



Installation

Le plugin d'entrée Telegraf pour Docker collecte des métriques via un socket UNIX spécifié ou un point de terminaison TCP.

Compatibilité

La configuration a été développée sur la version Docker 1.12.6.

Installation

Accéder à Docker via un socket UNIX

Si l'agent Telegraf s'exécute sur baremetal, ajoutez l'utilisateur Unix telegraf au groupe Unix docker en exécutant ce qui suit :

```
 sudo usermod -aG docker telegraf
Si l'agent Telegraf s'exécute dans un pod Kubernetes, exposez le socket
Docker Unix en mappant le socket dans le pod en tant que volume, puis en
montant ce volume sur /var/run/docker.sock.  Par exemple, ajoutez ce qui
suit au PodSpec :
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Ensuite, ajoutez les éléments suivants au conteneur :

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Notez que le programme d'installation de Data Infrastructure Insights fourni pour la plateforme Kubernetes prend en charge ce mappage automatiquement.

Accéder à Docker via un point de terminaison TCP

Par défaut, Docker utilise le port 2375 pour l'accès non chiffré et le port 2376 pour l'accès chiffré.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Moteur Docker	Espace de noms Docker Engine	Nom du nœud IP du nœud UUID du nœud Système d'exploitation du nœud Cluster Kubernetes Version Docker Unité	Conteneurs de mémoire Conteneurs Conteneurs en pause Conteneurs en cours d'exécution CPU arrêtés Routines Go Images Événements d'écoute utilisés Descripteurs de fichiers Données Données disponibles Données totales utilisées Métadonnées Métadonnées disponibles Métadonnées totales utilisées Taille de bloc du pool

Objet:	Identifiants :	Attributs:	Points de données :
Conteneur Docker	Espace de noms Nom du conteneur Moteur Docker	Hachage du conteneur Kubernetes Ports du conteneur Kubernetes Nombre de redémarrages du conteneur Kubernetes Chemin du message de fin du conteneur Kubernetes Politique de message de fin du conteneur Kubernetes Période de grâce de fin du pod Kubernetes Image du conteneur État du conteneur Version du conteneur Nom du nœud Chemin du journal du conteneur Kubernetes Nom du conteneur Kubernetes Type Docker Kubernetes Nom du pod Kubernetes Espace de noms du pod Kubernetes UID du pod Kubernetes ID du sandbox Kubernetes IP du nœud UUID du nœud Version Docker Configuration E/S Kubernetes vue Source de la configuration E/S Kubernetes OpenShift IO SCC Description Kubernetes Nom d'affichage Kubernetes Balises OpenShift Service Kompose Modèle de pod Contrôleur de hachage Révision du hachage Génération du modèle de pod Licence Date de build du schéma Nom du schéma de licence URL du schéma URL du VCS du schéma Fournisseur du schéma Version du schéma Schéma Responsable de la version du schéma Pod client Kubernetes StatefulSet Nom du pod Tenant Architecture de la console Web URL source faisant autorité Date de build Hôte de build RH Distribution des composants RH Portée	Mémoire active, anonyme, fichier actif, cache, limite hiérarchique, mémoire inactive, anonyme, fichier inactif, limite de mémoire, fichier mappé, mémoire, utilisation maximale, erreur de page, erreur majeure de page, mémoire paginée, mémoire paginée, mémoire sortante, taille de l'ensemble résident, mémoire, taille de l'ensemble résident, énorme mémoire, mémoire anonyme active totale, fichier actif, mémoire cache totale, mémoire anonyme inactive totale, fichier inactif, mémoire, fichier mappé, mémoire, erreur de page, erreur majeure de page, mémoire paginée, mémoire sortante, mémoire, taille de l'ensemble résident, mémoire, taille de l'ensemble résident, énorme mémoire, mémoire non supprimable, utilisation de la mémoire non supprimable, pourcentage d'utilisation de la mémoire, code de sortie, OOM, PID tué, commencé à la série d'échecs.

Objet:	Identifiants :	Attributs:	Points de données :
Bloc d’E/S du conteneur Docker	Espace de noms Nom du conteneur Appareil Moteur Docker	Hachage du conteneur Kubernetes Ports du conteneur Kubernetes Nombre de redémarrages du conteneur Kubernetes Chemin du message de fin du conteneur Kubernetes Politique de message de fin du conteneur Kubernetes Période de grâce de fin du pod Kubernetes Image du conteneur État du conteneur Version du conteneur Nom du nœud Chemin du journal du conteneur Kubernetes Nom du conteneur Kubernetes Type Docker Kubernetes Nom du pod Kubernetes Espace de noms du pod Kubernetes UID du pod Kubernetes ID du sandbox Kubernetes IP du nœud UUID du nœud Version Docker Configuration Kubernetes vue Source de la configuration Kubernetes OpenShift SCC Description Kubernetes Nom d’affichage Kubernetes Balises OpenShift Schéma Version du schéma Modèle de pod Contrôleur de hachage Révision Génération du modèle de pod de hachage Service Kompose Date de build du schéma Licence du schéma Nom du schéma Fournisseur de schéma Pod client Kubernetes StatefulSet Nom du pod Tenant Console Web Date de build Licence Fournisseur Architecture URL source faisant autorité Hôte de build RH Distribution des composants RH Portée Installation Responsable Publication Résumé de l’exécution Désinstallation	Octets de service d’E/S récursifs asynchrones Octets de service d’E/S récursifs en lecture Octets de service d’E/S récursifs en synchronisation Octets de service d’E/S récursifs Total d’octets de service d’E/S récursifs en écriture Octets de service d’E/S récursifs asynchrones avec service d’E/S récursifs en lecture Octets de service d’E/S récursifs en synchronisation avec service d’E/S récursifs Total d’E/S récursifs en écriture

Objet:	Identifiants :	Attributs:	Points de données :
Réseau de conteneurs Docker	Espace de noms Conteneur Nom Réseau Moteur Docker	Image du conteneur État du conteneur Version du conteneur Nom du nœud IP du nœud UUID du nœud Système d'exploitation du nœud Cluster K8s Version Docker ID du conteneur	RX Octets RX supprimés Erreurs RX Paquets RX TX Octets TX supprimés Erreurs TX Paquets TX

Objet:	Identifiants :	Attributs:	Points de données :
Processeur du conteneur Docker	Espace de noms Nom du conteneur CPU Moteur Docker	Hachage du conteneur Kubernetes Ports du conteneur Kubernetes Nombre de redémarrages du conteneur Kubernetes Chemin du message de fin du conteneur Kubernetes Politique de message de fin du conteneur Kubernetes Période de grâce de fin du pod Kubernetes Configuration Kubernetes vue Source de la configuration Kubernetes Image conteneur SCC OpenShift État du conteneur Version du conteneur Nom du nœud Chemin du journal du conteneur Kubernetes Nom du conteneur Kubernetes Type Docker Kubernetes Nom du pod Kubernetes Espace de noms du pod Kubernetes UID du pod Kubernetes ID du sandbox Kubernetes IP du nœud UUID du nœud Système d'exploitation du nœud Cluster Kubernetes Version Docker Description Kubernetes Nom d'affichage Kubernetes Balises OpenShift Version du schéma Modèle de pod Contrôleur de hachage Révision Génération du modèle de pod de hachage Service Kompose Date de build du schéma Licence du schéma Nom du schéma Fournisseur de schéma Pod client Kubernetes StatefulSet Nom du pod Tenant Date de build de la console Web Licence Fournisseur Architecture URL source faisant autorité Hôte de build RH Distribution des composants RH Portée Installer Responsable de	Périodes de limitation Périodes de limitation Durée de limitation Utilisation en mode noyau Utilisation en mode utilisateur Pourcentage d'utilisation Utilisation du système Total

Dépannage

Problème:	Essayez ceci:
Je ne vois pas mes métriques Docker dans Data Infrastructure Insights après avoir suivi les instructions sur la page de configuration.	Vérifiez les journaux de l'agent Telegraf pour voir s'il signale l'erreur suivante : E! Erreur dans le plugin [inputs.docker] : l'autorisation a été refusée lors de la tentative de connexion au socket du démon Docker. Si c'est le cas, prenez les mesures nécessaires pour fournir à l'agent Telegraf l'accès au socket Docker Unix comme spécifié ci-dessus.

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

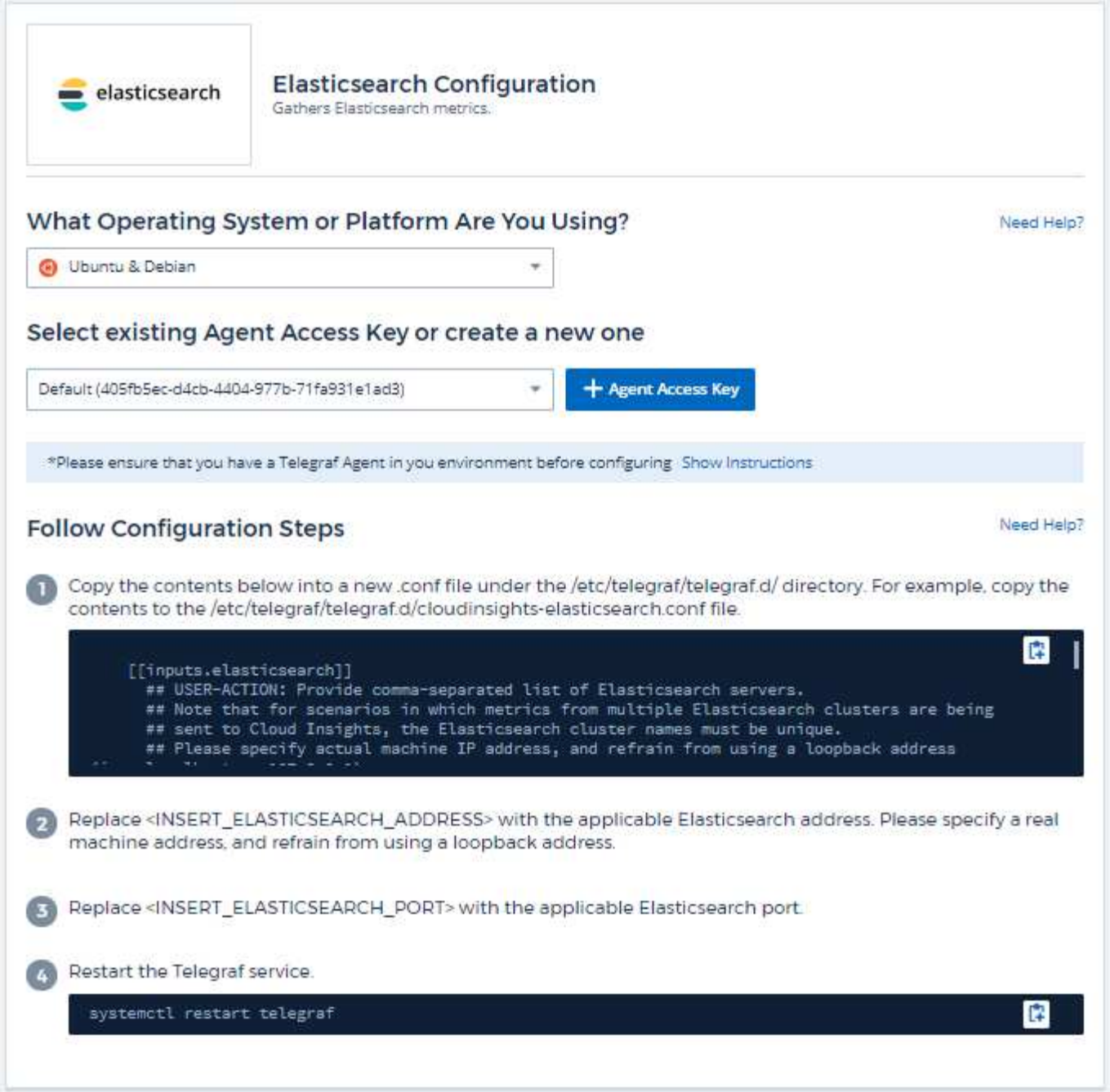
Collecteur de données Elasticsearch

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir d'Elasticsearch.

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Elasticsearch.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation d'Elasticsearch" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:
Cluster Elasticsearch	Cluster d'espace de noms	Nœud IP Nom du nœud Statut du cluster

Objet:	Identifiants :	Attributs:
Nœud Elasticsearch	Espace de noms Cluster ID du nœud ES IP du nœud ES Nœud ES	ID de zone

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Flink

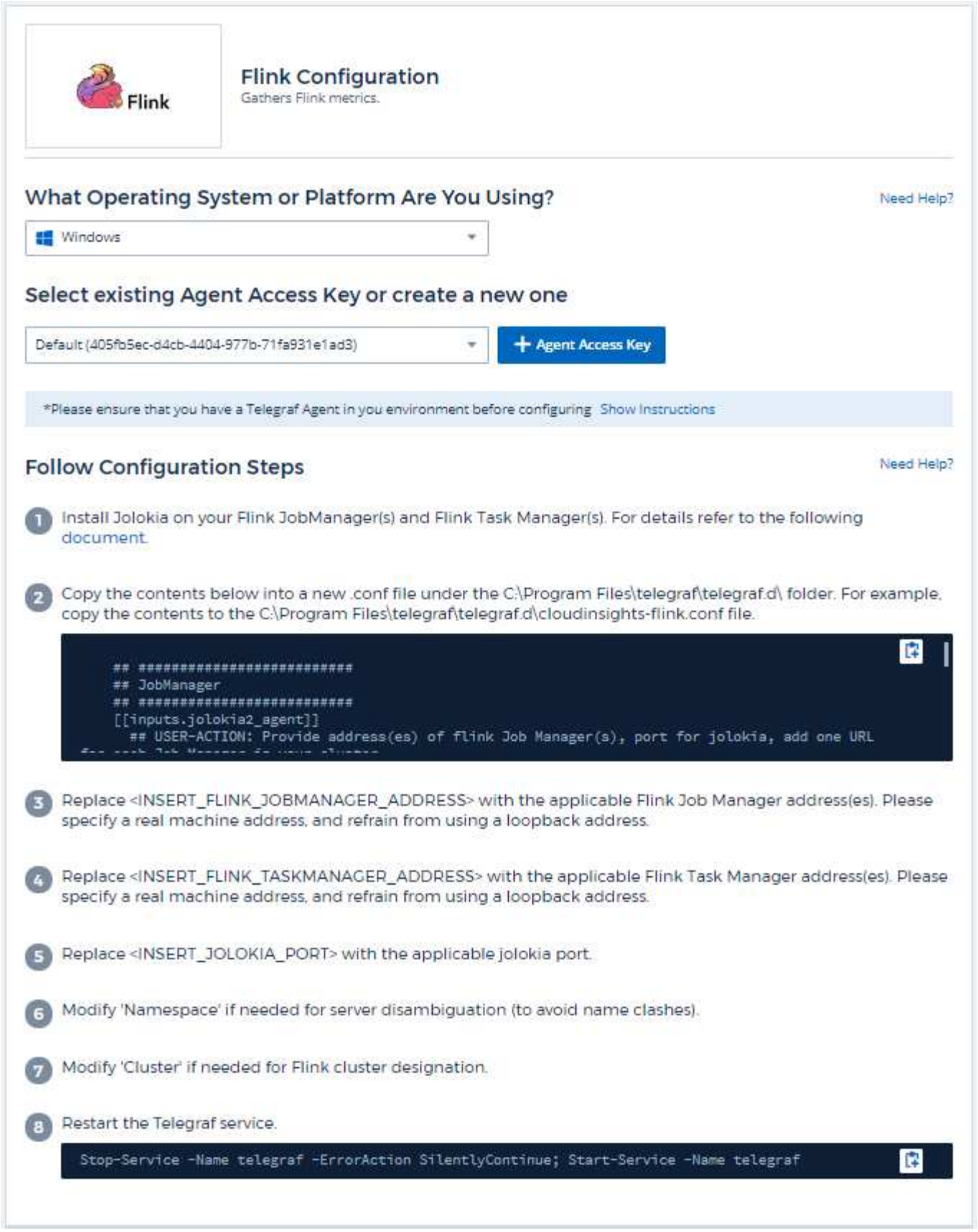
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques de Flink.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Flink.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Un déploiement Flink complet implique les composants suivants :

JobManager : le système principal de Flink. Coordonne une série de gestionnaires de tâches. Dans une configuration haute disponibilité, le système aura plus d'un JobManager. Gestionnaire des tâches : c'est ici que les opérateurs Flink sont exécutés. Le plugin Flink est basé sur le plugin Jolokia de Telegraf. En tant qu'exigence de collecte d'informations à partir de tous les composants Flink, JMX doit être configuré et exposé via Jolokia sur tous les composants.

Compatibilité

La configuration a été développée par rapport à la version 1.7.0 de Flink.

Installation

Agent Jar Jolokia

Pour tous les composants individuels, une version du fichier jar de l'agent Jolokia doit être téléchargée. La version testée était"Agent Jolokia 1.6.0" .

Les instructions ci-dessous supposent que le fichier jar téléchargé (jolokia-jvm-1.6.0-agent.jar) est placé sous l'emplacement « /opt/flink/lib/ ».

Gestionnaire de tâches

Pour configurer JobManager afin d'exposer l'API Jolokia, vous pouvez configurer la variable d'environnement suivante sur vos nœuds, puis redémarrer JobManager :

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Vous pouvez choisir un port différent pour Jolokia (8778).  Si vous
disposez d'une IP interne sur laquelle verrouiller Jolokia, vous pouvez
remplacer le « catch all » 0.0.0.0 par votre propre IP.  Notez que cette
IP doit être accessible depuis le plugin Telegraf.
```

Gestionnaire de tâches

Pour configurer les gestionnaires de tâches afin d'exposer l'API Jolokia, vous pouvez configurer la variable d'environnement suivante sur vos nœuds, puis redémarrer le gestionnaire de tâches :

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Vous pouvez choisir un port différent pour Jolokia (8778).  Si vous
disposez d'une IP interne sur laquelle verrouiller Jolokia, vous pouvez
remplacer le « catch all » 0.0.0.0 par votre propre IP.  Notez que cette
IP doit être accessible depuis le plugin Telegraf.
```

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Gestionnaire de tâches Flink	Serveur d’espace de noms de cluster	Nom du nœud ID du gestionnaire de tâches IP du nœud	Segments de mémoire réseau disponibles Segments de mémoire réseau totaux Nombre de nettoyages PS (nettoyage de la mémoire) Temps de nettoyage PS (nettoyage de la mémoire) Nombre de nettoyages PS (nettoyage de la mémoire) Temps de nettoyage PS (nettoyage de la mémoire) Mémoire du tas engagée Mémoire du tas d’initialisation Mémoire du tas max. utilisée Nombre de threads Nombre de threads du démon Nombre maximal de threads Nombre total de threads démarrés
Flink Job	ID de tâche du serveur d’espace de noms de cluster	Nom du nœud Nom du travail IP du nœud Dernier point de contrôle Chemin externe Heure de redémarrage	Temps d’arrêt Redémarrages complets Alignement du dernier point de contrôle Mise en mémoire tampon Durée du dernier point de contrôle Taille du dernier point de contrôle Nombre de points de contrôle terminés Nombre de points de contrôle échoués Nombre de points de contrôle en cours Nombre de points de contrôle Temps de disponibilité

Objet:	Identifiants :	Attributs:	Points de données :
Gestionnaire de tâches Flink	Serveur d’espace de noms de cluster	Nom du nœud IP du nœud	Nombre de nettoyages PS MarkSweep pour la collecte des déchets Temps de nettoyage PS MarkSweep Nombre de nettoyages PS pour la collecte des déchets Temps de nettoyage PS pour la collecte des déchets Mémoire du tas engagée Mémoire du tas d’initialisation Mémoire maximale du tas utilisée Nombre de gestionnaires de tâches enregistrés Nombre de tâches en cours d’exécution Emplacements de tâches disponibles Nombre total de threads Nombre de threads du démon Nombre maximal de threads Nombre total de threads démarrés

Objet:	Identifiants :	Attributs:	Points de données :
Tâche Flink	Espace de noms du cluster ID de travail ID de tâche	Nom du nœud du serveur Nom du travail Index des sous-tâches ID de tentative de tâche Numéro de tentative de tâche Nom de la tâche ID du gestionnaire de tâches IP du nœud Filigrane d'entrée actuel	Tampons dans le pool Utilisation Tampons dans la file d'attente Longueur Tampons en sortie du pool Utilisation Tampons en sortie Longueur de la file d'attente Nombre Tampons en local Nombre Tampons en local par seconde Nombre Tampons en local Taux par seconde Nombre Tampons en distant Nombre Tampons en distant par seconde Nombre Tampons en distant Taux par seconde Nombre Tampons en sortie Nombre Tampons en sortie par seconde Nombre Tampons en sortie par seconde Nombre Octets en local Nombre Octets en local par seconde Nombre Octets en local par seconde Nombre Octets en local par seconde Nombre Octets en distant Nombre Octets en distant par seconde Nombre Octets en distant par seconde Nombre Octets en sortie Nombre Octets en sortie par seconde Nombre Octets en sortie par seconde Nombre Enregistrements en entrée Nombre Enregistrements en entrée par seconde Nombre Enregistrements en entrée par seconde Nombre Enregistrements en sortie Nombre Enregistrements en sortie par seconde Nombre Enregistrements en sortie par seconde Nombre Enregistrements en sortie par seconde Nombre Enregistrements en sortie par seconde

Objet:	Identifiants :	Attributs:	Points de données :
Opérateur de tâche Flink	Espace de noms du cluster ID de travail ID d'opérateur ID de tâche	Nom du nœud du serveur Nom du travail Nom de l'opérateur Index des sous-tâches ID de tentative de tâche Numéro de tentative de tâche Nom de la tâche ID du gestionnaire de tâches IP du nœud	Filigrane d'entrée actuel Filigrane de sortie actuel Nombre d'enregistrements entrants Nombre d'enregistrements entrants par seconde Nombre d'enregistrements entrants par seconde Taux Nombre d'enregistrements sortants Nombre d'enregistrements sortants par seconde Taux Nombre d'enregistrements en retard abandonnés Partitions affectées Octets Taux de consommation Latence de validation Latence de validation moyenne Taux de validation maximal Validations échouées Validations réussies Taux de fermeture de connexion Nombre de connexions Taux de création de connexion Nombre Latence de récupération Latence de récupération moyenne Taux de récupération maximal Taille de récupération Taille moyenne de récupération maximale Délai de limitation de récupération Temps de limitation de récupération moyen Taux de pulsation maximal Taux d'octets entrants Rapport E/S Temps E/S moyen (ns) Rapport d'attente E/S Temps d'attente E/S moyen (ns) Taux de jointure Heure de jointure moyenne Il y a le dernier battement de cœur Taux E/S réseau Taux d'octets sortants Taux de consommation d'enregistrements Retard d'enregistrements Max Enregistrements par requête Taux de requête moyen Taille de requête Taille moyenne de requête

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Hadoop

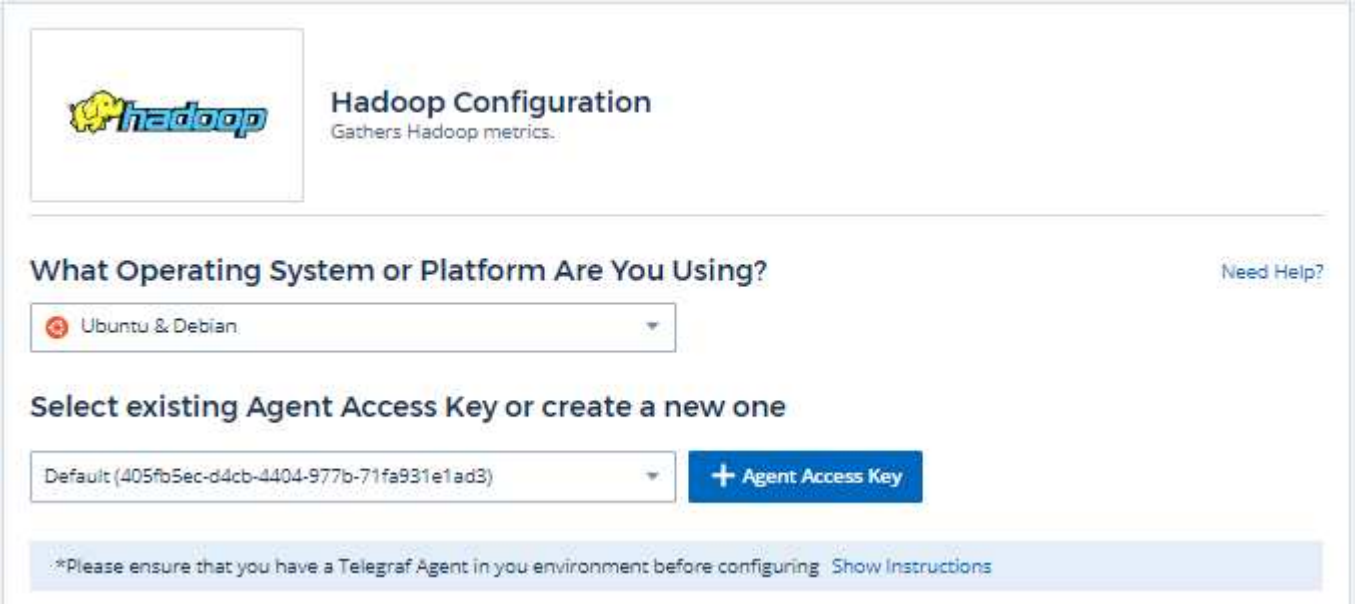
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Hadoop.

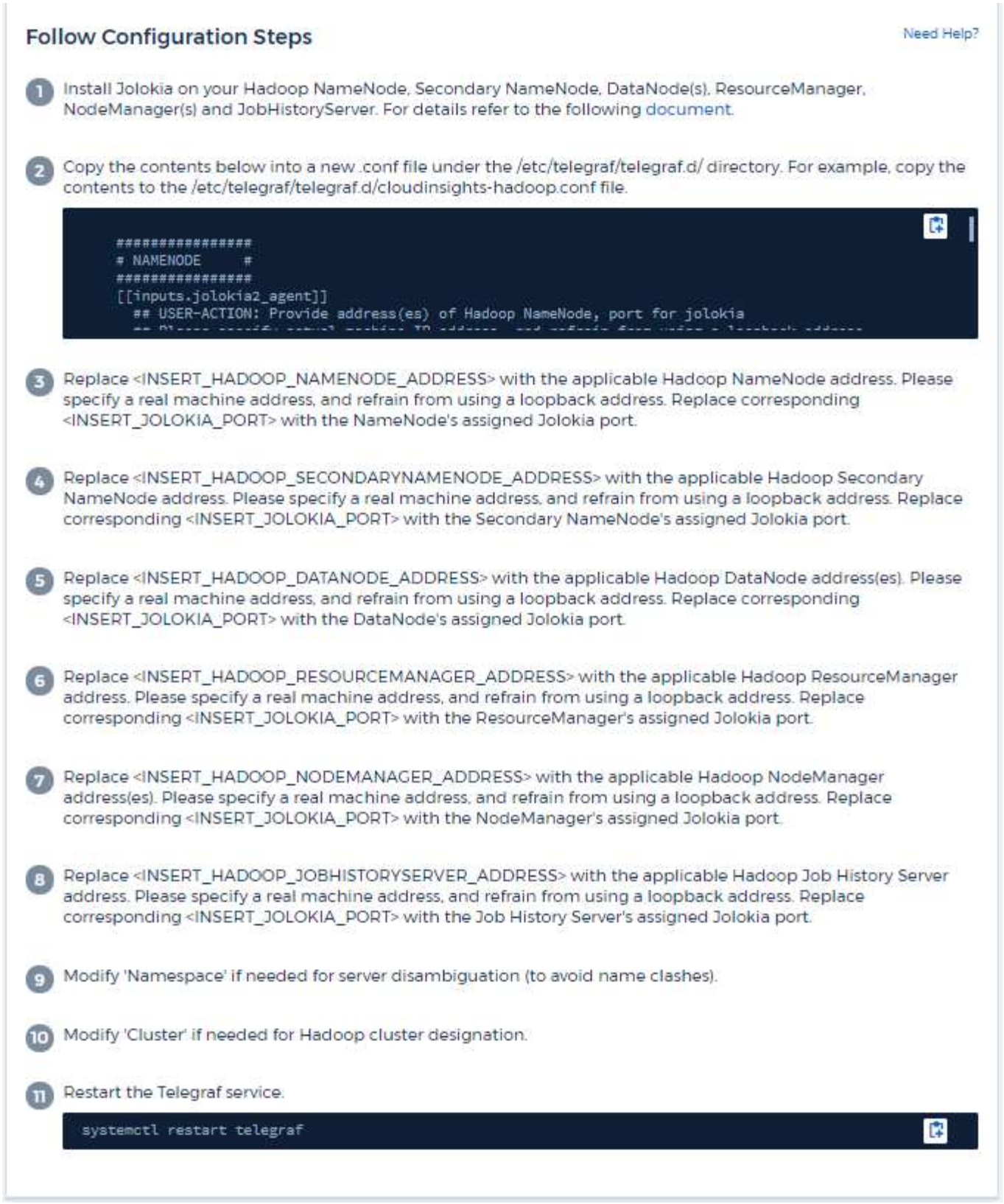
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Hadoop.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.





Installation

Un déploiement Hadoop complet implique les composants suivants :

- NameNode : le système principal du système de fichiers distribué Hadoop (HDFS). Coordonne une série de DataNodes.

- NameNode secondaire : un basculement à chaud pour le NameNode principal. Dans Hadoop, la promotion vers NameNode ne se produit pas automatiquement. Le NameNode secondaire collecte les informations du NameNode pour être prêt à être promu en cas de besoin.
- DataNode : propriétaire actuel des données.
- ResourceManager : le système de calcul principal (Yarn). Coordonne une série de NodeManagers.
- NodeManager : la ressource pour le calcul. Emplacement réel d'exécution des applications.
- JobHistoryServer : responsable du traitement de toutes les demandes liées à l'historique des tâches.

Le plugin Hadoop est basé sur le plugin Jolokia de Telegraf. En tant qu'exigence de collecte d'informations à partir de tous les composants Hadoop, JMX doit être configuré et exposé via Jolokia sur tous les composants.

Compatibilité

La configuration a été développée sur la version Hadoop 2.9.2.

Installation

Agent Jar Jolokia

Pour tous les composants individuels, une version du fichier jar de l'agent Jolokia doit être téléchargée. La version testée était"Agent Jolokia 1.6.0" .

Les instructions ci-dessous supposent que le fichier jar téléchargé (jolokia-jvm-1.6.0-agent.jar) est placé sous l'emplacement « /opt/hadoop/lib/ ».

NomNode

Pour configurer NameNode afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <HADOOP_HOME>/etc/hadoop/hadoop-env.sh :

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nom du nœud secondaire

Pour configurer le NameNode secondaire afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <HADOOP_HOME>/etc/hadoop/hadoop-env.sh :

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nœud de données

Pour configurer les DataNodes afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <HADOOP_HOME>/etc/hadoop/hadoop-env.sh :

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Gestionnaire de ressources

Pour configurer le ResourceManager afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <HADOOP_HOME>/etc/hadoop/hadoop-env.sh :

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Gestionnaire de nœuds

Pour configurer les NodeManagers afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <HADOOP_HOME>/etc/hadoop/hadoop-env.sh :

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Serveur d'historique des tâches

Pour configurer le JobHistoryServer afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <HADOOP_HOME>/etc/hadoop/hadoop-env.sh :

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:
Nom du nœud secondaire Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud Informations de compilation Version
Gestionnaire de nœuds Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud
Gestionnaire de ressources Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud
Nœud de données Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud ID du cluster Version
Nom du nœud Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud ID de transaction Dernière heure d'écriture depuis le dernier chargement Modifications État HA État du système de fichiers ID du pool de blocs ID du cluster Informations de compilation Nombre de versions distinctes Version
Serveur d'historique des tâches Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données HAProxy

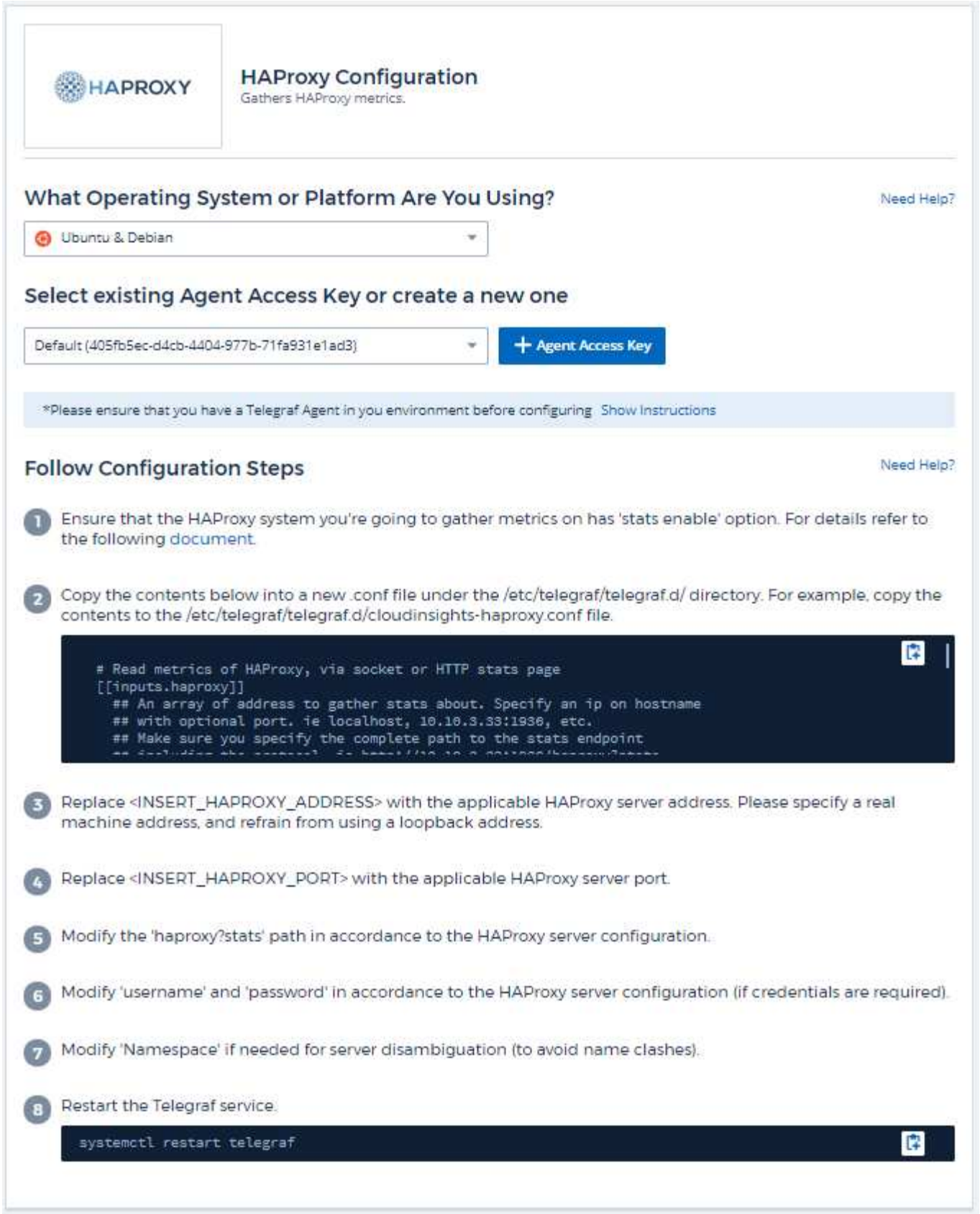
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de HAProxy.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez HAProxy.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Le plugin de Telegraf pour HAProxy repose sur l'activation de HAProxy Stats. Il s'agit d'une configuration intégrée à HAProxy, mais elle n'est pas activée par défaut. Lorsqu'il est activé, HAProxy exposera un point de

terminaison HTML qui peut être visualisé sur votre navigateur ou récupéré pour l'extraction de l'état de toutes les configurations HAProxy.

Compatibilité:

La configuration a été développée par rapport à la version HAProxy 1.9.4.

Installation :

Pour activer les statistiques, modifiez votre fichier de configuration haproxy et ajoutez les lignes suivantes après la section « defaults », en utilisant votre propre nom d'utilisateur/mot de passe et/ou URL haproxy :

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Voici un exemple simplifié de fichier de configuration avec les statistiques activées :

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Pour des instructions complètes et à jour, consultez le"Documentation HAProxy" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Interface HAProxy	Proxy d'adresse d'espace de noms	Nœud IP Nom du nœud ID proxy Mode ID de processus Limite de débit de sessions ID du serveur Limite de sessions Statut	Octets entrants Octets sortants Accès au cache Recherches dans le cache Compression Octets contournés Compression Octets entrants Compression Octets sortants Réponses Taux de connexion Taux de connexion Nombre maximal de connexions Nombre total de requêtes refusées par la règle de connexion Requêtes refusées par des problèmes de sécurité Réponses refusées par des problèmes de sécurité Requêtes refusées par la règle de session Erreurs de requêtes Réponses Réponses 1xx Réponses 2xx Réponses 3xx Réponses 4xx Réponses 5xx Autres requêtes Sessions interceptées Taux Sessions Taux Max Requêtes Taux Requêtes Taux Max Requêtes Total Sessions Sessions Max Sessions Total Requêtes Réécritures

Objet:	Identifiants :	Attributs:	Points de données :
Serveur HAProxy	Serveur proxy d'adresse d'espace de noms	Nœud IP Nom du nœud Heure de fin de vérification Configuration de chute Vérification de la valeur d'intégrité Vérification de la configuration de montée Statut ID proxy Heure de la dernière modification Heure de la dernière session Mode ID de processus ID du serveur Statut Poids	Serveurs actifs Serveurs de sauvegarde Octets entrants Octets sortants Vérifications échouées Abandons de vérification Client Connexions Temps moyen de connexion Temps d'arrêt Total des réponses refusées Erreurs de connexion Erreurs de réponse Réponses 1xx Réponses 2xx Réponses 3xx Réponses 4xx Réponses 5xx Autre serveur sélectionné File d'attente totale File d'attente actuelle Temps moyen maximal de la file d'attente Sessions par seconde Sessions par seconde Temps de réponse maximal de réutilisation de connexion Moyenne Sessions Sessions Transfert de serveur max. Abandons Sessions Total des sessions Temps total Moyenne des requêtes Redispatches Requêtes Nouvelles tentatives Requêtes Réécritures

Objet:	Identifiants :	Attributs:	Points de données :
Backend HAProxy	Proxy d'adresse d'espace de noms	Nœud IP Nom du nœud ID proxy Heure de la dernière modification Heure de la dernière session Mode ID du processus ID du serveur Limite de sessions Statut Poids	Serveurs actifs Serveurs de sauvegarde Octets entrants Octets sortants Accès au cache Consultations dans le cache Vérifications Abandons client Compression Octets contournés Compression Octets entrants Compression Octets sortants Réponses Connexions Temps moyen de connexion Temps d'arrêt Total des requêtes refusées pour des raisons de sécurité Réponses refusées pour des raisons de sécurité Erreurs de connexion Erreurs de réponse Réponses 1xx Réponses 2xx Réponses 3xx Réponses 4xx Réponses 5xx Autre serveur sélectionné File d'attente totale File d'attente actuelle Temps moyen de file d'attente Sessions par seconde Sessions par seconde Nombre maximal de requêtes Réutilisation totale des connexions Temps de réponse moyen Sessions Sessions Nombre maximal d'abandons de transfert de serveur Sessions Total des sessions Temps total Moyenne des requêtes Redispatches Requêtes Nouvelles tentatives Requêtes Réécritures

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données JVM

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques

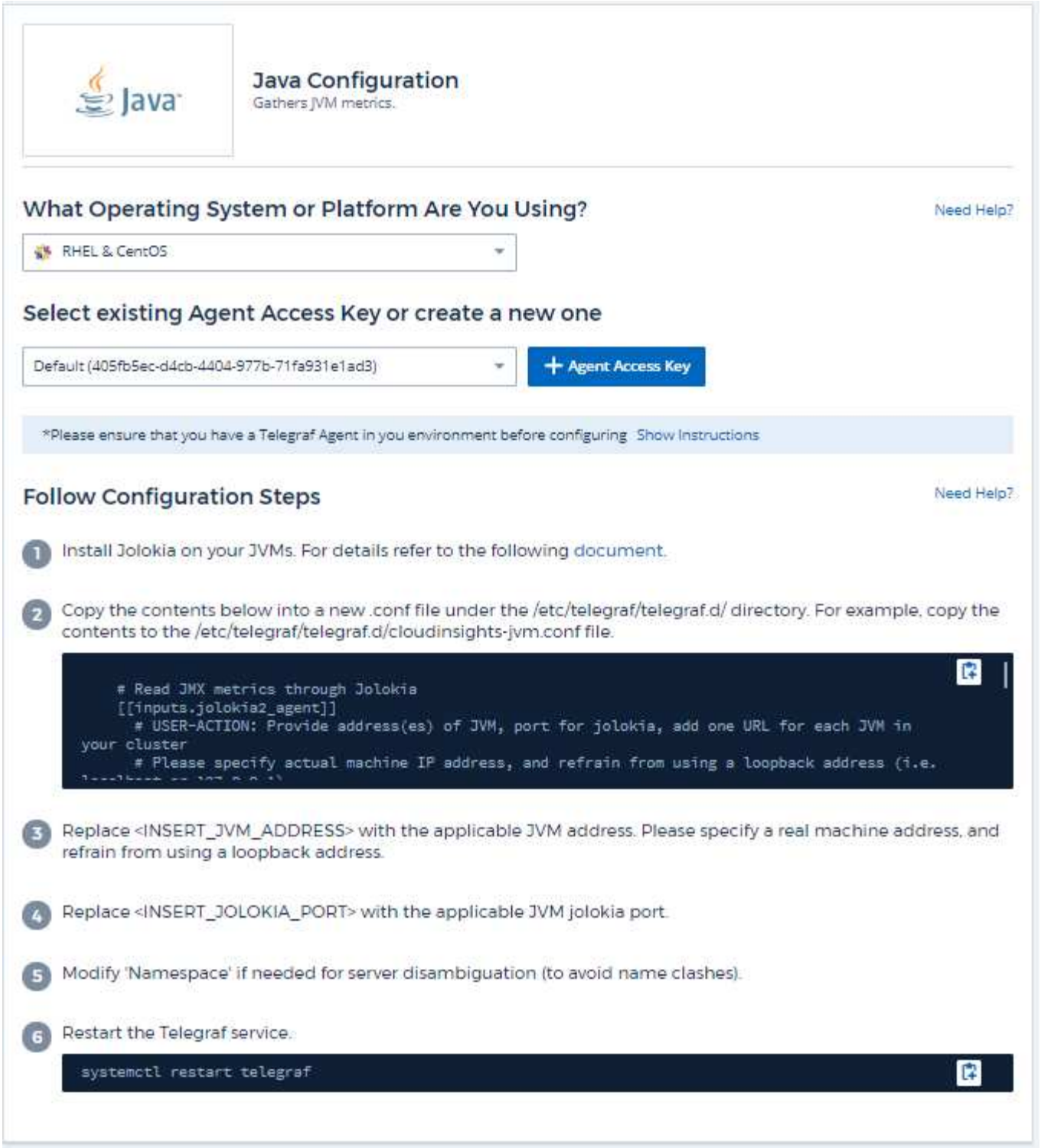
à partir de JVM.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez JVM.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans"Documentation JVM" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
JVM	Espace de noms JVM	Architecture du système d'exploitation Nom du système d'exploitation Version du système d'exploitation Spécification d'exécution Fournisseur de spécifications d'exécution Version de spécification d'exécution Temps de disponibilité Nom de la machine virtuelle d'exécution Fournisseur de la machine virtuelle d'exécution Version de la machine virtuelle d'exécution Nom du nœud IP du nœud	Classe chargée Classe chargée Classe totale déchargée Tas de mémoire Mémoire engagée Tas de mémoire d'initialisation Mémoire utilisée maximale du tas de mémoire utilisée Mémoire non engagée Mémoire non engagée Mémoire non utilisée du tas Mémoire maximale non utilisée du tas Objets en attente de finalisation Processeurs du système d'exploitation disponibles Taille de la mémoire virtuelle engagée du système d'exploitation Taille de la mémoire physique libre du système d'exploitation Taille de l'espace d'échange libre du système d'exploitation Nombre maximal de descripteurs de fichiers du système d'exploitation Nombre de descripteurs de fichiers ouverts du système d'exploitation Charge CPU du processeur du système d'exploitation Temps CPU du processeur du système d'exploitation Charge CPU système du système d'exploitation Charge moyenne du système d'exploitation Taille totale de la mémoire physique du système d'exploitation Taille totale de l'espace d'échange du système d'exploitation Nombre de démons de threads Nombre de pics de threads Nombre de threads Nombre total de threads démarrés Nombre de copies de collecte du ramasse-miettes Heure de collecte des copies du ramasse-miettes Nombre de collectes de marquage-balayage du ramasse-

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Kafka

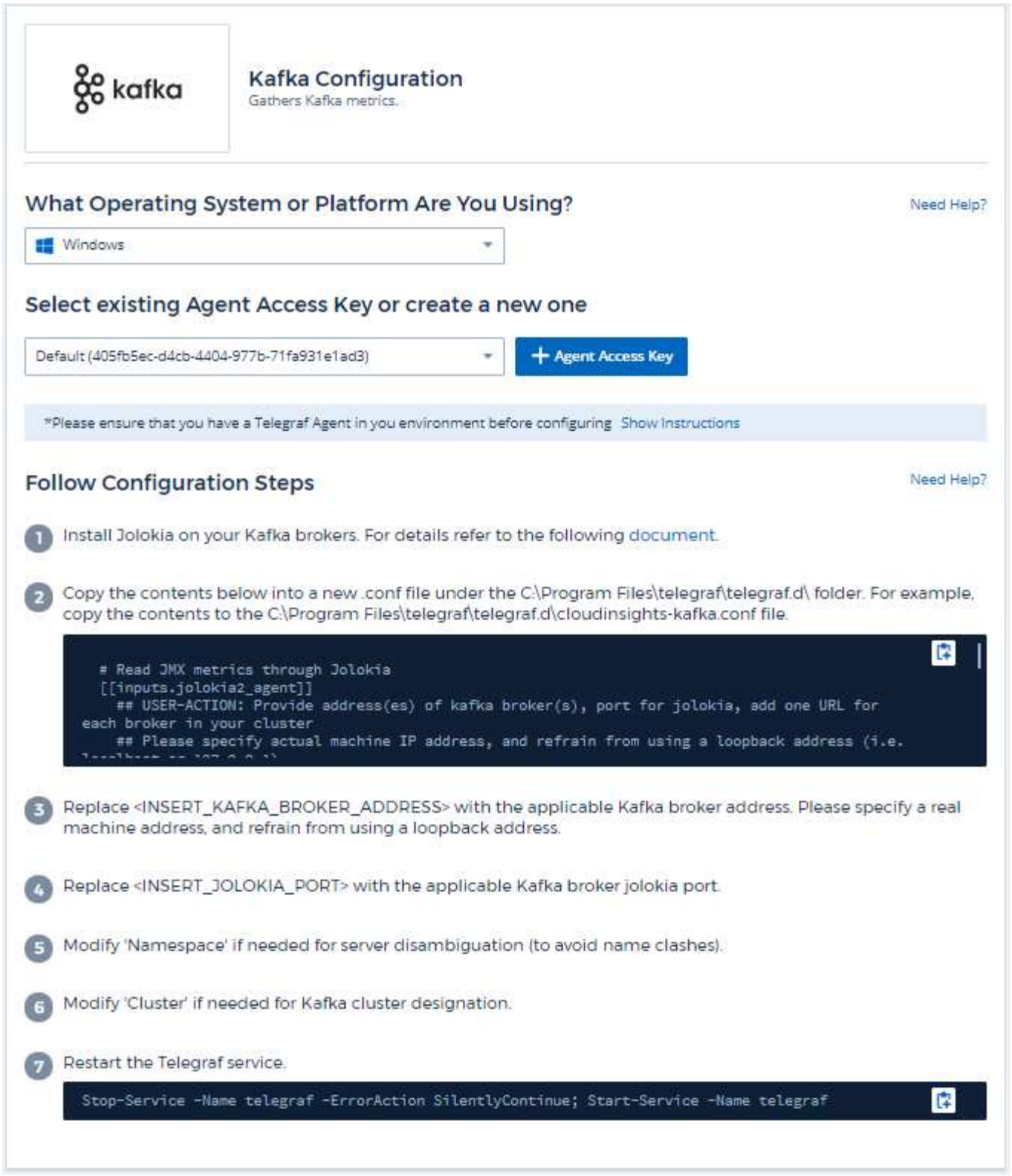
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Kafka.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Kafka.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Le plugin Kafka est basé sur le plugin Jolokia de Telegraf. En tant qu'exigence de collecte d'informations auprès de tous les courtiers Kafka, JMX doit être configuré et exposé via Jolokia sur tous les composants.

Compatibilité

La configuration a été développée sur la version 0.11.0.2 de Kafka.

Mise en place

Toutes les instructions ci-dessous supposent que votre emplacement d'installation pour Kafka est « /opt/kafka ». Vous pouvez adapter les instructions ci-dessous pour refléter votre emplacement d'installation.

Agent Jar Jolokia

Une version du fichier jar de l'agent Jolokia doit être"téléchargé" . La version testée était l'agent Jolokia 1.6.0.

Les instructions ci-dessous supposent que le fichier jar téléchargé (jolokia-jvm-1.6.0-agent.jar) est placé sous l'emplacement « /opt/kafka/libs/ ».

Courtiers Kafka

Pour configurer Kafka Brokers afin d'exposer l'API Jolokia, vous pouvez ajouter ce qui suit dans <KAFKA_HOME>/bin/kafka-server-start.sh, juste avant l'appel 'kafka-run-class.sh' :

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Notez que l'exemple ci-dessus utilise « hostname -I » pour configurer la variable d'environnement « RMI_HOSTNAME ». Dans le cas de machines à plusieurs IP, cela devra être modifié pour collecter l'IP qui vous intéresse pour les connexions RMI.

Vous pouvez choisir un port différent pour JMX (9999 ci-dessus) et Jolokia (8778). Si vous disposez d'une IP interne sur laquelle verrouiller Jolokia, vous pouvez remplacer le « catch all » 0.0.0.0 par votre propre IP. Notez que cette IP doit être accessible depuis le plugin Telegraf. Vous pouvez utiliser l'option '-Dcom.sun.management.jmxremote.authenticate=false' si vous ne souhaitez pas vous authentifier. Utilisez-le à vos propres risques.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:
Courtier Kafka	Courtier d'espace de noms de cluster	Nom du nœud IP du nœud

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Kibana

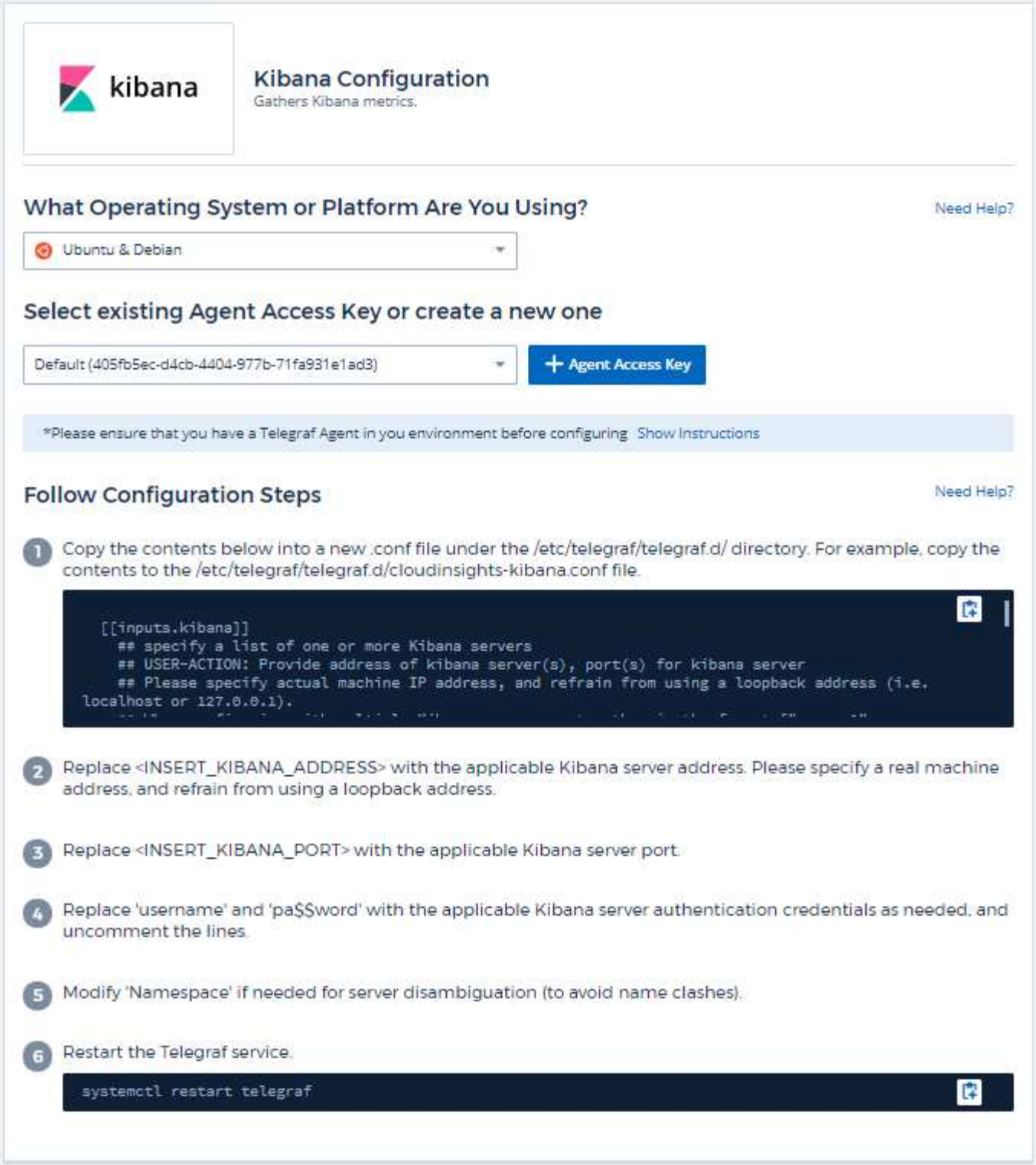
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Kibana.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Kibana.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation de Kibana" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Kibana	Adresse de l'espace de noms	Nœud IP Nom du nœud Version État	Connexions simultanées Tas Tas max. utilisé Requêtes par seconde Temps de réponse Temps de réponse moyen Temps de disponibilité maximal

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

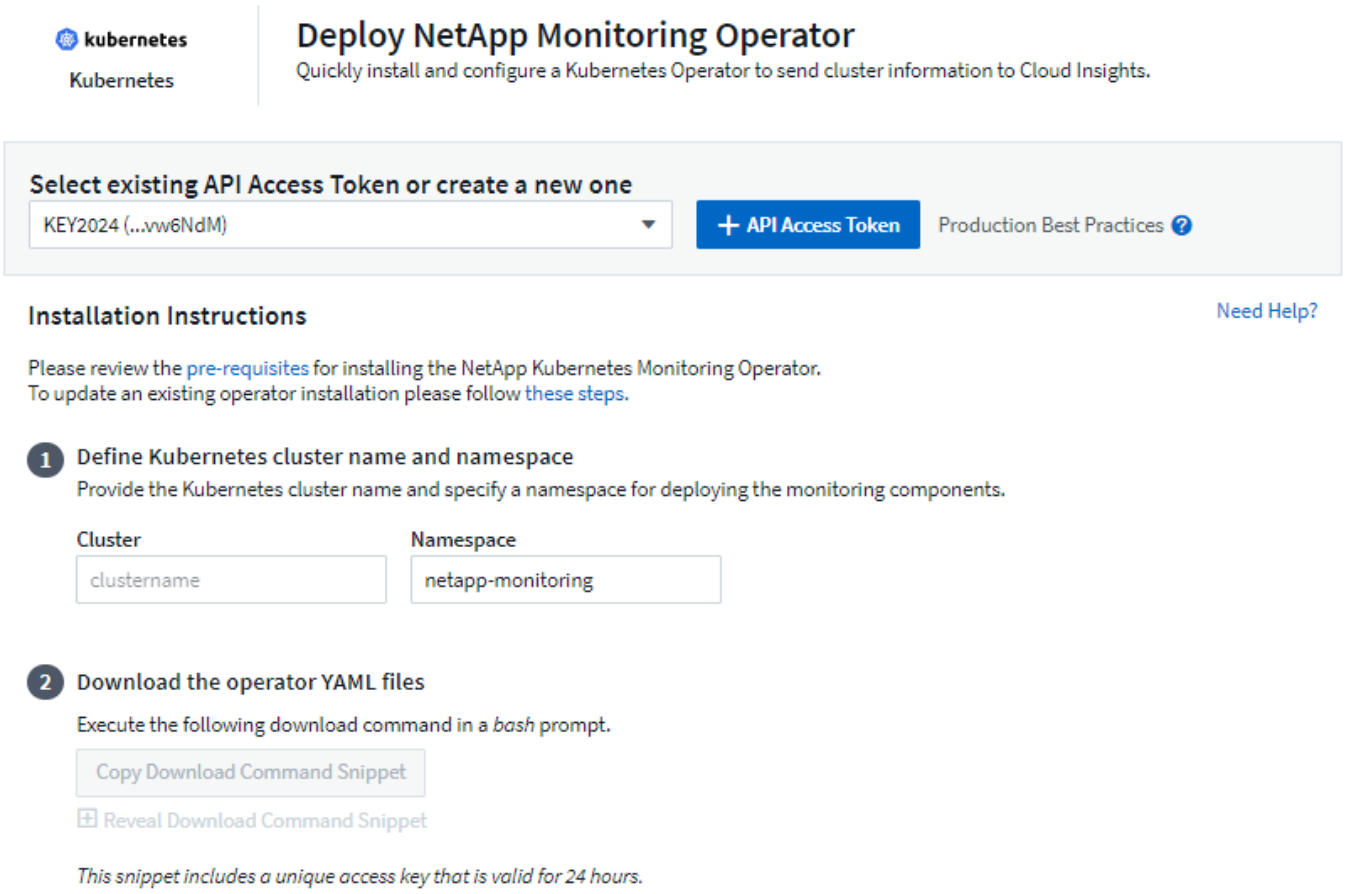
Installation et configuration de l'opérateur de surveillance Kubernetes

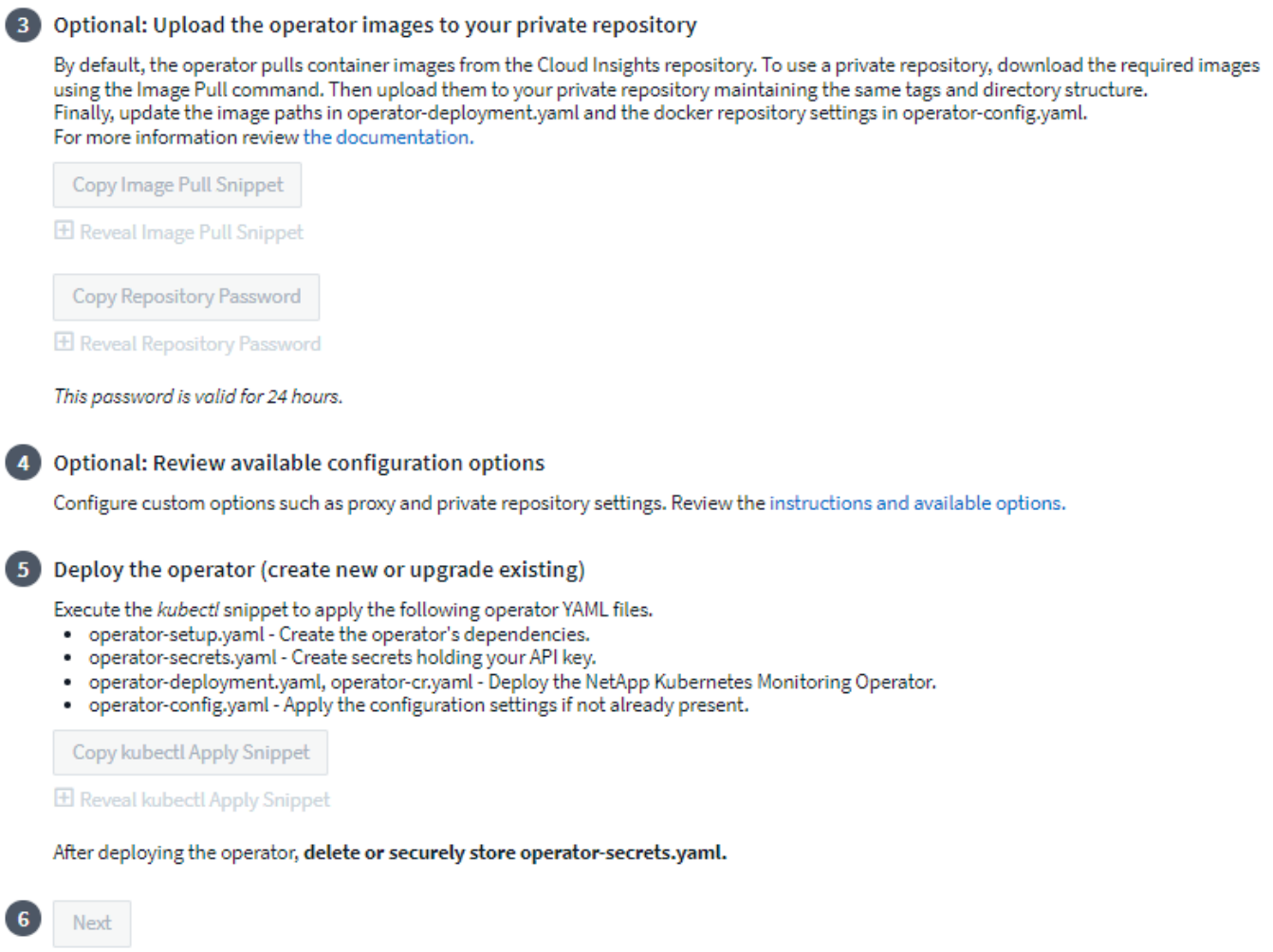
Data Infrastructure Insights propose l'opérateur de surveillance Kubernetes pour la collection Kubernetes. Accédez à **Kubernetes > Collecteurs > +Kubernetes Collector** pour déployer un nouvel opérateur.

Avant d'installer Kubernetes Monitoring Operator

Voir le"Prérequis" documentation avant d'installer ou de mettre à niveau Kubernetes Monitoring Operator.

Installation de l'opérateur de surveillance Kubernetes





Étapes pour installer l'agent Kubernetes Monitoring Operator sur Kubernetes :

1. Saisissez un nom de cluster et un espace de noms uniques. Si vous êtesmise à niveau à partir d'un opérateur Kubernetes précédent, utilisez le même nom de cluster et le même espace de noms.
2. Une fois ces informations saisies, vous pouvez copier l'extrait de commande de téléchargement dans le presse-papiers.
3. Collez l'extrait dans une fenêtre *bash* et exécutez-le. Les fichiers d'installation de l'opérateur seront téléchargés. Notez que l'extrait possède une clé unique et est valable 24 heures.
4. Si vous disposez d'un référentiel personnalisé ou privé, copiez l'extrait d'image facultatif, collez-le dans un shell *bash* et exécutez-le. Une fois les images extraites, copiez-les dans votre référentiel privé. Assurez-vous de conserver les mêmes balises et la même structure de dossiers. Mettez à jour les chemins dans *operator-deployment.yaml* ainsi que les paramètres du référentiel Docker dans *operator-config.yaml*.
5. Si vous le souhaitez, examinez les options de configuration disponibles telles que les paramètres de proxy ou de référentiel privé. Vous pouvez en savoir plus sur"options de configuration" .
6. Lorsque vous êtes prêt, déployez l'opérateur en copiant l'extrait kubectl Apply, en le téléchargeant et en l'exécutant.
7. L'installation se déroule automatiquement. Une fois terminé, cliquez sur le bouton *Suivant*.
8. Une fois l'installation terminée, cliquez sur le bouton *Suivant*. Assurez-vous également de supprimer ou de stocker en toute sécurité le fichier *operator-secrets.yaml*.

Si vous disposez d'un référentiel personnalisé, lisez à proposen utilisant un référentiel Docker

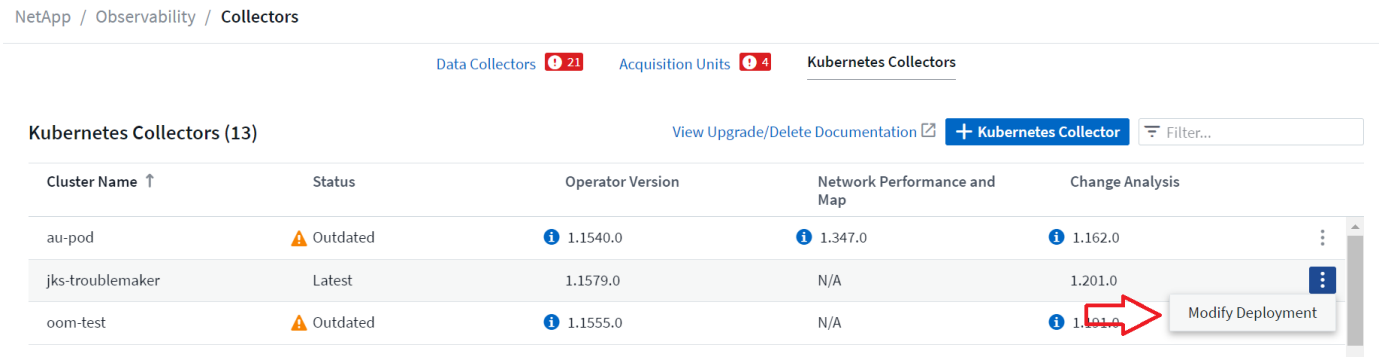
personnalisé/privé .

Composants de surveillance Kubernetes

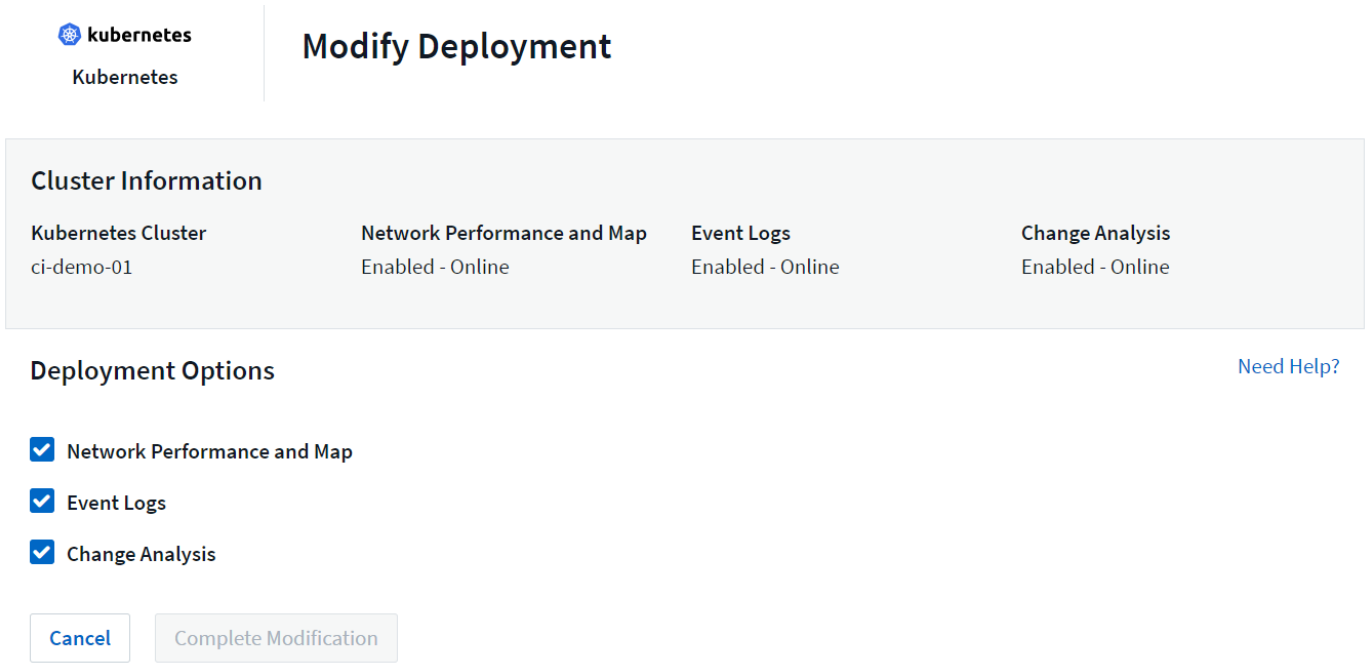
Data Infrastructure Insights Kubernetes Monitoring comprend quatre composants de surveillance :

- Mesures de cluster
- Performances et carte du réseau (facultatif)
- Journaux d'événements (facultatif)
- Analyse des changements (facultatif)

Les composants facultatifs ci-dessus sont activés par défaut pour chaque collecteur Kubernetes ; si vous décidez que vous n'avez pas besoin d'un composant pour un collecteur particulier, vous pouvez le désactiver en accédant à **Kubernetes > Collecteurs** et en sélectionnant *Modifier le déploiement* dans le menu « trois points » du collecteur à droite de l'écran.



L'écran affiche l'état actuel de chaque composant et vous permet de désactiver ou d'activer les composants de ce collecteur selon vos besoins.



Mise à niveau vers la dernière version de Kubernetes Monitoring Operator

Mises à niveau du bouton-poussoir DII

Vous pouvez mettre à niveau l'opérateur de surveillance Kubernetes via la page Collecteurs Kubernetes DII. Cliquez sur le menu à côté du cluster que vous souhaitez mettre à niveau et sélectionnez *Mettre à niveau*. L'opérateur vérifiera les signatures d'image, effectuera un instantané de votre installation actuelle et effectuera la mise à niveau. Dans quelques minutes, vous devriez voir l'état de l'opérateur progresser de « Mise à niveau en cours » à « Dernière mise à jour ». Si vous rencontrez une erreur, vous pouvez sélectionner le statut d'erreur pour plus de détails et vous référer au tableau de dépannage des mises à niveau par bouton-poussoir ci-dessous.

Mises à niveau par simple pression d'un bouton avec des référentiels privés

Si votre opérateur est configuré pour utiliser un référentiel privé, assurez-vous que toutes les images requises pour exécuter l'opérateur et leurs signatures sont disponibles dans votre référentiel. Si vous rencontrez une erreur pendant le processus de mise à niveau pour des images manquantes, ajoutez-les simplement à votre référentiel et réessayez la mise à niveau. Pour télécharger les signatures d'image dans votre référentiel, veuillez utiliser l'outil de cosignature comme suit, en veillant à télécharger les signatures pour toutes les images spécifiées sous 3 Facultatif : Télécharger les images de l'opérateur dans votre référentiel privé > Extrait d'image

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Revenir à une version précédemment exécutée

Si vous avez effectué une mise à niveau à l'aide de la fonction de mise à niveau par simple pression sur un bouton et que vous rencontrez des difficultés avec la version actuelle de l'opérateur dans les sept jours suivant la mise à niveau, vous pouvez rétrograder vers la version précédemment exécutée à l'aide de l'instantané créé pendant le processus de mise à niveau. Cliquez sur le menu à côté du cluster que vous souhaitez restaurer et sélectionnez *Restaurer*.

Mises à niveau manuelles

Déterminez si une *AgentConfiguration* existe avec l'opérateur existant (si votre espace de noms n'est pas le *netapp-monitoring* par défaut, remplacez-le par l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si une _AgentConfiguration_ existe :
```

- Installationle dernier opérateur sur l'opérateur existant.
    - Assurez-vous que vous êtesextraire les dernières images de conteneurs si vous utilisez un référentiel personnalisé.

Si *AgentConfiguration* n'existe pas :

- Notez le nom de votre cluster tel qu'il est reconnu par Data Infrastructure Insights (si votre espace de noms n'est pas le netapp-monitoring par défaut, remplacez-le par l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Créez une sauvegarde de l'opérateur existant (si votre espace de noms
n'est pas le netapp-monitoring par défaut, remplacez-le par l'espace de
noms approprié) :
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-
operator,Désinstaller>>l'opérateur existant.
* <<installing-the-kubernetes-monitoring-operator,Installation>>le
dernier opérateur.
```

  - Utilisez le même nom de cluster.
  - Après avoir téléchargé les derniers fichiers YAML de l'opérateur, reportez toutes les personnalisations trouvées dans *agent_backup.yaml* vers le fichier *operator-config.yaml* téléchargé avant le déploiement.
  - Assurez-vous que vous êtesextraire les dernières images de conteneurs si vous utilisez un référentiel personnalisé.

Arrêt et démarrage de l'opérateur de surveillance Kubernetes

Pour arrêter l'opérateur de surveillance Kubernetes :

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Pour démarrer l'opérateur de surveillance Kubernetes :
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Désinstallation

Pour supprimer l'opérateur de surveillance Kubernetes

Notez que l'espace de noms par défaut pour l'opérateur de surveillance Kubernetes est « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez cet espace de noms dans ces commandes et fichiers et dans tous les suivants.

Les versions plus récentes de l'opérateur de surveillance peuvent être désinstallées avec les commandes suivantes :

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Si l'opérateur de surveillance a été déployé dans son propre espace de noms dédié, supprimez l'espace de noms :

```
 kubectl delete ns <NAMESPACE>
Remarque : si la première commande renvoie « Aucune ressource trouvée »,
utilisez les instructions suivantes pour désinstaller les anciennes
versions de l'opérateur de surveillance.
```

Exécutez chacune des commandes suivantes dans l'ordre. Selon votre installation actuelle, certaines de ces commandes peuvent renvoyer des messages « objet non trouvé ». Ces messages peuvent être ignorés en toute sécurité.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Si une contrainte de contexte de sécurité a été créée précédemment :

```
kubectl delete scc telegraf-hostaccess
```

À propos de Kube-state-metrics

L'opérateur de surveillance NetApp Kubernetes installe ses propres métriques d'état Kube pour éviter tout conflit avec d'autres instances.

Pour plus d'informations sur Kube-State-Metrics, voir"cette page" .

Configuration/Personnalisation de l'opérateur

Ces sections contiennent des informations sur la personnalisation de la configuration de votre opérateur,

l'utilisation d'un proxy, l'utilisation d'un référentiel Docker personnalisé ou privé ou l'utilisation d'OpenShift.

Options de configuration

Les paramètres les plus fréquemment modifiés peuvent être configurés dans la ressource personnalisée *AgentConfiguration*. Vous pouvez modifier cette ressource avant de déployer l'opérateur en modifiant le fichier *operator-config.yaml*. Ce fichier comprend des exemples de paramètres commentés. Voir la liste des"paramètres disponibles" pour la version la plus récente de l'opérateur.

Vous pouvez également modifier cette ressource après le déploiement de l'opérateur à l'aide de la commande suivante :

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Pour déterminer si votre version déployée de l'opérateur prend en charge
_AgentConfiguration_, exécutez la commande suivante :
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Si vous voyez un message « Erreur du serveur (NotFound) », votre opérateur
doit être mis à niveau avant de pouvoir utiliser AgentConfiguration.
```

Configuration de la prise en charge du proxy

Il existe deux endroits où vous pouvez utiliser un proxy sur votre locataire afin d'installer Kubernetes Monitoring Operator. Il peut s'agir des mêmes systèmes proxy ou de systèmes proxy distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système où l'extrait est exécuté à votre environnement Data Infrastructure Insights
- Proxy requis par le cluster Kubernetes cible pour communiquer avec votre environnement Data Infrastructure Insights

Si vous utilisez un proxy pour l'un ou les deux, afin d'installer Kubernetes Operating Monitor, vous devez d'abord vous assurer que votre proxy est configuré pour permettre une bonne communication avec votre environnement Data Infrastructure Insights . Si vous disposez d'un proxy et pouvez accéder à Data Infrastructure Insights à partir du serveur/de la machine virtuelle à partir duquel vous souhaitez installer l'opérateur, votre proxy est probablement configuré correctement.

Pour le proxy utilisé pour installer Kubernetes Operating Monitor, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, vous devrez peut-être également définir la variable d'environnement *no_proxy*.

Pour définir la ou les variables, effectuez les étapes suivantes sur votre système **avant** d'installer Kubernetes Monitoring Operator :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
    a. Si le proxy en cours de configuration ne dispose pas d'authentification (nom d'utilisateur/mot de passe), exécutez la commande suivante :

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Si le proxy en cours de configuration dispose d'une
authentification (nom d'utilisateur/mot de passe), exécutez cette
commande :
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Pour que le proxy utilisé pour votre cluster Kubernetes communique avec votre environnement Data Infrastructure Insights , installez Kubernetes Monitoring Operator après avoir lu toutes ces instructions.

Configurez la section proxy de *AgentConfiguration* dans *operator-config.yaml* avant de déployer le Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utiliser un référentiel Docker personnalisé ou privé

Par défaut, l'opérateur de surveillance Kubernetes extrait les images de conteneur du référentiel Data Infrastructure Insights . Si vous disposez d'un cluster Kubernetes utilisé comme cible pour la surveillance et que ce cluster est configuré pour extraire uniquement des images de conteneur à partir d'un référentiel Docker personnalisé ou privé ou d'un registre de conteneurs, vous devez configurer l'accès aux conteneurs nécessaires à l'opérateur de surveillance Kubernetes.

Exécutez « Image Pull Snippet » à partir de la mosaïque d'installation de NetApp Monitoring Operator. Cette commande se connectera au référentiel Data Infrastructure Insights , extraira toutes les dépendances d'image pour l'opérateur et se déconnectera du référentiel Data Infrastructure Insights . Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande télécharge toutes les images utilisées par l'opérateur, y compris pour les fonctionnalités optionnelles. Voir ci-dessous pour les fonctionnalités pour lesquelles ces images sont utilisées.

Fonctionnalités de l'opérateur principal et surveillance de Kubernetes

- surveillance netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- utilisateur root sans distribution

Journal des événements

- ci-fluent-bit
- exportateur d'événements ci-kubernetes

Performances et carte du réseau

- ci-net-observer

Poussez l'image Docker de l'opérateur vers votre référentiel Docker privé/local/d'entreprise conformément à vos politiques d'entreprise. Assurez-vous que les balises d'image et les chemins d'accès aux répertoires de ces images dans votre référentiel sont cohérents avec ceux du référentiel Data Infrastructure Insights .

Modifiez le déploiement de l'opérateur de surveillance dans operator-deployment.yaml et modifiez toutes les références d'image pour utiliser votre référentiel Docker privé.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modifiez *AgentConfiguration* dans *operator-config.yaml* pour refléter le nouvel emplacement du dépôt docker. Créez un nouveau imagePullSecret pour votre dépôt privé, pour plus de détails, consultez *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Jeton d'accès API pour les mots de passe à long terme

Certains environnements (par exemple, les dépôts proxy) exigent des mots de passe à long terme pour le dépôt docker de Data Infrastructure Insights. Le mot de passe fourni dans l'interface utilisateur lors de l'installation n'est valable que 24 heures. Au lieu de cela, on peut utiliser un jeton d'accès API comme mot de passe du dépôt docker. Ce mot de passe sera valable aussi longtemps que le jeton d'accès API est valide. On peut générer un nouveau jeton d'accès API à cette fin ou en utiliser un existant.

"Lire ici" pour obtenir des instructions sur la création d'un nouveau jeton d'accès API.

Pour extraire un jeton d'accès API existant à partir d'un fichier *operator-secrets.yaml* téléchargé, les utilisateurs peuvent exécuter la commande suivante :

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Pour extraire un jeton d'accès API existant d'une installation d'opérateur en cours d'exécution, les utilisateurs peuvent exécuter la commande suivante :

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Instructions OpenShift

Si vous utilisez OpenShift 4.6 ou une version ultérieure, vous devez modifier *AgentConfiguration* dans *operator-config.yaml* pour activer le paramètre *runPrivileged* :

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift peut implémenter un niveau de sécurité supplémentaire qui peut bloquer l'accès à certains composants Kubernetes.

Tolérances et souillures

Les DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* et *netapp-ci-net-observer-l4-ds* doivent planifier un pod sur chaque nœud de votre cluster afin de collecter correctement les données sur tous les nœuds.

L'opérateur a été configuré pour tolérer certaines **souillures** bien connues. Si vous avez configuré des taches personnalisées sur vos nœuds, empêchant ainsi les pods de s'exécuter sur chaque nœud, vous pouvez créer une **tolérance** pour ces taches"dans *AgentConfiguration*" . Si vous avez appliqué des taches personnalisées à tous les nœuds de votre cluster, vous devez également ajouter les tolérances nécessaires au déploiement de l'opérateur pour permettre la planification et l'exécution du pod de l'opérateur.

En savoir plus sur Kubernetes"Souillures et tolérances" .

Retour à la"* Page d'installation de l'opérateur de surveillance NetApp Kubernetes*"

Une note sur les secrets

Pour supprimer l'autorisation permettant à l'opérateur de surveillance Kubernetes d'afficher les secrets à l'échelle du cluster, supprimez les ressources suivantes du fichier *operator-setup.yaml* avant l'installation :

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

S'il s'agit d'une mise à niveau, supprimez également les ressources de votre cluster :

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Si l'analyse des changements est activée, modifiez *AgentConfiguration* ou *operator-config.yaml* pour supprimer le commentaire de la section de gestion des changements et inclure *kindsToIgnoreFromWatch: '"secrets"'* sous la section de gestion des changements. Notez la présence et la position des guillemets simples et doubles dans cette ligne.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Vérification des signatures d'image de l'opérateur de surveillance Kubernetes

L'image de l'opérateur et toutes les images associées qu'il déploie sont signées par NetApp. Vous pouvez vérifier manuellement les images avant l'installation à l'aide de l'outil de cosignature ou configurer un contrôleur d'admission Kubernetes. Pour plus de détails, veuillez consulter le"Documentation Kubernetes" .

La clé publique utilisée pour vérifier les signatures d'image est disponible dans la mosaïque d'installation de l'opérateur de surveillance sous *Facultatif : téléchargez les images de l'opérateur dans votre référentiel privé >*

Clé publique de signature d'image

Pour vérifier manuellement une signature d'image, procédez comme suit :

1. Copiez et exécutez l'extrait d'image
2. Copiez et saisissez le mot de passe du référentiel lorsque vous y êtes invité
3. Stocker la clé publique de signature d'image (dii-image-signing.pub dans l'exemple)
4. Vérifiez les images à l'aide de cosign. Reportez-vous à l'exemple suivant d'utilisation de cosignature

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Dépannage

Quelques éléments à essayer si vous rencontrez des problèmes lors de la configuration de l'opérateur de surveillance Kubernetes :

Problème:	Essayez ceci:
Je ne vois pas d'hyperlien/connexion entre mon volume persistant Kubernetes et le périphérique de stockage back-end correspondant. Mon volume persistant Kubernetes est configuré à l'aide du nom d'hôte du serveur de stockage.	Suivez les étapes pour désinstaller l'agent Telegraf existant, puis réinstaller le dernier agent Telegraf. Vous devez utiliser Telegraf version 2.0 ou ultérieure et votre stockage de cluster Kubernetes doit être activement surveillé par Data Infrastructure Insights.

Problème:	Essayez ceci:
Je vois des messages dans les journaux ressemblant à ce qui suit : E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.MutatingWebhookConfiguration: the server could not find the requested resource E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.Lease: the server could not find the requested resource (get leases.coordination.k8s.io) etc.	Ces messages peuvent se produire si vous exécutez kube-state-metrics version 2.0.0 ou supérieure avec des versions de Kubernetes inférieures à 1.20. Pour obtenir la version de Kubernetes : *kubectl version* Pour obtenir la version de kube-state-metrics : *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Pour éviter que ces messages ne se produisent, les utilisateurs peuvent modifier leur déploiement kube-state-metrics pour désactiver les baux suivants : *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Plus précisément, ils peuvent utiliser l'argument CLI suivant : resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, La liste de ressources par défaut est : « certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,leases,limitranges,mutatingwebhookconfigurations,namespaces,networkpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas,secrets,services,statefulsets,storageclasses,validatingwebhookconfigurations,volumeattachments »
Je vois des messages d'erreur de Telegraf ressemblant à ce qui suit, mais Telegraf démarre et s'exécute : 11 oct. 14:23:41 ip-172-31-39-47 systemd[1] : Démarré L'agent serveur piloté par plug-in pour la création de rapports de métriques dans InfluxDB. 11 oct. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="échec de la création du répertoire de cache. /etc/telegraf/.cache/snowflake, err : mkdir /etc/telegraf/.ca che : permission refusée. ignoré\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827] : time="2021-10-11T14:23:41Z" level=error msg="échec d'ouverture. Ignoré. ouvrez /etc/telegraf/.cache/snowflake/ocsp_response_cache.json : aucun fichier ou répertoire de ce type\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct. 14:23:41 ip-172-31-39-47 telegraf[1827] : 2021-10-11T14:23:41Z Je ! Démarrage de Telegraf 1.19.3	Il s'agit d'un problème connu. Se référer à"Cet article GitHub" pour plus de détails. Tant que Telegraf est opérationnel, les utilisateurs peuvent ignorer ces messages d'erreur.

Problème:	Essayez ceci:
Sur Kubernetes, mes pods Telegraf signalent l'erreur suivante : « Erreur lors du traitement des informations mountstats : échec d'ouverture du fichier mountstats : /hostfs/proc/1/mountstats, erreur : ouverture de /hostfs/proc/1/mountstats : autorisation refusée »	Si SELinux est activé et appliqué, il empêche probablement les pods Telegraf d'accéder au fichier /proc/1/mountstats sur le nœud Kubernetes. Pour surmonter cette restriction, modifiez la configuration de l'agent et activez le paramètre runPrivileged. Pour plus de détails, reportez-vous aux instructions OpenShift.
Sur Kubernetes, mon pod Telegraf ReplicaSet signale l'erreur suivante : [inputs.prometheus] Erreur dans le plugin : impossible de charger la paire de clés /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key : ouvrir /etc/kubernetes/pki/etcd/server.crt : aucun fichier ou répertoire de ce type	Le pod Telegraf ReplicaSet est destiné à s'exécuter sur un nœud désigné comme maître ou pour etcd. Si le pod ReplicaSet n'est pas en cours d'exécution sur l'un de ces nœuds, vous obtiendrez ces erreurs. Vérifiez si vos nœuds maître/etcd sont contaminés. Si c'est le cas, ajoutez les tolérances nécessaires au Telegraf ReplicaSet, telegraf-rs. Par exemple, modifiez le ReplicaSet… kubectl edit rs telegraf-rs … et ajoutez les tolérances appropriées à la spécification. Ensuite, redémarrez le pod ReplicaSet.
J'ai un environnement PSP/PSA. Cela affecte-t-il mon opérateur de surveillance ?	Si votre cluster Kubernetes s'exécute avec la stratégie de sécurité des pods (PSP) ou l'admission de sécurité des pods (PSA) en place, vous devez effectuer une mise à niveau vers la dernière version de Kubernetes Monitoring Operator. Suivez ces étapes pour mettre à niveau vers l'opérateur actuel avec prise en charge de PSP/PSA : 1. Désinstaller l'opérateur de surveillance précédent : kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installation la dernière version de l'opérateur de surveillance.
J'ai rencontré des problèmes lors du déploiement de l'opérateur et j'utilise PSP/PSA.	1. Modifiez l'agent à l'aide de la commande suivante : kubectl -n <name-space> edit agent 2. Marquer « security-policy-enabled » comme « faux ». Cela désactivera les politiques de sécurité des pods et l'admission de sécurité des pods et permettra à l'opérateur de se déployer. Confirmez en utilisant les commandes suivantes : kubectl get psp (devrait indiquer que la politique de sécurité du pod a été supprimée) kubectl get all -n <namespace>
grep -i psp (devrait indiquer que rien n'est trouvé)	Erreurs « ImagePullBackoff » observées
Ces erreurs peuvent être observées si vous disposez d'un référentiel Docker personnalisé ou privé et que vous n'avez pas encore configuré l'opérateur de surveillance Kubernetes pour le reconnaître correctement. En savoir plus à propos de la configuration pour un référentiel personnalisé/privé.	J'ai un problème avec mon déploiement d'opérateur de surveillance et la documentation actuelle ne m'aide pas à le résoudre.

Problème:	Essayez ceci:
Capturez ou notez autrement la sortie des commandes suivantes et contactez l'équipe de support technique. ``` kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true ```	Les pods net-observer (Workload Map) dans l'espace de noms Operator sont dans CrashLoopBackOff
Ces pods correspondent au collecteur de données Workload Map pour l'observabilité du réseau. Essayez ceci : • Vérifiez les journaux de l'un des pods pour confirmer la version minimale du noyau. Par exemple : ---- {"ci-tenant-id":"votre-id-de-tenant","collector-cluster":"votre-nom-de-cluster-k8s","environment":"prod","level":"error","msg":"échec de validation. Raison : la version du noyau 3.10.0 est inférieure à la version minimale du noyau 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Les pods Net-observer nécessitent que la version du noyau Linux soit au moins 4.18.0. Vérifiez la version du noyau à l'aide de la commande « uname -r » et assurez-vous qu'elle est >= 4.18.0	Les pods s'exécutent dans l'espace de noms de l'opérateur (par défaut : netapp-monitoring), mais aucune donnée n'est affichée dans l'interface utilisateur pour la carte de charge de travail ou les métriques Kubernetes dans les requêtes.
Vérifiez le réglage de l'heure sur les nœuds du cluster K8S. Pour un audit et des rapports de données précis, il est fortement recommandé de synchroniser l'heure sur la machine Agent à l'aide du protocole Network Time Protocol (NTP) ou du protocole Simple Network Time Protocol (SNTP).	Certains des pods d'observateur réseau dans l'espace de noms Operator sont en état d'attente
Net-observer est un DaemonSet et exécute un pod dans chaque nœud du cluster k8s. • Notez le pod qui est en état d'attente et vérifiez s'il rencontre un problème de ressources pour le processeur ou la mémoire. Assurez-vous que la mémoire et le processeur requis sont disponibles dans le nœud.	Je vois ce qui suit dans mes journaux immédiatement après l'installation de Kubernetes Monitoring Operator : [inputs.prometheus] Erreur dans le plugin : erreur lors de la requête HTTP vers http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : obtenir http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : numérotation TCP : recherche kube-state-metrics.<namespace>.svc.cluster.local : aucun hôte de ce type

Problème:	Essayez ceci:
Ce message n'apparaît généralement que lorsqu'un nouvel opérateur est installé et que le pod *telegraf-rs* est opérationnel avant le pod *ksm*. Ces messages devraient cesser une fois que tous les pods sont en cours d'exécution.	Je ne vois aucune métrique collectée pour les CronJobs Kubernetes qui existent dans mon cluster.
Vérifiez votre version de Kubernetes (c'est-à-dire `kubectl version`). S'il s'agit de la version 1.20.x ou d'une version antérieure, il s'agit d'une limitation attendue. La version kube-state-metrics déployée avec l'opérateur de surveillance Kubernetes prend uniquement en charge la version v1.CronJob. Avec Kubernetes 1.20.x et versions antérieures, la ressource CronJob se trouve dans v1beta.CronJob. Par conséquent, kube-state-metrics ne peut pas trouver la ressource CronJob.	Après l'installation de l'opérateur, les pods telegraf-ds entrent dans CrashLoopBackOff et les journaux des pods indiquent « su : échec d'authentification ».
Modifiez la section telegraf dans *AgentConfiguration*, et définissez *dockerMetricCollectionEnabled* sur false. Pour plus de détails, consultez le "options de configuration" de l'opérateur. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Je vois des messages d'erreur répétés ressemblant à ce qui suit dans mes journaux Telegraf : E! [agent] Erreur lors de l'écriture dans outputs.http : Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb" : délai de contexte dépassé (Client.Timeout dépassé lors de l'attente des en-têtes)
Modifiez la section Telegraf dans *AgentConfiguration* et augmentez *outputTimeout* à 10 s. Pour plus de détails, reportez-vous au manuel de l'opérateur."options de configuration" .	Il me manque des données *involvedobject* pour certains journaux d'événements.
Assurez-vous d'avoir suivi les étapes décrites dans la"Autorisations" section ci-dessus.	Pourquoi est-ce que je vois deux pods d'opérateurs de surveillance en cours d'exécution, l'un nommé netapp-ci-monitoring-operator-<pod> et l'autre nommé monitoring-operator-<pod> ?
À compter du 12 octobre 2023, Data Infrastructure Insights a remanié l'opérateur pour mieux servir nos utilisateurs ; pour que ces changements soient pleinement adoptés, vous devezsupprimer l'ancien opérateur etinstaller le nouveau .	Mes événements Kubernetes ont cessé de manière inattendue d'être signalés à Data Infrastructure Insights.
Récupérer le nom du pod exportateur d'événements : `` `kubectl -n netapp-monitoring get pods ``	grep event-exporter

Problème:	Essayez ceci:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Il doit s'agir soit de « netapp-ci-event-exporter » soit de « event-exporter ». Ensuite, modifiez l'agent de surveillance `kubectl -n netapp-monitoring edit agent` et définissez la valeur de LOG_FILE pour refléter le nom de pod d'exportation d'événements approprié trouvé à l'étape précédente. Plus précisément, LOG_FILE doit être défini sur « /var/log/containers/netapp-ci-event-exporter.log » ou « /var/log/containers/event-exporter*.log » …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativement, on peut aussidésinstaller etréinstaller l'agent.
Je vois que des pods déployés par l'opérateur de surveillance Kubernetes se bloquent en raison de ressources insuffisantes.	Consultez l'opérateur de surveillance Kubernetes"options de configuration" pour augmenter les limites du processeur et/ou de la mémoire selon les besoins.
Une image manquante ou une configuration non valide a entraîné l'échec du démarrage ou de la préparation des pods netapp-ci-kube-state-metrics. Désormais, le StatefulSet est bloqué et les modifications de configuration ne sont pas appliquées aux pods netapp-ci-kube-state-metrics.	Le StatefulSet est dans un"cassé" État. Après avoir résolu les problèmes de configuration, faites rebondir les pods netapp-ci-kube-state-metrics.
Les pods netapp-ci-kube-state-metrics ne parviennent pas à démarrer après l'exécution d'une mise à niveau de l'opérateur Kubernetes, générant ErrImagePull (échec de l'extraction de l'image).	Essayez de réinitialiser les pods manuellement.
Les messages « Événement rejeté car plus ancien que maxEventAgeSeconds » sont observés pour mon cluster Kubernetes sous Analyse des journaux.	Modifiez l'opérateur *agentconfiguration* et augmentez *event-exporter-maxEventAgeSeconds* (c'est-à-dire à 60 s), *event-exporter-kubeQPS* (c'est-à-dire à 100) et *event-exporter-kubeBurst* (c'est-à-dire à 500). Pour plus de détails sur ces options de configuration, consultez le"options de configuration" page.

Problème:	Essayez ceci:
Telegraf avertit ou plante à cause d'une mémoire verrouillable insuffisante.	Essayez d'augmenter la limite de mémoire verrouillable pour Telegraf dans le système d'exploitation/nœud sous-jacent. Si l'augmentation de la limite n'est pas une option, modifiez la configuration de l'agent NKMO et définissez *unprotected* sur *true*. Cela indiquera à Telegraf de ne pas tenter de réserver des pages de mémoire verrouillées. Bien que cela puisse présenter un risque de sécurité, car les secrets déchiffrés peuvent être échangés sur le disque, cela permet l'exécution dans des environnements où la réservation de mémoire verrouillée n'est pas possible. Pour plus de détails sur les options de configuration *non protégées*, reportez-vous à la"options de configuration" page.
Je vois des messages d'avertissement de Telegraf ressemblant à ce qui suit : *W! [inputs.diskio] Impossible de récupérer le nom du disque pour « vdc » : erreur de lecture de /dev/vdc : aucun fichier ou répertoire de ce type*	Pour l'opérateur de surveillance Kubernetes, ces messages d'avertissement sont sans conséquence et peuvent être ignorés. Vous pouvez également modifier la section telegraf dans AgentConfiguration et définir *runDsPrivileged* sur true. Pour plus de détails, consultez le "options de configuration de l'opérateur".

Problème:	Essayez ceci:

Mon pod Fluent-bit échoue avec les erreurs suivantes : [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Trop de fichiers ouverts [2024/10/16 14:16:23] [error] échec d'initialisation de l'entrée tail.0 [2024/10/16 14:16:23] [error] [engine] échec d'initialisation de l'entrée	Essayez de modifier vos paramètres *fsnotify* dans votre cluster :
	
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	
	Redémarrez Fluent-bit.
	
	Remarque : pour que ces paramètres soient persistants après chaque redémarrage du nœud, vous devez placer les lignes suivantes dans */etc/sysctl.conf*
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problème:	Essayez ceci:
Les pods DS de Telegraf signalent des erreurs liées au fait que le plug-in d’entrée Kubernetes ne parvient pas à effectuer des requêtes HTTP en raison de l’impossibilité de valider le certificat TLS. Par exemple : E! [inputs.kubernetes] Erreur dans le plugin : erreur lors de la requête HTTP vers"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Obtenir"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls : échec de vérification du certificat : x509 : impossible de valider le certificat pour <kubelet_IP> car il ne contient aucun SAN IP	Cela se produit si le kubelet utilise des certificats auto-signés et/ou si le certificat spécifié n'inclut pas le <kubelet_IP> dans la liste *Subject Alternative Name* des certificats. Pour résoudre ce problème, l'utilisateur peut modifier le"configuration de l'agent" , et définissez *telegraf:insecureK8sSkipVerify* sur *true*. Cela configurera le plugin d'entrée Telegraf pour ignorer la vérification. Alternativement, l'utilisateur peut configurer le kubelet pour"serveurTLSBootstrap" , ce qui déclenchera une demande de certificat à partir de l'API « certificates.k8s.io ».
Je rencontre l'erreur suivante dans les pods Fluent-bit et le pod ne peut pas démarrer : [2026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	Assurez-vous que le répertoire hôte dans lequel le fichier DB réside dispose des permissions de lecture/écriture appropriées. Plus précisément, le répertoire hôte doit accorder des permissions de lecture/écriture aux utilisateurs non-root. L'emplacement par défaut du fichier DB est /var/log/ sauf si cela est remplacé par l'option fluent-bit-dbFile *agentconfiguration*. Si SELinux est activé, essayez de définir l'option fluent-bit-seLinuxOptionsType agentconfiguration sur 'spc_t'.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Memcached

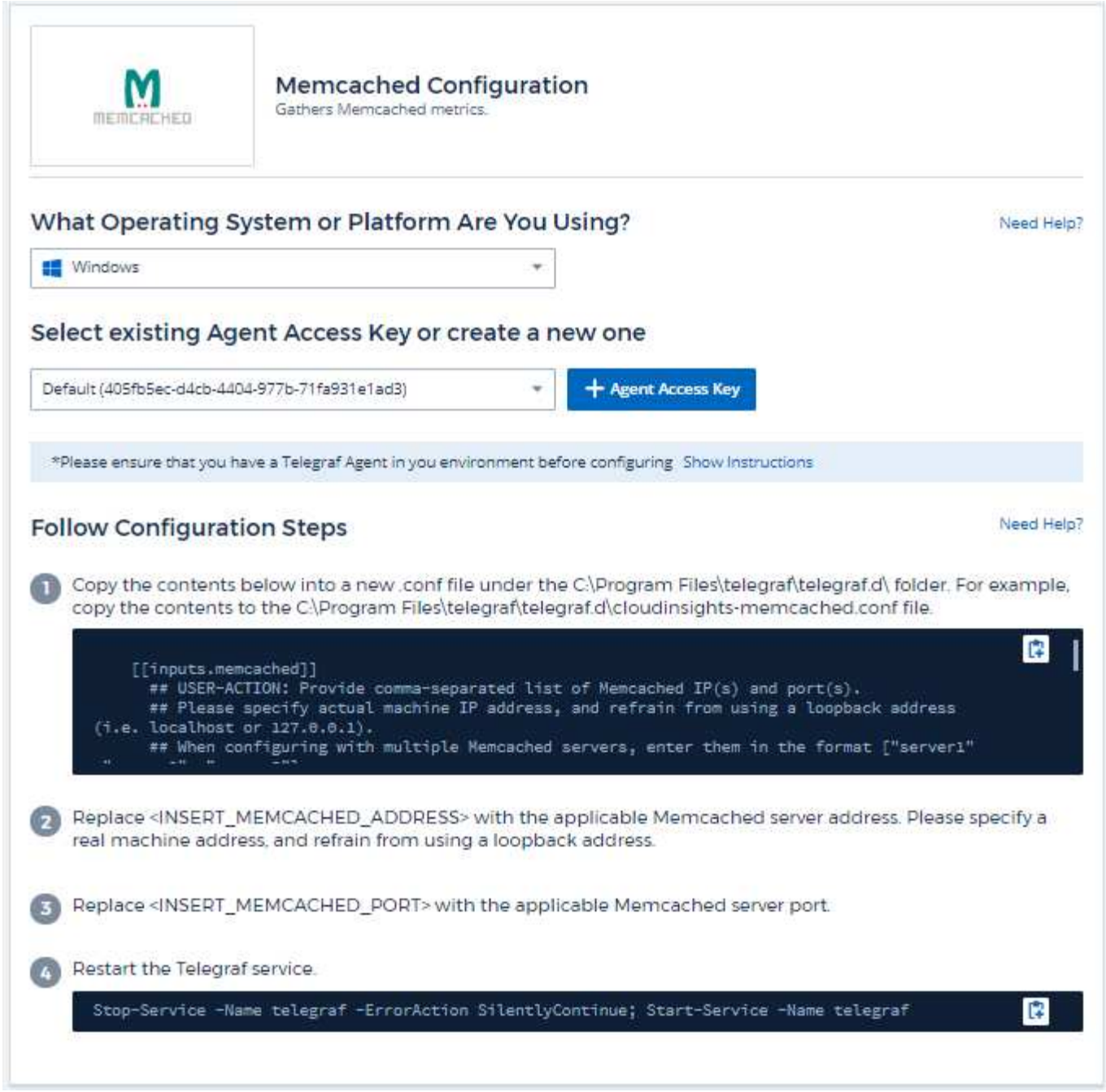
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Memcached.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Memcached.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Wiki Memcached" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Memcached	Serveur d’espace de noms	IP du nœud Nom du nœud	Acceptation des connexions Requêtes d’authentification traitées Authentifications échouées Octets utilisés Octets lus (par seconde) Octets écrits (par seconde) CAS Badval Succès CAS Échecs CAS Demandes de vidage (par seconde) Demandes d’obtention (par seconde) Demandes de définition (par seconde) Demandes tactiles (par seconde) Rendements de connexion (par seconde) Structures de connexion Connexions ouvertes Éléments stockés actuels Demandes de diminution Succès (par seconde) Demandes de diminution Échecs (par seconde) Demandes de suppression Succès (par seconde) Demandes de suppression Échecs (par seconde) Éléments expulsés Expulsions valides Éléments expirés Obtenir Succès (par seconde) Obtenir Échecs (par seconde) Octets de hachage utilisés Le hachage est en expansion Niveau de puissance de hachage Augmentation des requêtes Succès (par seconde) Augmentation des requêtes Échecs (par seconde) Serveur Nombre max. d’octets Écoute désactivée Nombre de threads de travail récupérés Nombre total de connexions ouvertes Nombre total d’éléments stockés Touch Succès Touch Échecs Temps de disponibilité du serveur

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données MongoDB

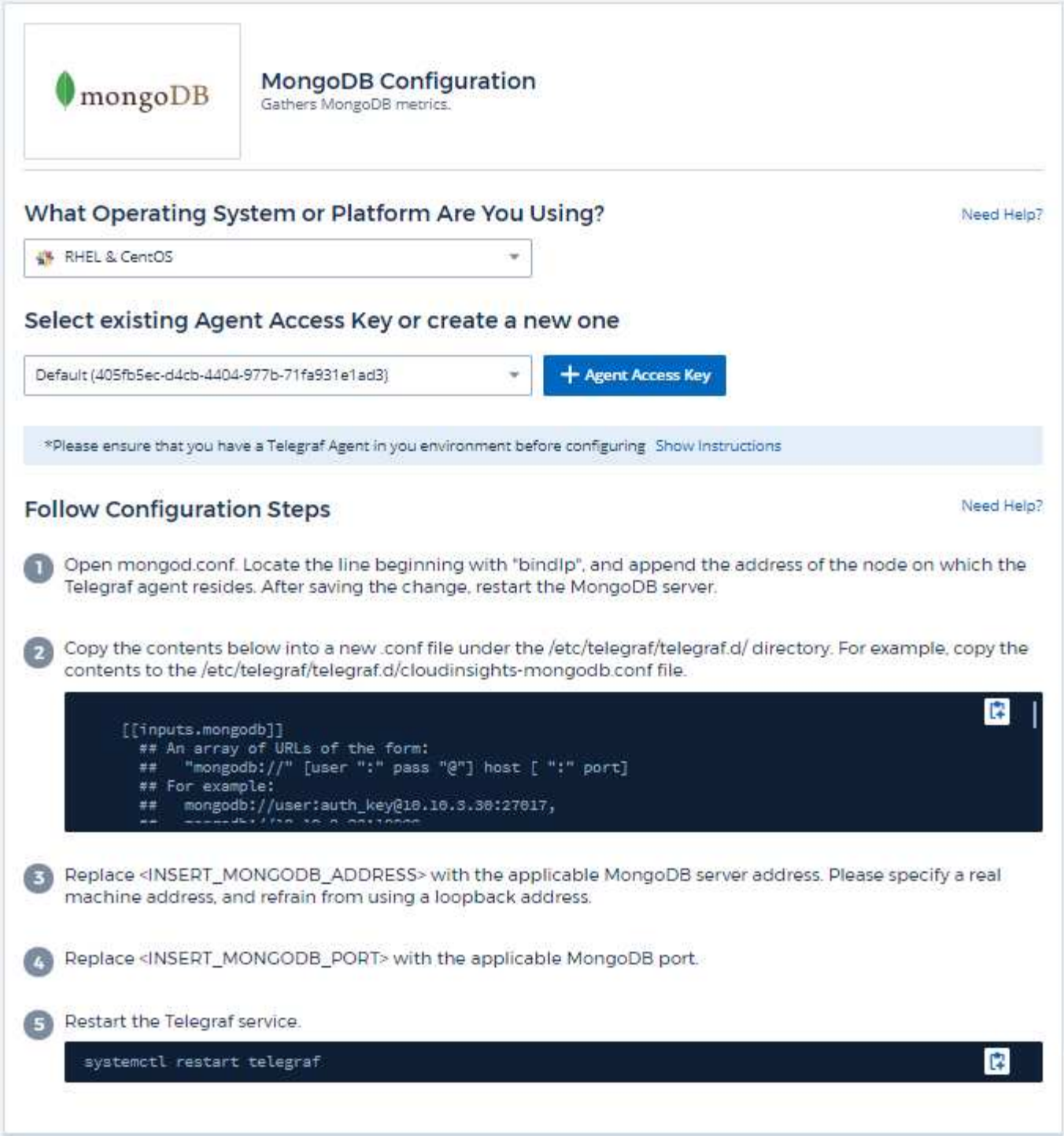
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de MongoDB.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez MongoDB.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation de MongoDB" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
MongoDB	Nom d'hôte de l'espace de noms		
Base de données MongoDB	Nom d'hôte de l'espace de noms Nom de la base de données		

Dépannage

Des informations peuvent être trouvées à partir du"Support" page.

Collecteur de données MySQL

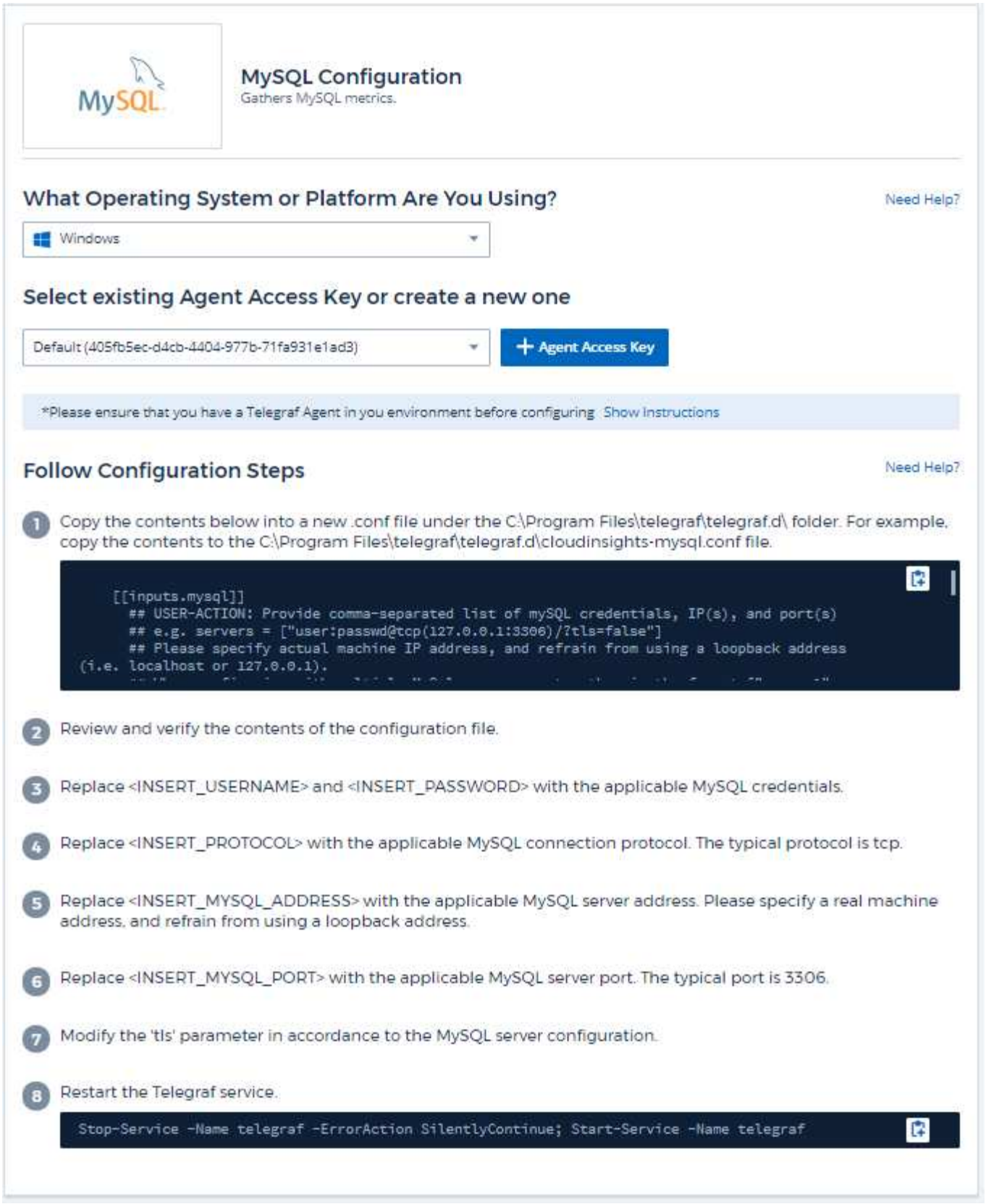
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de MySQL.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez MySQL.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation MySQL" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
MySQL	Espace de noms du serveur MySQL	IP du nœud Nom du nœud	Clients abandonnés (par seconde) Connexions abandonnées (par seconde) Octets RX (par seconde) Octets TX (par seconde) Commandes Admin (par seconde) Commandes Alter Event Commandes Alter Function Commandes Alter Instance Commandes Alter Procedure Commandes Alter Server Commandes Alter Table Commandes Alter Tablespace Commandes Alter User Commandes Analyze Commandes Assign To Keycache Commandes Begin Commandes Binlog Commandes Call Procedure Commandes Change DB Commandes Change Master Commandes Change Repl Filter Commandes Check Commandes Checksum Commandes Commit Commandes Create DB Commandes Create Event Commandes Create Function Commandes Create Index Commandes Create Procedure Commandes Create Server Commandes Create Table Commandes Create Trigger Commandes Create UDF Commandes Create User Commandes Create View Commandes Dealloc Erreurs de connexion SQL Accept Create Tmp Disk Tables Erreurs différées Commandes Flush Handler Commit Innodb Buffer Pool Octets Données Blocs de clés non vidés Requêtes de lecture de clé Requêtes d'écriture de clé Écritures de clé Temps d'exécution maximal Dépassement du

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Netstat

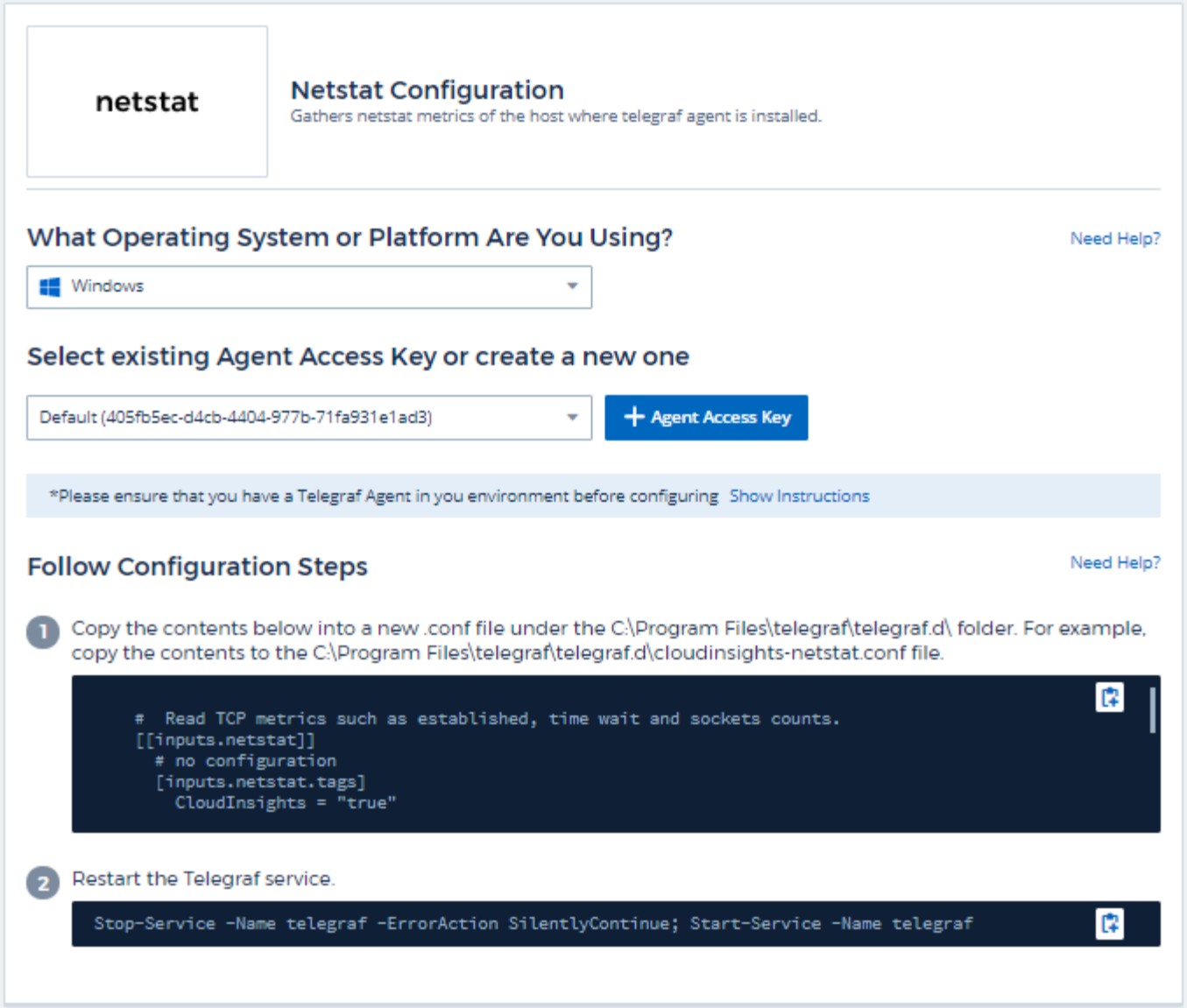
Data Infrastructure Insights utilise ce collecteur de données pour collecter les métriques Netstat.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Netstat.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Netstat	Nœud UUID	IP du nœud Nom du nœud	

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Nginx

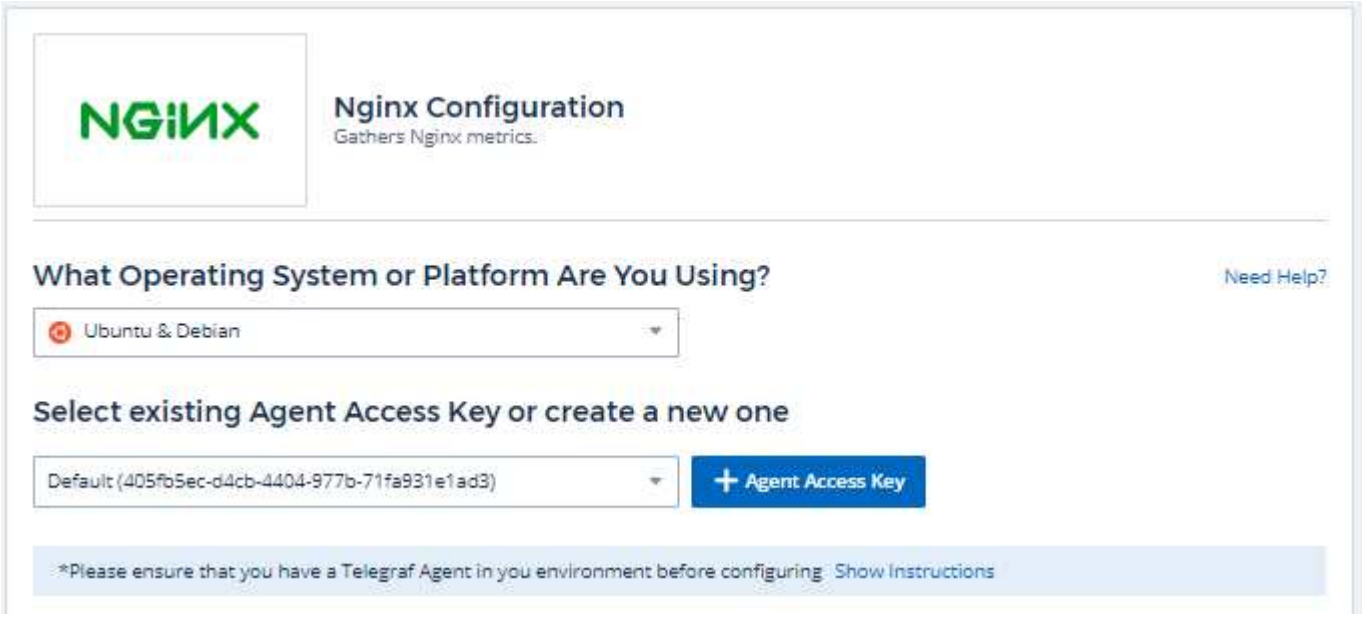
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Nginx.

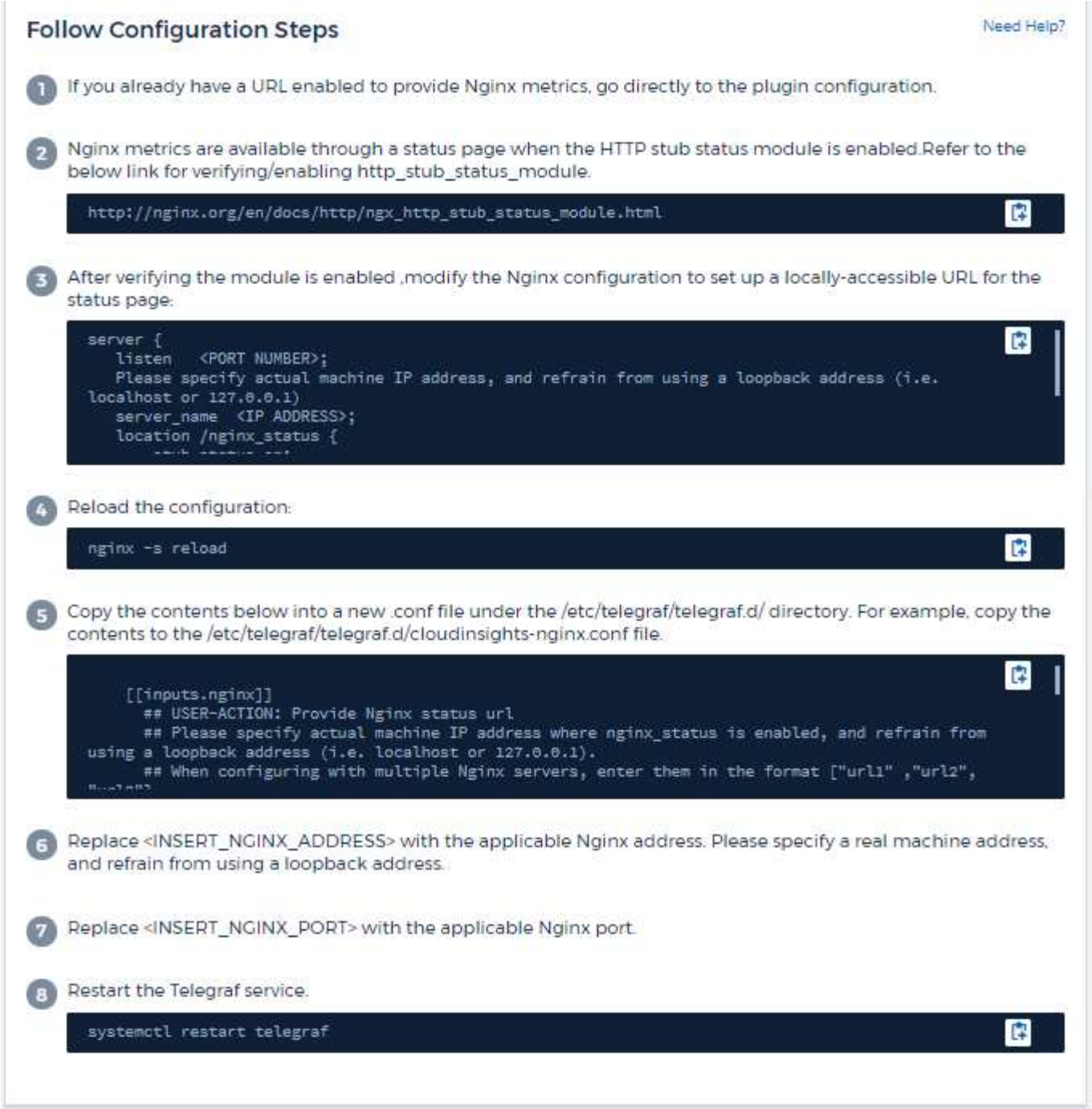
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Nginx.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.





Installation

La collecte de métriques Nginx nécessite que Nginx"module d'état http_stub" être activé.

Des informations complémentaires peuvent être trouvées dans le"Documentation Nginx" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Nginx	Serveur d'espace de noms	IP du nœud Nom du nœud Port	Accepte les demandes de lecture traitées actives en attente d'écriture

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données PostgreSQL

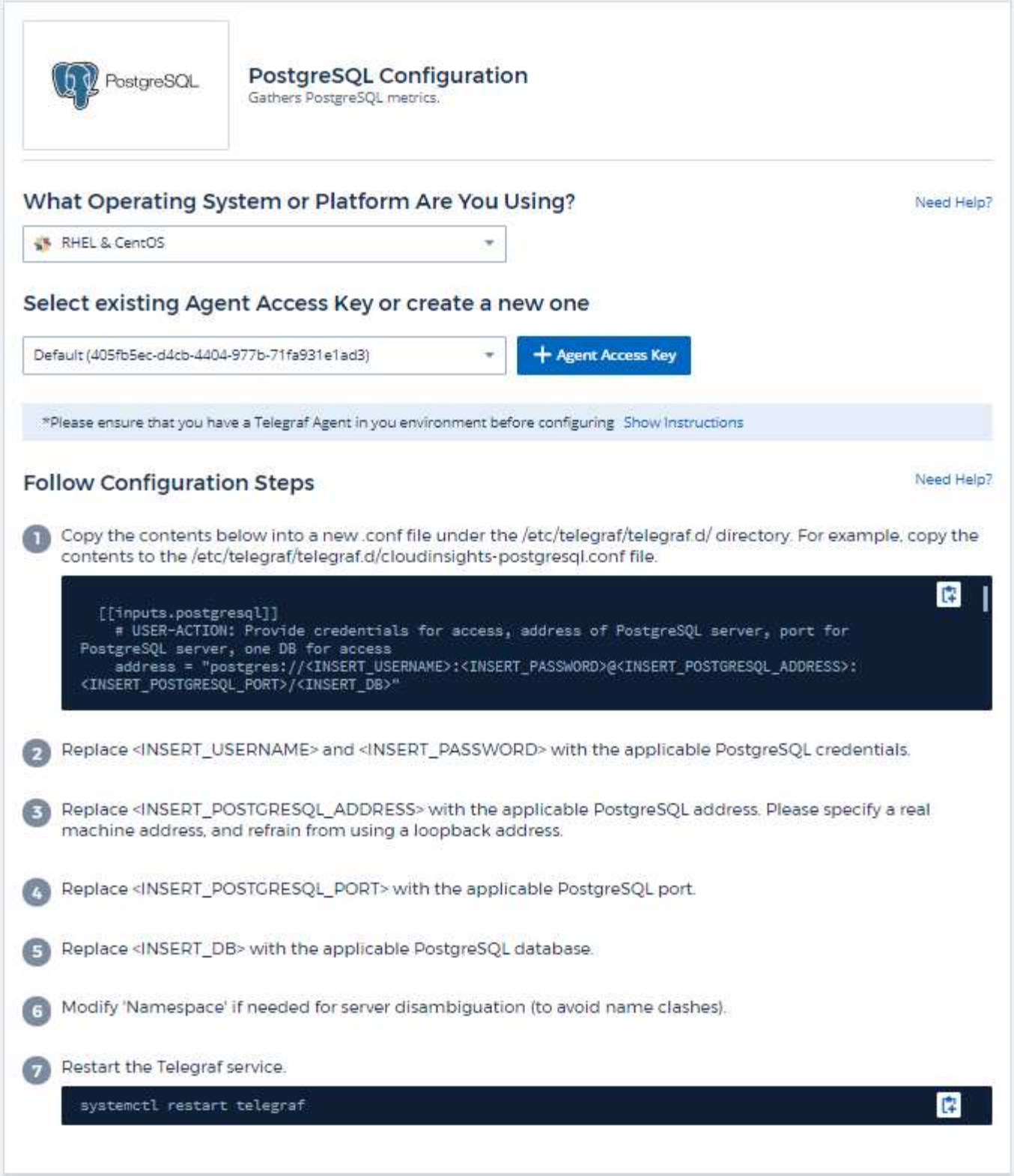
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de PostgreSQL.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez PostgreSQL.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation PostgreSQL" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Serveur PostgreSQL	Serveur de base de données d'espace de noms	Nom du nœud IP du nœud	Tampons alloués Tampons backend Tampons de synchronisation de fichiers backend Tampons de point de contrôle Points de contrôle propres Temps de synchronisation Points de contrôle Temps d'écriture Points de contrôle Requêtes Points de contrôle chronométrés Max Écrit Propre
Base de données PostgreSQL	Serveur de base de données d'espace de noms	Base de données OID Nom du nœud IP du nœud	Blocs Temps de lecture Blocs Temps d'écriture Blocs Hits Blocs Lectures Conflits Blocs Interblocs Numéro de client Fichiers temporaires Octets Numéro de fichiers temporaires Lignes Lignes supprimées Lignes extraites Lignes insérées Lignes renvoyées Transactions mises à jour Transactions validées Annulées

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données d'agent de marionnettes

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Puppet Agent.

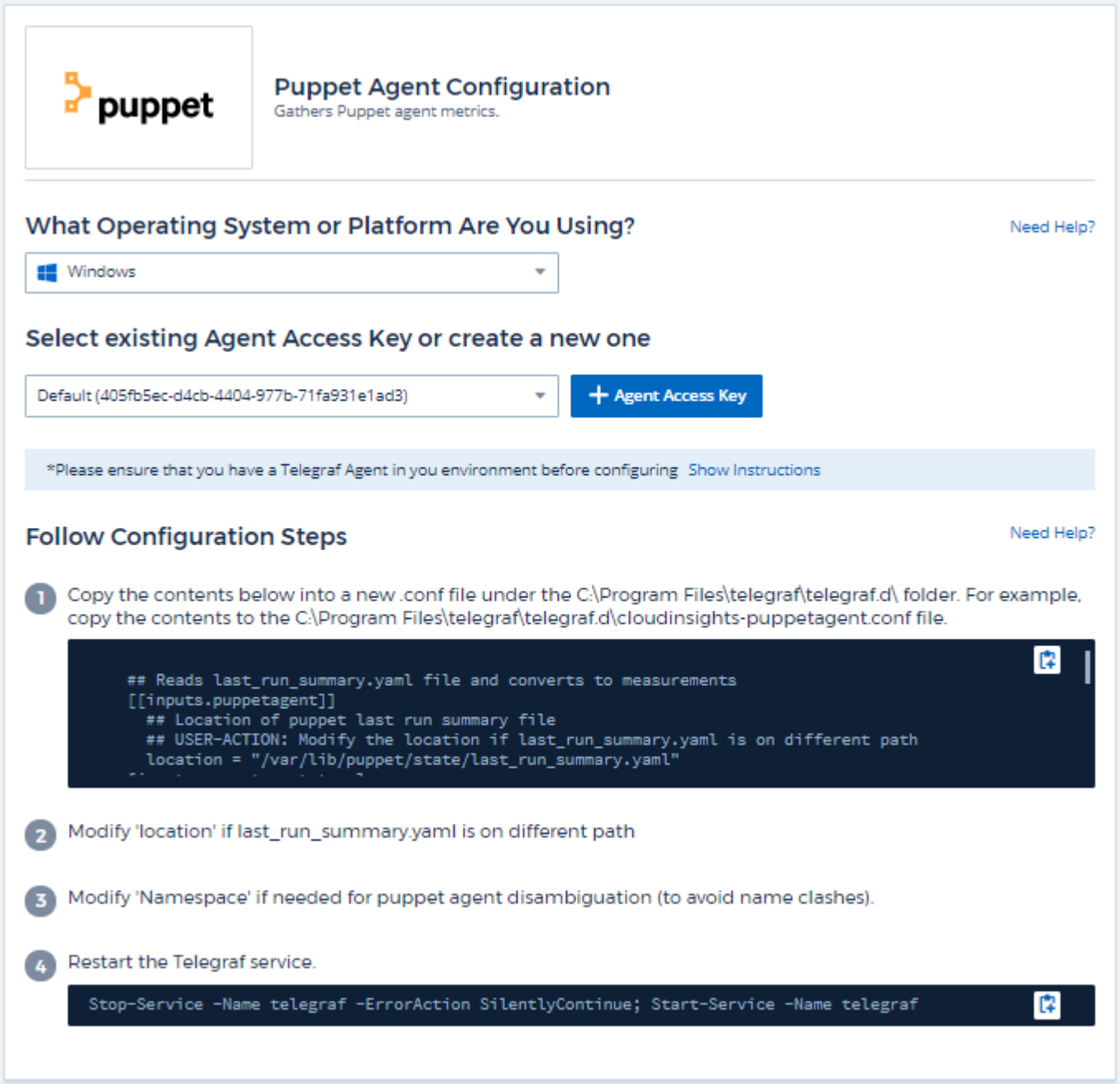
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Puppet.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.

4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le "Documentation des marionnettes"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :

Agent marionnette	UUID du nœud d'espace de noms	Nom du nœud Emplacement IP du nœud Version Chaîne de configuration Version Puppet	Modifications Total des événements Échecs Succès Ressources Total Ressources modifiées Ressources échouées Échec du redémarrage des ressources Ressources désynchronisées Ressources redémarrées Ressources planifiées Ressources ignorées Temps total Heure d'ancrage Heure de récupération de la configuration Heure cron Heure d'exécution Heure du fichier Heure du compartiment de fichiers Heure de la dernière exécution Heure du package Heure de planification Heure du service Heure de la clé Sshauthorized Heure totale Utilisateur

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Redis

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Redis. Redis est un magasin de structures de données open source en mémoire utilisé comme base de données, cache et courtier de messages, prenant en charge les structures de données suivantes : chaînes, hachages, listes, ensembles, etc.

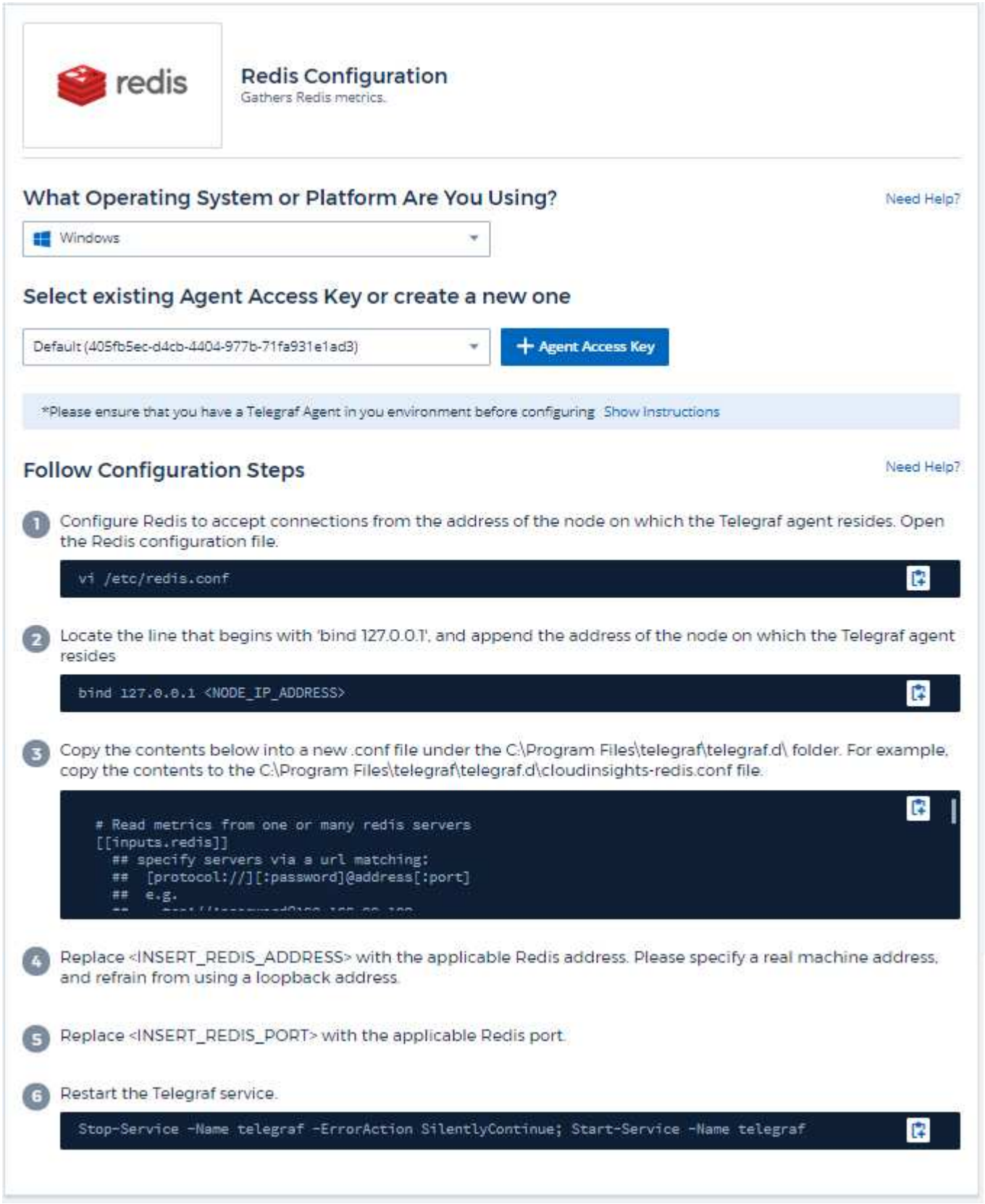
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Redis.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas encore installé d'agent pour la collecte, ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer le"Installation de l'agent" instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.

4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation Redis" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Redis	Serveur d'espace de noms		

Dépannage

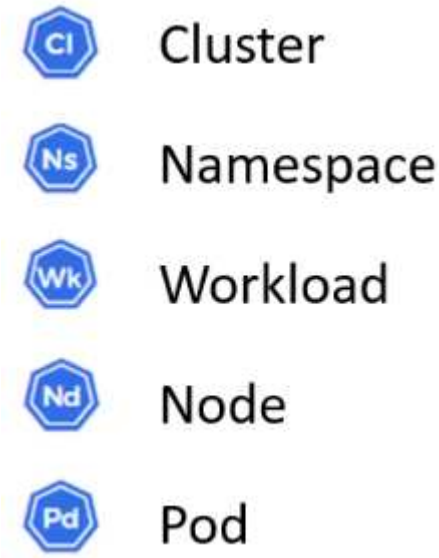
Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Référence d'icône d'objet

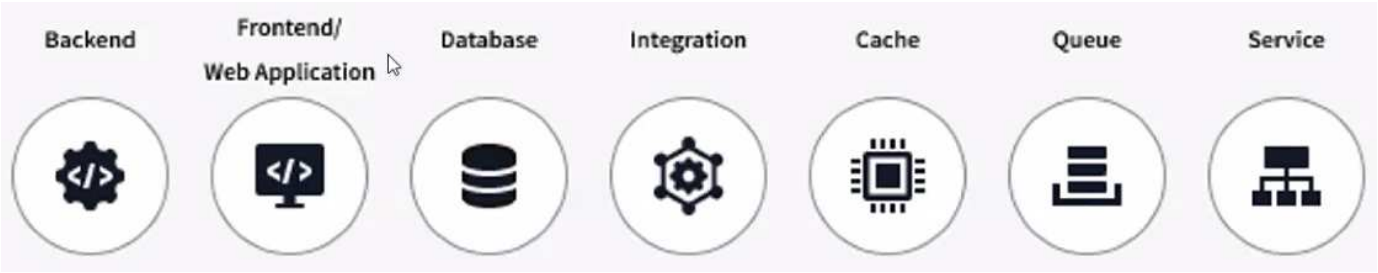
Icônes d'objet utilisées dans Data Infrastructure Insights.

Icônes d'infrastructure :

Icônes Kubernetes :



Icônes de surveillance et de carte des performances du réseau Kubernetes :



Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

Avis concernant Data Infrastructure Insights (anciennement Cloud Insights), fenêtre=_blank

Avis relatif à la sécurité des charges de travail (anciennement Cloud Secure), fenêtre=_blank

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.